T.C.
YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİ TEKNOLOJİLERİ GÜVENLİĞİ VE SİGORTA ŞİRKETİNDE ISO/IEC 27001 STANDARTLARI ÇERÇEVESİNDE BİLGİ GÜVENLİK YÖNETİM SİSTEMİ UYGULAMASI

BAHADIR MURAT KANDEMİRLİ

YÜKSEK LİSANS TEZİ
ENDÜSTRİ MÜHENDİSLİĞİ ANABİLİM DALI
SİSTEM MÜHENDİSLİĞİ PROGRAMI

DANIŞMAN
PROF. DR. HÜSEYİN BAŞLIGİL

İSTANBUL, 2012

T.C.

YILDIZ TEKNİK ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİ TEKNOLOJİLERİ GÜVENLİĞİ VE SİGORTA ŞİRKETİNDE ISO/IEC 27001 STANDARTLARI ÇERÇEVESİNDE BİLGİ GÜVENLİK YÖNETİM SİSTEMİ UYGULAMASI

Bahadır Murat KANDEMİRLİ tarafından hazırlanan tez çalışması 06.01.2012 tarihinde aşağıdaki jüri tarafından Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Endüstri Mühendisliği Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Tez Danışmanı

Prof. Dr. Hüseyin BAŞLIGİL

Yıldız Teknik Üniversitesi

Jüri Üyeleri

Prof. Dr. Hüseyin BAŞLIGİL

Yıldız Teknik Üniversitesi _____

Prof. Dr. Oya KALIPSIZ

Yıldız Teknik Üniversitesi _____

Doç. Dr. Ali Fuat GÜNERİ

Yıldız Teknik Üniversitesi _____

ÖNSÖZ

Tez çalışmam sırasında ilgi ve desteğini üzerimden eksik etmeyen tez danışmanım Prof. Dr. Hüseyin BAŞLIGİL' e , yorucu çalışmam sırasında büyük destek gördüğüm Özlen KURT'a ve Melike Pınar KANDEMİRLİ'ye teşekkürlerimi bir borç bilirim.

Ocak, 2012

Bahadır Murat KANDEMİRLİ

İÇİNDEKİLER

BÖLÜM 5

EK-A

KISALTMA LİSTESİ

ISACA	Information Systems Audit and Control Association
ITGI	IT Governance Institute
ISO	International Organization for Standardization
IEC	International Electrotechnical Commission
COBIT	Control Objectives for Information Technology
SOX	Sarbanes Oxley
ValIT	Value Information Technology
IT	Information Technology
ITAF	Information Technology Assurance Framework
BDDK	Banka Düzenleme ve Denetleme Kurulu
TCP/IP	Transmission Control Protocol/Internet Protocol
CERT	Compute Emergency Response Team
BGYS	Bilgi Güvenliği Yönetim Sistemi
ITIL	Information Technology Infrastructure Library
OGC	The Office Of Government Commerce
COSO	Committee of Sponsoring Organizations of Treadway Commission
CCTA	Central Computer and Telecommunications Agency
eTOM	enhanced Telecom Operations Map
BS	British Standard
BSI	British Standard Institute
CMMI	Capability Maturity Model Integration
SDL	Security Development Lifecycle
SAMM	Software Assurance Maturity Model
HTTP	Hypertext Transfer Protocol
RFID	Radio-frequency identification
TSE	Türk Standardları Enstitüsü
BTYS	Bilgi Teknolojileri Yönetim Sistemleri
BTHYS	Bilgi Teknolojileri Hizmet Yönetim Sistemleri
PUKÖ	Planla-Uygula-Kontrol Et-Önlem Al
ERP	Enterprise Resource Planning
CBK	Common Body of Knowledge
COBRA	Consultative, Objective and Bi-functional Risk Analysis
CRAMM	CCTA Risk Analysis and Management Method
DoD	Department of Defense
USAF	United States Air Force
EBIOS	Expression des Besoins et Identification des Objectifs de Security

DCSSI	Direction Centrale de la Sécurité des Systèmes d'Information
ISAMM	Information Security Assessment & Monitoring Method
ISS	Internet Security Systems
SQL	Structured Query Language
BG	Bilgi Güvenliği
US-NIST	United States National Institute of Standards and Technology
Infogov	Information governance limited
PCI DSS	Payment Card Industry Data Security Standard
HIPPA	Health Insurance Portability and Accountability Act
C/S	Client/Server
SSL	Secure Socket Layer
SSH	Secure Shell
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
TBD	Türkiye Bilişim Derneği
İSYS	İş Sürekliliği Yönetim Sistemi
CSI	Computer Security Institute
PIN	Personal Identification Number
RSA	Rivest-Shamir-Adleman
DNA	Digital Network Authorization
EKL	Erişim Kontrol Listesi
DDOS	Distributed Denial of Service
NATO	National Association of Theatre Owners
Gbps	Gigabit per second
PLC	Programmable Logic Control
SCADA	Supervisory Control and Data Acquisiton
VPN	Virtual Private Network

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

ÖZET

BİLGİ TEKNOLOJİLERİ GÜVENLİĞİ VE SİGORTA ŞİRKETİNDE ISO/IEC 27001 STANDARTLARI ÇERÇEVESİNDE BİLGİ GÜVENLİK YÖNETİM SİSTEMİ UYGULAMASI

Bahadır Murat KANDEMİRLİ

Endüstri Mühendisliği Anabilim Dalı

Yüksek Lisans Tezi

Tez Danışmanı: Prof. Dr. Hüseyin BAŞLIGİL

Bilgi, diğer önemli ekonomik varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilginin korunmaması, büyük ve çözülmesi zor problemlere neden olabilir. Bu problemin temel çözümü bilgi güvenliğinin sağlanmasıdır, ancak neyazık ki bilgi güvenliğini tam anlamı ile sağlamanın basit bir formulü yoktur. Bu noktada kurum stratejilerine ve süreçlerine, en uygun bilgi güvenliği yaklaşımının belirlenmesi ve bu yaklaşımlar arasındaki ilişkiler ve yapısal farklılıkların gösterilmesi gerekir.

Bilgi güvenliği bilgiyi, ekonomik sürekliliği sağlamak, ekonomik kayıpları en aza indirmek, fırsatların ve yatırımların dönüşünü en üst seviyeye çıkartmak için iç ve dış etkilerle meydana gelebilecek tehlike ve tehditlerden korur.

Güvenlik Yönetimi'nin görev tanımı, güvenlik ile ilgili olayların meydana gelmesini, kabul edilebilir maliyetler dahilinde, iş gereksinimleri ile aynı hizada gizliliği, bütünlüğü ve Bilgi İşlem servislerinin erişebilirliğini ve veriyi koruyarak önlemektir.

Bilgi teknolojileri güvenliği kavramını anlayabilmek için bilgi teknolojileri yönetim sistemlerini ve bilgi güvenliği içerisinde bu kavramlara verilen önemi anlamak gereklidir. Bilgi teknolojileri güvenlik yönetimi konusunda dünyada en yaygın uygulama alanı bulan üç standart, bu tez kapsamında incelenmiştir. Bu üç standarttan birincisi olan ISO 27001 standardı, ISO 27002 en iyi uygulama standardı çerçevesinde , bilgi teknolojileri güvenlik yönetimi için çok iyi sınıflandırılmış, taktik ve operasyonel seviyede işleyen ve kolay uygulanabilen bir standart iken, CobIT standardının bilgi

teknolojileri yönetimine stratejik açıdan bakan ve temelini yönetim kararları, yönetilebilirlik ve denetlenebilirlik üzerine kuran geniş kapsamlı bir yapısı vardır ve bilgi güvenliğini CobIT Security Baseline yani CobIT Güvenlik Temel Çizgisi çerçevesinde destekler.

ITIL Güvenlik Yönetimi Süreci, yönetim organizasyonunda güvenligin şeklen uyarlanmasını tarif eder ve böylece bu süreçte sadece temel seviyede bir güvenlik sağlanmakla kalınmaz ayrıca Servis Seviye Anlaşması'nda belirtilenlerin yanında diğer güvenlik gereksinimlere sağlanır.

Her üç standartta da, bilgi teknolojileri yönetiminin değişik öğelerinin bu yönetim sistemlerinde yer almakta olduğu değerlendirilmiştir.

Tez kapsamında, üzerine odaklanılan bilgi güvenliği ile ilgili standartları sağlayabilmek için , incelenen standartlardan hangisinin uygulanması gerektiği cevaplanması zor bir sorudur ve kesin bir cevabı yoktur. Bu standartların bilgi güvenliği alanında ortak noktalarıda fazla olmasına rağmen, kapsam ve derinlik bakımından birbirlerinden farklıdır. Bu sorunun cevabı şirketin stratejileri , politikaları ve gereksinimleri doğrultusunda, kullanılacak standardın kapsamı, uygulanabilirlik ve maliyet parametrelerine göre değişiklik göstermektedir.

Bu tezde, uygulama olarak ABC A.Ş.'de ISO/IEC 27001 standartlarında Bilgi Güvenlik Yönetim Sistemi kurmak için gereken bilgi risklerini belirleme yöntemleri vurgulanmakta ve bu risklerin giderilmesi için ihtiyaç duyulan temel safhalara ait teknoloji, politika ve prosedürler açıklanmaktadır.

Bu standartlar kapsamında oluşturulan Bilgi Güvenlik Yönetim Sistemi sayesinde, işletmelerin bilgi varlıklarının güvenlik sürekliliği, yalnızca teknoloji ile değil aynı zamanda tüm şirket çalışanlarının da uyguladığı iş süreçleri ile sağlanabilecektir.

Anahtar Kelimeler: BGYS, BTYS, ISO/IEC 27001, ISO/IEC 27002, CobIT, ITIL, Bilgi Güvenliği, Risk Yönetimi.

ABSTRACT

INFORMATION TECHNOLOGIES SECURITY AND ISO/IEC 27001 INFORMATION SECURITY MANAGEMENT SYSTEM IMPLEMENTATION AT INSURANCE COMPANY

Bahadır Murat KANDEMİRLİ

Department of Industrial Engineering

MSc. Thesis

Advisor: Prof. Dr. Hüseyin BAŞLIGİL

Information, like other economic assets, is a precious asset for an enterprise so it must be properly protected. If information is not protected, can cause a large and difficult to solve problems Information security protects information from a broad hazard and treats occurring in the internal and external reasons to assure economic continuity, to minimize economic loss and to maximize return of opportunities and investments.

Basic solution of this problem is providing "Information security". Basic solution of this problem is providing "Information security". Unfortunately there is no simple formula that can provide absolute information security. At this point, the most appropriate ISMS approach for corporate strategies and processes need to be determined, also relationships and structural differences between these approaches need to be demonstrated.

The mission statement for Security Management is to prevent the occurrence of security related incidents by managing the confidentiality, integrity and availability of IT services and data in line with business requirements at an acceptable cost.

To understand information technology security, it is fundamentals to understand importance of information technology management and governance concepts. The three most widely practiced and popular information technology management and governance standards are, first ISO 27001 standard, which is implements with ISMS

Best practices standard ISO 27002 and which is a quite easy to implement and understand information technology security management system with a tactical and operational point of view, and the second COBIT standard, which is an information technology governance system with a strategic perspective to implement information technology strategies for manageability and effective auditing of the system and COBIT standard supports information security within Security Baseline Framework of COBIT, and third ITIL Security Management Process describes the structured fitting of security in the management organization and thus by this process, not only a basic level of security but also the determination of the security requirements defined in the SLA and other external requirements can be achieved.

All of these three standards include key aspects of information technology security system elements.

The scope of the thesis, focused on information security related standards to provide, which examined the implementation of the standards required to answer a difficult question, and there is a definite answer. Although more common points-ofthese standards in the field of information security, in terms of scope and depth are different from each other. The answer to this question varies according to the parameters the company's strategies, policies and requirements, in line with the scope of the standard to be used, application, and the cost.

In this thesis, the basic technology, policies and procedures required for the enterprises to establish an information security management system at ABC Co. are explained in order to determine the real risks and eliminate them.

By means of this the job processes, not only applied with technology but also with all enterprise workers, created as security management system the continuity will be provided robustly.
Making decisions, determining, approaches and methodologies for providing “information security” , implementation process of ISMS according to ISO27001 and at the scope of ISMS , determining relationships and structural differences between COBIT, ITIL and ISO27001 standards are the basis of this study.

Key words: ISMS, ITMS, ISO/IEC 27001, ISO/IEC 27002, CobIT, ITIL, Information Security, Risk Management.

BÖLÜM 1

GİRİŞ

1.1 Literatür Özeti

Geçmişten günümüze kurumlar ve sahip oldukları bilgi sistemleri ve ağları bilgisayar destekli sahtekarlık, casusluk, sabotaj, deprem, yangın ve sel gibi çok geniş kaynaklardan gelen tehdit ve tehlikelerle karşılaşma riski artmıştır. Bilgisayar virüsleri, bilgisayar korsanları ve hizmet saldırıları gibi yıkıcı kaynaklar daha yaygın, daha hırslı ve daha karmaşık hale gelmeye başlamıştır.

Bilgi güvenliği çoğu işletme için basta gelen sorunlarından biridir. "Bilgisayar ağlarının yaygın olarak kullanılmaya başlamasıyla birlikte bilgisayar güvenlik olayları da yaşanmaya başlanmıştır. Bilgisayar olaylarının kısmına bilinçsiz kullanıcıların neden olmasına karşın bir kısmına da bilerek sisteme zarar vermek isteyen kötü niyetli kişiler neden olmaktadır. 1980'li yıllarda bilgisayar haberleşmelerinde TCP/IP protokol ailesi dünya çapında kabul görmüş ve internet bu protokolü aracılığı ile yaygınlaşmıştır. İnternetin yaygınlaşması ile bilgisayar haberleşmelerindeki atakların sayısı ve çeşidi de artmıştır [1]. Bu ataklar karşısında kimlik doğrulama, yetkilendirme, antivirüs programları gibi güvenlik çözümleri geliştirilmeye çalışılmıştır. İlk çıkan ataklar daha çok basit kod yürütme, parola tahminleri gibi etkisi ve olasılığı düşük ataklar olmasın karşın süreç içerisinde atakların karmaşıklığı ve etkileri artmıştır. Buna karşın bu atakları kullanabilmek için gereken bilgi düzeyi düşmüştür. Çünkü bu bilgiler çoğunlukla internet üzerinden kontrolsüz olarak yayılmıştır.

İnternet ortamında bilişim sistemlerine ilk büyük zararı Robert Morris tarafından yazılmış olan internet kurtçuğu (worm) vermiştir. 1988 yılında ortaya çıkan ve

bilgisayar başına 200-5300$ arasında zarar veren internet kurtçuğu internete olan güveni sarsmış ve interneti kullanan ve kullanmayı düşünenler üzerinde olumsuz etkiler yaratmıştır [1],[2],[23]. İnternet kurtçuğunun çok büyük zararlar vermesi sonucu bilgisayar olaylarına müdahale etmek, bilgisayar olayları ve onların etkileri konusunda kullanıcıları bilinçlendirmek için Bilgisayar Olaylarına Müdahale Takımı (Compute Emergency Response Team - CERT) kurulmuştur [9]. Bu tür önleyici ve kısa zamanda müdahale etmeyi sağlayan mekanizmalar geliştirilmesine karşın atak yapanlar hala bilgi sistemlerine ciddi zararlar vermektedir.

Bilgisayar zararlı yazılım ve ataklarına karşı proaktif önlemler alınması ve bu sistemlerde güvenliğin sağlanması için birçok kuruluş ve ülke tarafından çok sayıda araştırma geliştirme projesi yapılmış ve hala yapılmaktadır. Bu projeler sonucunda bilgisayar sistemlerinde kullanılan antivirüs yazılımları, güvenlik duvarları, VPN yazılım/donanımları, saldırı tespit ve önleme sistemleri, içerik kontrolcüler, merkezi yönetim yazılımları geliştirmiştir. Geliştirilen bu teknik çözümlere paralel olarak bilişim sistemlerinin güvenli olarak tasarlanmasını ve yönetilmesini sağlayacak standartlar ve çerçeveler de geliştirilmeye çalışılmıştır [4],[5],[23].

Günümüzde BT güvenliği araştırma geliştirme projelerine hem çok büyük bütçeler hem de büyük iş gücü ayrılmaktadır. Çok büyük bütçe ve insan kaynağı ayrılmasının başlıca nedenleri internetin insan hayatında vazgeçilmez bir araç olması, e-devlet, e-ticaret, e-sağlık, e-eğitim, askeri, iletişim, araştırma, eğlence gibi birçok uygulama için çok etkin ve ekonomik çözümler sunmasıdır. Ülkeler ve şirketler bilgisayar güvenliği alanlarındaki uygulamaları kendi ülkelerinde kullanmanın yanında diğer ülkelere satarak hem teknolojik hem de ekonomik olarak pazarda öne geçmek istemektedirler. Avrupa birliği 2007-2013 yılları arasında desteklenecek olan 7. Çerçeve programları kapsamında 32365 milyon Euro olan toplam bütçenin %32'sini güvenlik ve bilgi iletişim teknolojileri alanlarındaki araştırma geliştirme projelerini desteklemek için ayırmıştır [6].

"Kurumlar için en kritik varlık bilgidir. Kurumların değerleri, sahip oldukları bilgi ile ölçülmektedir. Bilgi, sadece bilgi teknolojileriyle işlenen bir varlık olarak düşünülmemelidir. Bilgi bir kurum bünyesinde çok değişik yapılarda bulunabilmektedir. Kurum bünyesinde yaratılan, işlenen, depolanan, iletilen, imha edilen ve kullanılan bilgi ile kurumlar arasında iletilen bilginin gizliliği, bütünlüğü ve erişilebilirliğini korumak güvenliğin temel hedefidir [27]".

Bilgi, diğer önemli ekonomik varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği bilgiyi, ekonomik sürekliliği sağlamak, ekonomik kayıpları en aza indirmek, fırsatların ve yatırımların dönüşünü en üst seviyeye çıkartmak için geniş tehlike ve tehdit alanlarından korur.

Bilgi sistemlerine ve hizmetlerine bağımlılık, işletmelerin güvenlik tehditlerine karşı daha savunmasız olduğu anlamına gelmektedir. Genel ve özel ağların birbiriyle bağlantısı ve bilgi kaynaklarının paylaşımı, erişim denetimini oluşturmadaki zorlukları arttırmaktadır.

Günümüzde, sadece çalışanlarıyla değil, müşterileri, iş ortakları ve hissedarlarıyla birlikte tanımlanan işletmelerde, bilginin gizliliği, bütünlüğü ve ulaşılabilirliğine ilişkin güven ortamının yaratılması, stratejik bir önem taşımaktadır.

İşletmelerde BGYS (Bilgi Güvenliği Yönetim Sistemi) uygulanabilmesi için bilgi güvenliği kavramlarından önce bilgi teknolojileri sistemlerinin yönetim stratejilerinin neler olacağının belirlenmesi gerekmektedir. "Bilgi Teknolojileri Yönetim Sistemleri" olarak anılan COBIT, ISO 20000-1,2 / ITIL , ve COSO (Committee of Sponsoring Organizations of Treadway Commission) gibi standartların amacı, bilgi teknoloji hizmetlerinin müşterilere arzu edilen seviyede ulaşmasını sağlamak, bilgi teknolojileri sistemlerinin denetimini, gözlemlenebilirliğini, ölçeklenebilirliğini, işlevselliğini, verimliliğini, güvenilirliğini ve sürekliliğini sağlamaktır.

Bilgi Güvenliği Yönetim Sistemi ise temel olarak aynı hedeflere atıflar yapsa da bilginin gizliliği, erişilebilirliği ve bütünlüğü ile ilgilidir.

Birçok durumda, tüm uygun model ve yapılar ele alınıp iş yönetim hedeflerine en uygun olanının adapte edilmesiyle çok daha iyi hizmet elde edilmiş olunur.

Bilgi sistemi ile ilgili tüm standartlarının atıf yaptığı kavramlar göz önünde bulundurulduğunda, yedi temel kavram öne çıkmaktadır ki bunlar etkinlik,

verimlilik, gizlilik, bütünlük, erişilebilirlik, uyumluluk ve güvenilirlik olarak sıralanırlar. Standartlar bu kavramların içini değişik oranlarda doldurmaya çalışırlar. Güvenlik, bilgi teknolojileri yönetim sistemlerinin içerisinde bir alt başlıktır. Bilişim dünyasında genel kabul gören yöntem, bilgi yönetimi sistemlerinden birini uygulamak, güvenlik standartları arasında en kabul göreni olan güvenlik Bilgi Güvenliği Yönetim Sistemi, ISO/IEC 17799:2005 ve ISO/IEC 27001 standartlarının kurumlarda oluşturdukları güvenlik yapısının adıdır. Standartlarının bilgi yönetimi sistemlerinin alt süreçleri olarak yürütülmesidir.

Bu şekilde kurumlar, sistemin güvenliğini garanti altına almakta, hizmet kalitesinin belli seviyelerin altına düşmemesini sağlamakta ve bu iki iş için iki ayrı sistem kurmak yerine tüm güvenlik ve bilgi teknolojileri yönetim sistemleri için merkezi bir sistem kurmaktadırlar.

Birçok yönetimsel yapı, bugünkü IT profesyonellerine IT süreçlerinde teknolojiyi kullanmada ve yönetiminde yardım etmektedir. Bunlardan biri olan ITIL (Information Technology Infrastructure Library®), servis yönetimi uygulamalarında en yaygın kabul görenidir. Orijinal olarak, İngiliz Birleşik Krallık Central Computer and Telecommunications Agency (CCTA) tarafından 1990'ların başında yaratılmış olan ITIL, en iyi iş yönetimi sonuçlarını almak üzere, karışık bir BT yapılanmasında nasıl organize olmayı ve yönetmeyi içeren sektör liderlerinden toplanmış görüşleri temsil eden bir dizi kitabın kütüphanesidir.

ITIL'ın resmi bir standart olmaması önemli bir tespittir. ITIL'ın bir standart olmamasından dolayı ITIL uyumlu/uyumsuz bir ürün ve/veya iş yönetimi bulunmamaktadır. ITIL'da sunulan bilgi, birçok farklı kaynaktan orijine olduğu için tekil bir müşteriye has olan duruma her zaman uymayabilir. Birçok ürün tedarikçisi, gerçek iş yönetim hedefi odaklı olacak şekilde diğer modeller gibi ITIL "en iyi uygulamalar" 'ını da destekler ve iş yönetiminin ITIL'ı değerlendirmesi ve yaymasına yardımcı olur.

“En iyi uygulamalar” ismi itibariyle bir miktar hatalı bir tanımlama olabilmektedir, çünkü “en iyi uygulama” denilen zamanla değişmektedir. COBIT (Control Objectives for Information Technology) ve enhanced Telecom Operations Map (eTOM) gibi diğer yapılarda, güvenilir bir rehberlik sağlarlar. Bazı durumlarda ITIL dışındaki bazı yapılar belirli iş yönetimlerine daha iyi karşılık verebilmektedir.

Bilgi güvenliğini sağlamak, teknolojik çözümlerle birlikte sağlam bir güvenlik yönetim sisteminin kurulması ile mümkün olabilmektedir. Etkin bir bilgi güvenlik yönetim sisteminin oluşturulması amacıyla, Bilgi güvenliği yönetimi konusunda ilk standart British Standard Institute (BSI) tarafından geliştirilen BS 7799'dur. BS 7799 "Pratik Kurallar" ve "BGYS Gerekleri" başlıklı iki kısımdan oluşmaktaydı. BS 7799 birinci kısım daha sonra ISO tarafından 2000 yılında "ISO 17799" olarak kabul edilmiştir. 2002'de BSI; BS 7799-2'yi çıkartmıştır. ISO, 2005 yılında ISO/IEC 1799:2005'i ve BS 7799-2'nin yeni hali olan ISO/IEC 27001:2005'i yayınlamıştır. ISO 27001, 2005 yılında yayınlanmasıyla yürürlüğe girmiş ve ISO/IEC 27000 standart serisi altında yerini almıştır. Söz konusu bu standart 2006 yılında Türk Standardı olarak kabul edilerek, "TS ISO/IEC 27001 Bilgi Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimleri" adıyla yayınlanmıştır[36]. Şirketler bilgi varlıklarını, TS ISO/IEC 17799 ve TS ISO/IEC 27001 standartlarında belirtilen Bilgi Güvenliği Yönetim Sistemini (BGYS) kurarak gerçek risklerini saptayabilir ve bu risklerin giderilmesi için gereken teknoloji, politika ve prosedürleri devreye alabilirler. ISO/IEC 27002:2005 bu standardın Temmuz 2007'den itibaren kullanılan ismidir, bu tarihe kadar standart ISO/IEC 17799:2005 olarak adlandırılıyordu [37].

1.2 Tezin Amacı

Bu tez kapsamında, birinci bölümde Bilgi Teknolojileri Yönetim Sistemleri-BTYS ile ilgili genel bilgilere, herkes tarafından sıkça konuşulan COBIT, ITIL, ISO 20000 hakkında genel bilgilere , bilgi kavramı, bilgi güvenliği, işletmelerde BGYS kurulma gereği ve önemine değinilmiş, ikinci bölümde risk yönetimi, üçüncü bölümde TS ISO/IEC 27001 ve ISO/IEC 27002:2005 standartlarına göre BGYS gerekleri ve uygulama adımları konusunda teorik bilgiler paylaşılmış, dördüncü bölümde finans-sigorta sektöründe faaliyet gösteren bir şirkette ISO 27001 çerçevesinde BGYS kurulumunun gerçekleştirilmesi süreçlerine, bu süreçlerde oluşturulan politika, prosedür ve uygulama sonucu değerlendirilmelerine yer verilmiştir.

Sonuç bölümünde bilgi güvenliği açısından COBIT, ITIL ve ISO27001 yaklaşımlarının değerlendirileceği ve genel yapılarının karşılaştırıldığı ilk kısıma ek olarak, BGYS

kurulum yöntem ve uygulaması aşamasında kritik başarı faktörleri, BGYS risk yönetim modelinin öneminin ve kurumların BGYS kurulumu ile elde edecekleri avantajların vurgulanacağı ikinci sonuç kısmı ile tamamlanacaktır.

1.3 Hipotez

Bilgi güvenliği kavramlarını açıklamadan önce, bilgi teknolojilerinin yönetimlerinin nasıl olacağı konusunda kriterler ortaya koymuş standartların bir özeti yapılmıştır. Böylece genelden özele doğru inilmiştir. Bilgi teknolojileri yönetimi konusunda birey ve kurumların konuştuğu önce gelen standartlara burada kısaca yer verilmesi gerekmektedir.

Bu Standartlar:

- ITIL (Information Technology Infrastructure Library - Bilgi Teknolojileri Altyapı Kütüphanesi)
- ISO 20000-1 "Bilgi Teknolojisi – Hizmet Yönetimi – Tanımlama" ve ISO 20000-2 "Bilgi Teknolojisi – Hizmet Yönetimi – Uygulama Prensipleri" Standartları,
- COBIT "Bilgi teknolojileri için denetim hedefleri/kıstasları" standartlarıdır.

1.4 Bilgi Teknolojileri Yönetim Sistemleri: ITIL ve ISO 20000-1,2

ITIL (Information Technology Infrastructure Library - Bilgi Teknolojileri Altyapı Kütüphanesi), BT (Bilgi Teknolojileri) Servislerini yönetmede ayrıntılı ve yapısal en iyi uygulama örnekleri serisidir. ITIL, 80'lerin sonunda İngiltere Ticaret Bakanlığı (OGC - Office of Government Commerce - İngiltere Ticaret Bakanlığı) tarafından geliştirilmiştir. Süreç yaklaşımı sayesinde ITIL müşteri, tedarikçi, BT bölümü ve kullanıcıları arasında başarılı bir şekilde iletişim kurulmasını mümkün kılmaktadır. İngiltere ve Hollanda da hızlı uyumu ile şimdi ITIL dünya çağında kullanılan ve tanınan bir iş standardı haline gelmiştir [38] .

İngiliz Hükümeti, pek çok değişik kurumunun farklı teknoloji altyapılarının fazla karmaşık hale gelmesi, arıza sayısının artması, planlamanın zor hale gelmesi ve hizmet sürekliliğinin gitgide artan oranlarda kesilmesi sonucunda tüm kamu kurumlarını ve bazı özel kurumları kapsayan bir "en iyi bilgi teknolojileri uygulamaları kütüphanesi

oluşturma" çalışmalarına başlamıştır. Bu çalışmalar kapsamında her kurumun bilgi teknolojileri alanındaki en iyi uygulamaları esas alınıp her kurum için geçerli olabilecek bir "en iyi uygulamalar kütüphanesi" oluşturulmuştur. Bu kütüphane İngiliz Standart Kurumu British Standart'ın 15000 numaralı standardı olarak 1980'lerde yayınlanmıştır. Bu standart özellikle 1990' lı yıllarda kendine geniş uygulama alanı bulmuştur. Bilişim teknoloji hizmetlerini sınıflama şekli ve getirdiği önlemler ile özel sektör ya da kâr amacı gütmeyen her kurumun bilişim teknolojileri hizmetlerine uygulanabilir bir standart geliştirmiştir.

ITIL, BT altyapı ve hizmet süreçlerinin nasıl olması gerektiğinin anlatıldığı ve gerçekleştirilmiş en iyi örneklerden yola çıkılarak standartların tanımlandığı bir süreç ve yordam kütüphanesidir.

ITIL yordamlarında; BT hizmetlerinin, bir bütün olarak, maksimum kalitede, düzende ve süreklilikte yürütülmesi, kurumların iş hedefleri ile maksimum seviyede uyumlu hale getirilmesi ve müşteri beklentilerinin en iyi biçimde karşılanması için hizmetlerin nasıl bir yapıda yürütülmesi gerektiği konularına yönelik süreçler ve yordamlar tanımlanmaktadır.

ITIL'ın tüm dünyada bir standart olarak kabul edilmesindeki sebepleri şu şekilde listeleyebiliriz (Office of Government Commerce, 2001)[50],[103] :

1) Ortak Kullanıma Açık Olması

ITIL, başlangıcından beri herkese açık bir altyapıdır. ITIL bünyesinde bulunan bütün süreçler, İngilterede bulunan CCTA (Central Computer and Telecommunications Agency) şimdiki adıyla OGC (Office of Government Commerce) tarafından basılan kitaplarla tüm dünyayla paylaşılmış böylece herkese açık süreçler olmuştur. Bu şekilde ister çok büyük isterse çok küçük olsun bütün organizasyonlar tarafından kullanılabilmektedir.

2) En İyi Uygulamalardan Oluşması

ITIL kütüphanesi gerçekleştirilmiş en iyi örneklerden yola çıkılarak standartların tanımlandığı bir süreç ve yordam kütüphanesidir.

ITIL Servis Yönetimi konusunda bizlere bir çerçeve, model sunmaktadır. Bu modelde ulaşılmak istenen hedefler, genel aktiviteler, süreçlerin girdi ve çıktıları bulunmaktadır. ITIL her organizasyonda farklılık gösterecek günlük işlerin nasıl olması gerektiği

konusunda bir teklif sunmaz, onun yerine organizasyonun ihtiyaçlarına göre birçok farklı şekilde kullanılabilecek en iyi yönteme odaklanır. Kısacası ITIL detaylarla uğraşmaz, mevcut metot ve aktiviteleri yapısal bir bağlam içine oturtabileceğiniz genel bir konsept sunar.

3) De Fakto Standart Olması

ITIL, 1990'ların ortalarından beri Servis Yönetimi konusunda defakto standart olarak görülmektedir. Genel kabul görmüş bir metodun en büyük avantajı ortak bir dil sunmasıdır. ITIL kullanan projelerin en önemli aşamalarından birisi de ITIL içerisinde kullanılan terminolojinin ortak dil olarak kabul edilmesi ve kullanılmasıdır. Çünkü bir projenin başarıya ulaşmasındaki en önemli etkenlerden birisi, proje ekibinin ortak bir dil, terminoloji kullanmasıdır.

4) Kalite Yaklaşımı Sunması

Geçmişte birçok BT firması kendi içlerinde sadece teknik konulara yoğunlaşmışlardı. Günümüzde ise iş dünyası, sunulan-alınan servislerde, en iyi kalite seviyesine ulaşma beklentisi içerisindedir. BT işletmeleri artan bu kalite beklentilerini karşılayabilmek için, "müşteri odaklı yaklaşım" konusuna yoğunlaşmaları ve sonucunda da sunulan servislerin, müşterilerin istediği şekilde verilmesi sağlanmalıdır.

BT firmalarında "Kalite Yönetiminin" getireceği faydaları şu şekilde sıralayabiliriz;

1) Sunulan servislerde kalitenin artması,
2) Kabul edilebilir servis maliyetleri,
3) Müşteri ve Kullanıcı istekleri ile örtüşen servislerin sağlanması,
4) Birbirleriyle entegre olmuş merkezi süreçlerin oluşması,
5) Servislerin sunulmasında görev alan herkesin kendi görev ve sorumluluklarını net olarak bilmesi,
6) Performans göstergelerinin belirlenerek, performans ölçümünün gerçekleştirilmesi.

Şekil 1.1'de görüldüğü üzere ITIL V3 yapısındaki beş temel pratiği aşağıdaki gibi tanımlamaktadır:

Hizmet Stratejisi: Hizmet yönetiminin nasıl tasarlanacağı, geliştirileceği ve uygulanacağını sadece bir organizasyon yeteneği değil aynı zamanda stratejik varlıktır.

Hizmet Tasarımı : Hizmet varlıkları ve hizmet portföyü içerisindeki staratejik nesnelerin dönüşümünde,hizmet ve hizmet yönetim süreçlerinin nasıl tasarlanlanacağını ve

geliştirileceğini ifade eder.

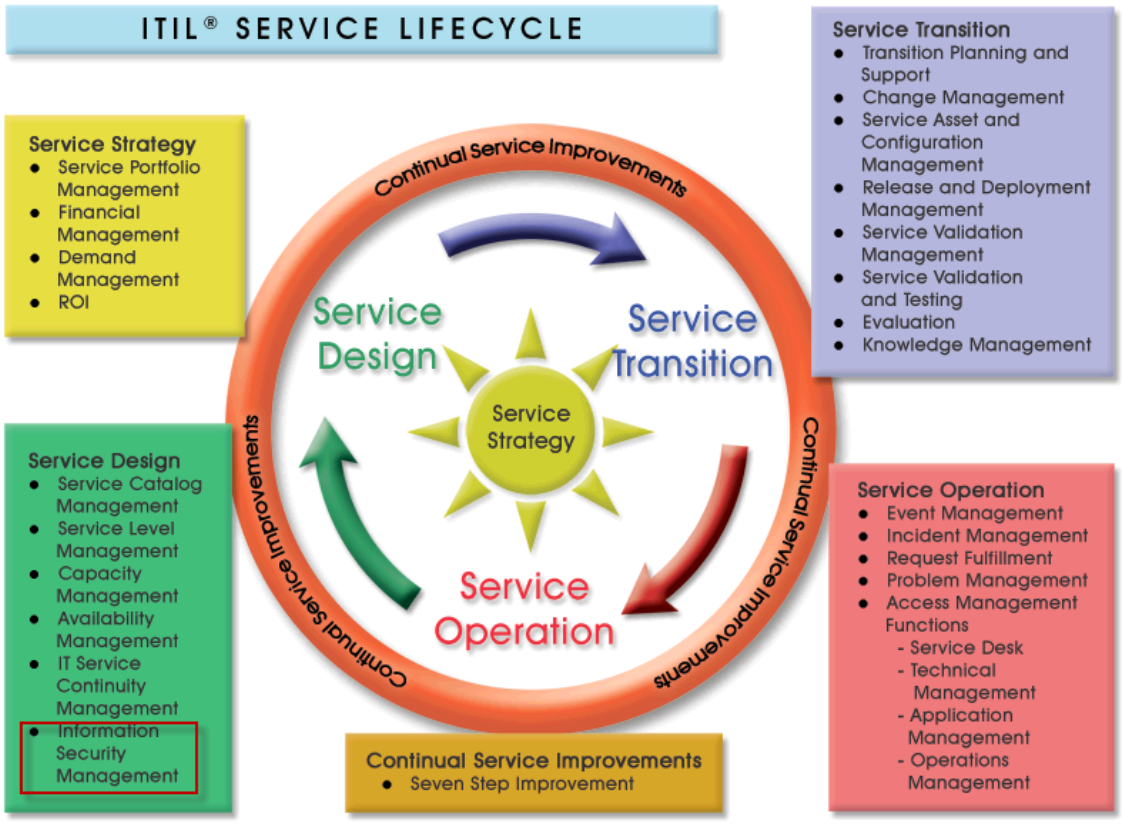
Hizmet Geçiş: Hizmetlerin canlı ortama aktarılmasını sürecini ifade eder.

Servis Operasyonu: Servis hizmetlerinin başarılı bir şekilde yönetilmesi ve sürekliliğin nasıl sağlanması gerektiğini ifade eder.

Sürekli Hizmet Geliştirme: Daha iyi tasarım, tanıtım ve operasyon hizmetleri yoluyla müşterileri için nasıl süredürülebilir bir değer yaratılacağını ifade eder.

ISO 20000 insandan güç alan ama insandan bağımsız çalışan, bir BT Hizmet Yönetimini kurmayı ve belgelendirmeyi hedefler. ITIL ve bir BT Yönetişimi çerçevesini uygulandıktan sonra kurulan bu yeni yapının sürekliliğini garanti etmeye yöneliktir. BT Yönetişimi çerçevelerinde seçilmesi gereken en doğru seçim de COBIT'dir.

Bilgi güvenliği yönetimi ITIL içerisindeki başarılı BT hizmet yönetim sisteminin her adımı için arka planda bilgi güvenliği risklerini dikkate alan ve farkındalık yaratan bir süreç ve fonksiyondur [103].



Şekil 1.1 ITIL Servis hayat döngüsü

ISO standartları etkin ve başarılı BGYS kurulumu için gereken,destekleyici rehberler, prosedürler, süreçler, iyileştirmeler, gereksinimler v.b. tüm başlıkları ile derinlemesine incelerken , ITIL bu başlıkların çoğunun derinlemesine irdelemez.

ITIL ,BT servis yönetimini sağlamak için bir veya daha fazla standardı-en iyi uygulama pratiğini birlikte kullanır, bu uygulamlardan bazıları [41], [105] ;

- COBIT (BT Yönetişimi ve Kontrolleri için bir çerçeve)
- Altı Sigma (Bir kalite metodolojisi)
- TOGAF (BT mimarisi için bir çerçeve)
- ISO 27000 (BT güvenliği için standart)

Bugün yürürlükte olan ve kökeni yukarıda anlatılan BSI 15000 standardına dayanan ve ITIL'ın en iyi BT hizmet yönetim uygulama örneği olarak 15.12.2005 tarihinde yürürlüğe girmiş , son güncellemesi 2011 yılında gerçekleşmiş olan ISO 20000 standardı iki bölümden oluşmaktadır;

ISO 20000–1 Bilgi Teknolojileri – Hizmet Yönetimi – Tanımlama

ISO 20000-2 "Bilgi Teknolojisi – Hizmet Yönetimi – Uygulama Prensipleri"

"ISO 20000 insandan güç alan ama insandan bağımsız çalışan, bir BT Hizmet Yönetimini kurmayı ve belgelendirmeyi hedefler. ITIL ve bir BT Yönetişimi çerçevesini uygulandıktan sonra kurulan bu yeni yapının sürekliliğini garanti etmeye yöneliktir".

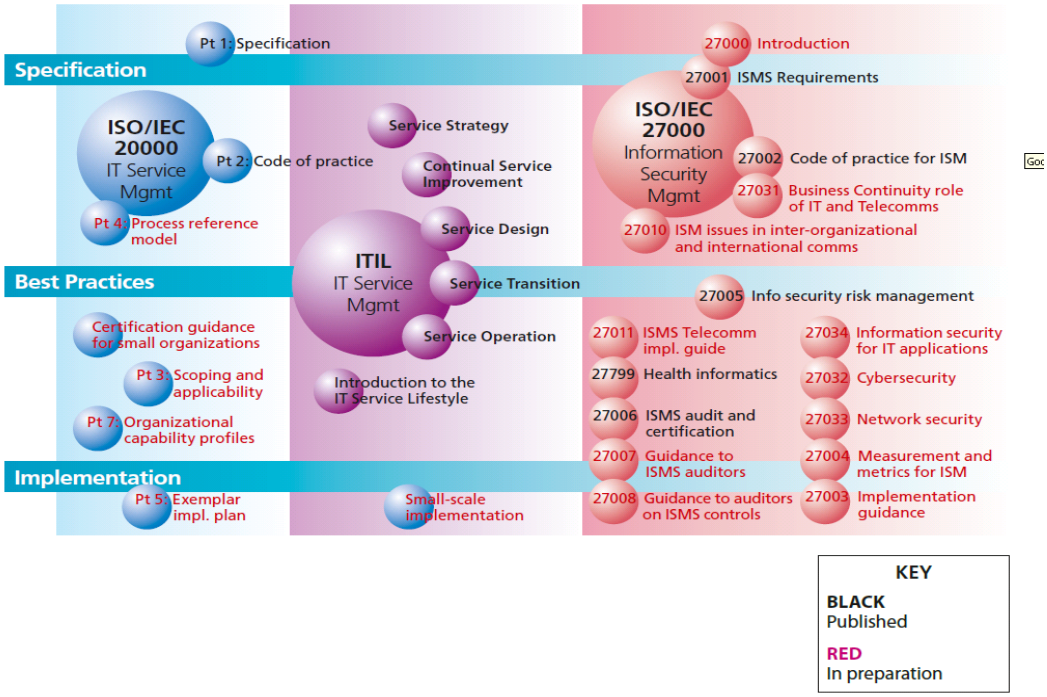
1.4.1 ISO 20000–1 Bilgi Teknolojileri Hizmet Yönetimi Tanımlama

BT işletimi ve hizmet yönetiminde sürekli iyileştirme, ISO 20000'in en temel unsurudur. Bir kere sistem kurulduktan sonra sürekli olarak süreçlerin performansı takip edilmelidir.

ISO 20000 BT Hizmet Yönetim Sistemi , hizmet kalitesinin artması, güvenilir kurumsal destek, hizmetler hakkında daha net veriler elde edilmesi, çalışanların daha iyi motivesi ve yeteneklerin doğru analizi yapılması, müşterilere tatmin ve doğru hizmet sunulması, hizmet süreçlerinin güvenliğinin sağlanması ve sürekli erişim gibi bir çok faydalar sağlayabilen bir sistemdir [38].

Şekil 1.2 ISO 20000 ve ITIL arasındaki ilişki

Şekil 1.2'de ISO 20000 ve ITIL arasındaki ilişki ifade edilmektedir, ISO 20000 standardının 1. bölümü ITIL kütüphanesini oluşturan parçacıkların neler olduğunu, tanımlamalarını, içeriklerini ve çıktı-girdi ilişkilerini açıklayan standarttır. Şekil 1.3 de ISO 20000, ITIL ve ISO 27000 serisi standartlar arasındaki ilişki detaylı olarak görülebilmektedir.

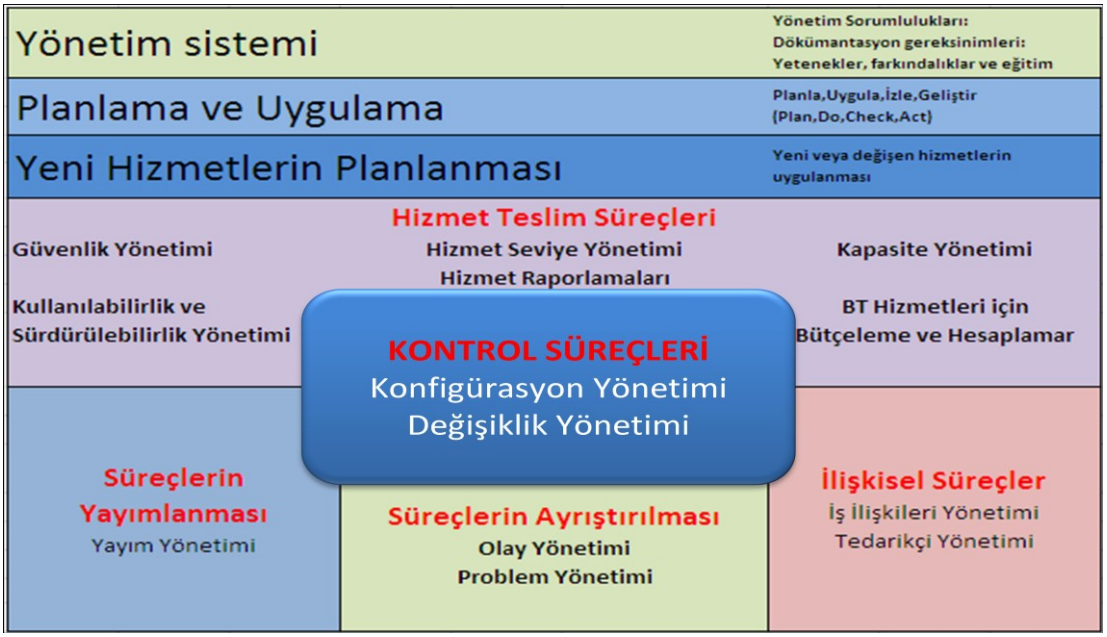


Şekil 1.3 ISO 20000 , ITIL ve ISO 27000 arasındaki ilişki

Şekil 1.4' ten de görülebileceği gibi hizmet yönetimi on iki alt yönetim prosedüründen oluşmaktadır.

Birbirleri ile ilişkileri gösterilen bu alt yönetimler ve açıklamaları şunlardır; (ISO/IEC 20000–1- 2005(E))

- Olay Yönetimi
- Sorun Yönetimi
- Konfigürasyon Yönetimi
- Değişim Yönetimi
- Sürüm Yönetimi
- Yardım Masası
- Servis Seviyesi Anlaşmaları
- Bilgi Teknolojileri Maliyet Yönetimi
- Bilgi Teknolojileri Kapasite Yönetimi
- Kullanılabilirlik (Mevcudiyet) Yönetimi
- Hizmet Sürekliliği Yönetimi
- Bilgi Teknolojileri Güvenlik Yönetimi



Şekil 1.4 ISO 20000 ve ITIL alt parçaları , birbirleri ile ilişkileri ve süreçleri

1.4.1.1 Olay Yönetimi

Kurumda standart olmayan, hizmetin ulaşmasını engelleyen veya hizmetin kalitesini düşüren olaylar "vaka" olarak adlandırılır. Bu tip bir olay gerçekleştiğinde servis hizmetinin ilk ve en temel aşamasında, gelen servis taleplerinin tanımlanarak ilgili kişi veya gruplara aktarılmasından sorun çözümünün gerçekleştirilmesi ve çözüm veritabanına aktarılmasına kadar tüm aşamaları takip eder [28]. Standart olarak gelen çağrıların (servis taleplerinin) ilk seviye servis elemanları tarafından çözülmesi, çözülemezse diğer çözüm seviyelerine aktarılması, olay kayıtlarının tutulması, alarm/uyarı mekanizması ve gelişmiş arama fonksiyonlarıyla diğer modül ve ürünlerle entegre olarak BT altyapısını ilgilendiren tüm olayların başlangıcından sonuçlanmasına kadar tüm aşamalarda yönetiminin yapılmasını sağlar [38].

1.4.1.2 Sorun Yönetimi

Vaka yönetiminden farklı olarak sorun yönetimi pek çok soruna yol açan temel bir sorunun teşhisini ve tedavisini yapar. Vaka yönetiminden farkı kapsamıdır. Sorun yönetimi çeşitli şekillerde kendini gösteren küçük sorunların temelindeki büyük sorunları çözmeye çalışır. Verilen hizmet esnasında sık karşılaşılan sorun / arızaların kaynaklarının bulunması, araştırma süresince geçici çözümlerin esas sorunla ilişkilendirilmesi, daha sonra sorunun kaynağı bulunduğunda, bu bilginin bilinen hatalar veritabanına otomatik olarak konulabilmesini sağlar. Bu sayede daha önce karşılaşılan problemlerin daha kısa sürede çözülmesine veya henüz ortaya çıkmadan müdahale edilmesine olanak tanır [28].

1.4.1.3 Konfigürasyon Yönetimi

Konfigürasyon yönetimi bilgi teknolojileri altyapısını oluşturan tüm bileşenlerin, bu bileşenlerin amacına uygun çalışabilmeleri için gereken tüm özelliklerinin kayıt altında tutulmasıdır. Kayıt altında tutulan her bir bileşene "konfigürasyon bileşeni" adı verilir. Bu yönetim şu alt aşamalardan oluşur [28]:

- Planlama
- Tanımlama ve isimlendirme

- Kontrol
- Mevcut durum muhasebesi
- Denetlem

1.4.1.4 Değişim Yönetimi

Değişim yönetimi, değişimle ilgili konuların hizmet sürekliliğini ve kalitesini etkilememesi için standart değişim yöntemleri oluşturulması sürecidir. Bu sürecin alt parçaları şunlardır:

- Değişim isteği yapılması
- Değişim isteklerinin incelenmesi ve konfigürasyon yönetimi tablosuyla karşılaştırılması
- Değişim isteklerinin filtrelenmesi
- Değişim isteklerinin değişim planlama tablosuna işlenmesi

Önemli veya geniş çapta yapılacak altyapı değişikliklerini planlı, iş akışları ve onay süreçlerine dayalı, riskleri ve olası sorunları minimize ederek yönetebilmeyi sağlar. Değişiklikler, kritik faaliyetleri yöneten altyapılarda yönetimi zor ve riski yüksek olabilirler. Değişim Yönetimi modülü detaylı iş akışı, onaylama mekanizması ve takip seçenekleri ile potansiyel olarak kritik değişim faaliyetlerinin kolaylıkla yapılmasını sağlar. Ayrıca son kullanıcıların yeni ürün veya parça taleplerinin onay mekanizması kontrollü yönetimine ve periyodik olarak yapılması gereken bakım işlemlerinin belirlenen herhangi bir zaman aralığı içinde otomatik uyarı ve eskalasyon mekanizmasıyla yönetimine olanak tanır. Olay yönetimi modülüne entegre olması sayesinde değişim ve bakım zamanı gelen işlemler için birer "olay kaydı" yaratılarak, Olay Yönetimi modülünün sağladığı geniş takip olanaklarından faydalanılmasını sağlar [38].

1.4.1.5 Sürüm Yönetimi

Sürüm yönetimi bir kurum içerisinde kullanımda olan yazılımların konfigürasyon bileşenlerinin yönetimidir. Sürüm yönetimi, kurum içerisinde hangi donanımların hangi yazılımları çalıştıracağı ile ilgilenir. Burada belirlenmesi gereken bu yazılımların

birbirleri ve üzerinde çalıştıkları donanımlar ile ne kadar uyumlu çalıştıklarıdır. Bu kıstaslara bakılarak kurumlarda "Belirleyici Yazılım Kütüphanesi" oluşturulur. Bu hem fiziksel hem de mantıksal bir kütüphanedir. Fiziksel olarak kurumda kullanımda olan her yazılımın kullanım lisansları ve bir kopyası tek bir yerde tutulur. Mantıksal olarak da kurumda her donanımın çalıştırmakta olduğu yazılımların listesi çıkarılır, olması gerekenle karşılaştırılır ve uygun olarak düzenlenir. Yazılımların değişimi ihtiyacı olduğunda bunun süreçleri değişim yönetimi basamaklarına göre yapılır ve her yazılım yapılandırmasına bir sürüm numarası verilir [28].

1.4.1.6 Yardım Masası

Yardım masası aynı zamanda "Tek İletişim Noktası" olarak da adlandırılır. Müşteri ya da kullanıcılar her türlü istek ya da sorunlarını kayıt numarası almak kaydı ile tek bir iletişim noktasına bırakırlar. Bu istekler bir sorun, vaka ya da değişim isteği olabilir. Buradaki kritik nokta kullanıcı ya da müşterinin ilgili kişiye kendisinin ulaşmak zorunda olmayışıdır. Kullanıcının tek bilmesi gereken, isteğinin hangi sınıflamaya girdiğini bilmek, isteğinin kabaca tanımını yapabilmek ve bunu tek iletişim noktasına iletmektir. İstekler, arka planda değerlendirilerek ilgili önlemler alınır ve kullanıcı gelişmelerden haberdar edilir [28].

1.4.1.7 Servis Seviyesi Anlaşmaları

Konfigürasyon bileşenlerinin işlevlerini yapamamaları ihtimaline karşı bu bileşenlerin uygun fiyat karşılığı bakım anlaşması altında tutulmaları esastır. Burada dikkat edilmesi gereken noktalar kullanıcı ihtiyaçları, hizmetin maliyet etkin tedariki, hizmetin güvenlik gereksinimlerini ihlal etmeden verilmesi ve hizmetin belirli bir kalite seviyesinin üzerinde tedarik edilmesidir [28].

1.4.1.8 Bilgi Teknolojileri Maliyet Yönetimi

Bilgi teknolojileri maliyet yönetimi, genel olarak bilgi teknolojileri hizmetlerinin en maliyet etkin yöntemlerle verilmesinin garanti altına alınmasıdır. Değişim planlama tablosundaki veriler yaklaşık maliyet hesaplamaları ile hesaplanarak kurumların bilgi teknolojileri yıllık maliyetleri ortaya konur. Bu maliyetler ortaya çıkarıldıktan sonra

kurum yapısı elveriyor ise bu maliyetler müşteri ya da kullanıcılardan tahsil edilir [28].

1.4.1.9 Bilgi Teknolojileri Kapasite Yönetimi

Bilgi teknolojileri kapasite yönetimi, bilgi teknolojileri ürünlerinin kurumlarda doğru fiyata, doğru hacimde ve verimliliği en yüksek düzeyde tutarak yönetilmesidir. Bu planlama yapılırken hangi hizmetin hangi kaynakları kullandığı, bu kaynakların ne kadar yedekliliğe ihtiyaç duydukları ve bunların maliyeti ortaya konulur. Kapasite yönetimi, iş, hizmet, kaynak gibi üç bileşenin yönetimini yapar [28].

Kapasite yönetimi şu değişkenler izlenerek yapılır;

- Performans takibi
- İş yükü takibi
- Uygulama ölçeklenmesi
- Kaynak ihtiyacı tahmini
- İstek tahmini

1.4.1.10 Kullanılabilirlik (Mevcudiyet) Yönetimi

Konfigürasyon bileşenlerinin her birinin kullanıma hazır ve çalışır halde bulunurluğunu sağlayan süreçtir. Bu süreç dahilinde her konfigürasyon bileşeni için aşağıdaki değişkenler belirlenir [28];

- **Hizmet Verilebilirlik:** Hizmet üçüncü taraflar tarafından veriliyor ise
- hizmet ya da parçanın ulaşma süresi
- **Güvenilirlik:** Bileşenin hata vermeden çalışma süresi
- **Geri Kazanım Süresi:** Bileşen hata verdikten sonra geri çalıştırmak için gereken süre
- **Dayanıklılık:** Hataya vermeye karşı sağlamlığı
- **Güvenlik:** Sızmalara karşı ne kadar güvenli olduğu, gizliliğe ne kadar izin verdiği açılarından değerlendirilirler.
- **Bakım Kolaylığı:** Bileşenin hem hata önleyici olarak, hem de hata verdikten sonra geri kazanımının ne kadar kolay olduğu kıstasları

1.4.1.11 Hizmet Sürekliliği Yönetimi

Hizmet sürekliliği yönetimi bilgi teknoloji bileşenlerini etkileyen ciddi bir hata ya da etki olduğunda bilgi teknoloji hizmetlerinin en kısa sürede çalışır hale getirilmesi planlarının yapılmasıdır. Bu plana "İş Süreklilik Planı" denir. İş süreklilik planı hazırlanmasının aşamaları şu şekildedir [28].

1. Hangi işlerin daha önemli ve önce çalışır hale getirileceği "İş Etki Analizi" sonucunda belirlenir.
2. Her hizmet için tehdit, zafiyet ve önlem analizi (risk yönetimi) yapılır.
3. Kurtarma alternatifleri değerlendirilir.
4. Plan düzenli olarak test edilir, tatbikat yapılır ve gözden geçirilir.

1.4.1.12 Bilgi Teknolojileri Güvenlik Yönetimi

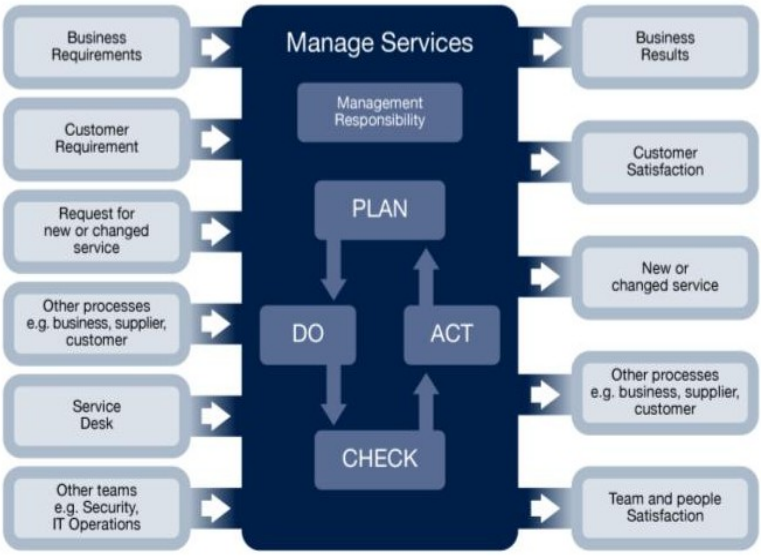
ISO 20000 güvenlik yönetimi için ISO 27002:2005' i adres gösterir. Burada ki kritik nokta, güvenliğin bilgi teknoloji hizmetlerinden biri olmasıdır. Bilgi teknolojileri güvenlik yönetimi bu tezin ana konusudur ve ikinci ve üçüncü bölümlerde tüm detaylarıyla anlatılmıştır. ISO 20000 kapsamında bilgi güvenliği hakkında söylenmesi gereken, güvenliğin bilgi teknolojileri yönetimi konusunun küçük ve öteki bileşenlerden ayrılmaz bir parçası olduğudur [33]. Bilgi teknolojisi yönetimi sisteminin diğer öğeleri olmadan, vaka ve olay yönetimi olmadan güvenlik olaylarının düzgün şekilde rapor edilmesi mümkün değildir. Konfigürasyon yönetimi olmadan hangi bileşenlerin güvenlik önlemi kapsamında olduğu, bu bileşenlerin kimin sorumluluğunda olduğu ve bileşenin fiziksel olarak nerede olduğu, teknik özellikleri bilinemeyecektir. Değişim yönetimi olmadan yapılacak değişimlerin güvenliğe etkileri analiz edilemez, yapılacak değişimlere göre güvenlik önlemleri de güncellenmelidir. Değişim yönetimi münferit değişimlere karşıdır, değişimler değerlendirilir ve planlanır. Bu planlama merkezi güvenlik önlemlerini belirli bir konfigürasyon üzerinde yapmayı kolaylaştırır. Hizmet masası yapılan tüm isteklerin ve olayların bir listesini tutarak kurumların bilgi teknolojileri güvenilirliğinin kolayca izlenmesini sağlar. Küçük parçalardan oluşan merkezi güvenlik açıklarının tespitini kolaylaştırır.Maliyet yönetimi olmadan güvenlik önlemlerinin belirli tehdit türlerine karşı alınması gerekip gerekmediği belirlenemez.

Kural olarak önlem tehditten daha pahalıya mal olamaz. Kapasite yönetimi olmadan hizmetlerin ne kadar yedekli olması gerektiği tespit edilemez. İş süreklilik ve mevcudiyet yönetimi hangi hizmetin ne kadar önemli olduğunu ortaya koyar ve güvenlik konusunun da bir alt başlığıdır.

1.4.2 ISO 20000–2 Bilgi Teknolojileri Hizmet Yönetimi Uygulama Prensipleri

ISO 20000 standardının ikinci bölümünde yukarıda ana hatları ve birbirleri ile ilişkileri anlatılan hizmetlerin alt başlıkları detaylı olarak ele alınır ve olası durumlara karşı nasıl davranılması gerektiği konusunda prensipler yazılıdır. İzlenmesi gereken değişkenler, geri besleme süreçleri, maliyet hesaplama yöntemleri, planlamaların nasıl yapılacağı, risklerin nasıl hesaplanacağı vb. konular detayları ile irdelenir.

Şekil 1.5' te ISO 20000 sürecinin girdileri, çıktıları ve sürecin içeriği görülmektedir. Planla – yap – kontrol et – harekete geç döngüsü olarak adlandırılan bu sistem, aynı zamanda ISO 27001 Bilgi Güvenliği Yönetim Sistemleri standardının da temelini oluşturmaktadır. ISO 20000 – 1,2 ve ISO 27002(ISO 17799) – ISO 27001 ailesi standartların 2005 yılı sürümleri, özellikle birbirleri ile uyumlu çalışacak şekilde tasarlanmışlardır. Bu standartlar kurumların aynı döngü süreci içerisinde bilgi teknolojileri yönetim sistemlerini ve bilgi teknolojileri güvenlik sistemlerini beraber çalıştırabilecekleri bir çerçeve oluşturmaktadırlar [28].



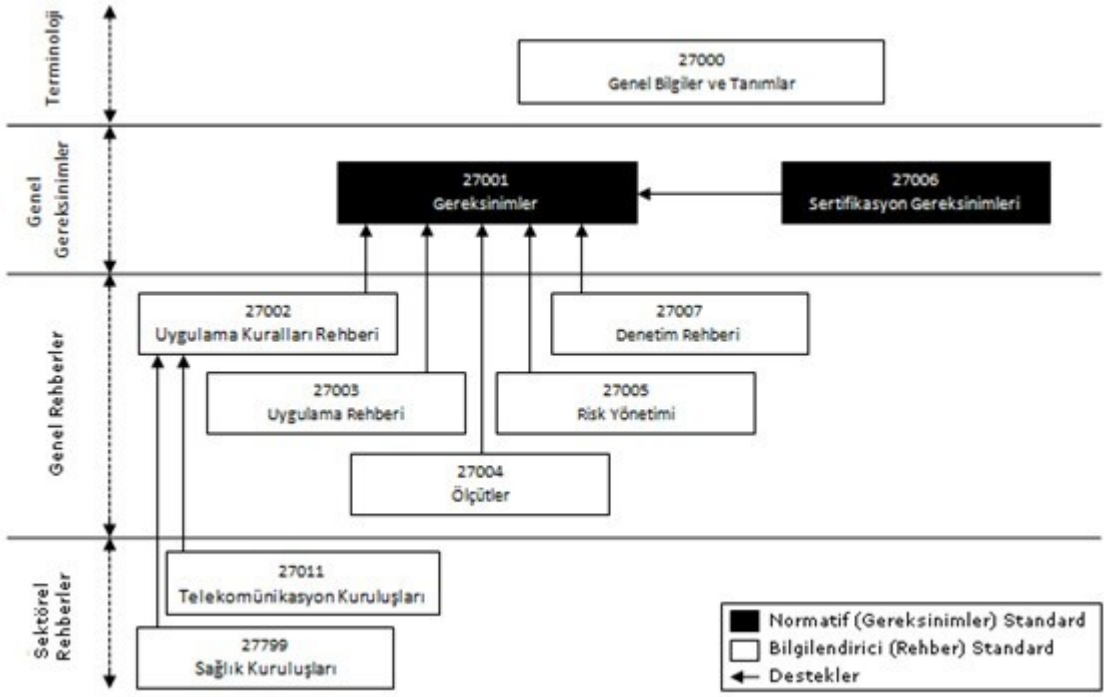
Şekil 1.5 ISO 20000 süreçlerini gözden geçirmek için kullanılan PUKÖ döngüsü

1.4.3 ISO 27000 Ailesi

Bilgi güvenliği ile ilgili olarak ISO 27000 serisi güvenlik standartları, Şekil 1.6' da ifade edildiği üzere kullanıcıların bilinçlenmesi, güvenlik risklerinin azaltılması ve de güvenlik açıklarıyla karşılaşıldığında alınacak önlemlerin belirlenmesinde temel bir başvuru kaynağıdır. Bu standartlar temel ISO'nun 9000 kalite ve 14000 çevresel yönetim standartlarıyla da ilgilidir [35].

ISO 27000 standardı, ISO 27000 standartlar ailesi ile ilgili kavramların açıklanmasını sağlayan ve bilgi güvenliği yönetimine yönelik temel bilgileri içeren bir standarttır. ISO 27000 standartlarının büyük bir çoğunluğu bilenen, diğerleri ise basım aşamasında olan standartlar olarak verilebilir.

ISO/IEC 27000 standart serisi altında yer alan ve ISO 27001 için gereken güvenlik kontrollerini içeren standart; ISO/IEC 27002:2005 - Bilişim Teknolojisi - Güvenlik Teknikleri - Bilgi Güvenlik Yönetimi için Uygulama Kılavuzu'dur. Bu standardın önceki adı ISO/IEC 17799:2005'dir. 1 Temmuz 2007 tarihinde, ISO tarafından yapılan teknik bir düzenlemeyle ISO/IEC 17799:2005 standardının adı, ISO/IEC 27002:2005 (ISO 27002) olarak değiştirilmiştir [34].



Şekil 1.6 ISO 27000 Standart Ailesi [36]

1.5 Bilgi Teknolojileri Yönetim Sistemleri: COBIT

Control Objectives for Information and Related Technology (COBIT) 'in Türkçe açılımı Bilgi ve ilgili Teknolojiler için Kontrol Hedefleri'dir. COBIT, ISACA (Information Systems Audit and Control Association) ve ITGI (IT Governance Institute) tarafından yaratılmış bilgi teknolojileri yönetimi riskleri için bir çerçevedir. COBIT bilgi teknolojileri yöneticileri, denetçileri ve bilgi teknolojileri kullanıcıları için bir kurumda bilgi teknolojileri kullanımının ve uygun bilgi teknolojileri yönetişiminin geliştirilmesi ve kontrol edilmesinin faydalarını artırmak için genel olarak kabul edilmiş bilgi teknolojileri kontrol hedef setleri sunmaktadır. COBIT'te dört alanda sınıflandırılan 318 kontrol hedefini içeren 34 yüksek seviye hedefler bulunmaktadır. COBIT 1992 yılında, IT Governance Institute ve Information Systems Audit and Control Foundation tarafından bilgi teknolojileri ile ilgili kontrol hedefleri ilk belirlendiğinde geliştirilmiştir. İlk basımı 1996'da, ikincisi 1998'de, üçüncüsü 2000'de yayınlanmış ve 2003'de çevrimiçi olarak yayınlanmıştır. Enron Skandalı ve Sarbanes Oxley'e geçiş gibi dış gelişmelerle önemi artmıştır. 2005 Aralıkta COBIT Versiyon 4.0 yayımlanmıştır [39]. 2007 Mayıs ayında Cobit Versiyon 4.1 yayımlanmıştır. Bu güncelleme ile hedef açıklamaları basitleştirilmiş ve süreçler ile "İşletme", "BT hedefleri" ve "BT süreçleri" arasındaki çift yönlü ilişki basamaklandırılmıştır [40].

COBIT'in misyonu "yöneticiler ve denetçiler için günlük kullanabilecekleri genel olarak kabul edilmiş bilgi teknolojileri kontrol hedeflerinden oluşan geçerli, güncel ve uluslararası bir set araştırmak, geliştirmek, tanıtmak ve teşvik etmektir." COBIT'in geliştirilmesinden yöneticiler, denetçiler ve kullanıcılar faydalanmaktadır çünkü COBIT bir bilgi teknolojileri yönetişim modeli geliştirilmesiyle birlikte, onların bilgi teknolojileri sistemlerini daha iyi anlamalarını ve kurumdaki bilgi teknolojileri varlıklarını korumak için gerekli güvenlik seviyesi ve kontrole karar vermelerini sağlamaktadır[39].

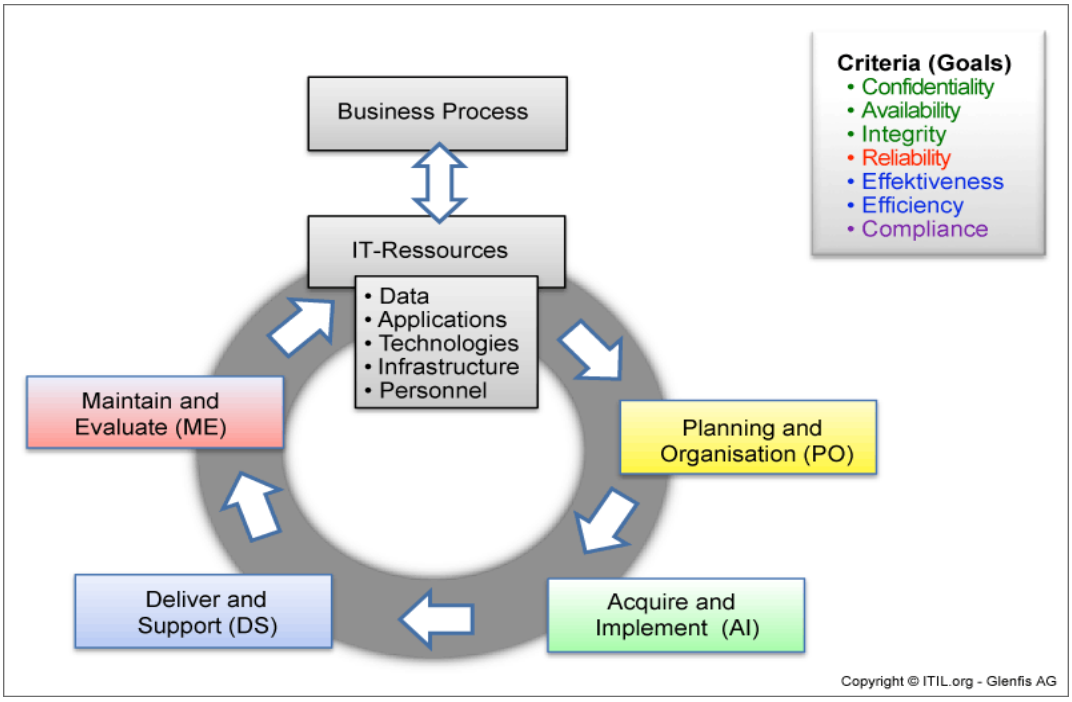
1.5.1 COBIT'in Yapısı

COBIT yöneticilere, bilgi teknolojileri kullanıcılarına ve denetçilere faydalar sağlamaktadır. Yöneticiler COBIT'ten faydalanmaktadır, çünkü COBIT onlara bilgi teknolojileriyle ilgili kararlarlarını ve yatırımlarını dayandırabilecekleri bir temel sunmaktadır. Stratejik bir bilgi teknolojileri planı tanımı yapma, bilgi mimarisini

tanımlama, bilgi teknolojileri stratejisini uygulamak için gerekli donanım ve yazılımını satın alma, hizmet sürekliliğini temin etme ve bilgi teknolojileri sisteminin performansını kontrol etme esnasında COBIT standartlarının uygulanması yönetime karar aşamasında yardım etmektedir. Bilgiyi toplamaya, işlemeye ve raporlamaya yardım eden uygulamaların COBIT'e uygun olması, teknolojileri kullanıcılarına iş süreçlerinin kontrolünün ve güvenliğinin sağlandığına ilişkin güvence vermektedir. Kurumun bilgi teknolojileri altyapısındaki bilgi teknolojileri kontrol sorunlarını belirlemek için denetçilere oldukça faydalı olmaktadır. COBIT onlara denetim bulgularını doğrulamada da yardımcı olmaktadır.

COBIT dört alandan oluşmaktadır.Bu alanların birbirleri ile ilişkileri Şekil 1.7' de verilmiştir [40].

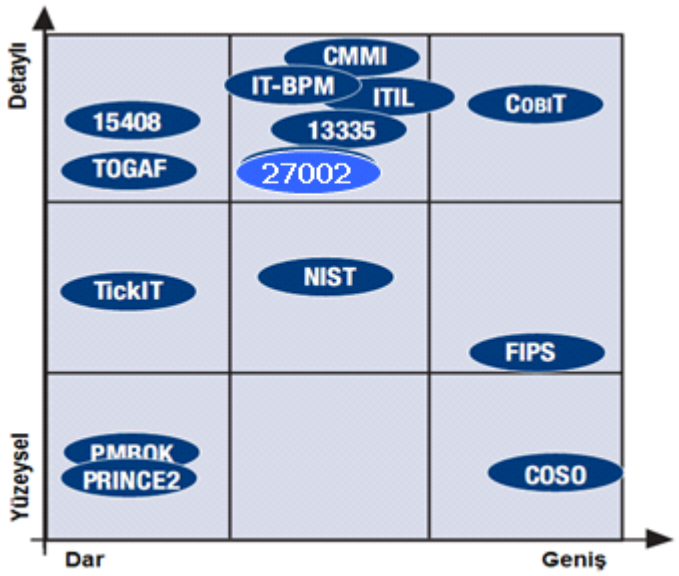
- Planlama ve Organizasyon
- Temin Etme ve Uygulama
- Ulaştırma ve Destek
- Gözlem ve Değerlendirme



Şekil 1.7 COBIT Temel alanları ve ilişkileri

ISO 20000 ve COBIT tamamen aynı konularla ilgilenmesine rağmen Bilgi teknolojilerine bakış açıları çok farklıdır.

Şekil 1.8' de COBIT' in göreceli kapsamı ve kapsanan COBIT alanları görülmektedir. Görüldüğü gibi BT Yönetiminde en geniş alan COBIT' tedir. COBIT en detaylı ve geniş standarttır. Bu iki standart arasındaki felsefi ve idari farkları açıklamak ve anlamak için bu iki standardın çıkış noktalarına bakmak gerekmektedir.



	PO	AI	DS	ME
COSO	+	+	0	0
ITIL	0	0	+	-
ISO/IEC 27002	0	+	+	0
FIPS PUB 200	0	+	+	0
ISO/IEC 13335	0	0	0	-
ISO/IEC 15408	-	0	-	-
PRINCE2	0	-	-	-
PMBOK	0	-	-	-
TickIT	-	+	-	0
CMMI	-	+	-	0
TOGAF 8.1	0	-	-	-
IT BPM	0	-	0	-
NIST 800-14	0	+	+	0

(+): Değinilen Alanlar (O): Kısmen Değinilen Alanlar
(-): Nadir Değinilen veya Değinilmeyen alanlar

Şekil 1.8 Kapsanan COBIT Alanları

(+): Değinilen Alanlar (O): Kısmen Değinilen Alanlar (-): Değinilmeyen alanlar

PO: Plan and Organise – Plan ve Organizasyon

AI: Acquire and Implement – Satınalma ve uygulama

DS: Deliver and Support – Ulaştırma ve Destek

M: Monitor - Gözlem

ISO 20000 bilgi teknolojileri hizmetlerinin belirli bir hizmet seviyesinde, süreklilikte, kalitede, hızda, maliyette yürütülmesini hedeflerken, COBIT iş gereksinimlerini ve doğasını öne alarak her şeyden önce işin tarifini yapıp, bilgi teknolojileri ihtiyaçlarını buna göre şekillendirme açısından yaklaşırlar. ISO 20000' in kökeni en iyi bilgi teknolojileri uygulamaları iken COBIT bilgi teknolojilerinin iş hedefleri hizmetinde en iyi nasıl kullanılacağını gösterir. COBIT tüm süreçlerini bilgi teknolojileri ortamına aktarmış ve iş hayatı bu bilgilerin sağlığına tamamen bağlı kurumlar tarafından tercih edilmektedir. Bankacılık Düzenleme ve Denetleme Kurumu COBIT' in tüm bankalarda uygulanması için çalışmalarına devam etmektedir [42].

COBIT, bilişim teknolojileri yönetimini bir proje yönetimi süreçlerine benzer şekilde ele almaktadır.

1.5.1.1 Planlama ve Organizasyon

Planlama ve Organizasyon alanı teknoloji kullanımını ve kurumun amaç ve hedeflerini gerçekleştirmeye yardımcı olmak için nasıl en iyi şekilde kullanılabileceğini kapsamaktadır. Bu alan enuygun sonucu elde etmek ve bilgi teknolojileri kullanımından en iyi şekilde faydalanmak için bilgi teknolojilerinin alması gereken organizasyonel ve altyapısal şekli ortaya çıkartmaktadır. Planlama ve Organizasyon alanındaki kontrol hedeflerinin ana başlıklarını içeren liste aşağıda yer almaktadır [39].

Çizelge 1.1 COBIT Planlama ve Organizasyon Kontrol Hedefleri Ana Başlıkları

PO1 Stratejik bir BT Planı Tanımlama
PO2 Bilgi Mimarisini Tanımlama
PO3 Teknolojik Yönü Belirleme
PO4 BT Süreçleri, Organizasyon ve İlişkilerini Tanımlama
PO5 BT Yatır ımını Yönetme
PO6 Yönetim Hedefleri ve Yönünü Bildirme

PO7 BT İnsan Kaynaklarını Yönetme
PO8 Kaliteyi Yönetme
PO9 BT Risklerini Değerlendirerek Yönetme
PO10 Projeleri Yönetme

1.5.1.2 Temin Etme ve Uygulama

Temin Etme ve Uygulama alanı bilişim teknolojileri gereksinimlerini belirleme, teknolojiyi satın alma ve kurumun mevcut iş süreçlerine uyarlama için kurumun stratejilerini adreslemektedir. Bu alan aynı zamanda bilgi teknolojileri sisteminin ve parçalarının hayatını sürdürebilmesi için kurumun kabulleneceği bir bakım planı geliştirilmesini içermektedir. Temin Etme ve Uygulama alanındaki kontrol hedeflerinin ana başlıklarını içeren liste aşağıda yer almaktadır[39].

Çizelge 1.2 COBIT Temin Etme ve Uygulama Kontrol Hedefleri Ana Başlıkları

AI1 Otomatize Edilmiş Çözümleri Tanımlama
AI2 Uygulama Yazılımını Geliştirilmesi ve Bakımı
AI3 Teknoloji Altyapısının Oluşturulması ve Bakımı
AI4 Çalışma ve Kullanımı Etkinleştirme
AI5 BT Kaynaklarını Elde Etme
AI6 Değişiklikleri Yönetme
AI7 Çözüm ve Değişikliklerin Kurulması ve Akreditasyonu

1.5.1.3 Ulaştırma ve Destek

Servis ve Destek alanı bilgi teknolojilerinin teslim yönüne odaklanmaktadır. Bu alan bilgi teknolojileri sistemindeki uygulamaların hayata geçirilmesi ve sonuçları ile bu bilişim teknolojileri sistemlerinin etkin ve elverişli uyarlanmasını sağlayan destek süreçlerini de kapsamaktadır. Bu destek süreçleri güvenlik konuları ve eğitimini içermektedir. Teslim ve Destek alanındaki kontrol hedeflerinin ana başlıklarını içeren liste aşağıda yer almaktadır. **COBIT 4.0 Control Objectives Management Guidelines Maturity Models,a.g.m s.109**

Çizelge 1.3 COBIT Servis ve Destek Kontrol Hedefleri Ana Başlıkları

DS1 Servis Düzeyi Yönetimi
DS2 Üçüncü taraf Hizmetlerin Yönetilmesi
DS3 Performans ve Kapasite Yönetimi
DS4 Sürekli Hizmetin Sağlanması
DS5 Sistem Güvenliğinin Sağlanması
DS6 Maliyetlerin Tanımlanması ve Dağıtımı
DS7 Kullanıcıların Eğitimi ve Öğretimi
DS8 Hizmet Masası ve Olaylar Yönetimi
DS9 Konfigürasyon Yönetimi
DS10 Sorun Yönetimi
DS11 Veri Yönetimi
DS12 Fiziksel Ortamların Yönetimi
DS13 Operasyonların Yönetimi

1.5.1.4 İzleme ve Değerlendirme

İzleme ve Değerlendirme alanı kurumun ihtiyaçlarını, mevcut bilişim teknolojileri sisteminin hedefleri kar şılayıp karşılamadığını ve yasal gereksinimlerle uyumluluk için kurumun stratejilerini irdelemektedir. İzleme ve Değerlendirme aynı zamanda bilgi teknolojileri sisteminin iş hedeflerini karşılamadaki etkinliği ile iç ve dış denetçilerce yapılan kurumun kontrol süreçlerinin bağımsız değerlendirmesi konularını kapsamaktadır. İzleme ve Değerlendirme alanındaki kontrol hedeflerinin ana başlıklarını içeren liste aşağıda yer almaktadır [39].

Çizelge 1.4 COBIT İzleme ve Değerlendirme Kontrol Hedefleri Ana Başlıkları

ME1 BT Performansının Gözlemi ve Değerlendirmesi
ME2 İç Kontrol Gözlemi ve Değerlendirmesi
ME3 Yönetmeliklere Uyumluluğun Sağlanması
ME4 BT Yönetimi Sağlanması

1.5.2 COBIT ‘ in Bileşenleri

COBIT’ in yapısında bulunan 4 adet sahanın altında toplam 34 adet bilişim teknolojileri süreci, bilişim teknolojileri süreçlerinin altında da toplam 318 adet detaylı kontrol hedefi bulunmaktadır. COBIT Versiyon 4.1 toplam 34 adet olan bilişim teknolojileri süreçlerini aşağıdaki bilgi kriterleri ve bilgi kaynakları ile ilişkilendirmektedir[43].

1.5.2.1 Bilgi kriterleri

- **Etkililik:** Bilginin iş süreçleri ihtiyaçları ile ilgili ve bu ihtiyaçlara cevap verir nitelikte olması.
- **Verimlilik:** Bilginin kaynakların en etkin kullanımı ile elde edilmesi.
- **Gizlilik:** Hassas bilginin yetkisiz erişime karşı korunması.
- **Bütünlük:** Bilginin kendi içinde ve çevresel veriler ile bütünlük göstermesi, yetkisiz değişikliğinin engellenmesi.
- **Devamlılık:** Bilginin ihtiyaç duyulduğunda erişilebilir olması.
- **Uyumluluk:** İş süreçlerinde kanun, düzenleme ve kontratlara uyum sağlanması.
- **Güvenilirlilik:** Yönetimin finansal ve diğer raporlamalar için güvenilir veriye ulaşabilmesi.

1.5.2.2 Bilgi kaynakları

- **İnsan Kaynakları:** Bilişim teknolojileri personel yetenekleri, bilinç, bilgi sistemleri planlama, organizasyon, uygulama, destek, gözetim üretkenliği.
- **Uygulama Sistemleri:** Manuel ve programlanmış iş süreçlerinin tümü.
- **Teknoloji:** Donanım, işletim sistemi, veritabanı yönetim sistemi, bilgi ağı ve diğer teknoloji altyapısı.
- **Fiziksel Ortam:** Bilgi sistemlerini barındıran ve koruyan fiziksel ortamlar.
- **Veri:** En geniş anlamıyla, iç, dış veri türlerinin tamamı.

Bilgi kriterlerinin kurum için önem dereceleri ortaya konduğunda kurum için öncelik ifade eden süreçler de ortaya çıkmaktadır. COBIT süreç, bilgi kriteri ve bilgi kaynakları matrisini bilgi kriterinin süreç ile ilişkisinin seviyesini (birincil, ikincil, ilgisiz) ve

süreç ile ilgili kullanılan bilgi kaynaklarını işaret ederek sunmaktadır.COBIT uygulanması için gerekli araçları uygulama araçları dökümanında sunmaktadır. Bilişim teknolojileri denetiminin beklenen sonuçları üretebilmesi, yönetimin desteğine, üst yönetim ve ilgili birim yönetiminin yapılan çalışma konusunda gayretlerine bağlıdır.

COBIT metodolojisi bir bilgi teknolojileri yönetişim ve denetim aracı olma vizyonu doğrultusunda her sürümde değişime uğramış olup son sürümü itibarı ile altı temel bileşeni barındırmaktadır. Bunlar, yönetim özeti, metodolojinin çerçevesi, kontrol hedefleri, denetim rehberi, performans ölçüm rehberi ve uygulama araçlarıdır.

1.5.3 Yönetim Özeti

COBIT metodolojisi hakkında genel bilgi verip üst yönetim kademelerinin COBIT hakkında bilgilendirilmesi ve desteklerinin kazanılmasını hedeflemektedir [39],[43].

1.5.4 Metodolojinin Çerçevesi

COBIT'in temel sahaları (4 adet), bilişim teknolojileri süreç sahaları (34 adet), bilişim teknolojileri süreç sahalarının iş süreçleri ile ilişkileri, bilgi kriterleri ve bilgi kaynaklarının bili şim teknolojileri süreç sahaları ile ilişkilerini ortaya koyar. Çerçeve dökümanının temel hedef kitlesini bilgi teknolojileri ve bilgi teknolojileri denetim yönetimleri oluşturmaktadır [39],[43].

1.5.5 Kontrol Hedefleri

Her bir bilişim teknolojileri süreci için yüksek seviye ve detaylı kontrol hedeflerinin belirtildiği dökümandır. Bu dökümanın temel hedef kitlesini orta düzey bilgi teknolojileri ve bilgi teknolojileri denetim yönetimleri oluşturmaktadır [39],[43].

1.5.6 Denetim Rehberi

Bilişim teknolojileri süreci bazında üst ve detay seviye kontrol hedeflerinin denetimi için gerekli rehberi, bilgi teknolojileri denetçilerinin kullanımına sunar. COBIT metodolojisine göre üst seviye kontrol hedefleri aşağıdaki gibi denetlenir :

İş ihtiyaçlarının, ilgili risklerin ve kontrol önlemlerinin elde edilmesi ve anlaşılması [39],[43].

1.5.7 Kontrollerin uygunluğunun değerlendirilmesi

Kontrollere belirtildiği gibi uyulup uyulmadığının sürekli biçimde test edilmesi ile kontrol uyum değerlendirmesinin yapılması [39],[43].

Analitik teknikler ve diğer kaynaklara başvurarak karşılanmayan kontrol hedeflerinin risklerinin somutlaştırılması.

1.5.8 Performans Ölçüm Rehberi

Performans Ölçüm Rehberi, orta ve üst seviye bilgi teknolojileri ve bilgi teknolojileri denetim yönetimi ile bilgi teknolojileri denetim uzmanlarına denetlenen alanlardaki olgunluk seviyelerinin ölçümlenmesi,hedeflenen olgunluk seviyelerine ulaşılması için gerekli kritik başarı faktörlerini sunar.

Uygulama Araçları

Bilgi teknolojileri denetim bölümü yönetici ve uzmanlarına COBIT'in başarılı biçimde uygulamaya alınabilmesi, gerekli yönetim desteğinin sağlanması, sıkça sorulan sorular ve diğer kurumların deneyimlerine ulaşabilmek için gerekli kaynağı sağlar.

1.5.9 COBIT Değerlendirmesi

COBIT özellikle denetimin ve kontrolün yasal zorunluluk olduğu kurumlarda önemlidir. Dünyada çoğu kurum, BT'nin denetlenebilir alanını tanımlamak için COBIT'ten yararlanmaktadır. COBIT, BT topluluğu tarafından anlaşılabilecek ve takip edilebilecek şekilde yazılmıştır. Sonuçta, etkili denetim kapsamını güvence altına alan stratejik planlar COBIT'le hazırlanabilir.

COBIT'in alan ve süreç yapısı, kontrol faaliyetlerini yönetilebilir ve tanımlanabilir bir yapı içinde sunuyor. Devlet gerekleri ve bilgisayar destekli denetim tekniklerinin kullanımı dahil olmak üzere, çeşitli alanları temel alan ayrıntılı denetim prosedürleri geliştiriliyor. BT alanında çalışan denetçiler uzmanlığa gereksinim duydukları için

beceri değerlendirmeleri gerçekleştirmek ve denetimin başarılı şekilde yapılmasını güvence altına almak için COBIT'i kullanıyor.

Çizelge 1.5 de COBIT'in BT ile ilgili alanlarda hangi süreçlerde kontrolü sağladığı açıklanmaktadır. Bütün bunların yanında COBIT ayrıca şu yaklaşımları da sergilemektedir [42].

–Süreç tesisi ve denetimi odaklı

–Bütüncül yaklaşım

–Dengeli ve hiyerarşik yapılandırılmış alanlar

–Ölçme ve Derecelendirme Mekanizması

–Etkili Kurumsal Yönetişim aracı (Yönetilebilirliğin sağlaması)

–Teknolojiden bağımsız

–ISO 17799/27002, ITIL, COSO yaklaşımlarına uygun

–AB Mevzuatında BS Denetimi çerçevesi olarak uygunluğuna onay veren düzenlemelerin olduğu bir yaklaşım sergiliyor [42].

Çizelge 1.5 COBIT ve BT Denetimi

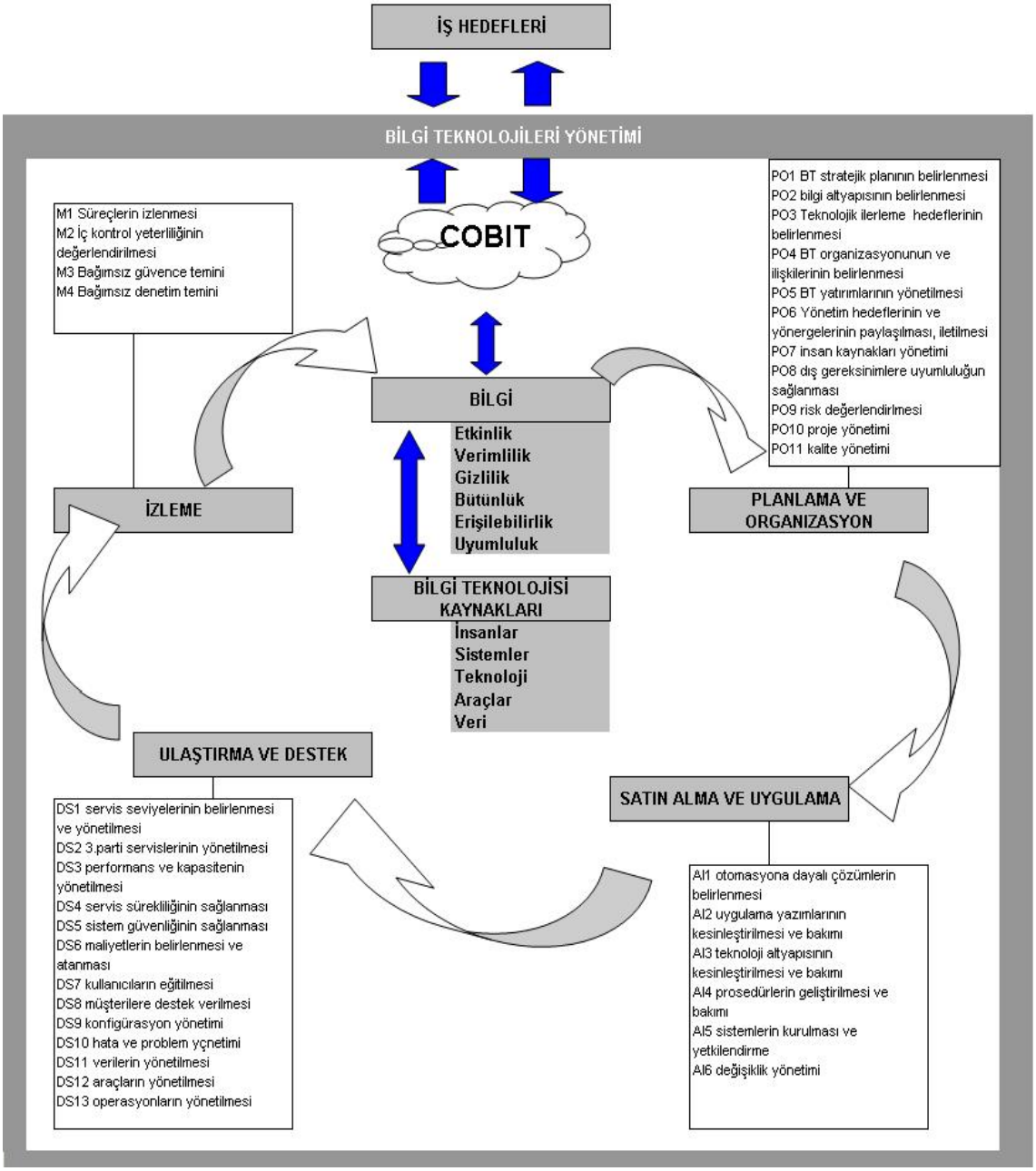
Basel II Olay Çeşitleri	**BT ile ilgili alanlar**	**COBIT Süreçleri**
İç Dolandırıcılık	• Programların kasıtlı değiştirilmesi • Değişiklik fonksiyonlarının yetkisiz kullanımı • Sistem yönergelerinin kasıtlı değiştirilmesi • Donanımın kasıtlı değiştirilmesi • Sistemin ve uygulama verilerinin Hackleme yoluyla kasıtlı değiştirilmesi • Lisansız yazılım kullanımı/kopyalanması • Erişim haklarının içeriden değiştirilmesi	•PO6 (Yönetimin amaçlarının ve talimatlarının iletilmesi) •DS5 (Sistem güvenliğinin sağlanması) •DS9 (Konfigürasyon yönetimi)
Dış Dolandırıcılık	• Sistemin ve uygulama verilerinin Hackleme yoluyla kasıtlı değiştirilmesi • Dışarıdan gelenlerin gizli fiziksel veya elektronik dökumanları görebilme imkanı bulabilmesi • Erişim haklarının dışarıdan değiştirilmesi • Haberleşme bağlantılarının kesilmesi veya dinlenmesi • Şifrelerin ele geçirilmesi • Virüsler	•DS5 (Sistem güvenliğinin sağlanması)

İstihdam Uygulamaları ve İş Ortamı Güvenliği	• BT kaynaklarının hatalı kullanımı • Güvenlik duyarlılığının düşüklüğü	•PO6 (Yönetimin amaçlarının ve talimatlarının iletilmesi) •PO7 (İnsan kaynakları yönetimi)
Fiziksel Değerlerin Zarar Görmesi	• Bilinçli veya kaza ile BT fiziksel altyapısına verilen zarar	•DS12 (Veri yönetimi)
İş Aksamaları ve Sistem Arızaları	• Donanım ve yazılım aksamaları • Haberleşme arızaları • Çalışanların sistemi sabote etmesi • Temel BT çalışanlarının işi bırakması • Yazılım/veri dosyalarının tahribi • Yazılımın veya hassas bilgilerin çalınması • Bilgisayar hataları • Sistemin geri yüklenememesi • DoS saldırısı • Konfigürasyon kontrol hatası	• DS3 (Performans ve kapasite yönetimi) •DS4 (Hizmet sürekliliğinin sağlanması) •DS5 (Sistem güvenliğinin sağlanması) •DS9 (Konfigürasyon yönetimi) •DS10 (Problem yönetimi)
Yürütme, Dağıtım ve Süreç Yönetimi	• Elektronik medyalara (CD, DVD,…) dokunma hatası • Kullanılmayan iş ortamları • Değişim kontrollerinde hata • Tamamlanmamış girdi veya transaction • Veri girdi/çıktısında hata • Programlama/deneme hatası • Operatör hatası, geri yükleme süreçlerinde mesela • Elle yapılan süreçlerde hata	•AI5 (Bilgi sistemleri kaynaklarının karşılanması) •AI6 (Değişiklik yönetimi) •DS5(Sistem güvenliğinin sağlanması) •DS10 (Problem yönetimi)

COBIT standardının ülkemizde üretim ,hizmet ve kamu alanlarında faaliyet gösteren tüm işletmelerde uygulanabilirliği konusundaki en büyük risk, bu standardın bankalar gibi denetimin hayati önem taşıdığı sistemler için tasarlanmış olması, bürokratik yapının katı oluşu, güvenlik ve denetim ihtiyaçları yüzünden gerektiğinde işlevsellikten feragat edilen bir çatısı olmasıdır.

COBIT tüm işletmelerde uygulanamasa dahi, bilgi teknolojileri uygulama planlarının COBIT kontrol hedefleri ışığında değerlendirilmeleri yerinde olacaktır. COBIT şu anda uygulamada olan en geniş kapsamlı bilgi teknolojileri yönetim sistemidir.

Şekil1.9'de COBIT' in işleyişini görülmektedir [39],[43],[44].



Şekil 1.9 COBIT Kontrol Alanlarının İş Hedeflerine Yönelik Akışı

Bilginin korunması için bütünlüğü (integrity), gizliliği (confidentiality) ve erişilebilirliliği (availability) özelliklerinin her zaman sağlanıyor olması gerekir. Bilginin üretilmesinden imha edilmesine kadar geçen süreçte güvenliğinin sağlanması için BT Güvenliği, Yedekleme, Fiziksel Güvenlik vb kontrollerinin de devreye alınmış olması gerekmektedir. Bu açıdan bakıldığında BT Güvenliği, Bilgi (Veri) Güvenliği'nin sağlanması için etkenlerden sadece bir tanesidir.

Kurumlar verilerinin güvenliğini sağlamak için BT altyapılarına çeşitli güvenlik ürünleri (Firewall, IPS vb) konumlandırmakta, sızma testleri ve zaafiyet analizleri yaptırmaktadırlar. Yasal düzenlemelere ve standartlara uyum için düzenli periyotlarda denetlenen firmalar, denetlemeye hazırlanırken çoğu zaman bu teknik ayrıntıların içinde kaybolup gitmekte Bilgi Güvenliği ve Bilgi Teknolojileri Güvenliği kavramlarını birbirine karıştırmaktadırlar.

Denetimlerde başarılı olmak için sadece en uygun teknolojiyi konumlandırmak yeterli değildir. Güvenlik denetimlerine denetim açısından bakmak gerekmektedir. Denetimde en temel konu, üründen ziyade Bilgi Güvenliği'nin nasıl yönetildiğidir. Denetlenen kurum, mevcut verilerini değerlendirmiş / sınıflandırmış / önceliklendirmiş ve varlıklar için tehdit-risk-kontrol matrisi oluşturarak gerekli kontrolleri devreye almış olmalıdır. Bu kontroller Firewall, IPS gibi teknolojilerinin yanısıra kontrollü giriş kapıları, kapalı devre tv sistemi gibi fiziksel güvenlik öğelerini de içermelidir. Ayrıca, verilerine erişim için gerekli süreçleri etkin bir şekilde işletiyor olması gerekmektedir.

COBIT Bilgi Güvenliği Denetimleri sırasında yukarıda bahsedilen şekilde bilgi güvenliğinin sağlanması için kullanılacak kontrol listesi ana başlıkları aşağıda yer almaktadır [104].

1. Bilgi Güvenliği Yönetimi
2. Bilgi Güvenliği Planı
3. İnsan Kaynakları Yönetim
4. Kimlik Yönetimi
5. Kullanıcı Hesapları Yönetimi
6. Güvenlik Teknolojilerinin Korunması
7. Kriptografik Anahtar Yönetimi
8. Veritabanı ve Yazılım Güvenliği
9. Zararlı Yazılımları Engelleme, Tespit ve Düzenleme
10. Ağ Güvenliği
11. Hassas Verilerin İletimi

12. Güvenlik Olayı Tanımlaması
13. Fiziksel Güvenliği Sağlanması
14. İş Sürekliliğinin Sağlanması ve Bilginin Yedeklenmesi
15. Bilginin İmha Edilmesi
16. Güvenlik Testi, Gözetleme ve İzleme

1.5.10 COBIT 'in Geleceği

COBIT'in şu andaki en son versiyonu COBIT 4.1'dir. Ancak, yaklaşık iki yıl önce başlayan çalışmalar sonucunda 5.0 versiyonunun yayınlanmasına çok yaklaşılmıştır. 2011 yılının sonlarında yayınlanması beklenen yeni versiyon ile ISACA tarafından yayınlanan Risk IT ve Val IT'nin COBIT içerisinde birleştirilmesi, COBIT sertifikasyonunun mümkün hale getirilmesi gibi pek çok yenilik bekleniyor.

Türkiye'de ise her geçen gün farklı sektörlerdeki pek çok şirkette COBIT'in kullanıldığına şahit oluyoruz. Yasal düzenlemeler tarafında ise BDDK'nın yanı sıra Hazine Müsteşarlığı ve SPK'nın da gelişmeleri izlediği ve BT'ye yönelik düzenlemelerinde COBIT'i göz önünde bulundurduğu bilinen konular [45].

Bilgi Sistemleri Denetim ve Kontrol Birliği ("Information Systems Audit and Control Association – ISACA") yönetim kurulunun, tüm ISACA ürünlerinin ve bilgi birikiminin bir araya getirilmesi amacıyla oluşturmaya başladığı Control Objectives for Information and related Technology ("COBIT") 5 BT Yönetişim Çerçevesinin 2011 sene sonu itibarıyla yayınlanması planlanmaktadır.

Bilgi ve ilgili teknolojilere ilişkin kurumsal seviyede daha etkin bir yönetim ve yönetişim kurulmasını hedefleyen COBIT 5 Çerçevesi, bu amaçla ISACA'nın değer yönetimi (Value IT), risk yönetimi (Risk IT), BT güvence Çerçevesi (IT Assurance Framework - ITAF) gibi diğer ürünlerini de kendi yapısı dahilinde bir araya getirmektedir. COBIT 5'e geçiş dönemi esnasındaki bu değişim, COBIT'in eski versiyonlarını denetim, yönetim veya yönetişim gibi farklı amaçlarla kullanan veya COBIT'le ilk kez bu yeni versiyonuyla tanışacak olan tüm kullanıcıların ve kurumların, aşağıdaki konulardaki sorularını da gündeme getirmektedir:

- Hayatımızda neler değişecek?
- Uyum için neler yapılmalı ve nereden başlanmalı?
- Geçiş dönemi ne kadar sürecek?

Özelikle Bankacılık Düzenleme ve Denetleme Kurumu'nun ("BDDK"), COBIT'i denetim standardı olarak kullandığı ve diğer düzenleyici kurumların da benzer hazırlıklar içinde olduğu düşünüldüğünde, bu değişimin Türkiye'de de oldukça fazla kurumu etkileyeceği açıkça görülmektedir [46].

1.6 Bilgi ve Bilgi Güvenliği

Bilgi, diğer ticari değerler gibi bir organizasyon için önemlidir ve uygun şekilde korunması gerekir. Elektronik sistemlerin birbirlerine bağlanmasıyla birlikte bilgilerin güvenliğiyle ilgilitehditlerde artmaktadır. Bu sebeple kuruluşlar, organizasyonları ve süreçleri çerçevesinde bilgilerin bütünlüğünü, gizliliğini ve ulaşılabilirliğini sağlama gereği ile gittikçe daha fazla karşı karşıya kalmaktadır.

Günümüzde bilgi, bireylerin, organizasyonların ve devletlerin sahip olabilecekleri en stratejik kaynak durumuna gelmiştir [24],[25].

Bilginin tanımını farklı biçimde yapmak mümkündür. Belirli bir zümreye hitap eden bilgiden uzak durarak, bilgi mutlak olmamakla birlikte uyarlanabilir bir tanımını yapmak için bilginin kabul edilmiş tanımlarına bakacak olursak;

Webster's Sözlüğü aşağıdaki tanımları veriyor:

Bilgi: 1. Çalışma, araştırma, gözlem yada tecrübe sonunda elde edilen hakikat yada fikir. 2. İnsanın bildiği şeyler. 3. Okullarda, çoğunlukla da yüksek okullarda öğrenim yoluyla edinilen bilgiler. 4. Öğretici kitaplar.

Bu demektir ki bilgi; çoğunlukla eğitimi de kapsayan tecrübelerle edinilen hakikat ve fikirlerdir [24].

Roget's Thesaurus eşanlamlılar sözlüğüne bakıldığında;

Bilgi-başlığı altında 19 kelime yer alıyor. Bu eşanlamlılardan meydana gelen dizi, Webster'in hayli daraltılmış tanımlamasından çok daha geniş bir anlam taşıyor ve

bilgi kavramına genişlik kazandırıyor. Buna göre bilgi; sezgi, anlama, beceri, idrakve tahminin de eklenmesiyle derinbir anlamkazanıyor, zenginleşiyor [24].

Uzlaşmaya varmak için her biri çok değerli ancak ulaşılması imkansız olan Davenport ve Prusak'ın bilgi tanımlarını birleştirelim. Bilgi; deneyimler , değerler, uzmanlaşmış içerikler ve köklü sezgilerin akışkan bileşimidir. Öğrenenlerin akıllarından doğar ve gelişir. İşletmelerde yalnızca belge ve yayınlara yansımakla kalmaz aynı zamanda düzeni, kurallar, deneyimler ve uygulamaları ifade eder. Kısacası; buda bilginin doğru zamanda alınacak yerinde kararların, tahminlerin, tasarımların, planlamaların yükünü taşıyabilmesini mümkün kılar. Bilgi; bireysel ve ortak akıllar tarafından oluşturulur ve paylaşılır. Sadece veritabanlarından edinilmez; deneyimler, başarılar, başarısızlıklar ve öğrenimle zaman içinde kazanılır [26].

Bilgi, mal ve hizmet üretimindeki, personel, malzeme, makine (tesis ve enerjiyi de içerir) ve para gibi temel girdilere ilave edilen belki de en pahalı ve önemli girdi olarak ifade edilmektedir [47].

Bilgi, toplanmış, organize edilmiş, yorumlanmış ve belli bir yöntemle etkin karar vermeyi gerçekleştirmek amacıyla ilgili birime iletilmiş, belirli bir amaç doğrultusunda süreçlenen, yararlı biçime dönüştürülmüş ve kullanıcıya değer sağlayan verilerdir. Bilgi, çoğulculuğu, çeşitliliği, kurum içi etkileşimleri ve organizasyon faaliyetlerinin mantıksal arka planını oluşturmaktadır. Ünlü savaş uzmanı Napolyon'a göre, doğru bilgiyi doğru zamanda temin etmek savaşın onda dokuzunu kazanmak demektir [48].

Sonuç olarak, bugün en büyük güçlerden birisinin bilgi olduğu gerçeği kabul edilmiş ve dünya bu gerçek ışığında yapılanmış ve hatta içinde yaşadığımız çağa bilgi çağı denmeye başlanmıştır. Üstün teknolojinin sağladığı inanılmaz kolaylıklara sınırları ortadan kalkan ve biri birine yaklaşan devletler, kuruluşlar ve kişilerin yarattığı global dünya ile birlikte bilginin önemi daha da artmıştır.

Günümüzde internetin yaygınlığının ve kullanımının artması, gittikçe üzerinden daha fazla kritik veri dolaşması, kurumların iş süreçlerini elektronik ortama taşıyarak kurumsal kaynak planlama (ERP) ile e-iş fonksiyonlarını birleştirme çabaları, bunun sonucunda daha hızlı işlem yapmaları ve dolayısıyla ürün ve hizmetlerine rekabet üstü değerler kazandırmaları git gide tüm bu unsurlara temel teşkil eden güvenlik

teknolojilerinin önemini arttırmaktadır. Veri güvenliği, ortam güvenliği, kullanıcı tanıma, e-ticaret gibi kavramlar giderek artan oranlarda kullanılmaktadır.

Bugünün "dijital ekonomi" dünyasında, bilgiye sürekli erişimi sağlamak ve bu bilginin son kullanıcıya kadar bozulmadan, değişikliğe uğramadan ve başkaları tarafından ele geçirilmeden güvenli bir şekilde sunulması giderek bir seçim değil zorunluluk haline gelmektedir [24],[49].

Bilgi diğer iş varlıkları kadar değerli bir servettir. Bilgi organizasyon için oldukça değerlidir ve bu nedenle en uygun biçimde korunması gerekmektedir. Bilgi güvenliği, şirketin bilgilerini çok çeşitli tehditlerden koruyarak şirketin iş devamlılığına olanak tanır, iş kaybını düşürür ve yatırımların iş imkanları olarak dönüşünü artırır.

Bilgi birçok biçimde bulunabilir. Kağıt üzerine yazılmış ve basılmış olabilir, elektronik olarak saklanmış olabilir, posta yoluyla veya elektronik imkanlar kullanılarak gönderilebilir, filmlerde gösterilebilir veya karşılıklı konuşma sırasında sözlü olarak ifade edilebilir. Bilgi hangi biçimi alırsa alsın veya paylaşıldığı veya toplandığı hangi anlama gelirse gelsin her zaman uygun bir şekilde korunmalıdır.

Bilgi güvenliği, bilgiyi ve bilgi sistemlerini yetkilendirilmemiş erişimden, kullanımdan, ifşa edilmesinden, kesintiye uğramasından,modifiye edilmesinden veya yok olmaktan korumaktır. Bilgi güvenliği, bilgisayar güvenliği ve bilgi güvencesi sıklıkla birbirlerinin yerine kullanılabilmektedir. Bu alanlar birbirleri ile dolaylı yoldan ilişkili olup, bilginin güvenilirliğini, bütünlüğünü ve erişilebilirliğini korumayı ortak emelleri olarak paylaşırlar; ancak birbirleri arasında ince bir fark bulunmaktadır. Bu farklılıklar, konuyu ele almada, kullanılan metodolojilerde ve konsantre olunan ilgi alanlarında yatar. Bilgi güvenliği, elektronik çıktı veya diğer formlarda olsun, verinin güvenirliği, tutarlılığı ve erişilebilirliği ile ilgilidir.

Hükümetler, askeriye, finansal enstitüler, hastaneler ve özel işletmeler işçileri, müşterileri, ürünleri, araştırmaları ve finansal statüleri hakkında büyük miktarda veri biriktirirler. Bu bilginin büyük bir kısmı artık bilgisayarlarda toplanmış, biriktirilmiş ve ağ boyunca diğer bilgisayarlarla paylaşılabilir haldedir. Bir işletmenin müşterileri veya finansal değerleri veya yeni bir ürün hakkındaki bilgilerin rakiplerin eline düşmesi halinde, böyle bir güvenlik aşımı, iş kaybına, davalara ve hatta işletmenin batmasına yol

açabilir. Gizli kalması gereken bilgiyi korumak bir iş yönetimi gerekliliğidir ve birçok anlamda etik ve yasal zorunluluktur [50].

1.6.1 Bilgi Güvenliği Tanımı ve Kavramları

Bilgi güvenliği, kurumların bilgi envanterindeki varlıkların gizliliğini, bütünlüğünü, erişilebilirliğini tehdit eden risklerin tanımlanıp, bu konuda risk yönetimi gereklerinin yapılmasıdır. Risk yönetimi kapsamında bilgilerin maruz kalabileceği tehditler bilgilerin önemine, tehlikenin olabilirliğine ve gerçekleştiğinde etkisine göre şu seçeneklerden biri tercih edilir [29]

- Riskin azaltılması,
- Riskin kabul edilmesi,
- Tamamen üçüncü bir tarafa devredilmesi (sigorta etmek gibi) veya
- Risk kaynağının yok edilmesi seçeneklerinden biri tercih edilir.

Risklerin tanımlanması ISO/IEC 13335-115 (ISO/IEC 13335-1:Guidelines for the management of IT Security Part 1: Concepts and models for IT Security) standardında da gösterilmektedir. Bu standardın tanımı itibariyle bilgi güvenliği, bilginin risk yönetimini yapmaktır.

Ayrıca Bilgi Güvenliği, bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin korunması olarak ifade edilmektedir. Burada;

1.6.1.1 Gizlilik

Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunun garanti edilmesidir. Ayrıca gizlilik Uluslararası Standartlar Örgütü (ISO) tarafından "Bilgiye sadece yetkilendirilmiş kişilerce ulaşılabilmesi" olarak nitelenir.

1.6.1.2 Bütünlük

Blginin ve işleme yöntemlerinin doğruluğunun ve bütünlüğünün temin edilmesi,

1.6.1.3 Erişilebilirlik

Yetkilendirilmiş kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişime sahip olabileceklerinin, garanti edilmesidir [30],[51].

Kısaca, gizlilik; önemli, hassas bilgilerin istenmeyen biçimde yetkisiz kişilerin eline geçmemesini, bütünlük; bilginin bozuk,çarpıkve eksik olmamasını, erişilebilirlik ise bilgi veya bilgi sistemlerinin kullanıma hazır veya çalışır durumda olmasını hedefler. Bugün şifreleme altyapılarının olmasının sebebi temel olarak gizlilik, ve bütünlüktür. Bilgi güvenliğinin her kavramı her kurum için eşit önemde olmayabilir. Gizlilik özellikle kamu kurumları ve bankalar gibi kuruluşlar için önemlidir.

İşte bilginin bu şekilde değerlenmesi, kurumların ürün ve hizmet bilgilerinin yanı sıra, stratejik, finansal, pazar bilgilerinin rakiplerden ve yetkisiz erişimlerden korunması, süreçlerin hızlı ve kusursuz bir yapıda işlerliği, tüm bunlara hizmet veren bilgi teknolojilerinin alt yapısı, işletim yazılımları, iletişim ağları, bilgi yönetimi vb unsurların bir sistem dahilinde düzenlenmesini ve ele alınması gereğini ortaya çıkarmıştır.

Gizlilik , bütünlük ve erişilebilirlik kavramlarına başka kurumlar iki kavram bakış açısı daha eklemektedirler. Bu beş kavram, CBK(Common Body of Knowledge-Ortak Bilgi Kitlesi) dahilindeki üçü olan gizlilik, bütünlük ve erişilebilirlik ile bu üçü kadar sık dile getirilmeyen diğer iki öğe olan hesap verebilirlik ve yetkilendirmedir. Bütün güvenlik konuları bu kavramlardan yola çıkılarak değerlendirilir, bilgi güvenliğinin tam tanımı bu kavramlar anlatıldıktan sonra ancak yapılabilir.

1.6.1.4 Hesap Verebilirlik

Hesap verebilirlik kişisel sorumluluğun bir ölçütüdür. Hesap verebilirliğin en kısa tanımı, kişilerin yaptıkları hareketlerden ve görevi olduğu halde yapmadıklarından sorumlu olmalarıdır. Hesap verebilirliğin alt kavramları olan sorumluluk, suçlanabilirlik, cevap verebilirlik gibi konular büyük tartışmaların merkez noktaları olduğundan hesap verebilirlik diğer üç kavramın yanında değil, biraz uzağında değerlendirmeye tabi tutulur [52].

Kurumlarda hesap verebilirliğin en önemli yansıması şeffaflıktır. Kamu kaynaklarını kullanmakla görevli yetkililerden eylemlerini ve planlarını anlaşılabilir bir halde kamuoyu denetimine açmaları beklenmektedir.

1.6.1.5 Yetkilendirme

Bilgi güvenliği bakış açısından yetkilendirme kimlik doğrulama sistemidir. Bilgiye erişim sürecinde yetkilendirme, bilgiye doğru kişinin ulaşıp ulaşmadığını kontrol eden alt sistemdir. Gündelik işlerimizde hemen her bilgisayar ağ kaynağına eriştiğimizde yetkilendirme çözümlerini kullanmaktayız. Microsoft Windows işletim sistemine her şifre girildiğinde, şifre alan kontrolcüsünün Kerberos sisteminde kontrol edilip, cevap geriye yollanır. Bu aşamadan sonra kişi her ağ kaynağı kullanmak istediğinde, bağlanılan sistem kişinin kimliğini gene "bilgisayar grubunda kimlik yönetimi gibi merkezi işlevleri yapan bilgisayar sunucusundan" yani "alan sunucusundan" teyit eder.

Yetkilendirme konusunda dikkat edilmesi gereken, bilgi sistemlerinde geçerli olan "en az bilgi"- "Need to know/Principle of least privilege" kuralıdır. Başlangıçta askeri olan bu kural, kişilerin işlerini yapmaları için gereken en az bilgiyi bilmeleri gerektiği prensibini kurumlara benimsetmektedir.

Sadece teknolojik önlemlerle (virüs koruma, güvenlik duvarı sistemleri, şifreleme vb.) iş süreçlerinde bilgi güvenliğini sağlama olanağı yoktur. Bilgi güvenliği, süreçlerin bir parçası olmalı ve bu bakımdan bir iş anlayışı, yönetim ve kültür sorunu olarak ele alınmalıdır. Her kurum mutlaka bireysel olarak ve kurum bazında bir güvenlik politikası oluşturmak, bunu yazılı olarak dökümante etmek ve çalışanlarına, iş ortaklarına, paydaşlarına aktarmak zorundadır. Tüm çalışanlar bilgi güvenliği konusunda bilinçli olmalı, erişebildikleri bilgiye sahip çıkmalı, özenli davranmalı, üst yönetim tarafından yayınlanan "BG politikası" şirket açısından bilgi güvenliğinin önemini ortaya koymalı, sorumlulukları belirlemeli, çalışanlarını bilgilendirmeli ve BG sistemi, iş ortaklarını (müşteri, tedarikçi, taşeron, ortak firma vb.) da kapsamalıdır.

Tüm bunlardan çıkan sonuç; Bilgi Güvenliği'nin bir teknoloji sorunu olmadığı, bunun bir iş yönetimi (sistem) sorunu olduğudur. Bu nedenle günümüzün rekabet ortamında küresel ekonominin içinde varolmak için bilgi varlıklarımızı koruma ve

güvence altına alma, bunu bir yönetim sistemi yaklaşımı içinde kurumsal düzeyde yaygınlaştırma mecburiyeti kurumları Bilgi Güvenliği Yönetim Sistemi kurmaya ve kullanmaya zorlayacaktır [49].

1.6.2 Bilgi Teknolojileri Güvenlik Tehditleri

1.6.2.1 İç ve Dış Tehditler

Bilgi güvenliği tehditleri arasında, organizasyon bünyesinde çalışan kişilerin oluşturabileceği bilinçli veya bilinçsiz tehditler olarak tanımlayabileceğimiz iç tehditler çok önemli bir yer tutmaktadır. Bilinçli tehditler iki kategoride ele alınabilir. Birinci kategori, organizasyonda çalışan kötü niyetli bir kişinin kendisine verilen erişim haklarını kötüye kullanmasını içerir. İkinci kategori ise bir kişinin başka birine ait erişim bilgilerini elde ederek normalde erişmemesi gereken bilgilere erişerek kötü niyetli bir aktivite gerçekleştirmesini kapsar. Veritabanı yöneticisinin, eriştiği verileri çıkar amacıyla başka bir firmaya satması ilk kategoriye verilecek örnektir. Veritabanı yöneticisi olmayan ve normalde veritabanına erişim hakkı bulunmayan birisinin erişim bilgilerini bir şekilde elde ederek verileri elde etmesi ve bunu çıkarı için kullanması ikinci kategoriye örnektir. CSI (Computer Security Institute) tarafından yapılan ankete göre katılımcıların %44'ü 2008 yılı içerisinde iç suistimal yaşamışlardır [7]. Söz konusu oran, iç suistimallerin %50'lik virüs tehdidinden sonra ikinci büyük tehdit olduğunu göstermektedir. Bu tür suistimallerin tespitinin zor olduğu ve çoğunlukla organizasyon dışına bu konuda çok bilgi verilmek istenemeyebileceği de düşünülürse aslında %44'lük oranın daha büyük olduğu düşünülebilir. Anket çalışmasında, suistimal tabiri ile sadece bilinçli oluşan iç tehditlerin kastedildiği anlaşılmaktadır.

İç tehditlerin tespit edilmesi ile ilgili yapılan araştırmalar, çoğunlukla yapay zeka temelli çözümleri içermektedir. Bu çözümlerde kullanıcıların normal davranış profillerinin, kullandıkları işletim sistemi komutlarından, farklı sistem bileşenleri üzerinde oluşturdukları kayıtlardan (web erişimi, veritabanı erişimi v.b) ya da kullanıcı programlarının işletim sistemleri üzerindeki erişim işlemlerinden (windows registry erişimleri gibi) yola çıkılarak tespit edilmesi sağlanır. Daha sonra günlük faaliyetlerinin bu profillere uyum sağlayıp sağlamadığı kontrol edilir [9],[23]. Bu çalışmalar, özellikle

başkasının erişim bilgisini elde eden kötü niyetli kişilerin tespit edilmesi konusunda daha başarılıdırlar. Çünkü erişim bilgisi bir şekilde çalınsa bile, bilgisi çalınan kişinin erişim profilini bilmek ve buna uygun hareket ederek sisteme erişmek kolay değildir. Söz konusu çalışmalar, bizzat kendi erişim haklarını suistimal eden kişileri yakalamada çok etkin değildirler. Bu tür kişilerin faaliyetlerinin tespit edilmesi önemli bir araştırma alanıdır [23].

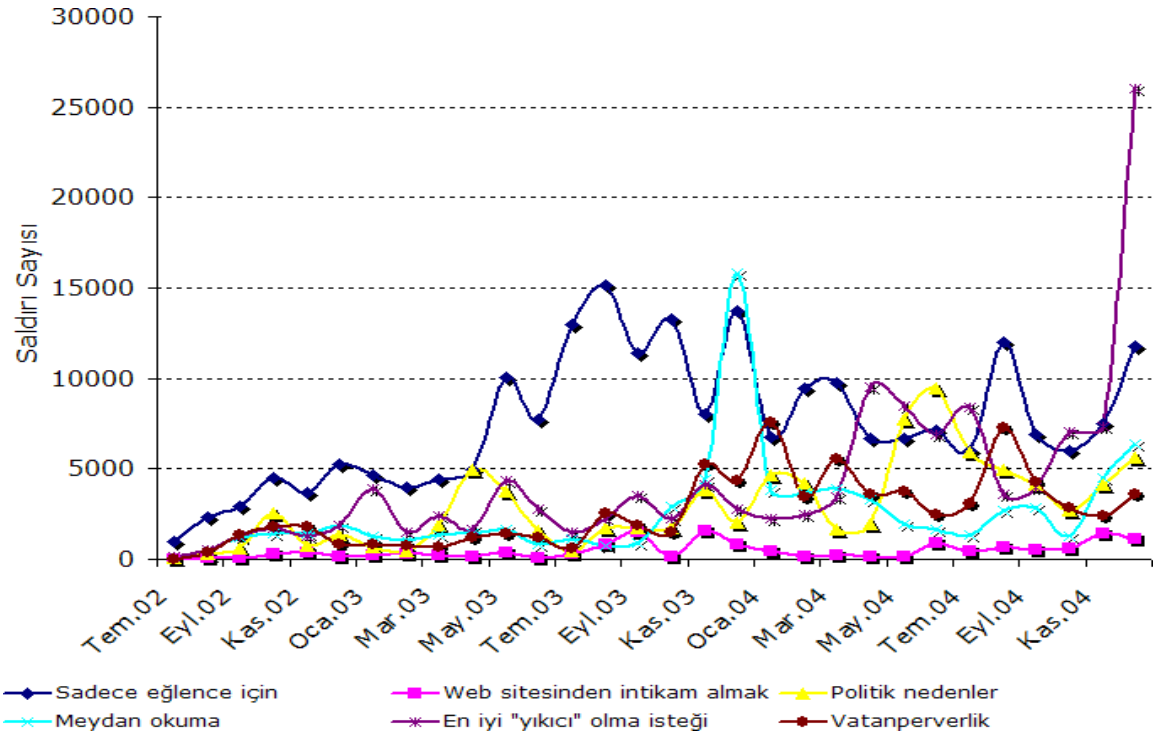
İç tehditler çoğunlukla uygulama seviyesinde oluşmaktadır [9]. Bunun sebebi, iç tehditlerin önemli bir kısmını bilişim alanında detaylı teknik bilgi sahibi olmayan kişilerin oluşturmasıdır. Söz konusu kişiler, çoğunlukla teknik saldırı yöntemlerini kullanmadan uygulamaların kendilerine verdiği haklar kapsamında ya da başka kişilerin erişim bilgilerini sosyal mühendislik yöntemleri ile ele geçirerek uygulamaları su-istimal ederek hedeflerine ulaşmaktadırlar. Dolayısıyla, iç tehdit tespit metotları uygulama kayıtlarını kullanma üzerine yoğunlaşmaktadırlar. Bu gerçek, ağ katmanı ve diğer katmanda tutulan sistem kayıtlarının bu tür tehditlerin tespiti kullanımında tamamen devre dışında kaldığı anlamına gelmez. Tespit sistemleri, gerekli durumlarda uygulama kayıtları ile diğer kayıtları ilişkilendirmektedirler.

İç tehdidin tespit edilmesinde son zamanlarda kullanılan en önemli yöntemlerden birisi de organizasyon için kritik olan bilgilerin tanımlarının yapılması, bu bilgilerin akışının ve depolanmasının tanımlar kapsamında kontrol edilmesidir [11]. Bunu gerçekleştiren tespit sistemleri veri kaçağı önleme olarak ele alınmaktadır. Örneğin, bir organizasyonun İnternet çıkışı üzerinde akan bilginin içeriğinde kontrolsüz bir şekilde T.C kimlik numaralarının var olup olmadığının kontrol edilmesi bu tür sistemlerle sağlanabilir. Son zamanlarda bu konuda ticari ürünler geliştirilmiştir. Ürünlerde halihazırda kullanılan kritik bilgi tanımları çok fazla yanlış alarm üretilmesine neden olabilmektedir. Dolayısıyla, kritik bilgilerin içeriğinin yazı madenciliği yöntemleri ile ayırt edilmesi önemli araştırma konularından birisidir [12],[23].

Bilgi ve bilgisayar güvenliğinde; karşı taraf, genel olarak kötü niyetli olarak nitelendirilen kişiler (korsanlar) ve yaptıkları saldırılardır. Var olan bilgi ve bilgisayar güvenliği sistemini aşmak veya atlatmak; zafiyete uğratmak; kişileri doğrudan veya dolaylı olarak zarara uğratmak; sistemlere zarar vermek, sistemlerin işleyişini

aksattırmak, durdurmak, çökertmek veya yıkmak gibi kötü amaçlarla bilgisayar sistemleri ile ilgili yapılan girişimler, saldırı veya atak olarak adlandırılmaktadır.

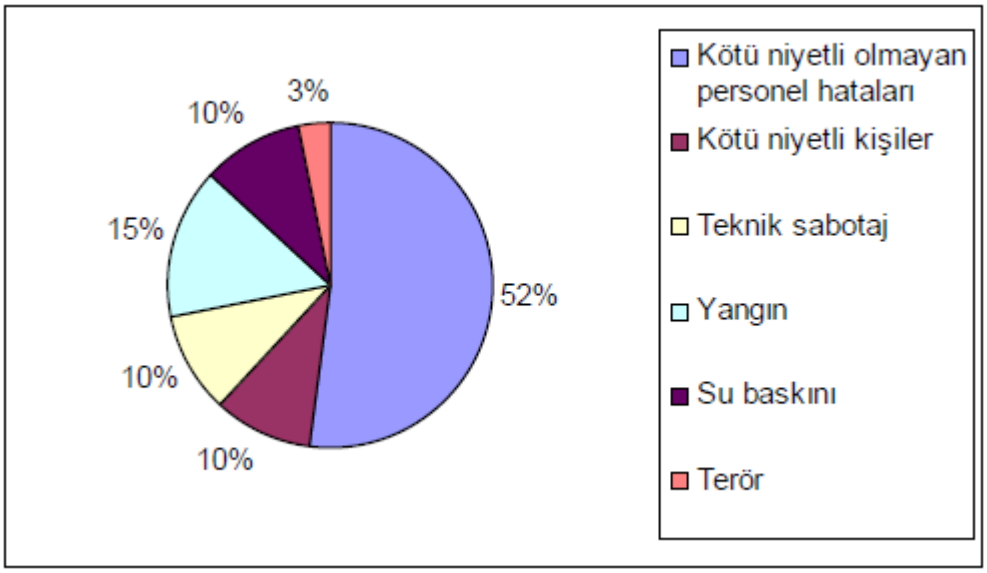
Bilgisayar sistemlerine yapılan saldırıların neden gerçekleştirildiğini anlamak, saldırıların ve alınabilecek önlemlerin belirlenmesinde önemli bir veri sağlayacaktır. Genel olarak bir saldırganı bu yola iten sebepler takip edilmelidir. Bu konuda İnternet web sunucularına yapılan saldırılara ait bilgileri, doğruladıktan sonra sınıflayıp, tutan Zone-H oluşumunun, yaklaşık bir milyon sunucuya ait, geçmiş yıllara dayanan istatistikleri saldırganın saldırı yapmaya iten sebepleri de göstermektedir [53],[54]. 2002-2004 yılları arasında saldırı sebepleri; "sadece eğlence için", "web sitesinden intikam almak için", "politik sebepler", "meydan okuma", "en iyi yıkıcı olmak için" ve "vatanperverlik" olarak sınıflandırılmıştır. Bu nedenlere göre yapılan saldırıların 2002-2004 yılları arasında dağılımı Şekil 1.8'de gösterilmektedir.



Şekil 1.10 Saldırı Nedenleri

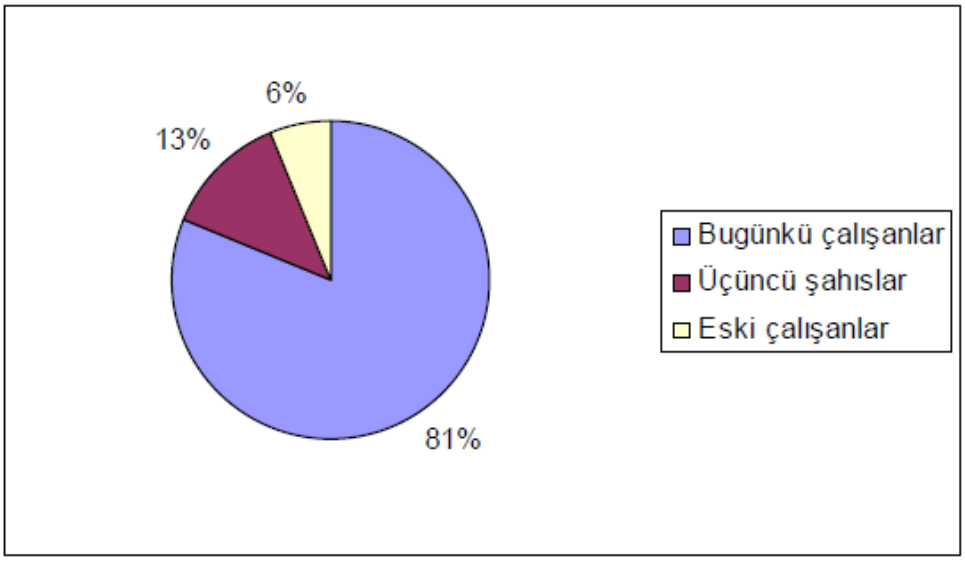
Şekil 1.10'dan da görülebileceği gibi, sanal dünyada sayısal vandalizm, saldırganları güdüleyen en büyük etken olarak karşımıza çıkmaktadır [53],[55],[56]. Korsanların İnternet sitelerine daha çok, en iyi yıkıcı (defacer) olmak için ve sadece eğlence için saldırdıkları görülmektedir.

Gartner Datapro Research şirketi tarafından yapılan araştırmanın sonuçları kurumsal bilgilerinizin nasıl, kimler tarafından tehdit edilebileceği ve zarar verilebileceği hakkında ilginç sonuçlar vermektedir. Bu araştırmanın sonuçlarına göre Bilişim Teknolojilerinde meydana gelen zararların genel sebepleri Şekil 1.11'de gösterilmiştir.



Şekil 1.11 Güvenlik Saldırılarının Nedenleri

Saldırıların kimler tarafından yapıldığı da aynı çalışmada Şekil 1.12'de olduğu gibi sıralanmıştır. İşletme personelinin bilgisayar suçlarına karışma oranı %81'e kadar çıkmaktadır [57]. Bu nedenle iç tehdit, dış tehdide göre iç tehditte bulunan personelin sistem konusunda kişisel bilgiye sahip olunmasından dolayı daha ciddi sorunlara neden olabileceği değerlendirilmektedir.



Şekil 1.12 Güvenlik Saldırılarını Gerçekleştirenler

Güvenliğe yönelik dış tehditlere karşı kontrol mekanizması kullanılır. Kontrol aynı zamanda güvenlik tehditlerini planlayan iç tehditlerin tahmin edilmeleri amacı ile de kullanılır [57].

1.6.2.2 Bilgi Güvenliği Kontrol Mekanizmaları

1.6.2.3 Kriptografi ve Dijital İmzalar

Kriptografi bir anahtar yardımı ile verinin (düzmetin olarak bilinir) kodlanmış bir şekle ("cipher-text") getirilmesi işlemidir. Kriptografi genellikle bilginin gizliliğini korumak için kullanılır. Örneğin o bilgiye ulaşabilen insanlar anahtarı bilenler olarak sınırlandırılmıştır. Güçlü bir kriptosistemde düzmetin şifrelimetinden ancak bir çözme("decryption") anahtarı yardımıyla elde edilebilir. Böylece düzmetin "meraklı gözlerden" saklanmış oluyor. Kriptografinin bilgisayarlarda kullanılan genel olarak iki yöntemi vardır:

1.6.2.4 Paylaşılmış/Simetrik Anahtar Şifreleme(Shared Key Cryptography)

Veriyi değişen iki tarafta anahtara sahiptir. Bu başkalarınca bilinmeyen anahtar verinin iletimden önce şifrelenmesi, iletildikten sonra karşı tarafta şifresinin çözülmesi için kullanılmaktadır. İki çeşit simetrik şifreleme yöntemi vardır:Blok (veriyi bloklar

şeklinde şifreler) ve “stream”(her bit/byte veya wordu sıralı olarak şifreler) şifrelemeler.

Avantajları:Simetrik şifrelemeler herkese açık(public) anahtarrakiplerine göre çok daha hızlıdırlar.

Dezavantajları:Her iki taraf anahtarı bilmeli ve iletimi için güvenli bir yol bulmalıdır.

Tipik Uygulamalar:Gizliliğin korunması için bilginin şifrelenmesi, veri oturum şifrelemesi, banka sistemleri(PIN şifreleme)

1.6.2.5 Açık Anahtar Şifreleme(Public Key Cryptography)

İki tarafta da bir gizli anahtar ve açık anahtar bulunur. Gizli anahtarlar sadece sahipleri tarafından bilinmektedir. Açık anahtarlar ise herkese açıktır. (telefon numaraları gibi). Gönderen mesajı alıcının açık anahtarı ile şifreler ve alıcı şifreli-mesajı gizli anahtarı ile çözer. Bu Diffie ve Hellman (Stanford Üniversitesi, 1975 Sonbahar) tarafından keşfedilen, algoritmaların ve bir anahtarın şifrelemek, bir başka anahtarın çözmek için kullanılabileceği keşifleri sayesinde mümkün olmaktadır. Açık ve gizli anahtar bir anahtar çiftini oluşturur.

Bu şifreleme yöntemleri gerçekten çözülmesi zor olan sonlu alanların logaritmalarını almak(Diffie ve Hellman), büyük sayıları asal çarpanlarına ayırmak (RSA) gibi matematiksel yöntemlerle tek-yönlü fonksiyonlardan yararlanır. Bu tip fonksiyonlar tek yönde hesaplama diğer yönde hesaplamaya göre daha kolaydır. Bugünün işleme gücü ve bilgisayarlarıyla bile brute-force kullanarak kırmak sanal olarak imkansızdır. Daha yeni Eliptik eğriler, karışım üreticiler (“mixture generators”)gibi teknikler daha hızlı açık anahtar sistemleri vadetmektedir [59],[60].

Avantajları:Sadece gizli anahtar gizli tutulmalıdır. Açık anahtar için herhangi bir gizli kanal gereksinimi yoktur. Sadece açık anahtar alıcıya bu anahtarın gerçek açık anahtar olduğundan emin olabileceği bir kanaldan gönderilmelidir. Ayrıca açık anahtar şifreleme ile dijital imzalara olanak sağlanmaktadır [60].

Dezavantajları:Matematikselkarmaşıklıkiçerenalgoritmalarındandolayıyavaş olmaları [60].

TipikUygulamalar:Sadecealıcınınçözebileceğindeneminolunmakistenen uygulamalar, simetrik oturum anahtar iletimleri [59],[60].

1.6.2.6 Hashing/Mesaj Şekillendirme(Message Digest)

Bir hash fonksiyonu bir blok veriden sabit uzunlukta karakter katarları oluşturur. Eğer fonksiyon tek yönlü ise ayrıca mesaj şekillendirme adını alır. Bu (hızlı) fonksiyonlar bir mesajı alır, analiz eder ve sabit uzunlukta özetler(digest) oluşturur(pratikolarakbuözetlertektir,benzeriyoktur).Çokhızlı bilgisayarlarla bile bir hash yardımı ile mesajların elde edilmesi mümkün değildir. Aynı özete(digeste) sahip bir başka mesajın elde edilmesi için bilinen bir makul yol yoktur. Bu algoritmalar genellikle mesajların bütünlüğünü onaylamak için imzalar hazırlamakta kullanılmaktadır.

Avantajlar:Şifrelemeden daha hızlıdır ve sabit bir çıktı üretilir(Bu demektir ki çok büyük dosyalar bile aynı digesti oluşturur, bu veri iletimi için çok verimli olur).

Dezavantajları:Sadecebütünlüğügarantieder.Bazımakalelerdebilinenbazı zayıflıkları anlatılmıştır [58].

Tipik Uygulamalar:Çoğu Internet sunucusu MD5 digestlerini önemli dosyaların indirilmesi durumlarında kullanır. Çoğu dijital imza sistemleri ve güvenli e-posta sistemleri bütünlük için bir digest fonksiyonu kullanır [58].

1.6.2.7 Kimlik Doğrulama

Bir nesnenin kimliğinin doğrulanması yöntemidir. Nesne kullanıcı, bilgisayar, makine yada bir süreç olabilir. Doğrulama iki tarafın bildiği ama başkalarının bilmediği şeyler kullanır. Bunlar biyolojik ölçüler (el tarama, DNA şekilleri, retina tarama, parmak izi tarama, el yazısı gibi), “passphrase”ler, şifreler, tek seferlik şifre listeleri, kimlik kartları, akıllı tokenler,“challenge-response”listeleri,vb.olabilir.Bazısistemler yukarıdakilerin kombinasyonlarını içerir [61].

Günümüzde çok karşılaşılan güçlü doğrulama yöntemleri tek seferlik şifreler (kağıt), otomatik şifre üreticileri (akıllı tokenler) ve zeki kimlik kartları diyebiliriz [61].

1.6.2.8 Erişim Kontrol Listeleri

Bir EKL(Erişim Kontrol Listesi) bir nesneye kimin veya neyin, ne şekilde erişebileceğini tutan listelerdir. EKL'ler veri gizliliğini ve bütünlüğünü sağlamakta kullanılan birincil mekanizmadır. Akıllı erişim kontrollü sistemler kullanıcıları ayırt eder ve her nesne için EKL yi yönetebilir. Eğer EKL kullanıcı(yada veri sahibi) tarafından değiştirilebiliyorsa akıllı erişim kontrolü olduğu kabul edilir. Eğer EKL kullanıcı tarafında değiştirilemiyor, sistem tarafından belirleniyorsa zorunlu erişim kontrolü kullanılmaktadır [61].

1.6.2.9 Fiziksel Kontroller

İstenmeyen kişilere karşı yapılan ilk koruma metodu bilgisayarın bulunduğu odanın kapısını kapamaktı. Bu konudaki gelişmeler daha gelişmiş kilit yapılarının, ses veya avuç izleri ile açılan, güvenlik kameraları ve korumalar gibi araçların da kullanılabileceğini göstermektedir.İşletmeler, bilgi işlem merkezlerini şehrin uzağına ve doğal afetlere karşı güvenli yerlere taşıyabilirler [61].

1.6.2.10 Güvenlik Duvarları

Bilgisayar kaynakları ağa bağlandıkları surece risk altındadırlar. Ağın tipi, ağ kanalıyla bilgisayara ulaşabilecek kişi sayısı riski belirler. Bir yaklaşım firmanın Web sitesini hassas bilgiler içeren iç ağından fiziksel olarak ayırmaktır. Diğer bir yaklaşım, iş ortaklarının şifre ile Internet üzerinden iç ağa ulaşımını sağlamaktır. Üçüncü bir yaklaşım ise koruyucu bir güvenlik duvarı kurmaktır. Güvenlik duvarı içeri ve dışarı veri akışını kısıtlayan bir filtre ve bariyer rolü oynar. Güvenlik duvarının arkasındaki kavram firmanın ağa bağlı bütün bilgisayarlarını bir bütün halinde korumaktır, her bilgisayar için ayrı bir koruma gerekmemektedir [61].

1.6.3 Bilgi Teknolojilerinde Güvenliğinde Yeni Eğilimler

1.6.3.1 Kişisel Gizlilik

Kişisel gizlilik, bir kişinin ya da bir grubun kendilerine ait bilginin kimlere ve hangi şartlar altında iletileceğinin bizzat o kişilerin/grubun onayı ile gerçekleştirilmesi anlamında kullanılmaktadır. Kişisel gizliliğin sağlanması iki farklı durumda da

gerçekleştirilmelidir [13]. İlk durum, kişisel verilerin kişilere ait bilgi sistemlerinde bulunduğu esnada tüm tehditlere karşı korunmasıdır ki bu anlamda herhangi bir bilginin korunması için geçerli tedbirler uygulanır. Bu tedbirler, erişim denetimi, yetkilendirme, sürekliliğin sağlanması gibi konuları içerir. İkinci durum ise kişisel verinin bir başka sistemle ihtiyaç dahilinde paylaşılmasında uygulanacak güvenlik tedbirlerini kapsar. Bu tedbirler, verinin içeriğinin kişi tarafından paylaşılması onaylanmamış kısmının filtrelenmesi, filtrelenmiş verinin ilgili sisteme güvenli aktarımı ve söz konusu verinin sadece veri sahibi kişiler tarafından onaylanmış organizasyonlarla paylaşılmasını içerir [23].

Kişisel gizlilik ile ilgili araştırmalar genellikle ikinci başlık üzerine yoğunlaşmıştır. Bu kapsamdaki çalışmalar literatürde verinin kişisel gizliliğinin korunarak yayınlanması (privacy preserving data publishing) adıyla ele alınmaktadır [14]. Bu metodlar, verilerin hiç bir şekilde sahibi ile sahibinin kritik bilgilerini eşleştirmeyecek şekilde anonimliğini sağlayarak iletilmesini gerçekleştirmeye yöneliktir. Örneğin, hastaneler araştırma projeleri için araştırma merkezleri ile hasta verilerini paylaşabilmektedirler. Burada paylaşılan bilgilerden, spesifik olarak herhangi bir kişinin hangi hastalığa sahip olduğuna araştırma merkezinin ulaşamaması beklenmektedir. Bu soru, sadece veri içerisinde kişiyi tekil olarak belirleyebilen T.C. kimlik numarası, isim ve soyisim gibi bilgilerin çıkarılması ile çözülememektedir [15]. Kişilere ait cinsiyet, adres gibi veriler de çoğunlukla spesifik olarak bir kişiyi tespit etmede yardımcı olmaktadır. Yapılan çalışmalarda, bu tip veri kısımlarının da kişisel gizliliği sağlayacak şekilde genelleştirilmesi (generalization) ya da silinmesi (suppression) sağlanmaktadır. Aslında verilerde bu tür işlemler, veri kalitesini düşürmektedir. Şu andaki ve gelecekteki çalışmalar çoğunlukla kişisel gizlilik ölçüm metriklerinin belirlenmesi, bu metriklere uyacak şekilde verinin olabilecek maksimum kalitede paylaşılabilmesine olanak sağlanması üzerinde yoğunlaşacaktır. Söz konusu metriklerin belirlenmesinin, sadece bilgisayar mühendislerinin değil, sosyoloji, psikoloji, hukuk alanlarında çalışanlarla yapılabilecek disiplinler arası çalışmalarla mümkün olabileceği değerlendirilmektedir [23].

Bilgi güvenliği araştırmalarında en önemli problemlerden birisi, araştırmacıların yeterli ve gerçek test verisi bulamamalarıdır. Bu durum, sistem işleten organizasyonların

kurum mahremiyeti açısından sistem verilerini paylaşmaması sebebiyledir. Verilerin kurum mahremiyetini de sağlayarak paylaşılabilmesi için ortaya konabilecek araştırmaların yakın gelecekte artacağı ve bu çalışmaların bilgi güvenliği alanının geneline de çok fayda getireceği öngörülmektedir.

1.6.3.2 Güvenli Yazılım Geliştirme

Yazılımlarda oluşan güvenlik açıklıklarının temel sebebi yazılım geliştirme döngüsü içerisindeki her adımda güvenliğin göz önüne alınmaması olarak görülmektedir. Gereksinim analizi aşamasında güvenlik gereksinimlerinin üzerinde durulmaması, yazılımın tehdit modellemesinin yapılmaması, yazılım testlerinin fonksiyonellik yanında güvenlik testlerini de içermemesi en temel problemlerdir [16]. Yazılımların kaliteli olarak geliştirilmesi amacıyla CMMI (Capability Maturity Model Integration) gibi standartlar ortaya konmuştur ama bu standartlara uyularak geliştirilen yazılımların güvenliği konusunda herhangi bir güvence oluşmamaktadır. Güvenli yazılım geliştirme döngüsü oluşturma ile ilgili standartlar geliştirilmektedir. Microsoft tarafından geliştirilen SDL (Security Development Lifecycle) metodu [17] ve OpenSAMM [18] metodolojisi bu tür standart çalışmalarına örnektir. Bu alandaki çalışmaların daha olgunlaşarak devam etmesi beklenmektedir.

1.6.3.3 Web Uygulamaları Güvenliği

HTTP protokolü ilk tasarlandığında sadece statik web sayfalarının gösterimi amaçlanmıştır. Sonraları dinamik sayfalar da bu protokol kapsamında iletilmiş ve günümüzde internet bankacılığı gibi karmaşık ve kritik sistemlerin üzerine bina edildiği bir protokol haline gelmiştir. Protokol baştan güvenlik düşünülerek tasarlanmadığı için özellikle protokol kapsamında birçok güvenlik açıklığı ortaya çıkmış ve bu açıklıkları kapatmak adına çözümler üretilmiştir. Web uygulamalarının İnternet üzerindeki en kritik sistemlerin temelini oluşturması ve http protokolünün güvenli olmayan altyapısı sebebiyle saldırganlar, web uygulamalarını çokça hedef almaktadır. IBM'in 2008 risk raporuna göre 2008 yılı içerisinde çıkan güvenlik açıklıklarının %55'i web uygulamaları ile ilgilidir [19]. Web uygulamaları açıklıklarının önemli bir kısmını da siteler arası betik yazma (cross-site scripting), sql-enjeksiyonu (sql-injection) ve dosya içerme (file

include) açıklıkları oluşturmaktadır. Özellikle açıklık arama ile ilgili araştırma yapanlar web uygulamaları açıklıkları üzerinde yoğunlaşmışlardır ve yoğunlaşmaya devam edeceklerdir.

1.6.3.4 Kablosuz Mobil Sensör Ağlar ve RFID Güvenliği

Kablosuz mobil sensör uygulamaları özellikle çevre gözleme, gözetleme, askeri aktiviteleri izleme, akıllı ev uygulamaları ve yardımcı yaşama desteği alanlarında yaygın olarak kullanılmaktadır. RFID sistemler ise ürün tedarik zincirinin işleyiş kalitesinde, otoyol gişeleri, alışveriş merkezleri gibi sürekli yoğunluk problemi olan yerlerde, kimlik ve güvenli geçiş uygulamalarında, takip uygulamalarında (öğrencilere, mahkûmlara, hayvanlara, vb.), envanter yönetimi uygulamalarında başarılı olarak kullanılmaktadır.

Bu teknolojilerin her ikisi de iş odaklı geliştirildikleri için iki teknoloji için de güvenlik problemi ikinci planda kalmıştır. Kablosuz mobil sensör ağlarının güvenliği, sensör ağların güvenlik engelleri, sensör ağların gereksinimleri, ataklar ve savunma önlemleri olmak üzere dört kategoride ele alınmaktadır [20].

Kablosuz mobil ağ sensörlerinin güvenlik engelleri aşağıdaki gibi verilebilir:

- Sınırlı güç tüketimi, bellek ve saklama alanı,
- Genel yayın olması, çarpışma ve gecikmeden dolayı güvenirliği düşük haberleşme,
- Merkezi olarak yönetilse bile fiziksel tehditlere açık olması

Taşıdığı önemli bilgilerlerden dolayı kablosuz mobil sensör ağlarında veri gizliği, veri bütünlüğü, süreklilik, verilerin tazeliği, kendi kendine organize olma, zaman sekronizasyonu, güvenli yerleşim ve kimlik doğrulama güvenlik gereksinimleri mevcuttur.
Kablosuz mobil sensör ağları servis dışı bırakma, trafik analizi, gizliliğin ihlal edilmesi, fiziksel ataklar gibi birçok atağa açıktır [23].

Kablosuz mobil sensör ağlarda yukarıda saydığımız ataklara karşı önlem almak için ve güvenlik gereksinimlerini karşılamak için kriptografik protokollerle savunma mekanizmaları kullanır. Fakat işlemci gücü, saklama, alanı, enerji sınırlılığından dolayı

etkin güvenlik protokolleri kullanmak kolay değildir. Son yıllarda ekonomik, kaynakları etkin kullanacak güvenli haberleşebilecek kablosuz mobil senör ağlar ve RFID sistemler konusunda projeler geliştirilmektedir [23].

1.6.3.5 Siber Güvenlik

11 Eylül 2001 ikiz kule saldırılarından sonra tüm dünyada kritik altyapıların korunması ve içeriden gelen veya gelebilecek ataklara karşı önlemler geliştirme konusunda önemli çalışmalar yapılmaya başlanmıştı. Enerji santralleri, hava limanları, nükleer santraller, barajlar, metrolar, limanlar vb ülke için hayati öneme sahip kritik altyapıların fiziksel ve BT güvenliğinin sağlanması, beklenmeyen olaylar karşısında iş sürekliliğinin devam ettirilmesi, felaket planının yapılması ve uygulanması için çok sayıda proje geliştirilmeye başlanmıştır. İnternetin yaygın olarak kullanılmaya başlanmasıyla birlikte kötü niyetli internet kullanıcıları veya teröristler ülkelerin kritik altyapılarının BT sistemlerine internet üzerinden saldırarak zarar vermeye çalışmışlardır. Hatta bu zaman zaman bir ülkenin diğer ülkenin BT altyapısına saldırmasına kadar varmıştır.

27 Nisan 2007 tarihinde Estonya, başkenti Tallinn'de bulunan Rusya'ya ait meçhul asker anıtını kaldırmasından sonra Estonya'da devlete ait web mail sunucuları ve bankacılık sistemlerine ataklar gerçekleştirilmiştir. Başlangıç atakları sonucunda bazı internet siteleri kötü niyetli kullanıcılar tarafından ele geçirilmiş bazıları devre dışı bırakılmış, bazılarının içeriği değiştirilmiştir. 30 Nisan-18 Mayıs tarihleri arasında Ulusal bilgi sistemleri, Internet hizmet sağlayıcıları ve bankalara yönelik daha geniş katılımlı ve koordineli dağıtık servis dışı bırakma (DDOS) atakları gerçeklenmiştir. Bu ataklar sonucunda Estonya'nın ulusal bilgi sistemleri ve ev kullanıcılarına hizmet veren diğer Internet sistemleri büyük zarar görmüştür. Internet bant genişliği büyük oranda saldırılar tarafından doldurulmuş ve ülkedeki Internet sistemi çökme noktasına getirilmiştir. Estonya ataklara karşı NATO'dan yardım istemiştir. Bu ataklarda botnet(köle bilgisayarlar) kullanıldığı için Avrupa, ABD ve diğer ülkelerden de çok sayıda bilgisayarın kullanıldığı görülmüştür. Bu ataklar sonucu NATO Estonya'nın başkenti Tallinn'de NATO Siber Savunma Mükemmeliyet Merkezini kurma çalışmaların başlamıştır. Bu konudaki çalışmalar hala devam etmektedir.

Estonya atağı ülkeler arasında ilk siber savaş denemesi olmamıştır. Gürcistan ile Rusya arasında Güney Osetya bölgesinden dolayı yaşanan politik çekişmeler sonucu 11 Ağustos 2008 tarihinde çıkan savaştan önce siber savaş başlamıştır. Rusya kaynaklı gerçekleştirildiği düşünülen siber saldırılar, askeri birliklerin savaşa girmesinden önce, 20 Temmuz 2008 tarihinde Gürcistan Devlet Başkanı Mihail Saakaşvili'nin İnternet sitesi olan www.president.gov.ge adresini hedef alarak başlamıştır. Ülkedeki birçok internet sitesi çökertilmiş ya da içeriği değiştirilmiştir. Bu ataklar dağıtık servi dışı bırakma (Distributed Denial of Service) türü ataklar olarak gerçekleştirilmiştir. Ataklarda çok sayıda köle bilgisayar kullanıldığı için atakları durdurmak ve kaynağını tespit etmek kolay olmamıştır.

4 Temmuz 2009 tarihinde ABD ve Güney Kore'ye ait çeşitli sitelere siber ataklar yapılmıştır. Güney Kore'de başta Ticaret ve Maliye bakanlığı sistemleri olmak üzere birçok kamu kurumu hedef alınmıştır. Ataklarda yaklaşık 50000 köle bilgisayar kullanılmış ve 20-40 Gbps'lık bir trafik oluşturulmuştur. Güney Kore yetkilileri atakların Kuzey Kore veya onun sempatizanları tarafından organize edildiğini ifade etmişlerdir [21].

NATO başta olmak üzere birçok organizasyon ve ülke siber atakları tespit etmek, önlemek ve atak sonrasında sistemleri normale dönüştürmek için organizasyonlar kurmakta ve projeler geliştirmektedir. Bu konudaki çalışmaların artarak devam etmesi beklenmektedir [23].

1.6.3.6 Endüstriyel Sistemlerin BT Güvenliği

Enerji santralleri, nükleer santraller, barajlar, petrol istasyonları gibi modern endüstriyel sistemler büyük karmaşık dağıtık sistemlerdir. İşletim esnasında bu sistemlerin değişik kısımlarının operatörler tarafından gözlenmesi ve kontrol edilmesi istenir. Günümüz ağ teknolojileri bu izleme ve kontrol işlemini mümkün kılmaktadır. Önceki ağ kontrol uygulamaları noktandan noktaya bir parçayı ya da cihazı kontrol edebilecek yapıda tasarlanmıştı. Bu yapılar zaman içerisinde merkezi kontrol ünitesi ve birçok uzak birim arasındaki haberleşmeyi ortak veri yolları ile haberleştirecek

şekilde geliştirilmiştir. Bu ağlardaki uzak birimler belli amaçlar için geliştirilmiş gömülü sistemleri içeren sensörler, harekete geçiriciler ve PLC (Programmable Logic Control) gibi parçalardan oluşmaktadır. Üstelik bu sistemler birbiri ile uyumlu değildir. Günümüzde bu endüstriyel komuta kontrol ağlarının gelişmiş hali SCADA (Supervisory Control and Data Acquisiton) olarak adlandırılmaktadır.

Günümüz rekabetçi ortamında endüstriyel ortamların düşük maliyeti ve etkin üretimi yakalaması için kendi SCADA sistemlerini modernize etmeleri gerekmektedir. Günümüz SCADA sistemleri kurum ağlarına ve internete bağlanabilmektedir. Bu bağlantı üretimi ve dağıtık veri işlemeyi kolaylaştırmasına karşın sistemi internetin güvenlik problemleri ile karşı karşıya bırakmaktadır. Eğer cihazlar internet üzerinde kontrol edilirse SCADA sistemine yapılan bir atak tüm sistemi etkileyebilir. Bu atak sonucunda fiziksel ve ekonomik kayıplar yanında insanlar diğer canlılar ve çevre zarar görebilir. Bu yüzden SCADA sistemlerin güvenliğinin birincil öncelikli olması gerekir [22].

TCP/IP protokolünün açık yapısı ve internet uygulamalarının yaygınlaşması ile birlikte ilk önceleri seri arabirimler aracılığı ile PLC gibi sistemler, bilgisayarlar aracılığı ile kontrol edilmeye başlanmış sonra ise SCADA sistemleri doğrudan Ethernet arayüzünü kullanılarak bilgisayar ağlarıyla haberleşmeye başlamıştır. Bu haberleşme bilgisayarın gelişmiş yazım yeteneği ve grafik arayüzünün SCADA sistemler tarafından kullanılmasını sağlamıştır. SCADA sistemlerin bilgisayar ağları ile haberleşmesi için çeşitli kuruluşlar tarafından Ethernet/IP, DeviceNet, ControNet, PROFIBUS, MODEBUS TCP/IP, DNP3, Foundadion Fieldbus gibi protokoller geliştirilmiştir.

İç tehditlerin, siber atakların arttığı günümüz internet yapısında çok kritik altyapıları işleten SCADA sistemlerin güvenliğinin sağlanması için erişim kontrolü, güvenlik duvarı, saldırı tespit sistemi, VPN gibi güncel sınır güvenliği önlemleri yanında protokol güvenlik analizi, SCADA sistemlerin işletim sistemleri güvenlik analizi gibi konularda çok sayıda proje geliştirilebilir [23].

1.6.4 ISO/IEC 27001/2 - ISO/IEC 7799/17799

ISO/IEC 27002, büyümekte olan ISO/IEC ISMS standart serisinin bir parçasıdır. ISO/IEC 27000 serisi, ISO ve IEC tarafından yayınlanmış Bilgi Güvenliği Standartlarıdır. 2007 Temmuz ayında , diğer ISO/IEC 27000 serisi standartlarla aynı çatı altında toplamak için ISO/IEC 17799:2005 standardı ISO/IEC 27002:2005 olarak yeniden numaralandırılmıştır ve "Bilgi Teknolojisi - Güvenlik Teknikleri – Bilgi Güvenliği Yönetimi İçin Uygulama Kuralları" olarak isimlendirilmiştir. Şu anda uygulanmakta olan standart, 2000 yılında BS(İngiliz Standardı) 7799-1:1999'dan kelime kelime kopyalanarak oluşturulan ISO/IEC' nin ilk basımının revize edilmiş halidir [62].

Bilgi güvenliği yönetimi konusunda en yaygın olarak kullanılan standart, "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardıdır. Bu standart, işletmeler içerisinde bilgi güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar. ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS'nin belgelendirmesi için "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardı kullanılmaktadır. Bu standart, dökümante edilmiş bir BGYS'ni kurumun tüm iş riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsamaktadır. İş risklerini karşılamak amacıyla ISO/IEC 27002:2005'te ortaya konan kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği ISO/IEC 27001:2005'te belirlenmektedir. Her iki standardın Türkçe hali TSE tarafından sırasıyla TS ISO/IEC 17799:2005 ve TS ISO/IEC 27001:2005 isimleri ile yayınlanmıştır. Söz konusu standardın belgelendirmesi konusunda TSE tarafından TS 13268-1 BGYS Belgelendirmesi İçin Gereksinimler ve Hazırlık Kılavuzu standardı yayınlanmıştır. ISO/IEC 27001 ve ISO/IEC 27002 standartları BGYS konusunda en temel başvuru kaynaklarıdır [63]. ISO 27002 ve buna bağlı ISO 27001 hiçbir zaman ISO 15408 (Common Criteria) veya CASPR (Commnonly Accepted Security Practices) gibi teknik bir standart olarak tasarlanmamış , her sektördeki şirketin kolayca uygulayabileceği bilginin korunması için gerekli esnek ve genel prensipleri oluşturmak amacı ile geliştirilmiştir. Her sektördeki şirketin kolayca uygulayabileceğibilginin korunması için gerekli esnek ve genel prensipleri içermektedir [24].

Bu iki standart da doğrudan bilgi güvenliği konusunu ele alırlar. Teknik ve teknoloji bağımlı standartlar değildirler. Belli bir ürün veya bilgi teknolojisi ile ilgilenmezler. Hatta bilgi teknolojileri güvenliği dahi bu standartların içerisinde yer almaz. Tek ilgi alanı vardır, o da bilgi güvenliğidir.

ISO 27002 Bilgi Güvenliği Yönetim Sistemini uygulamak, yerleştirmek ve sürekliliğini sağlamak ile sorumlu olan kişilere bilgi güvenliği yönetimi için en iyi uygulama çözümleri ile ilgili öneriler getirir. Bilgi Güvenliği kavramının temel ilkelerini kısaca G-B-U kısaltması ile gösterebiliriz [62]:

- **G**izliliğin korunması (Bilgiye ulaşımın, sadece yetki sahibi kişilerce olabildiğinin garanti altına alınması),
- **B**ütünlük (Bilginin ve bilgi işleme yöntemlerinin, doğruluğunun ve eksiksizliğinin korunması),
- **U**laşılabilirlik (Gereken durumlarda yetkili personelin, bilgiye ve ilgili varlıklara ulaşımının garanti edilmesi)

ISO 27002; bilgi güvenlik yönetiminin verimli yapılması için tasarlanmıştır. Teknik bir standart olmamasına rağmen, ISO 27002 bir şirketin güvenlik gereksinimlerini tanımlar ancak gerçekleştirme şeklini şirketlere bırakır. Diğer bir deyimle; şirket içi ve dışı yanlış ve kötü amaçlı kullanımına karşı bilginin korunması için gerekli beklentileri ve işlemleri tanımlar. ISO 27002, bilgi güvenliği yönetimi için uygulama prensiplerinin ortaya konulduğu dünyada kabul görmüş bir standarttır. ISO 27002 standardı bir kurumda bulunması gereken güvenlik önlemlerine yer vererek temel bir güvenlik çerçevesi çizer .

ISO/IEC 27002 standardı bilgi güvenlik yönetiminin verimli gerçekleştirilmesi için yayınlanmıştır. Teknik bir standart olmamasına rağmen, ISO/IEC 27002 bir şirketin güvenlik gereksinimlerini tanımlar ancak gerçekleştirme şeklini şirketlere bırakmaktadır. Diğer bir deyimle, şirket içi ve dışı yanlış ve kötü amaçlı kullanımına karşı bilginin korunması için gerekli beklentileri ve işlemleri tanımlamaktadır.

ISO/IEC 27002 standardında aşağıda genel kapsamı verilen 11 alan kapsanmaktadır. Bunlar, güvenlik politikası, organizasyon güvenliği, varlıkların sınıflandırılması/denetimi, personel güvenliği, fiziksel/çevresel güvenlik, iletişim yönetimi, erişim kontrol, sistem geliştirme, iş süreklilik yönetimi, bilgi güvenliği olay yönetimi ve uyumluluk olarak sıralanabilir [64]. Bütün güvenlik konuları bu kavramlardan yola çıkılarak değerlendirilecektir.

1.6.4.1 Güvenlik Politikası

Güvenlik politikası, şirket yönetimin destek ve katkıları ile güvenlik beklentilerinin karşılaması için gerekli güvenlik işlemlerini içeren, uyarlanmış kurallardır.

1.6.4.2 Organizasyon Güvenliği

Organizasyon güvenliği, güvenliğin koordine edilmesi, güvenlik yönetim sorumlulukların atanması ve güvenlik tehlikesi olaylarında takip edilecek işlemleri de kapsamak üzere bir güvenlik yönetim alt yapısının oluşturulmasıdır.

1.6.4.3 Varlıkların Sınıflandırılması ve Denetimi

Varlıkların sınıflandırılması ve denetimi, şirkete ait detaylı bilgi alt yapı envanterinin çıkarılıp değerlendirilmesi ve bilgi varlıklarının en uygun güvenlik sınıfına atanması işlemleridir.

1.6.4.4 Personel Güvenliği

Personel güvenliği, insan kaynakları ve iş süreçleri açısından güvenliğin önemli bir bileşen olarak ele alınmasıdır. Şirket çalışanlarının (Bilişim elemanları ve son kullanıcılar da dahil) görevlerine güvenlik beklentilerinin tanımlanması, işe alınmadan önceki personel araştırmaları, güvenlik kritik işlemlerde gizlilik anlaşmalarının devreye alınması, güvenlik olaylarının personel tarafından raporlanması gibi bir dizi konu içerir.

1.6.4.5 Fiziksel ve Çevresel Güvenlik

Fiziksel ve çevresel güvenlik, bilişim alt yapısı, bina ve çalışanların korunmasını sağlayan güvenlik politikasının tanımlanmasıdır. Kapsamında, binaya giriş, yedekli

güç kaynağına sahip olma, periyodik bilgisayar bakımı ve bina dışında bilişim kaynaklarının barındırılması gibi konular vardır.

1.6.4.6 İletişim ve Operasyon Yönetimi

İletişim ve operasyon yönetimi, güvenlik olaylarının önlenmesini sağlayan anti virüs koruma, günlük alma ve izlenmesi, güvenli uzaktan erişim, güvenlik olay takip sistemin devreye alınması gibi güvenlik önlemlerini içerir.

1.6.4.7 Erişim Kontrol

Erişim kontrolü, parola yönetimi, kimlik denetimi, günlük alma yöntemleri ile ağ ve uygulama kaynaklarına olabilecek iç ve dış saldırılara karşı korunma beklentilerini kapsar.

1.6.4.8 Sistem Geliştirme ve Bakım

Sistem geliştirme ve bakım faaliyetleri, yazılım geliştirme ve bakım süreçlerinde güvenliğin ele alınması ve mevcut uygulamaların güvenli olarak bakımının sağlanması beklentilerini içerir.

1.6.4.9 Bilgi Güvenliği Olay Yönetimi

Şirkete değer yaratan her türlü fikri mülkiyet, insan, teknoloji, bina ve donanım varlıkları ile kurumsal belleği oluşturan süreçler ile ilgili oluşmuş veya oluşabilecek bilgi güvenliği olaylarının yönetilmesi ve benzer olayların tekrarlanmaması için çalışmalar yürütülür.

1.6.4.10 İş Süreklilik Yönetimi

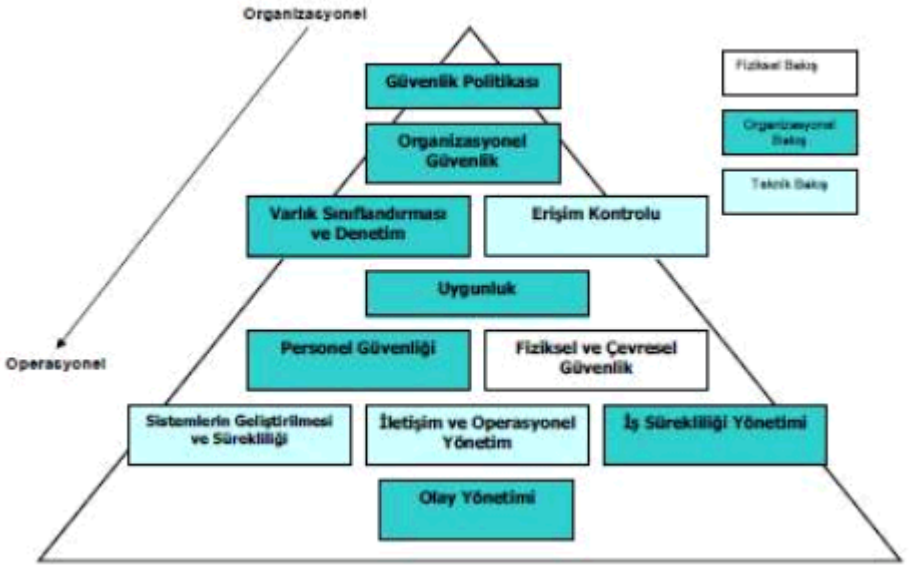
İş süreklilik yönetimi, doğal veya insan temelli felaketlerde şirket operasyonlarının sürekliliğinin sağlanması için gerekli planların yapılması faaliyetlerini içerir.

1.6.4.11 Uyumluluk

Uyumluluk, şirketin bağlı olduğu güvenlikle ilgili kanun ve yönetmeliklere uyumlu olması için gerekli kontrolleri kapsar [49].

Şekil 1.13'de bu 11 alanın standart yapılanması görülmektedir. Her bir alan, yukarıdan aşağıya, ayrı başlıklar altında, yönetsel, teknik ve fiziksel önlemler ile ilgili bilgiler içerir. Başka bir deyişle, yönetsel seviyeden yürütsel seviyeye kadar

faaliyetleri kapsar [65].



Şekil 1.13 BGYS Kontrol şeması

15 Haziran 2011 tarihi itibarı ile halen dünyada 7346 adet işletme , ISO 27001 ve ISO 27002 standardına göre başarıyla tetkikten geçerek akredite edilmiş kurumlarca sertifikalandırılmıştır. Bu ülkelerden Türkeye'deki işletmelerin adı ve sertifikasyon bilgilerin Çizelge 1.6 da sunulmuştur.

Çizelge 1.6 Türkiye' de BS 7799-2:2002 veya ISO/IEC 27001:2005 sertifikasyonuna sahip organizasyonlar

Sıra Numarası	Organizasyon Adı	Ülke	Sertifika Numarası	Sertifika Kökeni	BS 7799-2:2002 veya ISO/IEC 27001:2005
1	Anadolu Bilisim Hizmetleri A.S.	Türkiye	IS 548547		ISO/IEC 27001:2005
2	ATLAS MEDICAL SERVICES LTD.	Türkiye	809001		ISO/IEC 27001:2005
3	Bankalarasi Kart Merkezi A.S., Istanbul	Türkiye	212748	Bureau Veritas Certification	ISO/IEC 27001:2005

4	BDH	Türkiye	Gb10/81921	SGS United Kingdom Ltd	ISO/IEC 27001:2005
5	BEKO ELEKTRONİK A.Ş.	Türkiye	GB05/64028	SGS United Kingdom Limited	ISO/IEC 27001:2005
6	Borcelik Celik Sanayii Ticaret A.S.	Türkiye	29		ISO/IEC 27001:2005
7	Bursagaz Bursa Sehirici Dogalgaz Dagitim Ticaret ve Taahhut A.S.	Türkiye	GB07/72173	SGS United Kingdom Limited	ISO/IEC 27001:2005
8	Corbuss Kurumsal Telekom	Türkiye	IS 514424		ISO/IEC 27001:2005
9	E-Kart Elektronik Kart Sistemleri San. Ve Tic. A.Ş	Türkiye	192589	Bureau Veritas Certification	ISO/IEC 27001:2005
10	Global Bilgi Pazarlama, Danisma ve	Türkiye	IS 510931		ISO/IEC 27001:2005
11	Haci Omer Sabanci Holding A.S.	Türkiye	IS 530644		ISO/IEC 27001:2005
12	Hitit Bilgisayar Hizmetleri	Türkiye	GB09/78023	SGS United Kingdom Ltd	ISO/IEC 27001:2005
13	Hitit Bilgisayar Hizmetleri Ltd. Sti.	Türkiye	GB09/78027	SGS United Kingdom Ltd	ISO/IEC 27001:2005
14	İGDAŞ İSTANBUL GAZ DAĞITIM SANAYİ VE TİCARET A.Ş.	Türkiye	218289	Bureau Veritas Certification	ISO/IEC 27001:2005
15	Koc.net Haberlesme Teknolojileri	Türkiye	IS 514232		ISO/IEC 27001:2005
16	Merkezi Kayıt Kuruluşu A.Ş	Türkiye	GB09/77358	SGS United Kingdom Ltd.	ISO/IEC 27001:2005
17	PROBIL	Türkiye	GB10/81920	SGS United Kingdom Ltd	ISO/IEC 27001:2005
18	PWC / BASARAN NAS BAGIMSIZ DENETIM VE SMMM A.S.	Türkiye	IND82112	Bureau Veritas Certification	ISO/IEC 27001:2005
19	Sampas Bilisim VE Iletisim	Türkiye	GB08/75847	SGS	ISO/IEC 27001:2005
20	Siemens AG	Türkiye	302147 ISMS		ISO/IEC 27001:2005
21	Teknosa Ic ve Dis Ticaret A.S.	Türkiye	IS 544215		ISO/IEC 27001:2005
22	TEMSA SANAYI ve TICARET A.S.	Türkiye	GB07 / 73225	SGS United Kingdom Limited	ISO/IEC 27001:2005
23	TUBITAK	Türkiye	GB05/65232	SGS	ISO/IEC 27001:2005

24	Turk Traktor ve Ziraat Makineleri A.S	Türkiye	IS 96691		ISO/IEC 27001:2005
25	TURKTRUST	Türkiye	GB05/65355	SGS	ISO/IEC 27001:2005
26	Tusas Aerospace Industries, Inc., Ankara	Türkiye	203376	Bureau Veritas Certification	ISO/IEC 27001:2005
27	ULUSAL CAD ve GIS	Türkiye	2011/1293	Certification Europe	ISO/IEC 27001:2005

BÖLÜM 2

RİSK YÖNETİMİ VE ANALİZİ

2.1 Risk Yönetimi

"TS ISO/IEC 27001:2005 Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardına göre risk yönetimi bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler olarak tanımlanmıştır.

Risk yönetimi, bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla koruyucu önlemlerin maliyetlerinin dengelenmesi ve organizasyonun hedeflerine ulaşması için gerekli kritik sistemlerin korunması gibi konularda BT yöneticilerinin yararlandığı süreçtir. Bu süreç risk analizi, risk işleme ve değerlendirme ve takip alt süreçlerinden oluşur [67].

Risk, bir olayın ya da olaylar setinin ortaya çıkma olasılığıdır [68]. Risk, gerek belirsizlik gerekse belirsizliğin sonuçları olarak tanımlanabilir [69]. Genel anlamda risk, belirli bir zaman aralığında, hedeflenen bir sonuca ulaşmada, kayba ya da zarara uğrama olasılığıdır ya da bir olayın beklenenden farklı olarak gerçekleşebilme olanağıdır. Olabilecek sonuçların sayısı artması ile risk meydana gelir. Riskin mevcut olması demek bir olayın sonucunun tam olarak tahmin edilemeyeceği demektir. Risk, gelecekte oluşabilecek potansiyel sorunlara, tehdit ve tehlikelere işaret eder. Risk genellikle tam ve net olarak bilinemez ya da öngörülemez, belirsizdir. Belirsizliğin sonuç üzerinde olumsuz etkileri vardır. Riskin sübjektif ve objektif tarafları olduğunu savunanlar ve bu yargıya karşı çıkanlar olmasına rağmen, genel olarak riskin objektif ve ölçülebilen bir faktör olduğu söylenebilir. Risk, objektif ve ölçülebilen bir faktör olduğu sürece yönetilebilir bir olgudur.

Riskin temel bileşenleri, oluşma olasılığı ve oluşması durumunda sonucu ne ölçüde etkileyeceğidir. Ancak riski, yalnızca olumsuz etkileri olan bir kavram olduğunu düşünmek büyük bir yanlış olur. Riske kazanç elde etme fırsatı olarak bakılmalı, fırsata dönüştürülmesi için sistematik bir çaba gösterilmelidir. Riskler birbiriyle etkileşim içerisinde olan 3 temel alanda ele alınır [70]:

- Teknik risk, hedeflenen (tahmin edilen ve planlanan) performans değerine ulaşamamanın bir ölçüsüdür. Teknik riskler, maliyet ve çizelge risklerinin temel nedenidir.
- Maliyet riski, tahmin edilen ve planlanan maliyet değerinin aşılması durumudur. Örneğin ekonomik koşullardaki belirsizlikler önemli maliyet risk kaynaklarından biridir.
- Çizelge riski ise bir işin tahmin edilen ve planlanan sürede gerçekleştirilememesinin bir ölçüsüdür.

Risk analizi TS ISO/IEC 27001:2005 standardında kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımı olarak tanımlanmıştır. Risk analizi süreci kapsam belirlenmesi ile başlar. Belirlenen kapsamda bulunan varlıklar belirlendikten sonra, tehditler, açıklıklar ve mevcut kontroller belirlenir. Daha sonra olasılık değerlendirmesi ve etki analizi gerçekleştirilir. Son olarak bulunan riskler derecelendirilerek dökümante edilir [67].

2.2 Risk Yönetim Yaklaşımı ve Risk Yönetim Metodojileri

2.2.1 Risk Yönetim Yaklaşımı

Bilgi ve bilgi teknolojileri güvenliğine ilişkin riskleri yönetmek amacıyla her kurum kendi yapıları, kurumsal ve yasal bağlılıkları dikkate alan, bu alanda yer alan standartları destekleyen,aynı zamanda yönetimin onayladığı bir metodolojiyi benimsemeli ve buna uygun uygulamaları ya seçmeli ya da kendisi geliştirmelidir.

Risk metodolojisinin seçimi ya da geliştirilmesinde karar veren ya da bu alanda çalışan proje ekiplerince risk yönetimine ilişkin kavramlarının tam olarak anlaşılması ve aynı dilin kullanılmasında büyük yarar vardır.

Temel risk kavramı ve uluslararası kabul görmüş standart yada en iyi uygulamalar, bazı yasal düzenleyiciler tarafından belirlenen kuralların risk yönetiminden beklentilerine yönelik özet bilgiler bu bölümde açıklanmaya çalışılmıştır [71].

Risk kavramı; zarara ve kayba neden olacak bir olayın bilgi varlığı üzerinde gerçekleşme olasılığı olarak tarif edilebilir.

Risk yönetimi ise; var olan risklerin minimize edilmesi için oluşturulmuş süreçler bütünüdür. Risk yönetimi, ne kalite yönetiminin ne de proje yönetiminin faaliyetlerinden biridir. Risk yönetimi ayrı bir disiplindir, ancak tüm yönetim disiplinlerinde olduğu gibi, tek başına ve bağımsız olarak uygulanması da pek mümkün değildir. Risk yönetimine, proje yönetiminde kullanılan bir teknik olarak bakılması risk yönetimi ile sağlanacak kazançları azaltacaktır. Risk yönetiminin başlı başına bir disiplin olarak ele alınması, risk kültürünün, stratejisinin, prosedürlerinin, planlarının geliştirilmesini, sorumlulukların, yetkilerin ve nasıl bir organizasyonla yürütüleceğinin, süreçlerin net bir şekilde tanımlanmasını sağlayacaktır. Diğer ilişkili yönetim disiplinlerle bir bütün olarak uygulanması sonucunda, tekrarlayan faaliyet ve süreçlerin ortadan kaldırılması sağlanarak, yönetimin etkinliğini arttırılır [70].

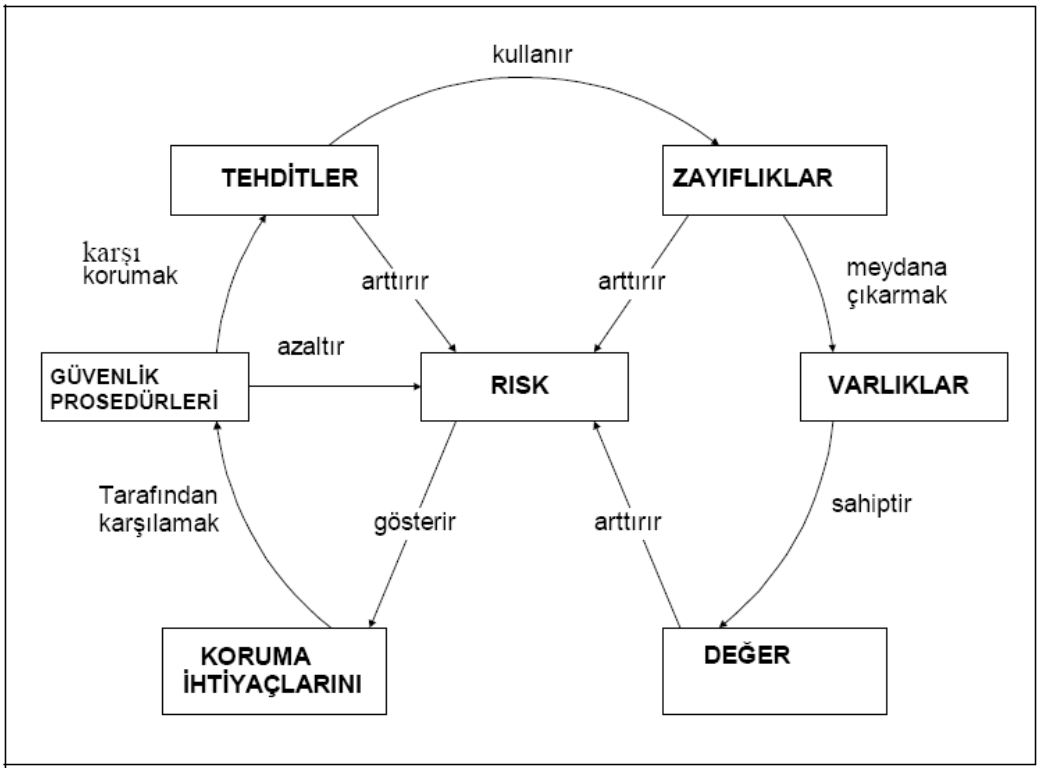
Risk yönetimi; risk analizi, risk değerlendirme, risk önleme, tehditlerin ve kontrollerin değerlendirilmesi olmak üzere dört ana süreçten oluşmaktadır.

ISO 27001, ISO 27005, COBIT, BASEL II gibi standartlar ve BDDK İlkeler Tebliği risk yönetimi üzerinde önemle durmaktadır;

ISO 27001, kuruma ait tüm bilgi varlıklarının değerlendirilmesi ve varlıklar üzerindeki tehditlerin ve açıklıkların göz önünde tutulup risk analizi yapılmasını gerekli kılar [4].

ISO 27005, bilgi güvenliği risk yönetim standardıdır. Bu standart kurumların ihtiyaçları doğrultusunda bir risk yönetim metodolojisi geliştirmesi gerektiğini ifade eder ve risk yönetim metodojilerine ilişkin örnekler verir [72].

Şekil 2.1’ de bilgi güvenliği ile risk yönetimi arasındaki ilişkiler gösterilmiştir. Örnek verecek olursak, tehditler riski arttırırken, güvenlik prosedürleri riski azaltır.



Şekil 2.1 Bilgi Güvenlik ile ISO/IEC TR 13335-1 Risk Yönetimi Arasındaki İlişkiler

COBIT'e göre öncelikle kurumlar risk yönetim çerçevesini oluşturmalıdır.

Risk yönetim çerçevesi oluşturduktan sonra mevcut riskler tanımlanmalı ve tanımlanan risklere ilişkin aksiyon planları oluşturulmalı planların uygulanabilirliği ve sonuçları izlenmeli, değerlendirmelidir .

Tüm bu standartlar, yasal otoritelerin koymuş olduğu uyulması gereken çeşitli kurallar ve kurumsallığın gereklilikleri bize kurumlarda etkin bir risk yönetiminin gerçekleştirmesini önem ve gerekliliğini göstermektedir .

Kurumların kendi ihtiyaçlarına özgü risk metodojisi geliştirmesi veya mevcut kabul görmüş bir metodolojiyi benimseyerek bunu risk yönetim araçları ile otomatize hale getirmesi gerekmektedir [71].

2.2.2 Risk Yönetim Metodojileri

Risk yönetim metodolojilerinin temelini teşkil eden risk değerlendirme yaklaşımlarından yaygın olarak nicel ya da nitel analiz yöntemlerinden biri veya her ikisi esas alınabilmektedir.

Nitel (qualitative) risk metodolojileri; çok yüksek, yüksek, orta, düşük, çok düşük gibi sözel ifadelere dayanır.

Nicel (quantitative) risk metodojileri ise; 0, 1, 2, 3, 4 gibi sayısal ifadelere dayanır.

Başlıca risk yönetim metodojileri şunlardır [71]:

2.2.2.1 COBRA (Consultative, Objective and Bi-functional Risk Analysis)

Nitel analiz yöntemine dayanan, anket tabanlı olup İngiliz danışmanlık şirketi tarafından geliştirilmiştir. Metodu destekleyen uygulamada geliştirilmiş olup uygulama 2 ana modül olmak üzere beş modülden oluşmaktadır [73];

- ISO 17799 COMPLIANCE KNOWLEDGE BASE
- E-SRUCTURE KNOWLEDGE BASE
- HIGH LEVEL RISK ANALYSIS
- IT SECURITY ASSESSMENT KNOWLEDGE BASE
- OPERATIONAL RISK KNOWLEDGE BASE

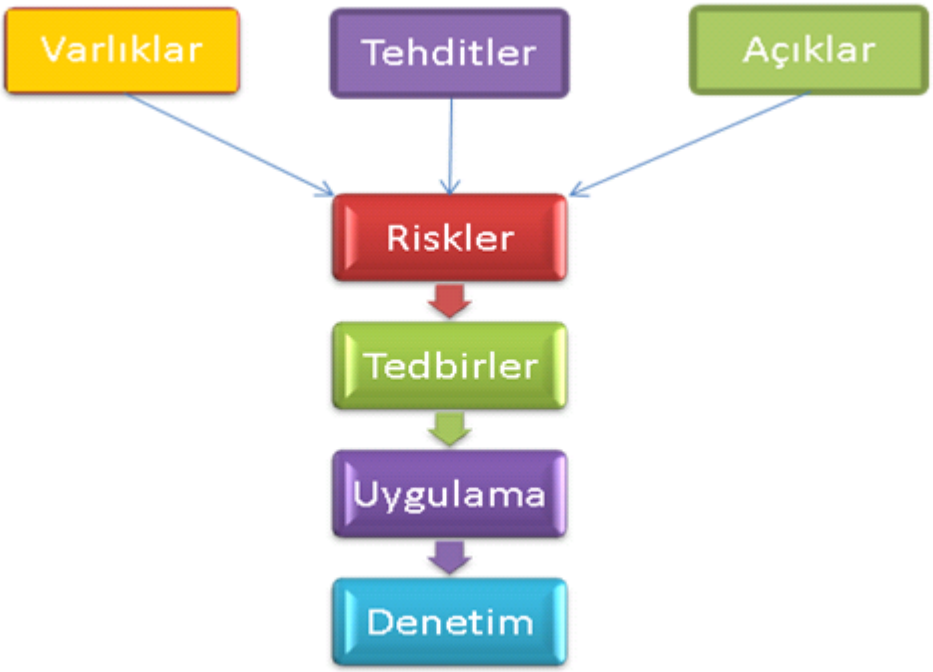
Risk Danışmanı: Standart sorulardan oluşur. Bu sorular kurum ile bilgi toplamak için kullanılır. Toplanan bilgiler risk analizinde kullanılır

Standartlara Uyum: Kurumun standartlara uyumunu ölçen sorular sorulur ve değerlendirilir.

2.2.2.2 CRAMM (CCTA Risk Analysis and Management Method)

İngiliz hükümetinin tercih ettiği resmi risk analizi ve yönetimidir. 1987 United Kingdom Central Computer and Telecomunication Agency's tarafından geliştirilmiş ve nitel yönteme dayanan risk analiz ve risk yönetim metodolojisidir [74].

CRAMM metoduna ait genel şema Şekil 2.2'de verilmektedir



Şekil 2.2 CRAMM Metodu

CRAMM metodu analiz ve yönetim olarak iki ana bölümde ele alınabilir. Risk analizi bölümünde bilgi varlığı, varlık üzerindeki açıklıklar(korumasızlıklar) ve tehditlerin bu açıklıkları kullanması sonucunda oluşabilecek risklerin analizini, yönetim bölümünde ise ölçümleme, uygulama ve denetim bölümlerinden oluşmaktadır.

CRAMM yaşam döngüsü ele alında 3 aşamada gerçekleştirildiği görülmekte. Buna ait bilgiler Şekil 2.3'te yer almaktadır.

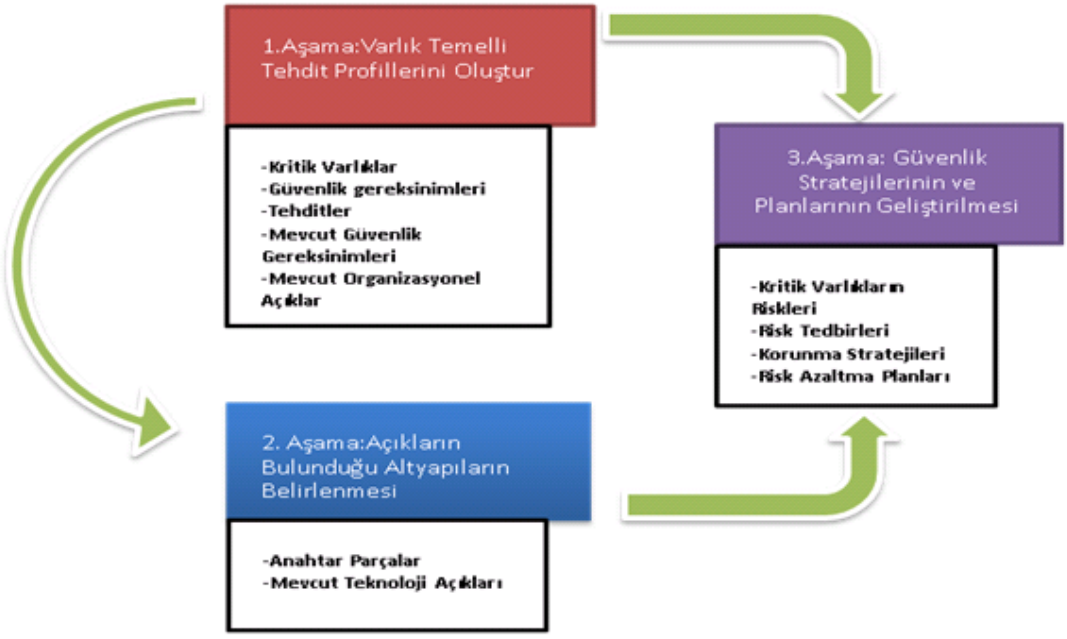
<table>
<tr><td colspan="3">CRAMM</td></tr>
<tr><td colspan="2">Bölüm 1 ve 2</td><td>Bölüm 3</td></tr>
<tr><td>Varlıklar</td><td></td><td></td></tr>
<tr><td>Tehditler</td><td>Riskler</td><td>Tedbirler</td></tr>
<tr><td>Açıklar</td><td></td><td></td></tr>
<tr><td colspan="2">Analizler</td><td>Yönetim</td></tr>
</table>

Şekil 2.3: CRAMM Yaşam Döngüsü

2.2.2.3 OCTAVE

Risk tabanlı stratejik görüş sağlayan planlama tekniğidir. Octave, Cert, DoD, USAF tarafından bilgi güvenliği risk değerlendirme metodu olarak kurumlar için

oluşturulmuştur. Octave, varlık tabanlı bilgi güvenliği risk değerlendirmesi yapamaktadır. Octave metodunun evreleri Şekil 2.4'te gösterilmektedir [76].

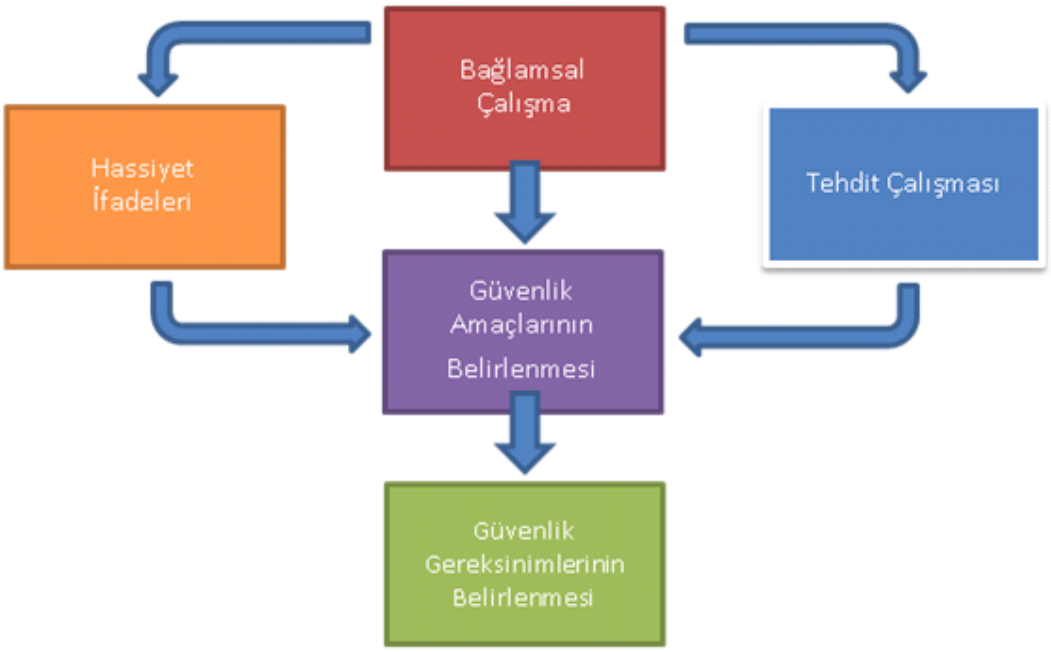


Şekil 2.4 OCTAVE Süreçleri

2.2.2.4 EBIOS (In French-Expression des Besoins et Identification des Objectifs de Security)

Bu risk metodolojisi; DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information) tarafından Fransa'da oluşturulmuştur.

EBIOS Method; Bilgi Güvenliği Sistemi ile ilgili riskleri ele alır ve değerlendirir. EBIOS metodunun genel şeması Şekil 2.5'te verilmektedir [77].



Şekil 2.5 EBIOS Metodu

2.2.2.5 ISAMM (Information Security Assessment & Monitoring Method)

ISAMM nitel yöntemlere dayanan risk analiz metodolojisidir. ISAMM ISO/IEC 27002'de yer alan en iyi uygulama örneklerini ve kontrollerini temel almaktadır[83]. ISAMM'da risk değerlendirme evresi üç kısımdan meydana gelmektedir [77];

- Kapsamlaştırma
- Tehdit ve açıklıkların değerlendirilmesi
- Riskin hesaplanması ve raporlanması

2.2.3 Risk Yönetim Yazılımları

Bu bölümde, risk metodolojileri hakkında ayrıntılı bir analiz yapabilmek amacıyla Art of Risk, Real ISMS, Callio, ISMart, Proteus, Risk Watch, ISMS-Rat uygulama yazılımlarının kullanmış olduğu risk yönetim metodolojileri incelenmiştir [71].

2.2.3.1 Art Of Risk

ISO 27001 tabanlı nicel metodu kullanan bir risk analizi yazılımıdır [79].

Başlıca üç modülden oluşur;

Bilgi Toplama Modülü: ISMS alanı, dökümanları ve dökümanların kayıt numaraları, risk politikaları ve kapsamları, risk değerlendirmeleri, varlıklar ve varlıkların gizlilik, bütünlük, erişilebilirlik ve diğer güvenlik özelliklerini tanımlar.

Risk Tanımlama ve Değerlendirme Modülü: Tanımlanan varlıklar için tehditler, açıklıklar ve risk değerleri ve hesaplamaların yapıldığı modüldür.

Risk Yönetimi Karar Modülü: Risk tedavi seçeneğinde tanımlanmış riskler için kontroller ve kontrol hedefleri oluşturur. Riskleri minimum seviyeye çekebilmek için seçilmiş kontrol amaçlarını, belirlenmiş kontrollerin ve uygulanabilirlik durumunun takip edildiği modüldür.

Kontrollerin Uygulanması: Seçilmiş kontrollerin uygulanması planlanır.

2.2.3.2 Real ISMS

ISO 27001 ve Cobit temelli internet tabanlı bir risk analiz yazılımıdır. Web sunucusu olarak ISS ve Apache'yi desteklemekte, veri tabanı olarak ise MS SQL, ORACLE ve POSTGRESS veri tabanlarını desteklemektedir [80]. Real ISMS'nin başlıca modülleri şunlardır;

Yönetim: Bu modülden kullanıcıların tanımlanması, değer skalalarının belirlendiği bölümdür.

Raporlama: Grafiksel ve istatistiksel bilgilerin alınabildiği, kullanıcıların hareketlerinin izlendiği ve raporlamanın yapıldığı modüldür.

Risk Yönetimi: Bilgi varlıkların belirlendiği, varlıklara ait risklerin eklendiği ve risk hesabının yapıldığı modül olup yine kontroller de bu bölümde eklenebilmektedir.

Politika Yönetimi: BG politikalarına ilişkin bilgilerin yer aldığı modüldür. (Yayınlanan, revize edilen politikalar vs.)

İyileştirme: Aksiyon planlarının oluşturulduğu, olayların düzenlendiği ve raporlamanın yapıldığı modüldür.

Kütüphaneler: Organizasyona ait BG olaylarının yer aldığı, yeni olayların eklendiği, döküman şablonlarının bulunduğu,

Arama: Veri ya da eleman filtrelemesine göre aramaların yapıldığı modüldür [71].

2.2.3.3 ISMart

Biz Net, TSE ve ISO–17799 / 27001 standardına uygun olarak bilgi güvenliği yönetimi sistemi kurmak ve uygulamak isteyen kurumlar için geliştirilmiş, Linux, Unix, veya Windows üzerinde çalışabilen Java ile yazılmış web tabanlı bir programdır.

Programda öncelikler varlık, tehdit, risk kategorileri oluşturulur. Kategoriler birbiri ile ilişkilendirilir. Varlık kategorilerine varlıklar eklenir ve varlığa ilişkin tehditler girilir. Bu kapsamda risk değerlendirilmesi yapılır [81].

2.2.3.4 Risk Watch

RiskWatch firması tarafından bilgi güvenliği risklerini analiz etmek için oluşturulmuş bir uygulamadır. Risk metodolojisi olarak nicel yaklaşımı benimsemiştir.

Bu uygulama bilgi sistemleri açıklıklarının değerlendirilmesi ve risk analizini içerir. Kurumların ihtiyacına göre şekillendirilebilir, yeni varlık, tehdit, açıklık kategorileri, soru kategorileri ve setleri oluşturulabilir [82].

ISO-17999 ve US-NIST-800–26 standartlarına ilişkin kontrolleri içerir.

2.2.3.5 Proteus

Infogov (Information governance limited) Limited şirketi tarafından geliştirilmiş web tabanlı bir risk yönetim yazılımıdır. Proteus ile kurumlar COBIT, SOX, ISO 17799, PCI DSS gibi standartların kontrolleri uygulanabilir.

Nitel ve nicel risk analizini destekler. Her iki yöntemde de varlık yönetimi, tehditlerinin belirlenmesi, risk aksiyon planlarının oluşturulması ve olay yönetimi mevcuttur.

Riskler ile ilgili pdf, doc formatında raporlama yapılır ve dashboard'dan grafiksel bilgiler alınabilir.

ISO 27001, BS 25999, PCI DSS, Cobit, SOX gibi standartları destekler [83].

2.2.3.6 Callio

Secura 17799; şirketlere BS 7799/ISO 17799 bilgi güvenliği yönetimi standardını sağlayan web tabanlı bir yazılımdır. Nitel bir değerlendirme yapılır

- **Risk Tanımlama:** Varlıklar açısından riskleri tanımlanır.
- **Risk Değerlendirmesi:** Risk hesaplama ve değerlendirmesi yapılır. Varlık envanteri oluşturulur ve değerlendirilir.
- **Risk tedavi:** ISO 17799 Kontrolleri: Farklı senaryoları değerlendirmek (Risk Tedavi plan taslağı)
- **Risk İletişimi:** Döküman Yönetimi, Bilinçlendirme Merkezi
- **Bilinçlendirme Merkezi Portalı:** Farklı personel grupları için bilgi güvenliği belgeleri yayınlanır.

ISO 17799 Ön Teşhis: Anket, güvenlik durumu ile ilgili ilk karar, uyum raporları alınır [84].

2.2.3.7 ISMS-Rat

ISMS- Rat client tabanlı basit bir risk analiz programıdır [85]. Uygulama veri tabanı olarak MS Access kullanmakta, standart yaklaşımı ISO 17799 ve ISO 27001 standardı bilgi güvenliği yönetim sistemini ve dolayısı ile risk yönetimini desteklemekte olup risk değerlendirme metodu olarak nitel analiz yaklaşım kullanılmıştır. Uygulama yazılım geliştirme platform bilgisine ise ulaşılamamıştır.

Varlık değerlendirme: Bilgi varlıklarının ‘gizlilik’, ‘bütünlük’,

‘erişilebilirlik’ nitelikleri bakımından ayrı ayrı ele alınır. Değerlendirme önceden tanımlanmış değer skalaları üzerinden gerçekleştirir.

Tehdit değerlendirme: Varlıkla ilişkili tehditler ve bunların gerçekleşme olasılık değerlerinin tanımlaması yapılarak tehditlerin değerlendirilmesi sağlanır.

Açıklık değerlendirme: Varlıkla ilgili varsa güvenlik zafiyetleri-açıklıkları tanımlanır.

Risk hesaplama: Standart yaklaşımları esas alan, bilgi varlık değeri, tehdit ve açıklık değerlerinin toplamından elde edilmektedir.

2.2.4 Risk Yönetimi Yazılımlarının Karşılaştırılması

Bilgi güvenliği risk yönetimine ait bilinen belli başlı uygulama yazılımları Mayıs-Ekim 2009 tarihleri arasında kapsamlı bir şekilde araştırılmıştır. İnceleme, ilgili uygulamaların demo yazılımlarının elde edilmesi ve/veya internet ortamında yer alan bilgilerin taranması yoluyla elde edilmiştir. İncelenen risk yönetim yazılımlarının uygulama türü, standart yaklaşımları, risk metodolojisi, yazılım geliştirme platformu ve çalıştığı veri tabanı bakımından karşılaştırma özeti Şekil 2.6'da gösterilmektedir [71].

Kriter-Nitelik		Art Of Risk	Asset Track	Callio Secura	COBRA	CRAMM	EBIOS	GRC	GSTOOL	ISAMM	ISMART	ISMS RAT	OCTAVE	PROTEUS	Real ISMS	Risk Watch	Secure Aware
Uygulama Türü	BGYS	+	+	+							+	+			+		+
	Risk Yönetimi				+	+	+	+	+	+			+	+		+	
Standart Yaklaşımı	BS 7799			+		+											
	ISO 17799	+		+	+		+				+	+				+	+
	ISO 27001	+	+	+		+		+		+	+	+		+	+		+
	ISO 13335-						+										
	BS 25999							+						+			
	SOX							+						+		+	
	COBIT							+						+	+	+	
	ITIL							+									
	HIPPA					+											
	Risk IT							+									
	PCI DSS							+		+				+	+		
	NIST 800-26													+		+	
	Basel II									+							
	GLBA					+											
Kendi Metodolojisi	Diğer (*)				+	+	+		*				+				*
Risk Değerlendirme Yaklaşımı	Nitel Analiz	+	+	+	+	+	+	+	+		+	+	+	+	+		+
	Nicel Analiz					+				+				+	+	+	
Yazılım Platformu	Php		+														
	XML						+										
	Java						+	+			+						
	Ulaşılamadı	+		+	+	+			+	+		+	+	+	+	+	+
Veri Tabanı	SQL Server			+					+						+		
	MS Access	+										+	+				
	My SQL			+										+			
	ORACLE							+							+		
	Ulaşılamadı		+		+	+	+			+	+					+	+
Araştırma Kaynağı	Demo	+	+	+				+			+	+			+		+
	İnternet	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+

Şekil 2.6 Risk yönetim yazılımlarının karşılaştırılması

Uygulamaların bir kısmı sadece "risk yönetimi" yaparken diğerleri risk yönetimini de içerisinden barındıran bir Bilgi Güvenliği Yönetim Sistemi (BGYS)'ni işletmek amaçlı geliştirildiği görülmektedir.

Standart yaklaşımlar bakımından incelendiğinde GSTOOL(IT Baseline Protection Manuel) ve kendi metodolojisini kullanan OCTAVE hariç hepsi bir şekilde bilgi güvenliği standardı olan (BS7799, ISO 17799, 27001, 27005) standartlarını referans aldığı, kartlara ilişkin standart olan PCI DSS, İş sürekliliğine yönelik BSI 25999, BT yönetişimi'ne ilişkin COBIT ve diğer NIST 800–26, SOX, Basel II, HIPPA, Risk IT ve ITIL gibi bilinen pek çok standardı destekleyen uygulamalardan oluştuğu görülmektedir.

Risk değerlendirme yaklaşımı bakımından incelendiğinde yazılımların çoğu nitel analiz yöntemini esas aldığı, nicel analiz yaklaşımın ise çok nadir kullanıldığı, CRAMM, PROTEUS ve Real ISMS uygulamalının ise hem nitel hem de nicel yaklaşımı kullanıldığı gözlemlenmiştir.

Araştırma esnasında yazılım platformu ve veri tabanı bilgisi gibi teknik bilgiler kısmen elde edilebilmiştir. İncelemeler sonrasında, uygulama platformlarının genellikle web tabanlı (Real ISMS, ISMART, GRC, Callio vb) olarak geliştirildiği, Art of Risk, ISMS Rat gibi uygulamalar ise istemci tabanlı (C/S) olarak geliştirildiği görülmektedir. Günümüz kullanıcı talepleri ve internet teknolojilerinin gelişimi, taşınabilirlik, kolay erişilebilirlik ve kurulum ve bakımda sağladığı avantajlar bakımından internet tabanlı uygulamaları öne çıkarmakta. Buna karşın farklı bölgelerde dağıtık yapıda olmayan, küçük işletmeler için güvenlik riski/maliyeti daha düşük olan C/S olarak geliştirilen ürünler tercih edilebilir.

Uygulamanın kullandığı yada desteklediği veri tabanları incelendiğinde uygulamaların yarıya yakınında bilgiye ulaşılamadı. Elde edilebilende ise MS Access, My SQL, SQL Server ve ORACLE veri tabanlarının kullanılabildiği görülmüştür [71].

2.2.5 Değerlendirme

Bilgi ve bilgi teknolojisinden kaynaklanan risklerin yönetiminde; günümüz iş dünyası gereksinimleri, yasal düzenlemeler, teknolojik gelişmeler ve artan rekabet koşulları, kurumsal risk yönetimini zorunlu kılmaktadır. Diğer taraftan kurumsallaşmayı

hedefleyen şirketler artık kurumsallığın bir gereksinimi olarak yaptığı işlerde ilgili standartları da dikkate almak zorundadır.

Gerçekleşecek bir bilgi güvenlik riskinin kuruma maliyetini önceden tam olarak kestirebilmek zor olsa da bu riskleri kabul edilmiş bir risk metodolojisini kullanarak önceden kestirebilmek ve yönetebilmek mümkündür.

Kurumlar madden ve manen varlıklarını etkin bir şekilde devam ettirebilmek için, kendi ihtiyaçları doğrultusunda bir risk yönetim metodolojisi belirlemeli ya da var olan risk metodolojilerinden birini seçmelidir. Seçilen metot kurumda etkin bir şekilde uygulanmalı, periyodik olarak izlenmeli ve alınan risk iyileştirme kararları doğrultusunda giderilmeli ya da kurumun kabul edebileceği bir seviyeye indirgenerek revize edilmelidir.

Bu çalışma, risk yönetim metodolojileri yapmak isteyen kurum ya da kuruluşlara mevcut belli başlı risk metodolojileri hakkında bilgilendirilmesine yönelik inceleme sonuçlarının paylaşımından oluşmaktadır.

Bu çalışmada incelenen uygulama yazılımların pek çoğu aynı zamanda bilinen bir standardı da referans almaktadır. İnceleme sonuçlarına göre en yaygın, bilinen ve aynı zamanda bilgi güvenliği yönetim sistemi (ISO 27001)'ni de destekleyen uygulamalara; Art Of Risk, Real ISMS ve ISMart'ı tercih edilebilecek örnek uygulamalar olarak verebilir [71]. Ancak ticari yazılımlar ise her kurum tarafından tercih edilmemektedir. Bunun nedenleri arasında, yazılımın pahalı bulunması, tam olarak kurumun ihtiyaçlarına yönelmemesi, yazılımın karmaşık olması ve kurumun yazılım çerçevesinde kalmak istememesi yer almaktadır[86]. Bununla birlikte her kurum kendi ihtiyacı doğrultusunda ihtiyaçlarına cevap verecek uygulama yazılımını kullanmalı ya da kendi ihtiyacı doğrultusunda uygun yazılımını geliştirmelidir [71].

2.3 Kurumsal Bilgi Güvenliğinde Risk Analizi

2.3.1 Kapsam Belirlenmesi

Risk analizinin ilk adımı kapsam belirlenmesidir. Kapsamın ilk aşamada doğru ve kurum hedeflerine uygun olarak belirlenmesi ileride gereksiz çaba harcanmasını önler ve

risk analizinin kalitesini arttırır. Kapsamda risk analizine tabi her şey açık olarak belirlenmelidir. Örneğin risk analizinde dikkate alınacak tüm BT varlıkları(yazılım donanım gibi), personel, tesisler, operasyonlar açıkça belirtilmelidir. Örnek bir kapsam şu şekilde olabilir. "Bu risk analizi kurumun muhasebe işlemlerinde kullanılan tüm donanım, yazılım ve personeli kapsar." Bu durumda muhasebe işlemleri için kullanılan tüm sunucular, kullanıcı bilgisayarları, işletim sistemleri, veri tabanı yazılımları, uygulamalar ve tüm bunları kullanan ve yöneten kurum personeli risk analizi içerisinde yer alır [88].

2.3.2 Varlıkların Belirlenmesi

Varlık, sistemin bir parçası olan ve kurum için değeri olan her şeydir. Varlık kurum için değer taşıdığından korunması gerekir. Bir BT sisteminde sadece yazılım ve donanımlar varlık olarak düşünülmemelidir. Aşağıdaki örnekler varlık olarak nitelendirilebilecek değerlerdir.

- bilgi (satış bilgilerini içeren dosyalar, ürün bilgileri)
- donanım (kişisel bilgisayarlar, yazıcılar, sunucular)
- yazılım (işletim sistemleri, geliştirilen uygulamalar, ofis programları)
- haberleşme cihazları (telefonlar, hatlar, kablolar, modemler, anahtarlama cihazları)
- dökümanlar(stratejik toplantıların tutanakları, sözleşmeler)
- üretilen mallar
- servisler
- mali değerler (çekler, para, fonlar)
- personel
- kurumun prestiji / imajı

Varlıkların belirlenmesinde kullanılabilecek bazı bilgi toplama teknikleri mevcuttur. Aşağıdaki tekniklerden biri veya birkaçı varlıkların belirlenmesinde kullanılabilir [88].

2.3.2.1 Anketler

Varlıkların belirlenmesinde ve risk analizi için gerekli bilgilerin toplanmasında anketler kullanılabilir. Anketler BT sistemini kullanan, tasarlayan ve destekleyen tüm personele uygulanabilir [88].

2.3.2.2 Birebir görüşmeler

BT sistemini yöneten ve bu sisteme destek sağlayan personel ile yapılacak görüşmeler sistemin nasıl işlediği ve nasıl yönetildiği konularında yararlı bilgiler edinilmesini sağlar. Bu görüşmeler sırasında operasyonun işleyişi ile ilgili edinilen bilgiler sayesinde gözden kaçabilecek bazı varlıklar daha rahat belirlenir [88].

2.3.2.3 Dökümantasyonun İncelenmesi

Politikaların, sistem dökümantasyonun (işletme talimatları ve ağ diyagramı gibi), önceki risk değerlendirme raporlarının incelenmesi varlıkların çoğunun hızlı ve doğru bir şekilde belirlenmesini sağlar [88].

2.3.2.4 Otomatik Tarama Araçları

Ağ tarama araçları gibi otomatik tarama araçları büyük bir sistemde bulunan varlıkların belirlenmesini kolaylaştırır ve bazı varlıkların gözden kaçırılmasını engeller [88].

2.3.3 Tehditlerin Belirlenmesi

Tehdit, herhangi bir tehdit kaynağının kasıtlı olarak veya kazayla bir açıklığı kullanarak varlıklara zarar verme potansiyelidir. Tehdit kaynağı ise varlıklara zarar verme olasılığı olan olaylar ve durumlar olarak tanımlanabilir. En bilinen tehdit kaynakları şunlardır:

- **Doğal tehditler:** Deprem, sel, toprak kayması, yıldırım düşmesi, fırtına gibi tehditler.
- **Çevresel tehditler:** Uzun süreli elektrik kesintileri, hava kirliliği, sızıntılar vs.

- **İnsan kaynaklı tehditler:** İnsanlar tarafından yapılan veya yol açılan bilinçli veya bilinçsiz olaylar. Örneğin yanlış veri girişi, ağ saldırıları, zararlı yazılımların yüklenmesi, yetkisiz erişimler vs.

Tehdit değerlendirmesi sırasında hiçbir tehdidin küçümsenerek göz ardı edilmesi doğru değildir. Göz ardı edilen tehdit kurum güvenliğinde zayıflık yaratabilir.

Tehdit değerlendirmesi için gerekli girdi varlık sahiplerinden, kullanıcılardan, BT uzmanlarından, kurumun korunmasından sorumlu kişilerden elde edilebilir. Ayrıca tehditlerin belirlenmesinde tehdit katalogları da kullanılabilir. Aşağıdaki Çizelge 2.1' de BT sistemlerinde sıklıkla karşılaşılan tehditleri ve bunların kaynaklarını içermektedir (tehdidin kaynağı bölümünde kullanılan kısaltmalar B: İnsan kaynaklı ve bilerek, K: İnsan kaynaklı ve kazayla, D: Doğal, Ç: Çevresel) [88].

Çizelge 2.1 BT sistemlerinde karşılaşılan tehditler ve kaynakları.

Tehdit	**Tehdidin kaynağı**
Deprem	D
Sel	D
Fırtına	D
Yıldırım	D
Endüstriyel bilgi sızması	B, K
Bombalama veya silahlı saldırı	B
Yangın	B, K
Güç kesintisi	B, K, Ç
Su kesintisi	B, K, Ç
Havalandırma sisteminin arızalanması	B, K, Ç
Donanım arızaları	K
Güç dalgalanmaları	K, Ç
Tozlanma	Ç
Elektrostatik boşalma	Ç
Hırsızlık	B
Saklama ortamlarının izinsiz kullanılması	B, K
Saklama ortamlarının eskiyip kullanılmaz duruma gelmesi	K
Personel hataları	K
Bakım hataları/eksiklikleri	K
Yazılım hataları	B, K
Lisansız yazılım kullanımı	B, K
Yazılımların yetkisiz kullanılması	B, K

Kullanıcı kimlik bilgilerinin çalınması	B, K
Zararlı yazılımlar	B, K
Yetkisiz kişilerin ağa erişimi	B
Ağ cihazlarının arızalanması	K
Hat kapasitelerinin yetersiz kalması	B, K
Ağ trafiğinin dinlenmesi	B
İletim hatlarının hasar görmesi	B, K
İletişimin dinlenmesi	B
Mesajların yanlış yönlendirilmesi	K
Mesajların yetkisiz kişilere yönlendirilmesi	B
İnkar etme(repudiation)	B
Kaynakların yanlış kullanımı	K
Kullanıcı hataları	K
Personel yetersizliği	K

2.3.4 Açıklıkların Belirlenmesi

Açıklık, sistem güvenlik prosedürlerinde, tasarımda, uygulamada veya iç kontrollerde bulunan ve bilgi güvenliği ihlal olayına sebep olabilecek zayıflık, hata veya kusurlardır. Açıklıklar tek başlarına tehlike oluşturmazlar ve gerçekleşmeleri için bir tehdidin mevcut olması gerekir.

Açıklık değerlendirmesi, tehditler tarafından gerçekleştirilebilecek açıklıkları ve bu açıklıkların ne kadar kolay gerçekleştirilebileceğini ele alır. Açıklıkların belirlenmesinde de varlık belirlemesinde anlatılan anket, birebir görüşme, dökümantasyon ve otomatik tarama araçları gibi yöntemler kullanılabilir. Ayrıca aşağıdaki kaynakların kullanımı da önerilmektedir.

- Açıklık listeleri ve açıklık veritabanları (Örneğin http://nvd.nist.gov/ , http://www.us-cert.gov/cas/techalerts/, http://www.securityfocus.com/vulnerabilities)
- Önceki BT sistemi denetim raporları, test raporları, hata raporları
- Önceki risk değerlendirme dökümanları
- Üreticiler tarafından yayınlanan uyarılar
- Güvenlikle ilgili web sayfaları ve e-posta listeleri
- Yazılım güvenlik analizleri

- Sistem güvenlik taramalarının ve sızma testlerinin sonuçları

Aşağıdaki listede bazı örnek açıklıklar ve bu açıklıkları gerçekleyebilecek tehditler verilmiştir.

- Altyapı ve çevreyle ilgili açıklıklar
    - Binada yeterli fiziksel güvenliğin bulunmaması (hırsızlık)
    - Binalara ve odalara girişlerde yetersiz fiziksel kontrol (kasten zarar verme)
    - Eski güç kaynakları (güç dalgalanmaları)
    - Deprem bölgesinde bulunan yapılar (deprem)
    - Herkesin erişebildiği kablosuz ağlar (hassas bilginin açığa çıkması, yetkisiz erişim)
    - Dış kaynak kullanımında işletilen prosedür ve yönetmeliklerin veya şartnamelerin eksikliği/yetersizliği (yetkisiz erişim)
- Donanımlarla ilgili açıklıklar
    - Periyodik yenilemenin yapılmaması (saklama ortamlarının eskimesi, donanımların bozulması nedeniyle erişimin durması)
    - Voltaj değişikliklerine, ısıya, neme, toza duyarlılık (güç dalgalanmaları, erişim güçlükleri vs.)
    - Periyodik bakım eksikliği (bakım hataları)
    - Değişim yönetimi eksikliği (kullanıcı hataları)
- Yazılımlarla ilgili açılıklar
    - Yama yönetimi eksikliği/yetersizliği (yetkisiz erişim, hassas bilginin açığa çıkması)
    - Kayıt yönetimi eksikliği/ yetersizliği (yetkisiz erişim)
    - Kimlik tanımlama ve doğrulama eksiklikleri (yetkisiz erişim, başkalarının kimliğine bürünme)

- Şifre yönetimi yetersizliği (yetkisiz erişim, başkalarının kimliğine bürünme)
- Şifre veritabanlarının korunmaması (yetkisiz erişim, başkalarının kimliğine bürünme)
- Erişim izinlerinin yanlış verilmesi (yetkisiz erişim)
- İzinsiz yazılım yüklenmesi ve kullanılması (zararlı yazılımlar, yasal gerekliliklere uyum)
- Saklama ortamlarının doğru silinmemesi ve imha edilmemesi (hassas verinin ortaya çıkması, yetkisiz erişim)
- Dökümantasyon eksikliği/yetersizliği (kullanıcı hataları)
- Yazılım gereksinimlerinin yanlış veya eksik belirlenmesi (yazılım hataları)
- Yazılımların yeterli test edilmemesi (yetkisiz erişim, yazılımların yetkisiz kullanımı)

- Haberleşmeyle ilgili açıklıklar
  - Korunmayan haberleşme hatları (haberleşmenin dinlenmesi)
  - Hat üzerinden şifrelerin açık olarak iletilmesi (yetkisiz erişim)
  - Telefon hatlarıyla kurum ağına erişim (yetkisiz erişim)
  - Ağ yönetimi yetersizliği/eksikliği (trafiğin aşırı yüklenmesi)
- Dökümanlarla ilgili açıklıklar
  - Dökümanların güvensiz saklanması (hırsızlık)
  - Dökümanların kontrolsüz çoğaltılması (hırsızlık)
  - Dökümanların imha edilmemesi (hırsızlık, hassas bilginin açığa çıkması)
- Personel ile ilgili açıklıklar
  - Eğitimi eksikliği (personel hataları)
  - Güvenlik farkındalığı eksikliği (kullanıcı hataları)

- Donanımların veya yazılımların yanlış kullanılması (personel hataları)
- İletişim ve mesajlaşma ortamların kullanımını düzenleyen politikanın eksikliği/yetersizliği (yetkisiz erişim)
- İşe alımda yetersiz özgeçmiş incelemesi ve doğrulaması (kasten zarar verme)

2.3.5 Mevcut ve Planlanan Kontrollerin Belirlenmesi

Yukarıda belirlenen tehditlerin, açıklıkları gerçekleme olasılıklarını azaltacak veya ortadan kaldıracak kontrollerin halihazırda uygulanıp uygulanmadığı veya bu kontrollerin uygulanmalarının planlanıp planlanmadığı incelenmelidir. Uygulanan veya uygulaması planlanan kontroller açıklıkların gerçekleşme olasılıklarını düşüreceği için olasılık değerlendirmesinde ve dolayısıyla risk derecelendirmesinde önem kazanacaktır.

Kontrollerle ilgili detaylı bilgi Uygun Kontrollerin Belirlenmesi başlıklı bölümde yer almaktadır.

2.3.6 Olasılık Değerlendirmesi

Risk analizinde bir açıklığın gerçekleşme olasılığının belirlenmesi büyük önem taşır ve tespit edilen tüm açıklıklar için olasılık değerlendirmesi yapılmalıdır. Olasılığın belirlenmesi için tehdit kaynağının motivasyonu ve becerisi, açıklığın cinsi, mevcut kontrollerin varlığı ve etkinliği göz önünde bulundurulmalıdır.

Olasılık değerlendirmesi için kurum kaç kademeli bir değerlendirme yapacağını ve kademelerin nasıl belirleneceğini tanımlamalıdır. Üç seviyeli bir olasılık değerlendirmesi için aşağıdaki örnek tablo kullanılabilir.

Çizelge 2.2 Üç seviyeli bir olasılık değerlendirmesi için olasılık tanımları

Olasılık seviyesi	Olasılık tanımı
Yüksek	Tehdit kaynağı çok kabiliyetli ve motivasyonu yüksektir, açıklığın gerçeklenmesini engelleyecek kontroller bulunmamaktadır veya etkisizdir.
Orta	Tehdit kaynağı kabiliyetli ve motivasyonu yüksektir, açıklığın gerçeklenmesine engel olacak kontroller mevcuttur.
Düşük	Tehdit kaynağı daha az kabiliyetli ve motivasyonu daha düşüktür, açıklığın gerçeklenmesini engelleyecek veya çok zorlaştıracak kontroller mevcuttur.

2.3.7 Etki Analizi

Risk derecelendirmesi yapabilmek için olasılık değerlendirmesinden sonra gelen adım etki analizidir. Etki analizinde herhangi bir açıklığın gerçeklenmesi halinde yaşanacak olası olumsuz etki seviyesi belirlenir. Bunun için varlığın görevi, kritikliği, varlığın etkilediği verinin hassasiyeti ve varlığın mali değeri göz önüne alınmalıdır. Bu bilgiler daha önceden yapılmış iş etki analizi raporlarından alınabilir. Eğer daha önce yapılmış böyle bir çalışma yoksa sistemin kritiklik seviyesi sistemin (ve sakladığı veya işlediği verinin) bütünlüğünü, gizliliğini ve erişilebilirliğini korumak için gerekli koruma göz önüne alınarak niceliksel olarak çıkarılabilir. Ayrıca sistemin yenilenme maliyeti, çalışmaması durumunda oluşabilecek gelir kaybı gibi bazı niteliksel etkiler de etki analizinde göz önüne alınabilir.

Niceliksel bir etki analizinde olasılık değerlendirmesinde olduğu gibi kurum kaç kademeli bir değerlendirme yapacağını ve kademelerin nasıl belirleneceğini tanımlamalıdır. Üç seviyeli bir etki değerlendirmesi için aşağıdaki örnek tablo kullanılabilir.

Çizelge 2.3 Üç seviyeli bir etki değerlendirmesi için etki tanımları.

Etki derecesi	Etki tanımı
Yüksek	Açıklığın gerçeklenmesi durumunda: Kurumun en önemli varlıkları çok fazla etkilenir veya kaybedilir ve mali zarar çok büyük olur. Kurumun çıkarları, misyonu ve prestiji büyük zarar görebilir veya etkilenebilir. İnsan hayatı kaybı veya ciddi yaralanmalar gerçekleşebilir.
Orta	Açıklığın gerçeklenmesi durumunda: Kurumun önemli varlıkları etkilenir ve kurum mali zarara uğrar. Kurumun çıkarları, misyonu ve prestiji zarar görebilir veya etkilenebilir. Yaralanmalar gerçekleşebilir.
Düşük	Açıklığın gerçeklenmesi durumunda: Kurumun bazı varlıkları etkilenir Kurumun çıkarları, misyonu ve prestiji etkilenebilir.

2.3.8 Risk Derecelendirmesi

Bu adımın amacı, varlıkları tehdit eden risklere değerler atayıp onları derecelendirmektir. Uygun kontrollerin seçilmesi burada belirlenen risklere ve seviyelere göre yapılır. Risk bir tehdidin bir açıklığı gerçekleme olasılığının, açıklığın ne kadar kolay gerçekleştirilebildiğinin ve mevcut veya planlanan kontrollerin yeterliliğinin bir fonksiyonudur. Yani kısaca olasılık değerlendirmesinde ve etki analizinde belirlenen değerlere bağlıdır.

Risklerin ölçülebilmesi için risk sınıflandırma matrisi oluşturulmalıdır ve bu sınıflandırma için tanımlamalar yapılmalıdır.

2.3.8.1 Risk Derecelendirme Matrisi

Yukarıda örnek olarak verilen üç seviyeli olasılık değerlendirmesi ve etki analizi için şu şeklide bir risk derecelendirme matrisi oluşturulabilir.

Çizelge 2.4 Örnek risk derecelendirme matrisi

		Etki seviyesi		
		Düşük	Orta	Yüksek
Olma olasılığı	Düşük	Düşük	Düşük	Düşük
	Orta	Düşük	Orta	Orta
	Yüksek	Düşük	Orta	Yüksek

Bu matristeki değerleri kurum kendisi belirlemelidir. Bunun için istenirse sayısal değerler kullanılabilir. Örneğin olma olasılıklarına 0 ile 1 arasında, etki seviyesine ise 0 ile 100 arasında değerler atanır. Risk dereceleri için aralıklar belirlenir. Olma olasılığı ve etki seviyesi çarpımının düştüğü aralık risk derecesini belirler. Örneğin bu matrise göre olma olasılığı "Orta" ve etki seviyesi "Yüksek" olan bir açıklığın risk derecesi "Orta" olarak sınıflandırılmıştır.

2.3.8.2 Risk Derecelerinin Tanımı

Risk derecelendirme matrisinde belirlenen risk dereceleri bir açıklığın gerçeklenmesi halinde karşı karşıya olunan riski belirlemektedir. Bu risk derecelerinin tanımlanması yönetimin risklerle ilgili alacağı kararlar açısından önemlidir. Ayrıca bu aşamada kurumun kabul edebileceği risk seviyesi de belirlenmelidir. Belirlenen bu seviyeye göre kurum bazı riskleri kabul ederek karşı önlem almamayı tercih edebilir.

Yukarıdaki risk seviye matrisine uygun olarak aşağıdaki tanımlamalar örnek olarak gösterilebilir.

Çizelge 2.5 Risk dereceleri ve tanımları

Risk derecesi	Risk açıklaması ve yapılması gerekenler
Yüksek	Düzeltici önlemlerin alınması şarttır. Mevcut sistem çalışmaya devam edebilir ama hangi önlemlerin alınacağı ve nasıl uygulanacağı olabildiğince çabuk belirlenmelidir ve önlemler uygulanmalıdır.
Orta	Düzeltici önlemlerin alınması gerekmektedir. Hangi önlemlerin alınacağı ve nasıl uygulanacağına dair plan makul bir süre içersinde hazırlanmalı ve uygulanmaya başlanmalıdır.
Düşük	Önlem alınıp alınmayacağı sistem sahibi/sorumlusu tarafından belirlenmelidir. Eğer yeni önlemler alınmayacaksa risk kabul edilmelidir.

2.3.9 Uygun Kontrollerin Belirlenmesi

Yapılan risk derecelendirme çalışmalarının sonucunda risklerin azaltılmasını veya ortadan kaldırılmasını sağlayacak kontrol önerileri belirlenmelidir. Önerilecek kontrollerin amacı riski kurumun kabul edebileceği bir değere düşürmek olmalıdır. Önerilecek kontrollerde kontrollerin etkinliği, yasalar ve düzenlemeler, iş yapma biçimine getireceği değişiklikler, kurum politikaları ve güvenlik konuları dikkate alınması gereken başlıca konulardır.

Uygulanabilecek olası kontroller belirlenirken başvurabilecek kaynaklardan biri "TS ISO/IEC 27001:2005 Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardıdır. Bu standart, güvenlik politikası, bilgi güvenliği organizasyonu, varlık yönetimi, insan kaynakları güvenliği, fiziksel ve çevresel güvenlik, haberleşme ve işletim yönetimi, erişim kontrolü, bilgi sistemleri edinim, geliştirme ve bakımı, bilgi güvenliği ihlal olayı yönetimi, iş sürekliliği yönetimi ve uyum ana başlıkları altında pek çok kontrol önerisi içermektedir. Ayrıca bu kontrollerin gerçekleştirilmesine ait öneriler ve en iyi uygulamalar için TS ISO/IEC 27002:2005 standardına başvurulmalıdır.

2.3.9.1 Kontrol Kategorileri

Açıklıkların gerçeklenmesini önlemek veya gerçekleşen ihlallerin takibini yapabilmek için uygulanabilecek kontroller teknik, yönetimsel ve operasyonel kontroller olarak üçe ayrılabilir. Uygun kontroller belirlenirken bu kontrol kategorilerden birkaçı veya hepsi kullanılabilir. Uygun kontrole yine kurumun kendisi karar vermelidir. Örneğin teknik bir kontrolün uygulanması daha pahalı ve daha bir zahmetli iş olabilir fakat yönetimsel kontrollere göre daha etkin olacaktır.

2.3.9.2 Teknik Güvenlik Kontrolleri

Teknik güvenlik kontrolleri risk önlemede oldukça etkin kontrollerdir. Bu kontroller yazılım, donanım, sistem mimarisi vb. gibi çözümleri içerir. Teknik güvenlik kontrolleri destekleyici, önleyici, tespit edici ve düzeltici olmak üzere dört çeşittir.

2.3.9.3 Destekleyici Teknik Kontroller

Destekleyici kontroller diğer kontrollerin uygulanmasını sağlayan temel kontrollerdir. Bu kontroller şu şekilde tanımlanabilir.

Kimlik tanımlama: Bu kontrol bir kullanıcının, sürecin veya sistemin eşsiz/benzersiz olarak tanımlanmasında kullanılır. Diğer kontrollerin uygulanabilmesi için (örneğin erişim kontrol listeleri) kimlik tanımlaması şarttır.

Kriptografik anahtar yönetimi: Diğer kontrollerde kriptografik işlemlerin güvenli bir şekilde gerçekleştirilebilmesi için kriptografik anahtar yönetiminin güvenli bir şekilde gerçekleştirilmesi gerekir. Anahtar üretimi, saklanması, dağıtımı ve bakımı kriptografik anahtar yönetiminin içerisindedir.

Güvenlik yönetimi: Bir BT sisteminin güvenlik özellikleri kurumun ihtiyaçlarını karşılayacak şekilde ayarlanabilmelidir. Örneğin bir veritabanındaki bilgileri kimin okuyacağı, kimin oluşturucağı ve kimin güncelleyebileceği ayarlanabilmelidir. Böylece gereğinden fazla yetki verilmemiş olur.

Sistem koruma kontrolleri: Bu kontroller bir sistemin güvenliğinin sağlanabilmesi için gerekli temel konuları içerir. Örneğin bilmesi gereken prensibi, süreçlerin ayrımı,

objelerin tekrar kullanılması, katmanlı yapılarda çalışma, güvenilecek nesne sayısının en aza indirgenmesi gibi prensipler bu tip kontrollerdir.

2.3.9.4 Önleyici Teknik Kontroller

Bu kontroller güvenlik ihlallerinin gerçekleşmesini önleyici kontrollerdir

Kimlik doğrulama: Bu kontrol kullanıcının belirttiği kimlik tanımlamasını doğrulamaya yarar. Bunun için şifre, PIN numarası, akıllı kart gibi mekanizmalar kullanılmaktadır.

Yetkilendirme: Yetkilendirme bir sistemde izin verilen işlemlerin belirlenmesini ve yönetimin alt birimlere dağıtılabilmesini sağlayan kontroldür.

Erişim kontrolü: Verinin gizliliği ve bütünlüğü erişim kontrolleri ile sağlanır. Bir kaynağa erişim için yetkilendirme yapıldıktan sonra uygun politikalara göre erişim kontrolü sağlanmalıdır. Gizlilik derecesi etiketleri, dosya izinleri, kullanıcı profilleri erişim kontrolünde kullanılan mekanizmalardan bazılarıdır.

İnkar edememe: Bilgiyi gönderenin gönderdiğini, alanın da aldığını inkar edememesi sistemin izlenebilirliği açısından önemlidir.

Güvenli iletişim: Günümüzde sık kullanılan dağıtık yapılarda güvenliğin korunmasındaki en önemli faktörlerden biri iletişim sırasında verinin gizliliğinin ve bütünlüğünün korunabilmesidir. Bunun için iletişim sırasında çeşitli şifreleme metotları ve kriptografik önlemler kullanılarak hat dinlemesi, paket dinleme, tekrar gönderme gibi saldırılara karşı önlem alınabilir.

İşlem gizliliği (Transaction privacy): Kişisel işlemlerin gizliliği gittikçe önem kazanmaktadır. Secure Socket Layer(SSL) ve Secure Shell(SSH) gibi teknolojiler kişilerin yaptığı işlemlerin gizliliğinin kaybolmasını engellemek aracıyla kullanılır.

2.3.9.5 Tespit Edici Teknik Kontroller

Tespit edici kontroller güvenlik ihlalleri gerçekleştikten sonra nelerin, kimin tarafından, ne zaman

ve nasıl yapıldığını bulmak için kullanılır.

Denetleme: Güvenlikle ilgili olayların ve sistemdeki anormalliklerin izlenmesi, güvenlik ihlallerinin tespitinde ve olası bir ihlalden geri dönmede en önemli kontroldür

Saldırı tespiti: Ağ sızmaları ve şüpheli olaylar gibi güvenlik ihlali olabilecek durumların tespiti, uygun kontrolün alınması ve gerekli düzeltmelerin yapılabilmesi için çok önemlidir.

Bütünlük: Sistemin veya verinin bütünlüğünün takip edilmesi, ihlallerin tespit edilmesi açısından önemlidir. Örneğin işletim sisteminin kullandığı dosyalar sadece gerekli işlemler için okunurlar ve bu dosyaların üzerinde değişiklik yapılmaz. Bu dosyaların bütünlüğü virüs veya zararlı bir yazılım tarafından değiştirilirse anti virüs programları bunu tespit edebilir.

2.3.9.6 Düzeltici Teknik Kontroller

Güvenlik ihlalleri tespit edildikten sonra sistemi eski haline getirmek için kullanılan kontroller bu kategoride incelenebilir.

Yedekleme: Kaybedilen veya bütünlüğü bozulan veri yedeklerden geri dönülerek eski haline getirilebilir.

2.3.9.7 Yönetimsel Kontroller

Yönetimsel kontroller kurumda uygulanan politika, prosedür, standart gibi kuralların uygulanmasını sağlayacak kontrollerden oluşur ve önleyici, tespit edici ve düzeltici olmak üzere üç kategoriye ayrılır.

2.3.9.8 Önleyici Yönetimsel Kontroller

Önleyici yönetimsel kontroller için bazı örnekler aşağıda verilmiştir.

- BT sistemlerinde güvenliği sağlamak üzere kişilere sorumluluklarının atanması.
- Mevcut ve planlanan kontrollerin dökümante edilmesini sağlayacak sistem güvenlik planlarının geliştirilmesi ve uygulanması.
- Görevlerin ayrılığı, gerekli en düşük yetkilerin verilmesi, hakların tahsis edilmesi ve sonlandırılması gibi personelle ilgili güvenlik kontrollerinin uygulanması

- Güvenlik farkındalığı ve teknik eğitimlerinin verilerek sistem kullanıcı ve yöneticilerinin bilgi seviyelerinin artırılması.
- Güvenlik politikalarında belirtilen kuralların çalışanlar tarafından bilinmesinin sağlanması.
- Çalışanların özgeçmişlerinin doğrulanması, geçmişlerinin incelenmesi.

2.3.9.9 Tespit Edici Yönetimsel Kontroller

Tespit edici yönetimsel kontroller için bazı örnekler aşağıda verilmiştir.

- Güvenlik önlemlerinin periyodik olarak test edilmesi.
- Risk yönetiminin uygulanması ve risk işleme için gerekenlerin yapılması.
- Periyodik olarak sistemlerin denetlenmesi.

2.3.9.10 Düzeltici Yönetimsel Kontroller

Düzeltici yönetimsel kontroller için bazı örnekler aşağıda verilmiştir

- Sistemlerinin devamlılığının sağlanması ve acil durumlarda veya felaket anlarında BT sisteminin tekrar kullanılabilir hale getirilmesini sağlayacak planların, prosedürlerin ve testlerin yapılmasının sağlanması.
- Acil durum müdahale ekiplerinin kurulması ve yetkin hale getirilmesinin sağlanması.

2.3.9.11 Operasyonel Kontroller

Kurumun güvenlik politikalarının BT varlıklarının kullanılması sırasında doğru şekilde uygulanmasını sağlamak için operasyonel kontrollerin geliştirilmesi ve yönetim tarafından takip edilmesi gerekir. Operasyonel kontroller kurumdaki işlerin yapılması sırasında kasten veya bilmeden yapılabilecek hataları engeller. Bunun için operasyonel kontrollerin nasıl uygulanacağının adım adım açıklandığı dökümanların bulunması ve bu dökümanların kontrolleri uygulayanlar tarafından biliniyor olması gerekmektedir. Önleyici ve tespit edici operasyonel kontroller için bazı örnekler aşağıda verilmiştir.

2.3.9.12 Önleyici Operasyonel Kontroller

- Veri ortamlarına erişimin ve veri ortamlarının yok edilmesinin kontrol edilmesi (fiziksel erişim kontrolü uygulanması, veri saklama cihazlarının uygun şekilde imha edilmesi)
- Verinin yetkisiz kişilerin eline geçmesinin engellenmesi (veri sınıflandırma etiketlerinin kullanılması)
- Zararlı yazılım içerebilecek veri kaynaklarının kontrol edilmeden kullanılmasının engellenmesi
- Ziyaretçilere refakat edilmesi, kimlik kartı taşınması, anahtarların dağıtımının kontrolü gibi fiziksel güvenliği sağlayıcı operasyonel kontroller
- Yedeklerin alınmasını ve güvenli bir yerde saklanmasını sağlayacak operasyonel adımları içeren kontroller
- Mobil bilgi işleme cihazlarının kullanım şartlarının belirlenmesi ve güvenliğinin sağlanması
- Varlıkların yangın, yanlış kullanım vb. sebeplerden etkilenmemesi için uygulanan kontroller (sistem odasında yiyecek ve içecek bulundurulmaması, yangın tespit ve söndürme sistemlerinin kullanılması, kesintisiz güç kaynakları gibi)

2.3.9.13 Tespit Edici Operasyonel Kontroller

- Güvenlik kameraları, hareket algılayıcıları ve alarm sistemleri gibi tespit edici fiziksel kontrollerin uygulanması
- Çevresel etkilerin takip edilmesi (duman ve yangın detektörlerinin kullanılması)
- Düzeltici Edici Operasyonel Kontroller
- Yapılan işlerin dökümante edilmesi olası değişikliklerde doğru ayarlamaların tekrar yapılabilmesini sağlar.

- Yapılan değişikliklerin dökümante edilmesi ve bir sorun halinde değişiklik yapılmadan önceki duruma geri dönülebilmesi, yapılan değişikliklerden dolayı oluşabilecek sorunların düzeltilmesini sağlar.

2.3.10 Sonuçların Dökümantasyonu

Sonuçların dökümantasyonu risk analizi sürecinde en önemli adımlardan biridir. Bu dökümanlar mevcut risk ve kontrollerin herkes tarafından bilinmesini sağlarlar. Ayrıca bu dökümanlar daha sonraki risk analizlerine girdi teşkil ederler.

Risk analizi süreci tamamlandığında sonuçlar bir rapor olarak dökümante edilmelidir. Bu rapor yönetimin ve süreç sahiplerinin politikalarda, prosedürlerde, bütçede ve sistemin kullanımında veya yönetiminde yapılacak değişikliklerde karar verirken kullanacağı yönetimsel bir rapordur. Yönetimin riskleri rahat bir şekilde anlayabilmesi için açık ve sistematik olmalıdır. Belirlenen riskler için uygulanacak kontrollere bu rapor göz önünde bulundurularak karar verilecektir [88].

2.4 Risk İşleme

Risk yönetiminde ikinci aşama risk işleme aşamasıdır. Bu aşama risk analizinde belirlenen risklerin nasıl işleneceğine karar verilmesi, önceliklendirilmesi ve riski azaltacak kontrollerin seçilerek uygulanmasından oluşur.

Risklerin tamamen ortadan kaldırılması için bütün kontrollerin uygulanması çoğu zaman mali açıdan imkansızdır. Risk işleme için burada belirtilen risk işleme yöntemlerini kullanılır. Yönetim, riski azaltmak istediğinde sisteme gelebilecek zararı en aza indirmek için “en düşük maliyetli” ve “en uygun” kontrolü seçmekle sorumludur. Bu bölüm “en düşük maliyetli” ve “en uygun” kontrolün nasıl seçilmesi gerektiğini anlatmaktadır [88].

2.4.1 Risk İşleme Yöntemleri

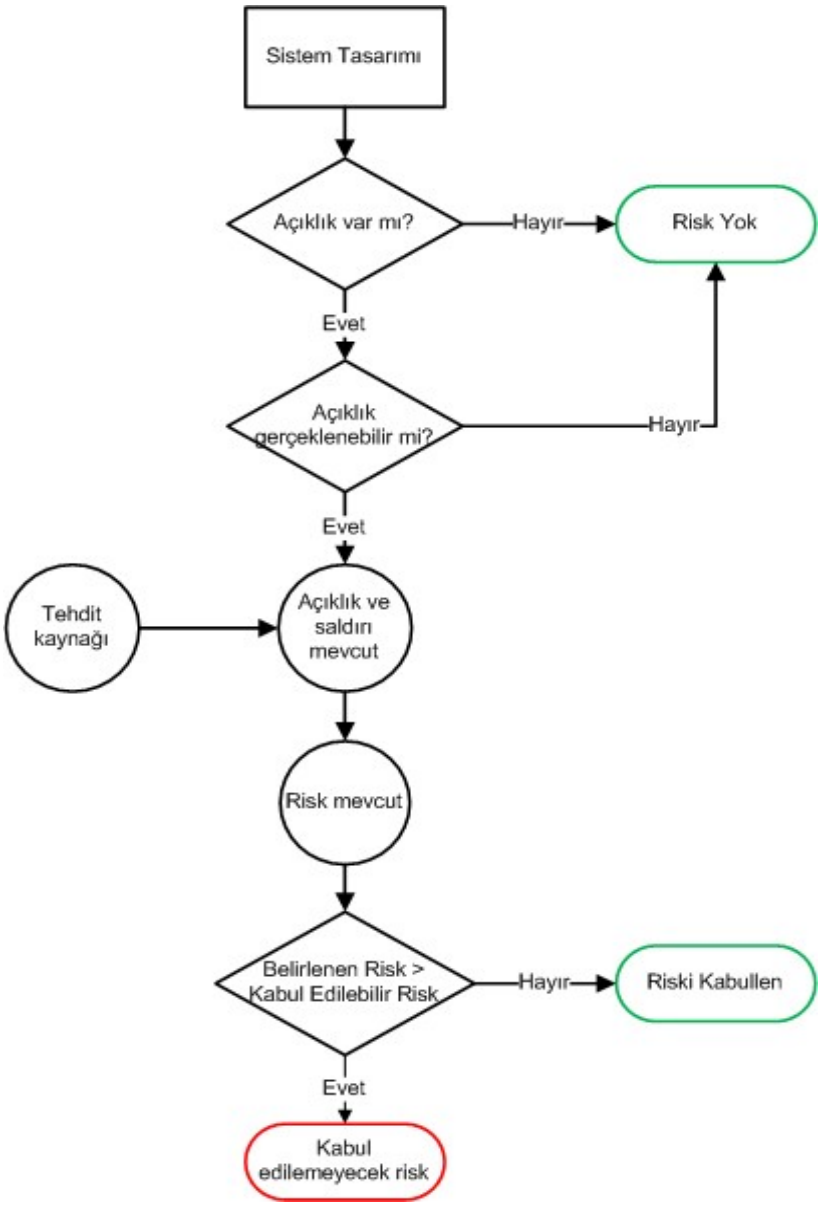
Risk işleme yöntemleri kurumun iş hedeflerine ve misyonuna uygun olarak seçilmelidir. Riski azaltmak için kullanılabilecek yöntemler şu şekilde sıralanabilir.

- **Riskin Kabulü:** Riskin var olduğunu kabul ederek BT sistemlerini kullanmaya devam etmektir.

- **Riskten Kaçınma:** Riski yaratan sebebi ortadan kaldırmaktır (örneğin bir yazılımın risk yaratan kısmının yüklenmemesi ve kullanılmaması gibi)
- **Riskin Azaltılması:** Açıklığın gerçeklenmesi halinde oluşacak etkinin uygulanan kontroller ile azaltılması.
- **Riskin Transferi:** Riskin gerçekleşmesi durumunda oluşabilecek zararı karşılayacak çözümler bularak (örneğin sigorta yaptırmak) riskin başkalarına aktarılmasıdır.

2.4.2 Kontrollerin Uygulanması

Risk analizi sonrasında sistemdeki mevcut riskler ve bu risklere karşı kullanılabilecek olası kontroller belirlenmektedir. Fakat her risk önlem almaya değecek bir risk olmayabilir. Bu durumda hangi riskler için önlem alınacağı ve olası kontroller içerisinden hangisinin kullanılacağını belirlemek kurumun maliyetleri açısından çok önemlidir. Bunu belirlemek için iki önemli nokta vardır. Saldırganın kazancının saldırı maliyetinden düşük olduğu veya tahmini kaybın belirlenen eşik değerinden küçük olduğu durumlarda risk için önlem almak yerine risk kabul edilebilir. Yani kısacası mevcut risk daha önce belirlenen kabul edilebilir riskten küçükse risk kabul edilebilir, aksi takdirde riski azaltacak uygun kontroller uygulanmalıdır. Bu süreç aşağıdaki akış diyagramında daha detaylı olarak açıklanmıştır [88].



Şekil 2.7 Önlem alınacak risklerin belirlenmesinde kullanılacak süreç

Ayrıca yukarıdaki akış diyagramında bulunan riskle ilgili karar adımları ile ilgili uygulanabilecek bazı yaklaşımlar şunlardır [88].

- Eğer açıklık mevcutsa açıklığın uygulanma olasılığını azaltacak kontroller uygulanabilir.
- Eğer açıklık gerçeklenebiliyorsa kademeli güvenlik anlayışı, güvenli mimariler ve yönetimsel kontroller kullanılarak risk azaltılabilir

- Saldırının maliyeti saldırı sonucu elde edilecek kazançtan fazlaysa saldırganın maliyetlerini arttıracak ve motivasyonunu düşürecek önlemler alınabilir.
- Tahmini kayıp çok büyük olduğunda doğru tasarım prensipleri, güvenli mimariler, teknik ve teknik olmayan kontroller kullanarak saldırının yaratacağı kayıp azaltılabilir .

2.4.3 Kontrollerin Uygulanmasında İzlenecek Yaklaşım

Kontroller, en büyük risklerden başlayarak, kurumun süreçlerine en az zarar verecek, riski en aza indirecek ve en düşük maliyetli olacak şekilde seçilmelidir. Bu süreçte aşağıdaki adımlar izlenebilir [88].

2.4.3.1 Risklerin Önceliklendirilmesi

Risk analizinde belirlenen risk seviyelerine göre riskler önceliklendirilmelidir. Risk işleme için kaynak aktarımı yapılırken öncelik yüksek risk dereceli risklere verilmeli, bu riski oluşturan açıklıklar ve tehditlere karşı önlemler daha önce alınmalıdır [88].

2.4.3.2 Uygun Kontrollerin Değerlendirilmesi

Riskler öncelendirildikten sonra bu riskler için daha önceden belirlenmiş kontroller değerlendirilmelidir. Belirlenen her kontrol en efektif veya en az maliyetli kontrol olmayabilir. Bir fizibilite çalışması yapılarak riski en aza indirecek en uygun kontrol belirlenmelidir. Bu aşamada kontroller için maliyet-fayda analizi yapmak uygun olacaktır [88].

2.4.3.3 Kontrollerin Seçilmesi

Fizibilite çalışmasının ve maliyet-fayda analizinin sonuçlarına göre riski en aza indirecek en uygun kontroller, risk analizinde belirlenen kontroller arasından yönetim tarafından seçilir. Seçilen kontroller teknik, yönetimsel ve operasyonel kontrollerin bir araya getirilmesinden oluşturulmalıdır [88].

2.4.3.4 Sorumluların Atanması

Seçilen kontroller uygulanması için bu kontrolleri uygulama yetkinliğine sahip kişiler belirlenmeli ve bu kişilere sorumluluk atanmalıdır [88].

2.4.3.5 Kontrol Uygulama Planın Hazırlanması

Seçilen kontrolün nasıl uygulanacağını, uygulamanın hangi adımları içereceğini ve ne kadar süreceğini belirleyen bir kontrol uygulama planı oluşturulmalıdır [88]. Bu plan en az:

• riskleri ve risk seviyelerini

• risk analizi sonucunda belirlenen kontrol önerilerini

• önceliklendirmeleri

• seçilen kontrolleri

• gerekli kaynakları

• kontrolü uygulamakla yetki ve sorumluluğu verilen kişileri

• kontrolün uygulanması için belirlenen başlama ve bitiş tarihlerini içermelidir.

2.4.3.6 Seçilen Kontrolün Uygulanması

Hazırlanan kontrol uygulama planına uygun olarak seçilen kontroller uygulanmalıdır. Uygulanması uzun zaman alabilecek kontroller için uygulamanın gidişini değerlendirmek üzere uygun aralıklara toplantılar yapılıp sonuçlar raporlanabilir [88].

2.4.4 Artık Risk

Uygulanan kontroller var olan riski tamamen ortadan kaldırmak zorunda değildir. Risk işleme sonrası kalan riske artık risk adı verilir. Uygulanan kontroller sonrası artık risk belirlenmelidir. Eğer bulunan risk seviyesi kabul edilebilir risk seviyesinin üzerinde ise risk analizi ve risk işleme tekrar yapılmalıdır, eğer bulunan artık risk seviyesi kabul edilebilir riskin altında ise artık risk dökümante edilmeli ve varlığı yönetim tarafından onaylanıp kabul edilmelidir [88].

2.5 Değerlendirme ve İzleme

Risk yönetimi bir döngüdür ve burada belirtilen risk analizi ve risk işleme süreçleri periyodik olarak uygulanmalıdır. Bu sayede uygulanan kontrollerin amacına ne kadar ulaştığı belirlenmiş olur. Ayrıca bilişim teknolojileri çok hızlı değişmektedir. Kurum sistemine yeni dahil olan varlıkların risk yönetimine dahil edilmesi önem arz etmektedir. Bunlara ek olarak zaman içerisinde kurumun iş hedefleri, iş yapma şekli ve önem verdiği konular değişebilir. Bütün bu değişiklikler varlıklarda, varlıkların değerlerinde, açıklıklarda ve tehditlerde değişiklik olmasına neden olur. Risk yönetim döngüsünün sürekli olarak işletilmesi tüm bu değişikliklerin getirdiği risklerin yönetim tarafından farkına varılmasını ve ele alınmasını sağlayacaktır [88].

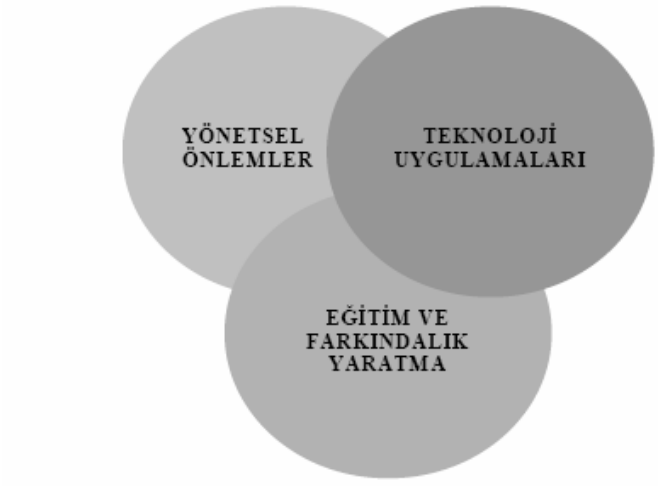
BÖLÜM 3

BİLGİ GÜVENLİK YÖNETİM SİSTEMİ KURULUMU

3.1 TS ISO 27002/17799 Bilgi Güvenlik Yönetim Sistemi Gereksinimleri

Bilgi sistemlerinin güvenli hale getirilmesi konusu, kapsamlı ve bütünleşik bir yaklaşımla ele alınmadığı takdirde, başarı kazanmak büyük olasılıkla mümkün olmayacaktır. Bilgi güvenliğinin sağlanması üç temel açıdan ele alınabilir. Bu üç süreç alanı Şekil 3.1'de gösterildiği gibi:

- Yönetsel önlemleri,
- Teknoloji uygulamalarını,
- Eğitim ve farkındalık yaratmayı, kapsamaktadır.



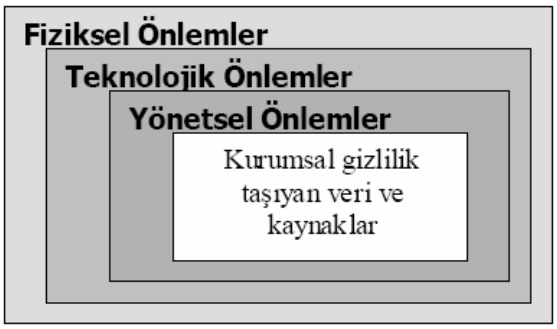
Şekil 3.1 Bilgi Güvenliğinin Sağlanmasında Bütünleşik Yaklaşım Bilişim Güvenliği

Güçlü bir güvenlik altyapısı kurabilmek için bu üç parçayı birbiri ile bütünleştirmek ve hepsini birlikte bütünsel bir yaklaşımla ele almak gerekir. Bu bahsedilen süreç alanlarının içinde, bilgisayar ve bilişim güvenliği teknolojilerinin dışında kalan farklı alanlar da bulunmaktadır. Diğer bir deyişle, bir kurumun, kurumsal bilgi güvenliği sağlamak amacıyla, sadece bilişim teknolojilerini devreye sokarak başarıya ulaşma şansı oldukça azdır. Bütün bunlara ek olarak, bu üç süreç alanından her biri, başarıya ulaşmak için diğer iki süreç alanının tam ve eksiksiz çalışıyor olmasına ihtiyaç duyar. Bu üç alan birbirileri ile ayrılmaz ve sıkı bağlara sahiptir. Birlikte çalışmalarından oluşacak sinerji, kuruma bilişim güvenliği yönünden tehdit oluşturacak tüm etkenlere karşı güçlü bir kalkan görevini üstlenecektir.

Yönetsel Önlemler, güvenlik yönetimi ile ilgili bir dizi kuralın ortaya koyulması ve uygulanması şeklinde özetlenebilir. Hemen her konuda olduğu gibi, bilişim güvenliğinin yönetiminde de başarı; iyi bir planlama ve üst düzey politikaların doğru ve tutarlı bir şekilde belirlenmesi ile elde edilebilir. Bunun ardından, belirlenenlerin yazıya dökülmesi, diğer bir deyişle prosedür, yönerge ve talimatlar gibi dökümanların oluşturulması gelmelidir [89].

Yönetsel önlemlerle ortaya konulan kurumun güvenlik ihtiyaçlarının karşılanmasında, teknolojik uygulamalardan da faydalanılır. Günümüzde bir bilgisayar ağına ya da tek başına bir bilgisayara yapılacak bir saldırının sonuçlanması saniyelerle ifade edilen çok kısa bir süre içinde oluşur. Bu tür saldırılara, ancak teknolojik bir takım önlemler ile karşı koyulabilir. Bunun yanında kullanılan teknolojiler, güvenlik yöneticilerinin hayatının kolaylaştırılması ve kurumun, bilişim güvenliği açısından bütün resminin görülmesi gibi yararlar da getirirler.

Şekil 23'te gösterildiği gibi, işletmenin sahip olduğu bilgi varlıklarının korunması için yönetsel önlemlerin uygulanması, teknoloji uygulamaları ve eğitim süreçlerinin yanında fiziksel güvenlik uygulamaları ile de desteklenmelidir [89].



Şekil 3.2 İşletmenin Sahip Olduğu Bilgi Varlıklarının Korunması

Bilgi güvenlik yönetiminde, uygulamaya gelindiğinde, bu alanda uluslar arası tanınan ve yaygın olarak, güvenlik politikaları taslağı hazırlanmasında kullanılan ISO/IEC-27001 ve ISO/IEC-27002 en iyi başvuru kaynağınızdır. ISO/IEC-27001 ve ISO/IEC-27002 standardı iki parça halinde yazılıp yayınlanmaktadır:

- ISO/IEC-27002(ISO/IEC-17799) Bolum 1: Bilgi güvenlik yönetimini uygulamakta kullanılacak kodu içermektedir. İçerdiği tavsiye ve önerilerle, şirketinizin bilgi güvenliğinden emin olmanız için on ayrı alanda uygulamalarıyla rehberlik etmektedir.
- ISO/IEC-27001(BS-7799): Bilgi güvenlik yönetimi etkili bir Bilgi Güvenlik Yönetim Sistemi (BGYS) oluşturulmasında kullanılmak üzere vereceği tavsiyelerle yol göstermektedir [65].

ISO/IEC-27002 (ISO/IEC-17799) , güvenlik politikası geliştirme ve güvenlik denetlemesi yapma konularını kapsayan uluslararası bir standarttır. Bu standart, 10 alt bölümden oluşur. Her bölümde, o bölümde anlatılan konunun, kurumsal güvenlik politikasına nasıl dahil edileceği ve bu faaliyetlerin nasıl denetleneceği ile ilgili bilgiler vardır.

ISO, ISO/IEC-27001(BS-7799)' i temel alarak ISO/IEC-27002(ISO/IEC-17799 standardını hazırlamıştır. Aşağıda söz konusu standardın bilgi güvenliği yönetiminde yer alan on temel güvenlik önlemlerinin neler olduğu açıklanmaktadır [24],[89].

3.1.1 Güvenlik Politikası

Güvenlik politikasından beklenen amaç, bilgi güvenliği için yönetimin yönlendirilmesi ve desteğini sağlamaktır. Bu amaçla yönetim, tüm işletme içinde bilgi güvenliğine ilişkin açık bir politika ortaya koymalı ve bunun için destek vermeli ve bağlılık

göstermeli, bilgi güvenliği politikasını herkese bildirmeli ve sürekliliğini sağlamalıdır [51].

Güvenlik Politikası, bilgi güvenliğinin sağlanması için kurum çapında kullanılacak bilgi güvenliğinin omurgasını oluşturacaktır. Yapının sağlıklı olabilmesi için bu politika ile birlikte kullanılacak ilişkili alt politikaların ve prosedürlerin de hazırlanması gerekmektedir. Bilgi Güvenlik Politikaları kurum yönetimi tarafından onaylandıktan sonra iki faz olarak bilgi güvenliği yapısının oluşturulması ve Bilgi Güvenlik Politikası'nın uygulanması hedeflenmelidir [57]

Güvenlik Politikası, kurumda güvenliğin oynadığı rolün genel bir anlatımıdır.

Güvenlik Politikası üst yönetim, seçilmiş bir Kurul ya da bir Komite tarafından yazılabilir. Güvenlik Politikaları, bireylerden ve teknolojiden bağımsız hazırlanmalıdır. Kurumda uygulanacak güvenlik kontrolleri, ayrıntıya girilmeden kavramsal olarak tanımlanmalıdır [Bilişim Güvenliği (Oracle Türkiye, Pro-G Bilişim Güvenliği ve Araştırma Ltd., 2003), s.25.]

Sonuç olarak, işletmeler bilgi güvenliğinin sağlanmasında öncelikle bilgi güvenliği politika belgesi yayınlamalı ve yayınlanan bu politikanın belirli aralıklarla uygulama durumu ve güncelliğinin korunmasıaçısındangözden geçirilmesi gerekmektedir. Bu süreçlere ilişkin ihtiyaçların detayları aşağıda sunulmuştur.

3.1.1.1 Bilgi Güvenliği Politika Belgesi

Bu bağlamda bilgi güvenlik politika ve alt politikaların hazırlanarak birim onayına sunulması gerekmektedir [90] .

Bu bağlamda aşağıdaki politika ve alt politikaların hazırlanarak birim onayına sunulması gerekmektedir.

- Bilgi Güvenlik Politikası
- İnternet Güvenliği ve Güvenlik Ürünlerinin Yönetimi Politikası
- İnternet Kullanım Prosedürü
- Virüslerden Korunma Prosedürü
- B.İ.D. Başkanlığı kullanımı için ek olarak
    - Kullanıcı Kodu Şifre Politikası
    - Kullanıcı kodu Şifre Tahsis ve Kullanım Prosedürü

- Özel Yetkilendirme Prosedürü

Bilgi Güvenlik Politikasının, alt politika ve prosedürlerinin kurum onayına sunulması:

Aşağıdaki politika ve alt politikaların hazırlanarak kurum onayına sunulması gerekmektedir.

- Bilgi Güvenlik Politikası
- İnternet Güvenliği ve Güvenlik Ürünlerinin Yönetimi Politikası
- İnternet Kullanım Prosedürü
- Virüslerden Korunma Prosedürü

Bir politika belgesi, yönetim tarafından onaylanmalı, tüm çalışanlara uygun olarak yayınlanmalı ve bildirilmelidir. Yönetim politika belgesine bağlılığını belirtmeli ve bilgi güvenliğini yönetmek için işletmenin yaklaşımını ortaya koymalıdır. Bir politika belgesi aşağıdakileri içermelidir:

-Bilgi güvenliğinin tarifi, geniş kapsamlı hedefi ve amacı ve bilgi paylaşımını etkinleştiren bir yöntem olarak güvenliğin önemini,

-Hedefleri ve bilgi güvenliğinin prensiplerini destekleyen yönetim amacını,

-Güvenlik politikalarının, prensiplerinin, standardlarının ve işletme için belirli öneminin uygun gereklerinin kısa bir açıklamasını,

-Güvenlik raporlaması konuları da dahil, bilgi güvenliği yönetimi için genel ve belirli sorumlulukların tarifini,

-Politikayı destekleme ihtimali olan belgelendirmeler için referanslar, örneğin belirli bilgi sistemleri için daha detaylı güvenlik politikaları ve süreçleri veya kullanıcıların uyması gereken güvenlik kurallarını [91]. Güçlü ve anlamlı bir bilgi güvenliği politikası her başarılı bilinçlendirme çalışmasının temelini oluşturur.

Bilinçlendirme çalışmasına başlamadan önce tüm üst seviye hedeflerin ve güvenlik programının gereklerinin yazılı olması kritik önem taşımaktadır. Politika açık ve kısa

ifadeler ile yazılmış olmalı ve kurumun bilgi güvenliği konusundaki önceliklerini yansıtmalıdır. Politika ortaya konduktan sonra kullanıcılar politikanın varlık ve

içeriğinden haberdar olmalıdır. Kullanıcılar aynı zamanda politikaya uymamanın doğuracağı sonuçlar hakkında da bilgi sahibi olmalıdır [Fatih Emiral, Bilgi Güvenliği Bilincinin Genele Yayılması, (14 Nisan 2006)]

Bir kurumun en büyük hedefi, her türlü ortam (kağıt, cd, teyp, bilgisayar, ağ, Internet vb.) üzerinde bulunan veri ve bilgilerin güvenliğini sağlamak, veri bütünlüğünü korumak ve veriye erişimi denetleyerek gizliliği ve sistem devamlılığını sağlamaktır. Bunun yapılabilmesi için bütün güvenlik çözümlerinin bir arada değerlendirilmesi ve uygulanacak politika doğrultusunda güvenlik önlemlerinin alınması erekmektedir [90].

3.1.1.2 Bilgi Güvenlik Politikasının Gözden Geçirilmesi

Politikanın, sürekliliğinin sağlanmasından ve tanımlanmış yöntemlere göre gözden geçirilmesinden sorumlu bir sahibi olmalıdır. Ayrıca, belirli aralıklarda politikaların etkinliği, denetimlerin etkileri ve teknolojik gelişimlerin etkileri açısından, Bilgi Güvenlik Politikaları gözden geçirilmelidir [91].

3.1.2 Organizasyon Güvenliği

Bilgi güvenliği, yönetim takımının tüm bireylerince paylaşılan bir iş sorumluluğudur. İşletme içersinde bilgi güvenliğinin gerçekleşmesini başlatmak ve kontrol etmek üzere bir yönetim sistemi kurulmalıdır. Bilgi güvenlik politikasını onaylamak, güvenlik rolleri tayin etmek ve tüm işletme içinde güvenlik yürütümlerini düzenlemek için yönetim önderliğiyle uygun yönetim sistemi kurulmalıdır. Eğer gerekirse, bir uzman bilgi güvenliği tavsiyesi kaynağı kurulmalı ve işletme içinde etkin kılınmalıdır. Endüstriyel eğilimleri yakalamak, standardları ve değerlendirme yöntemlerini gözlemek ve güvenlik olaylarıyla ilgilenirken uygun irtibat sağlamak için, harici güvenlik uzmanlarıyla iletişim geliştirilmelidir.

Organizasyon güvenliğinin sağlanmasında, organizasyon içi bilgi güvenlik altyapısının kurulması, üçüncü taraf erişim güvenliğinin oluşturulması ve gerek duyulduğunda bilgi işleme sorumluluğunun başka bir organizasyondan sağlandığında alınacak tedbirleri içermektedir. Söz konusu üç konu alt başlığına ilişkin detaylar, aşağıda gözden geçirilmektedir.

3.1.2.1 Bilgi Güvenliği Altyapısı

Güvenlik süreçlerinin yönetilmesi için, sorumluluklar açıkça tanımlanmalıdır. Bilgi güvenlik altyapısının kurulmasında temel olarak; bilgi güvenlik sorumluluklarının organizasyon içinde dağıtılması, bilgi işleme araçları için yetkilendirme, gerektiğinde uzman desteği alınması, organizasyonlar arası işbirliğine gidilmesi, tüm yönetim desteğinin alınması için güvenlik forumu oluşturulmalıdır.

Güvenlik öncelikleriyle ilgili açık bir yönlendirmenin ve görünür yönetim desteğinin olduğunu garanti eden bir yönetim forumu oluşturulmalıdır. Bu forum, uygun bağlılık ve doğru kaynaklar aracılığıyla organizasyon içersindeki güvenliği desteklemelidir. Bu forum varolan yönetim yapısının bir parçası da olabilir.

Organizasyonların tümü uzman danışman istihdam etmek istemeyebilir. Böyle durumlarda, sürekliliği temin etmek ve güvenlikle ilgili karar verme aşamalarında yardım sağlamak üzere, firma içi bilgi ve deneyimleri düzenlemesi için uygun harici uzman danışman görevlendirilebilir. Söz konusu danışmana, en üst seviyede verimlilik ve etki için, tüm organizasyon içinde yönetime doğrudan erişim izni verilmelidir.

İlave olarak, güvenlik arızasının gerçekleşmesi durumunda uygun eylemlerin hızlıca harekete geçirilmesini ve tavsiyelerin alınabilmesini temin etmek üzere bilgi sağlayıcı yasa koyucu organizasyonlar arası uygun ilişkiler kurulmalıdır [91].

Bilgi güvenlik organizasyonu oluştururken ekip çalışması ve iş bölümlerinin yapılması gerekmektedir. Bu ekipler Bilgi Güvenlik Birimi, Bilgi İşlem Birimi ve kurumun diğer birimleri olarak sıralanabilir. Ancak güvenlikle ilgili tüm faaliyetlerden bir yönetici sorumlu olmalıdır. Bu birimlerin görevleri aşağıda listelenmiştir.

Bilgi Güvenlik Birimi Görevleri:

-Proje koordinasyonu,

-Proje raporlama ve dökümantasyonu,

-Kapsam ve detay çalışmaları için kullanılacak standartların ve uygulanacak yöntemin

yer aldığı, yol gösterici dökümanların hazırlanması,

-Bilgi güvenlik politikasının kapsam ve içeriğinin belirlenerek hazırlanması,

-Bilgi güvenlik politikasının alt politikaları ve prosedürlerinin belirlenerek hazırlanması,

-Birimlerden gelen isteklerin değerlendirilerek gerekli görülmesi durumunda proje dökümanlarına yansıtılması,

-Proje çalışmalarının planlanması, varlıkların belirlenmesi, sınıflandırılması, risk analizi, bilgi güvenlik planları, iş devamlılık planları hazırlanması gibi proje aktiviteleri için kullanılacak yöntem, standartların ve yardımcı dökümanların hazırlanması,

-Yapılacak çalışmalar için eğitimlerin verilmesi,

-Birimlerden gelen çalışma sonuçlarının değerlendirilmesi, incelenmesi, takibi ve kontrolü.

Bilgi İşlem Biriminin Görevleri:

-Bilgi Güvenlik Birimi tarafından belirlenen yöntemlerle yapılacak varlık belirlenmesi ve sınıflandırılması, risk analizi, iş devamlılık planları hazırlanması, bilgi güvenlik planlarının hazırlanması vb. proje çalışmalarına katılmak,

-Bilgi Güvenlik politikasının alt politikaları ve prosedürlerinin hazırlanması çalışmalarına destek olmak.

Kurum Birimlerinin Görevleri:

-Kurum için hazırlanan Bilgi Güvenlik politikası ve alt politikaları ile prosedürlerinin incelenmesi,

-Yürütülen çalışmalarda, Kurumun Bilgi Güvenlik Politikasına uyumunun değerlendirilmesi için gerekli desteğin verilmesi,

-Kurumdaonaylanan politikaların duyurulması veeğitimplanlamasının yapılması şeklindedir.95

3.1.2.2 Üçüncü Taraf Erişiminin Güvenliği

Bilgi, eksik güvenlik yönetimiyle üçüncü tarafların erişimi aracılığıyla risk altına girebilir.

Bir üçüncü tarafla ticari ilişki kurulması gerektiğinde, belirli denetimler için her gerekeni tanımlamak üzere bir risk değerlendirmesi yürütülmelidir. Bu risk değerlendirmesi, istenen erişim biçimini, bilginin değerini, üçüncü tarafça kullanılan denetimleri ve bu erişimin organizasyonun bilgi güvenliğine dahil edilmesini dikkate almalıdır. Denetimler üçüncü tarafla yapılacak bir sözleşme içersinde karşılıklı olarak onaylanmalı ve tanımlanmalıdır.

3.1.2.3 Dışarıdan Kaynak Sağlama

Bilgi işleme sorumluluğu başka bir işletmenin kaynaklarından dışarıdan sağlandığında bilgi güvenliğinin sürdürülmesi amaçlanmıştır. Yönetim ve bilgi sistemleri, ağlar ve masaüstü ortamların tümü veya bir kısmı için dışarıdan kaynak sağlayan organizasyonların güvenlik gerekleri, taraflar arasında yapılması anlaşılmış bir sözleşme içinde belirtilmelidir [91].

3.1.3 Varlıkların Sınıflandırması

Varlıkların sınıflandırılmasındaki amaç, işletmeye ait varlıklar için uygun korunmanın sağlanmasıdır. Bilgi varlıklarıyla ilgili atanmış bir sorumlu sahibi olmalıdır. Bu sorumluluk, uygun korumanın sağlandığının garanti edilmesine yardımcı olur. Bu amaçla öncelikle işletmeye ait varlıkların envanteri çıkarılmalı, takiben varlıların güvenlik seviyesi ve değerlerine göre sınıflandırması yapıldıktan sonra varlığın işleme yöntemine uygun olarak etiketlenmelidir. Bu kapsamda süreçlerin detaylarına ilişkin faaliyetler aşağıda sunulmuştur.

3.1.3.1 Bilgi İşlem Varlıklarının Envanteri

Bilgi sistemiyle bağlantılı olan önemli bilgi varlıklarını içerecek şekilde, ilgili yönetim birimlerince hazırlanmalı, korunmalı ve bu envanter periyodik olarak ve değişiklikler oldukça güncellenmelidir. Bu çalışmada:

-Her bir varlık açıkça tanımlanmalı,

-Varlık sahipleri belirlenmeli,

-Varlıkların güvenlik sınıflandırmaları yapılmalı,

-Varlığın mevcut bulunduğu yer (bu kayıp ve hasarlar giderilmeye çalışıldığında önemlidir) belirtilmelidir.

Bilişim sistemleriyle ilgili varlıklar, Bilgi Varlıkları, Yazılım Varlıkları, Fiziksel Varlıklar ve Hizmetler olarak kategorize edilebilir. Bunlar:

Bilgi Varlıkları: Veritabanları ve veri dosyaları, sistem belgeleri, kullanıcı el kitapları, eğitim malzemeleri materyalleri, işlemsel ve destek uygulamaları, devamlılık (süreklilik) planları, yedek anlaşmaları, arşivlenmiş bilgiyi,

Yazılım Varlıkları: Uygulama yazılımları, sistem yazılımları, geliştirme araçları ve yazılımlarını,

Fiziksel Varlıklar: Bilgisayar ekipmanları (kasa, ekranlar, diz üstü bilgisayarlar, modemler), iletişim ekipmanları (yönlendirici, telefon, faks), manyetik kayıt ortamları (teyp, kartuş, disket, disk, CD), diğer teknik ekipmanlar (güç kaynakları, adaptör, havalandırma üniteleri), mobilyayı,

Hizmetler: Bilgi işleme (bilgisayar) ve iletişim (haberleşme) hizmetleri, genel hizmetleri (ısıtma, aydınlatma, elektrik, havalandırma), kapsamaktadır.

3.1.3.2 Varlıkların Sınıflandırılması

Bilgi varlığı, korunma gereksiniminin, önceliklerinin ve derecesinin belirlenmesi için sınıflandırılmalıdır. Varlık sınıflandırması için kullanılacak standartlar ve prosedürler belgelenmeli ve uygulanmalıdır. Bilgi varlığı aşağıdaki şekilde sınıflandırılabilir [90]:

- Çok Gizli

- Gizli

- Kuruma Özel

- Hizmete Özel

- Kişiye Özel

- Tasnif Dışı

Bilgi çoğu kez belirli bir süre geçtikten sonra hassas ve önemli olmaktan çıkar, örneğin bilginin genel olarak duyurulması verilebilir. Bu açılar dikkate alınmalıdır, çünkü

gerektiğinden fazla sınıflandırma gereksiz ilave ticari harcamalara sebep olabilir. Sınıflandırma kılavuzu, bilgiyle ilgili verilmiş her öğenin sınıflandırılmasına, her zaman uygulanmasına gerek olmadığının ve önceden belirlenmiş politikalara göre değişebileceğinin gerçeğinin önceden tahmin edilmesine izin vermelidir [90],[91].

3.1.3.3 Bilgi Etiketleme

Gerekli olduğu durumda, fiziki ve elektronik ortamda olan bilgi varlıkları; sınıflandırma derecesini gösterecek şekilde etiketlenmelidir. Bilgi etiketleme ve işleme için kullanılacak standartlar ve prosedürler belgelenmeli ve uygulanmalıdır. Bilgi etiketleme ve işlemede aşağıdaki kurallar uygulanmalıdır [90].

- Fiziksel etiketler, mümkün olduğu durumlarda kullanılmalıdır. Bununla beraber,

elektronik biçimdeki belgeler gibi bazı bilgi varlıkları, fiziksel olarak etiketlenemezler. Bu nedenle, bu tür belgelerde elektronik anlamda etiketlemenin kullanılması gerekmektedir.

- Dökümanlar, içerdiği bilginin en yüksek güvenlik seviyesi göz önüne alınarak sınıflandırılmalı ve bu sınıflandırma derecesi her sayfanın sol üst ve alt köşesinde büyük harflerle ve altı çizili olarak yer almalıdır.

- Manyetik kayıt ortamındaki (kartuş, disk, disket, CD, kaset vb.) bilgiler yine en üst güvenlik seviyesi dikkate alınarak etiketlenmeli ve sınıflandırma seviyesi büyük harflerle ve altı çizili olarak medya üzerine yazılmalıdır.

- Elektronik ortamdaki belgelerde de (Word, Excel, Powerpoint dosyaları vb), bilginin güvenlik seviyesini gösteren ibare, dosya içerisinde her sayfada sol üst ve alt köşede büyük harflerle ve altı çizili olarak bulunmalıdır.

- Çok gizli, gizli, hizmete özel bilgilerin gerekli güvenlik önlemi alınmadan posta, faks veya elektronik ortamda aktarılmaması gerekmektedir. Yine bu seviyedeki bilgiler, izinsiz kişilerce eline geçirme riski olduğundan, cep telefonu, sesli mesaj, telefon gibi ortamlarda aktarılmamalıdır.

- Çok gizli, gizli, hizmete özel güvenlik seviyesine sahip bilgi varlıklarına sahip kişiler, bu varlığın bilmesi gerekenlerden başkasının görmemesini sağlamalıdır.

Her sınıflandırma için, işleme yöntemleri, aşağıdaki bilgi işleme faaliyetleri biçimlerini kapsayacak bir biçimde tanımlanmalıdır [91]

- Kopyalama

- Depolama

- Posta, faks ve elektronik mesaj aracılığıyla aktarma

- Cep telefonu, sesli mesaj, telefonlar gibi sözlü kelimelerle aktarımı

- Yok etme

3.1.4 Personel Güvenliği

Personel güvenliğinden amaçlanan, insan hatalarını, hırsızlığı, sahtekarlığı ve araçların yanlış kullanılması risklerinin azaltılmasıdır. Bu nedenle, personel güvenlik sorumlulukları işe alma sırasında belirtilmeli, sözleşmeler içinde yer almalı ve bir kişinin işe alınması süresince gözlenmelidir. Olası işe alınmalar uygun bir şekilde elenmeli, özellikle hassas görevler için dikkat edilmelidir. Bilgi işleme araçlarının tüm çalışanları ve üçüncü taraf kullanıcılar bir gizlilik anlaşması imzalamalılardır.

Özetle, işletmeler personel güvenliğinin sağlanmasında, personel iş tanımlarına güvenlik ifadesi eklenerek, tüm personelin tehditlere karşı alınabilecek önlemler konusunda eğitim aldırarak ve güvenlik saldırılarında personel sorumlulukları belirlenerek aşılabilecektir. Personel güvenliğini oluşturan bu konu başlıklarının detayları aşağıda sunulmuştur.

3.1.4.1 İş Tanımlarında Güvenlik

İşletmeye yeni alınacak personelin sorumlulukları arasına işletme politikası gereği güvenliğin ilavesi, yeni alınacak personelin işe alım kriteri olarak uygulanması, güvenlik politikası gereği personel elemeleri ve çalışanlar ile gizlilik anlaşmaları takip edilerek güvenlik kriterleri sağlanabilir. Bu süreçlerin içeriklerini alt başlıklar altında açacak olursak, şu şekilde sıralanabilir:

İş sorumluluklarına güvenliğin dahil edilmesi: Güvenlik rolleri ve sorumlulukları, organizasyonun bilgi güvenliği politikasında sunulduğu gibi, uygun olan yerde

belgelenmelidir. Bunlar, güvenlik politikasını gerçekleştirmek ve sürdürmek için her türlü genel sorumluluğun yanında, belirli varlıkların korunması veya belirli güvenlik işlemlerinin veya faaliyetlerinin yürütülmesi için her özel sorumluluğu içermelidir.

İşe alma koşulları ve şartları: İşe almanın koşul ve şartları, çalışanın bilgi güvenliği ile ilgili sorumluluklarını belirtmelidir. Uygun olan yerde, istihdam sona erdikten sonra bu sorumluluklar tanımlanmış bir zaman dilimi için devam etmelidir. Çalışanın güvenlik gereklerine uymaması karşısında ne gibi önlemler alınacağını da içermelidir.

Personel eleme ve personel politikası: Sürekli personel üzerinde doğruluk kontrolü, işe başvurulduğu zaman yapılmalıdır. Bu aşağıdaki denetimleri içermelidir:

-Tatminkar kişisel referansların varlığı (örneğin bir işle ilgili, bir şahsi)

-Başvuranın özgeçmişinin kontrolü (bütünlük ve doğruluk)

-İddia edilen akademik ve uzman niteliklerin teyidi

-Bağımsız kimlik kontrolü (pasaport ve benzeri belgeler)

Yönetim, hassas sistemlere erişim için yetkilendirilmiş yeni ve deneyimsiz personel için gereken gözetimleri değerlendirmelidir. Tüm personelin çalışmaları, kıdemli personel tarafından belirli zaman dilimlerine gözden geçirilmeli ve onaylama yöntemlerinden geçirilmelidir.

Yöneticiler personellerinin kişisel şartlarının da çalışmalarını etkileyebileceğinin farkında olmalıdırlar. Kişisel veya mali sorunlar, davranışlarındaki veya yaşam şekillerindeki değişiklikler, tekrarlama dalgınlığı ve stres veya depresyon belirtileri, sahtekarlığa, hırsızlığa, hataya veya diğer güvenlik arızalarına yöneltebilir. Bu bilgiyi, yasal yetki sınırları çerçevesi içinde yer alan uygun hükümlere göre ele alınmalıdır. Gizlilik anlaşmaları:Gizlilik veya kapalılık (ifşa etmeme) anlaşmaları, bilginin gizli veya sır olduğunun bildirimini vermek için kullanılır. Çalışanlar normalde böyle bir anlaşmayı işe alınmalarının öncelikli şartları ve koşullarının bir parçası olarak imzalamalılardır.

3.1.4.2 Kullanıcı Eğitimi

İşletmenin tüm çalışanları ve ilgili yerlerde, üçüncü taraf kullanıcılar, organizasyona ait politikalar ve yöntemlerle ilgili uygun eğitim ve düzenli güncelleme almalıdırlar. Bu,

bilgiye veya hizmetlere erişimi tayin etmeden önce, güvenlik gereklerini, yasal sorumlulukları ve iş denetimlerinin yanı sıra, oturuma giriş yöntemleri, yazılım paketlerinin kullanımı gibi bilgi işleme araçlarının doğru kullanım eğitimini almayı içermektedir.

3.1.4.3 Güvenlik Saldırılarının Bildirilmesi

Güvenlik saldırılarında meydana gelen hasarın en aza indirilmesi ve bu gibi olayların gözlenmesi ve bunlardan öğrenilmesi amaçlanmaktadır.

Tüm çalışanlar ve sözleşmeli kimseler, işletmeye ait varlıkların güvenliği üzerinde etkisi olabilecek farklı biçimdeki saldırılar (güvenlik kırılması, tehdit, zayıflama veya bozulma) rapor etme yöntemlerinden haberdar olmalıdırlar. Bu kişilerden, gözlemlenmiş ve şüphelenilmiş beklenmedik her olayı, mümkün olan en kısa süre içince belirlenmiş iletişim noktalarına rapor etmeleri istenmelidir. İşletme, güvenlik kırılmaları suçu işleyen çalışanlarla ilgilenmek üzere resmi bir disiplin süreci kurmalıdır [91].

3.1.5 Fiziksel ve Çevresel Güvenlik

Geçmiş zamanlarda önemli bilgiler, taşlara kazılarak daha sonra da kağıtlara yazılarak fiziksel ortamlarda saklanmış, duvarlarla, kale hendekleriyle ve başlarına dikilen nöbetçilerle koruma altına alınmıştır. Çoğu zaman fiziksel koruma yeterli olmamış ve bilgilerin çalınması ve başka kişilerin eline geçmesi engellenememiştir. Bu durum, verileri korumak için fiziksel güvenliğin tek başına yeterli olmadığını göstermektedir.

Günümüzde de fiziksel güvenlik önemini korumakta ve bu konuyla ilgili gerekli çalışmalar yapılmaktadır. Örneğin, bina etrafına yüksek duvarlar ya da demirler yapılması, bina girişinde özel güvenlik ekiplerinin bulundurulması, önemli verilerin tutulduğu odaların kilitlenmesi ya da bu odalara şifreli güvenlik sistemleri ile girilmesi

gibi önlemler kullanılmaktadır [90].

Fiziksel ve çevresel güvenlikten amaç, iş alanına ve bilgilerine yetkisiz erişim, hasar ve müdahalenin engellenmesidir. Önemli ve hassas ticari bilgi işleme araçları güvenli bir yere yerleştirilmeli, uygun güvenlik engelleri ve giriş denetimleriyle, tanımlanmış güvenli bir çevre aracılığıyla korunuyor olmalıdır. Bu araçlar, fiziksel olarak yetkisiz

erişimlerden, hasarlardan ve müdahalelerden korunmalıdır. Sağlanan koruma, tanımlanmış risklerle orantılı olmalıdır. Temiz masa ve temiz ekran politikası, belgelere, ortama ve bilgi işleme araçlarına yetkisiz erişim veya hasar risklerini

azaltmak için tavsiye edilmektedir.

Fiziksel ve çevresel güvenlik sağlamak için gereken kriterleri, güvenli bölgeler oluşturmak, teçhizat güvenliğini sağlamak ve gerekli denetimleri oluşturacak önlemler başlıkları altında inceleyebiliriz [24].

3.1.5.1 Güvenli Bölgeler

Fiziksel ve çevresel güvenlik, işyerine yetkisiz erişimlerin engellenmesi ve bilgi varlıklarının hırsızlığa veya tehlikeye karşı korunmasıdır.

Geçmiş zamanlarda önemli bilgiler, taşlara kazınarak daha sonra da kâğıtlara yazılarak fiziksel ortamlarda saklanmış, duvarlarla, kale hendekleriyle ve başlarına dikilen nöbetçilerle koruma altına alınmıştır. Çoğu zaman fiziksel koruma yeterli kalmamış ve bilgilerin çalınması ve baska kişilerin eline geçmesi engellenememiştir. Bu durum, verileri korumak için fiziksel güvenliğin tek başına yeterli olmadığını göstermektedir [92].

TS ISO/IEC 27002 – 17799 ‘ e göre; Fiziksel güvenlik, firmaların kaynaklarını ve değerli bilgilerini tehdit eden açıklarını kapatmakta kullanılan en önemli yöntemlerden biridir. Fiziki korunma, iş ve bilgi işleme araçları çevresinde sayısız fiziki engeller yaratarak sağlanabilir. Her bir engel, her biri sağlanan toplam korumayı arttıran bir güvenlik çevresi oluşturur. İşletmeler güvenlik çevrelerini, bilgi işleme araçları içeren alanları korumak için kullanmalıdırlar. Güvenlik çevresi, bir engel oluşturan, örneğin bir duvar, kart kontrollü giriş kapısı veya bir kişi tayin edilmiş danışma masası gibi her şeydir. Her bir engelin yerleştirilmesi ve gücü, risk değerlendirmesinin sonucuna bağlıdır.

Güvenli bölgeler oluşturulabilmesi için, bilginin bulunduğu alanlara girişin fiziksel giriş denetimi yapılması, bilgi kaynaklarının bulunduğu alanların fiziki çevresel koruma altında tutulması, güvenli alan denetimleri ve yükleme alanlarının bilgi kaynaklarına ulaşımına engellenecek şekilde ayrılması faaliyetlerini içermektedir. Bu faaliyetlerin yönetilmesinde dikkat edilecek konular şu şekilde sıralanabilir:

Fiziki giriş denetimleri: Güvenli alanlar, sadece yetkili personelin erişimine izin verildiğinin temin edilmesi için uygun giriş denetimleriyle korunuyor olmalıdırlar. Aşağıdaki denetimler göz önüne alınmalıdır:

- Güvenli alanlarda ziyaretçilere eşlik edilmeli veya üstleri aranmalıdır ve giriş ve çıkış tarihleri ve saatleri not edilmelidir. Sadece belirli, yetkili amaçlar çerçevesinde erişimlerine izin verilmeli ve alana ait güvenlik gereklerinin direktifleriyle ilgili ve acil durum yöntemleriyle ilgili bilgilendirilmelidirler.

- Hassas bilgilere ve bilgi işleme araçlarına erişim denetlenmeli ve sadece yetkili kullanıcılara sınırlı olmalıdır. Kimlik doğrulama denetimleri, örneğin giriş kartı ve parola, tüm erişimleri yetkilendirmek ve geçerli kılmak için kullanılmalıdır. Tüm erişimlerin bir kontrol zinciri güvenli olarak korunmalıdır.

- Tüm personelden, görünür biçimde kimlik kartı taşımaları istenmelidir ve eşlik edilmeyen bir yabancıya veya kimlik kartı taşımayan birine rastlandığında hemen bildirmeleri teşvik edilmelidir.

- Güvenli alanlara erişim hakları düzenli aralıklarla gözden geçirilmeli ve güncelleştirilmelidir [91].

Günümüzde bu konu üzerine çalışan bir çok güvenlik firması ve bu firmaların yeterince geniş yelpazede ürünleri vardır. Firmalar genellikle, akıllı giriş kartları kullanmaya başlamıştır. Bu kartların en önemli avantajı giriş çıkışların kayıtlarını tutmasıdır. Fakat bir dezavantajı ise kaybolma riski taşımasıdır. Zaten bu riski nasıl azaltılabilir şeklinde düşünen üretici firmalar, çalışanların yanlarında taşıdıkları ve kaybolma riski bulunmayan fiziksel özellikleri kullanmaya karar vermektedirler. Böylece biyometrik giriş sistemleri kullanıma sürülmüştür. Bu kapsamda gözümüzü veya parmak izimizi kullanarak erişim hakkımız olan bölgelere girip çıkmaya başlanmıştır.

Diğer önemli bir konu ise şirkete gelen ziyaretçilerin şirket içindeki hangi bölgelere nasıl gireceğinin ve yanlarında eşlik edecek bir kişinin gerekip gerekmediğinin belirlenmesidir. Ayrıca ziyaretçi giriş çıkışlarının düzenli olarak kaydının tutulması çok önemlidir. Bu konuda ziyaretçilere verilecek ve adlarına kayıt yapılacak kartlar kullanılabilir [24],[93].

Bürolar, odalar ve araçların güvenlik altına alınması: Güvenli bir alan, kilitlenmiş bir büro veya içinde birçok oda bulunan, kilitlenmiş olan ve kilitlenebilir dolaplar veya korumalar içeren fiziki bir güvenlik çevresi olabilir. Güvenli bir alanın seçimi veya tasarımı, yangın, sel, patlama, askeri saldırı ve diğer biçimdeki doğal veya insan yapımı afetlerden meydana gelebilecek hasar ihtimallerini göze almalıdır. Ayrıca ilgili sağlık ve korunma standardlarına ve kurallarına da dikkat edilmelidir. Ayrıca komşu çevrelerden, örneğin diğer alanlardan su borusu akıntısı gibi, gelebilecek olan güvenlik tehditleri de göz önünde bulundurulmalıdır. Aşağıdaki denetimler dikkate alınmalıdır:

-Herkes tarafından erişimi engellemek için anahtar araçlar yerleştirilmelidir.

-Binalar göze çarpmayan bir şekilde olmalıdır ve bilgi işleme faaliyetlerinin, bina içinde veya dışında, varlığını tanımlayan belirgin bir işaret olmaksızın amaçlarıyla ilgili en az göstergeyi vermelidir.

-Fotokopiler, faks makineleri gibi destek fonksiyonları ve donanımları, bilgiyi tehlikeye atan erişim taleplerini engellemek için güvenli alan içine uygun bir şekilde yerleştirilmiş olmalıdır.

-Pencereler için özellikle de zemin kat seviyesinde ihmal edilmiş ve harici koruma göz önüne alındığında, kapılar ve pencereler kilitlenmiş olmalıdır.

-Profesyonel standardlarda uygun izinsiz girişleri tespit sistemi ve düzenli olarak denetlenmesi, tüm harici kapıları ve erişilebilir pencereleri kapsayacak şekilde yerleştirilmelidir. Boş alanlar her zaman uyarı sinyalleriyle donatılmış olmalıdır. Kapsama, bilgi işlem odası veya haberleşme odaları gibi diğer alanları da kapsamalıdır.

-İşletme tarafında yönetilen bilgi işleme araçları, fiziksel olarak üçüncü taraflarca yönetilenlerden ayrılmış olmalıdır.

-Hassas bilgi işleme araçlarının yerini gösteren telefon rehberi veya dahili telefon kitapçıkları, başkaları tarafından erişilebilir yerlerde olmamalıdır.

-Tehlikeli ve patlamaya hazır maddeler, güvenli alandan uygun bir uzaklıkta güvenli bir şekilde toplanmalıdır. Kırtasiye malzemeleri gibi tedarikler, gerek duyulmadıkça güvenli alan içinde toplanmamalıdır.

-Yedek donanımlar ve yedekleme ortamı, ana alanda oluşabilecek felaketler

sonucundaki yıkımı önlemek üzere uygun bir uzaklıkta yerleştirilmelidir [91].

Cihaza fiziksel olarak erişebilen saldırganın konsol arabirimi aracılığıyla cihazın kontrolünü kolaylıkla alabileceği unutulmamalıdır. Ağ bağlantısına erişebilen saldırgan ise kabloya özel ekipmanla erişim sağlayarak, hattı dinleyebilir veya hatta trafik gönderebilir. Açıkça bilinmelidir ki fiziksel güvenliği sağlanmayan cihaz üzerinde alınacak yazılımsal yöntemlerin hiç bir kıymeti bulunmamaktadır [94].

Güvenli alanlarda çalışmak: Personel, güvenli alanın varlığını ve içerde yürütülen

faaliyetleri, bilmesi gerektiği kadarından haberdar edilmelidir. Güvenlik sebeplerinden dolayı ve kötü niyetli faaliyetlere fırsat vermemek için güvenli alanlarda denetlenmemiş çalışmalardan kaçınılmalıdır. Güvenli bir alanın güvenliğini genişletmek için ilave denetimler ve kılavuzlar gerekebilir. Bunlar, güvenli alanda çalışan personel veya üçüncü tarafların denetiminin yanında burada yer alan üçüncü taraf faaliyetlerinin denetimini de içermelidir.

Ayrılmış dağıtım ve yükleme alanları: Dağıtım ve yükleme alanları denetlenmeli ve eğer mümkünse yetkisiz erişimi engellemek için bilgi işleme araçlarından ayrılmalıdır. Bu gibi bölgeler için güvenlik gerekleri risk değerlendirmesi aracılığıyla belirlenmelidir. Aşağıdaki denetimler göz önünde bulundurulmalıdır .

-Bina dışından bulundurma bölgesine erişim, tanımlanmış ve yetkili personelle sınırlandırılmalıdır.

-Bulundurma bölgesi, dağıtım elemanlarının binanın diğer kısımlarına erişimi kazanmaksızın malzemeleri boşaltabilecekleri şekilde tasarlanmış olmalıdır.

-Dahili kapı açık olduğunda, bulundurma bölgesine ait harici kapıların güvenli olması gerekmektedir.

-Dışarıdan gelen malzemeler, bulundurma bölgesinden kullanım noktasına taşınmadan önce, olası tehlikelere karşı kontrol edilmelidir

-Dışarıdan gelen malzemeler, eğer uygunsa alana girişinde kaydedilmelidir.

3.1.5.2 Teçhizat Güvenliği

TS ISO/IEC 27002 – 17799' e göre; Teçhizat güvenliğinden amaç, varlıkların kayıplarını,

hasar veya tehlikelerini ve ticari faaliyetlerdeki kesilmenin önlenmesidir. Teçhizatlar güvenlik tehditlerinden ve çevresel tehlikelerden fiziki olarak korunmalıdır. Teçhizatların korunması (alan dışında kullanılanlar dahil) veriye yetkisiz erişim riskini azaltmak ve kayıp ve hasara karşı korumak için gereklidir.

Tehlikelere veya yetkisiz erişimlere karşı teçhizatları korumak için, donanım yerleştirilmesi, güç kaynakları, kablo güvenliği, donanım bakımı, işletme dışında güvenlik ve donanımların tekrar kullanımı için özel denetimlere gerek duyulabilir. Bu süreçlerde alınacak önlemleri aşağıdaki başlıklar altında özetlenmiştir:

Donanım yerleştirilmesi: Teçhizatlar, çevresel tehditler ve tehlikelerden oluşan riskleri ve yetkisiz erişim fırsatlarını azaltmak üzere yerleştirilmeli ve korunmalıdır. Aşağıdaki denetimler göz önünde bulundurulmalıdır.

-Teçhizatlar iş alanları içinde gereksiz erişimi azaltmak üzere yerleştirilmelidir.

- Hassas veriler tutan bilgi işleme ve yükleme araçları, kullanımları sırasında gizlice izlenme riskini düşürmek üzere yerleştirilmelidir.

-Özel koruma gerektiren öğeler, gereken genel koruma seviyesini düşürmek için ayrılmalıdır.

- Denetimler, olası tehditlerle ilgili riskleri en aza indirmek için kurulmalıdır.

-Bir organizasyon, yiyecek, içecek ve sigara içme politikalarını bilgi işleme araçlarına yakınlığına göre gözden geçirmelidir.

-Çevresel şartlar, bilgi işleme araçlarının faaliyetlerini geri dönülemez biçimde etkileyen şartlara göre gözlemelidir.

-Endüstriyel çevreler içindeki teçhizatlar için, dokunmaya duyarlı klavyeler gibi özel koruma yöntemleri düşünülmelidir.

-Yakın çevrede oluşan felaketler örneğin komşu binada çıkan bir yangın, çatıdan akan su veya zemin kat seviyesinden aşağıdaki katlara akan su veya caddede olan bir patlama göz önünde bulundurulmalıdır.

Güç kaynakları: Teçhizatlar, güç kaynağı bozulmalarından veya diğer olağandışı elektriksel olaylardan korunmalıdır. Donanım üreticisinin belirttiği özelliklere uygun

elektrik kaynağı sağlamalıdır.

Kablo güvenliği: Veri taşıyan veya bilgi hizmetlerini destekleyen güç ve haberleşme kabloları, durdurmalardan veya hasarlardan korunmalıdır.

Donanım bakımı: Teçhizatların, erişilebilirliğinin ve güvenilirliğinin garanti edilmesi için doğru bir biçimde bakımı sağlanmalıdır.

Çevre dışı teçhizatların güvenliği: Sahibine bakmaksızın, bilgi işleme için organizasyonun çevresi dışında her donanımın kullanımı yönetim tarafından yetkilendirilmelidir. Sağlanan güvenlik organizasyonun çevresi dışında çalışmanın risklerini dikkate alarak, aynı amaçla alan içinde kullanılan teçhizatlarla eşit olmalıdır. Bilgi işleme teçhizatları, ev çalışması için tutulan veya normal iş yerleşiminden uzağa taşınan her çeşit kişisel bilgisayarları, düzenleyicileri, cep telefonlarını, kağıt veya diğer belgeleri içerir.

Teçhizatların düzenlenmesi ve tekrar kullanımı: Bilgi, teçhizatların dikkatsizce düzenlenmesi ve tekrar kullanımıyla tehlikeye girebilir. Hassas bilgiler içeren depolama aygıtları, standart silme fonksiyonunu kullanmak yerine, fiziksel olarak yok edilmeli veya güvenli olarak üstüne yazılmalıdır. Depolama ortamı içeren, örneğin takılmış sabit diskler, teçhizatların tüm öğeleri, tüm hassas verilerin ve lisanslı yazılımların düzenlenmeden önce kaldırılmış olduğunu veya üstüne yazılmış olduğunu temin edilmesi için kontrol edilmelidir [91].

3.1.5.3 Genel Denetimler

Güvenlik denetimi, bir kurumun güvenlik altyapısının, güvenlik politikasının, prosedürlerinin ve personelinin ayrıntılı bir biçimde ele alınması, zayıf yönlerin tespiti ve bu zayıflıkların giderilmesi için öneriler sunulmasıdır. Başarılı bir denetim, tüm ilgili tarafların işbirliği ile gerçekleştirilebilir. Genelde güvenlikle ilgili bir denetim söz konusu olduğunda, birçok insan olumsuz bir önyargıya kapılır ve rahatsız olur. Bununla birlikte, güvenlik denetimi kurum içinde güvenlik politikasına uygun çalışılıp çalışılmadığının tespitinde kullanılabilecek tek yoldur [89].

Denetlenecek faaliyetler, personel tarafından temiz masa ve ekran politikasının uygulanabilirliği ve teçhizatların uygun kullanımı başlıkları altında sınıflandırabilir ve

bunlara ilişkin detaylar aşağıda sunulmaktadır:

Temiz masa ve temiz ekran politikası: Organizasyonlar, normal çalışma saatleri süresince ve dışında bilgiye yetkisiz erişim, bilgi kaybı ve hasarı risklerini azaltmak amacıyla kağıtlar ve kaldırılabilir depolama ortamları için temiz masa politikasını uygulamayı ve bilgi işleme araçları için temiz ekran politikasını uygulamayı göz önünde bulundurmalıdır. Politika, bilgi güvenlik sınıflandırmalarını, yerini tutan riskleri ve organizasyonun kültürel konularını dikkate almalıdır. Masalarda bırakılmış bilgilerin yangın, sel veya patlama gibi felaketlerde hasar görme ve yok olma olasılığı çok yüksektir. Aşağıdaki denetimler göz önünde bulundurulmalıdır.

-Uygun olan yerlerde, kağıt ve bilgisayar ortamı, kullanılmadığında özellikle de çalışma saatleri dışında uygun kilitli depolarda veya diğer çeşit güvenlik mobilyalarında depolanmalıdır.

-Hassas ve önemli iş bilgileri, gerekmedikleri zamanda özellikle de büro boş olduğunda, kilitlenmelidir (ideal olarak yangına dayanıklı korumalarda veya dolaplarda)

- Kişisel bilgisayarlar ve bilgisayar terminalleri ve yazıcılar, başıboş olduklarında oturum açık olarak bırakılmamalılardır ve anahtar kilitler, şifreler veya diğer denetimler aracılığıyla kullanılmadıkları zamanlarda korunmalıdırlar.

- Gelen ve giden mesaj noktaları ve başıboş faks veya teleks makineleri korunmalıdır.

- Fotokopi makineleri, normal çalışma saatlerinin dışında kilitlenmelidir (veya yetkisiz kullanımlardan başka yollardan korunmalıdır).

- Hassas ve sınıflandırılmış bilgi basıldığında yazıcıdan hemen temizlenmelidir. Teçhizatların kullanımı: Teçhizat, bilgi veya yazılım yetkisiz olarak alan dışına çıkarılmamalıdır. Uygun ve gerekli olan yerlerde, geri döndürüldükleri zaman teçhizatların kaydedilmeleri gerekir. Teçhizatların yetkisiz kaldırımını tespit etmek için nokta denetimler üstlenilmelidir. Nokta denetimlerin uygulanacağı hakkında kişiler haberdar edilmelidir.

3.1.6 Haberleşme ve İşletim Yönetimi

Haberleşme ve işletim yönetiminden amaçlanan, bilgi işlem tesislerinin doğru ve

güvenle işletildiğinden emin olunmasıdır. Bu amaçla tüm bilgi işlem tesislerinin işletim ve yönetim prosedürleri ile sorumlulukları tesis edilmelidir. Haberleşme ve işletim yönetimi, işletim prosedürleri ve sorumlulukların belirlenmesi, sistem planlama, kötü niyetli yazılımlara önlemler, yedekleme, ağ yönetimi, bilgi ortamı yönetimi ve bilgi/yazılım değişimi toplam yedi başlık altındaki süreçleri kapsamaktadır.

3.1.6.1 İşletim Prosedürleri ve Sorumluluklar

İşletim prosedürlerinin ve sorumlulukların belirlenmesi ile bilgi işleme olanaklarının doğru ve güvenli işletimi sağlanmaktadır. Prosedürlerde sistemin, bilerek ya da bilmeyerek yanlış kullanım riskini bulunduğu yerlere göre görevler ayrılmalıdır. İşletim prosedürleri ve sorumlulukları, temel olarak beş alt başlık altında incelersek, bunlar; yazılı prosedürler, olay yönetim prosedürleri, değişim yönetimi, görevlerin ayrılması ve geliştirme ve işletim tesislerinin ayrılmasından oluşmaktadır.

Yazılı işletim prosedürleri: Güvenlik politikasında tanımlanan işletim prosedürleri, yazılı ve sürekli olmalıdır. İşletim prosedürleri, gücünü yönetimden alan resmi belge ve değişiklikler şeklinde işlem görmelidir. Bilgisayarların açılıp kapanması, yedekleme, teçhizatın bakımı, bilgisayar odası ve posta alma-gönderme yönetimi ve emniyet gibi işlem ve iletişim tesisleriyle beraber yürütülen sistem idame faaliyetleri için yazılı prosedürler hazırlanmalıdır.

Olay Yönetim Prosedürleri: Olay yönetim prosedürleri ve sorumlulukları, güvenlik olaylarına çabuk, etkin ve bir sıra dahilinde müdahale edilmesini sağlamak maksadıyla tesis edilmiştir. Bu konu ile ilgili olarak aşağıdaki kontroller göz önüne alınmalıdır.

- Güvenlikle ilgili tüm potansiyel türleri kapsayan prosedürler oluşturulmalıdır.

- Prosedürler, normal, ani durum planlarını içerecek şekilde hazırlanmalıdır.

- Resmi bulgular ve kanıta benzer şeyler, uygun şekilde toplanıp emniyet altına alınmalıdır.

- Güvenlik ihlallerinin giderilmesi hareketi ve düzgün sistem arızaları, dikkatli bir biçimde ve resmi olarak kontrol altında olmalıdır.

Değişim Yönetimi: Bilgi işlem tesisleri ve sistemlerine dair değişiklikler kontrol

altında tutulmalıdır. Bilgi işlem tesisleri ve sistemlerinin değişikliklerine ilişkin kontrolün yetersizliği, sistem ya da emniyet konusundaki aksaklıkların en önde gelen nedenlerindendir. Resmi yönetim sorumlulukları ve prosedürler, teçhizat, yazılım ve prosedürlere ilişkin tüm değişiklerin tatmin edici bir şekilde kontrolünü sağlayan bir konumda olmalıdır. İşletim kuralları, en katı değişiklik kurallarına maruz kalmalıdır. Programlar değiştiğinde, konu ile ilişkili tüm hususları kapsayan bir izleme kaydı tutulmalıdır.

Görevlerin Ayrılması: Görevlerin ayrılması, kazara ya da kasten sistemin yanlış kullanım riskini azaltan bir metottur. Yetki verilmeyen değişikliklerin meydana gelmesini ya da bilgi veya servislerin yanlış kullanımını azaltmak maksadıyla belli görevlerin yerine getirilmesi ya da yönetimi veya sorumluluk alanlarının ayrılması değerlendirilmelidir. Küçük organizasyonlar, bunu başarılması zor bir kontrol metodu olarak değerlendirebilirler, fakat bu prensip mümkün olabildiği kadar uygulanmalıdır. Ne zaman ayrım yapmak zorlaşırsa, faaliyetlerin izlenmesi, yönetim gözetimi ve kayıtların denetimi gibi diğer kontroller dikkate alınmalıdır. Güvenlik denetiminin bağımsız olması büyük önem arz etmektedir.

Bilgisayar ağlarındaki güvenliği tesis edip sürekliliğini sağlamak için, bir dizi kontrole gereksinim duyulur. Ağ yöneticileri, ağlardaki verinin güvenliği ve bağlı bulunulan servislere yetkisiz kişilerce erişilmesinden korunmasını sağlamak maksadıyla kontrolleri gerçekleştirmelidirler [91].

3.1.6.2 Bilgi Ortamı Yönetimi

Bilginin yetkisiz kişilerce erişimine, ifşa edilmesi ya da yanlış maksatlarla kullanılmasını önlemek için bilgi güvenliği ve yönetimi için prosedürler oluşturulmalıdır. Kendi içindeki sınıflandırmayla tutarlı olarak, yazılı belgeler, bilgisayar sistemleri, ağlar, mobil bilgisayarlar, mobil iletişim, posta, sesli posta, sesli iletişim, çoklu ortam, posta hizmetleri/tesisleri, faks makinesi ve diğer hassas parçaların kullanılırken (örneğin, boş çekler, fatura vb.) bilginin yönetilmesi için prosedürler düzenlenmelidir. Bu maksatla aşağıdaki hususlar dikkate alınmalıdır:

- Tüm ortamın etiketlenmesi ve yönetilmesi ,

- Yetkisiz kişileri tanımlamak için erişim sınırlamaları,

- Veri kullanan yetkisiz kişiler için bir resmi kaydın tutulması,

- İşlemin doğru bir şekilde tamamlayan ve çıktı geçerliliğinin uygulamaya koyan girdi verisinin eksiksiz olmasının sağlanması,

- Kendi duyarlılığı ile uygun bir seviyede çıktıyı bekleyen zarar görmüş verinin korunması,

- Ortamın, üretici firma şartlarına uygun bir yerde bulundurulması,

- Veri dağıtımını en alt düzeyde tutulması,

- Yetkisiz kişilerin dikkatini çekebileceğinden verinin tüm kopyalarındaki işaretlemelerin temizlenmesi,

- Düzenli aralıklarla yetkisiz kişilerin ve dağıtım listelerini gözden geçirilmesidir. Gereksinim ortadan kalktığında, emniyetli ve kesin bir şekilde bilgi ortamından kurtulmak gerekir. Hassas bilgiler ortamın yok edilmesi esnasında dikkatsiz kişilerce başka insanlara sızabilir. Ortamın kesin olarak yok edilmesindeki resmi prosedürler oluşturulmalı ve bu tehlikeyi en aza indirmek maksadıyla denetimler yapılmalıdır.

3.1.6.3 Bilgi ve Yazılım Değişimi

BGYS'de organizasyonlar arasında yazılımın ve bilginin değişimi, kontrol altında bulundurulmalı ve ilgili yasalarla uyumlu olmalıdır. Bilgi ve yazılım değişimleri, anlaşma esaslarına göre yapılmalıdır. Nakil esnasındaki ortam ve bilgiyi korumak için prosedürler belirlenmelidir. Karşılıklı elektronik veri değişimi, elektronik ticaret ve elektronik posta ile kontrol tedbirlerinin gereksinimleriyle birleşen iş ve güvenlik konuları göz önünde tutulmalıdır.

Bilgi ve yazılım değişimi süreçlerinin kapsamı:

- Bilgi ve yazılım değişim anlaşmaları,

- Nakil esnasındaki bilgi ortamının güvenliği,

- Elektronik ticaret güvenliği,

- Elektronik ofis sistemlerinin güvenliği,

- Halka açık sistemler,

- Bilgi değişiminin diğer şekilleri, başlıkları altında aşağıda sunulmuştur.

Bilgi ve yazılım değişim anlaşmaları: Bazıları resmi olan ve uygun olan hallerde üçüncü şahıslarla yapılan yazılım antlaşmalar, organizasyonlar arasında bilgi ve yazılımın değişimi için yapılmalıdırlar. Bu tür bir anlaşmanın güvenlik içeriği, ilişkili olduğu işin duyarlılığını yansıtmalıdır.

Nakil esnasındaki bilgi ortamının güvenliği: Bilgi, postaya verildiği ya da kurye ile gönderildiği hallerde fiziki olarak hareket halindedir ve yetkisiz kişilerin erişimine, yanlış maksatlarla kullanılmalara ya da zarar görmeye karşı hassastır. Siteler arasında gidip gelen bilgisayar ortamının güvenliği için aşağıdaki kontrol tedbirleri uygulanmalıdır.

- Güvenilir kuryeler ve ulaşım vasıtaları seçilmelidir. Yetkili kuryelerin bir listesi, kuryeler için yapılan tanımları kontrol eden bir prosedür ve yönetimle kararlaştırılmalıdır.

- Üretici firmanın şartlarına uygun ve içerdiği bilginin hareket halinde iken zarar görmekten koruyan yeterli bir paketleme olmalıdır.

- Gerektiğinde, yetkisiz açma ve değiştirmeleri önlemek maksadıyla, özel kontrol tedbirleri uygulanmaktadır.

Elektronik ticaret güvenliği: Elektronik ticaret, karşılıklı elektronik veri değişimi, elektronik posta ve Internet gibi geniş halk kitlelerinin erişimine açık çevrim içi işlemlerin kullanımını içerir. Elektronik ticaret, hileli kazanç faaliyetleri, anlaşma itilafları ya da bilginin değişikliğe maruz kalması gibi bir dizi ağ şebekesi tehditlerine karşı hassastır. Elektronik ticareti bu tür tehditlerden korumak için kontrol tedbirleri uygulanmalıdır.

Elektronik ofis sistemlerinin güvenliği: Elektronik ofis sistemleriyle müşterek iş ve güvenlik tehlikelerini kontrol etmek maksadıyla politikalar ve genel hatlar belirlenmeli ve uygulanmalıdır. Bunlar; belgelerin, bilgisayarların, mobil bilgi işlem ve mobil iletişimin, postanın, sesli mesajın, sesli haberleşmenin, çoklu ortamın, posta teşkilatının ve faks makinelerinin kombinasyonunu kullanarak iş bilgilerinin paylaşılması ve

düşüncelerin daha hızlı yayılması konusunda fırsat sağlamaktadır.

Halka açık sistemler: Yetkisiz kişilerin şirketin itibarını zedeleyebilecek şekildeki değişiklikler yapmalarını önleyerek elektronik olarak yayılan bilginin bütünlüğünü korumaya özen gösterilmelidir. Halka açık sistemlerdeki bilgi, örneğin, Internet yolu ile erişilen Web sayfasındaki bilgiler, ticaretin yapıldığı ya da sistemin bulunduğu mahkemelerdeki yasalar, kurallar ve düzenlemelerle uyumlu olmaya ihtiyaç gösterir. Bilgi halka yayılmadan önce resmi bir yetkilendirme süreci oluşturulmalıdır.

Bilgi değişiminin diğer şekilleri: Ses, faks ya da video iletişim gereçlerini kullanarak bilgi değişimini önlemek yerine, prosedürler ve kontrol tedbirleri kullanılmalıdır. Bilgi, farkında olmadan ve kullanılan politika ve prosedürler nedeniyle doğru olarak kullanılmayabilir. Örneğin, halka açık bir yerde cep telefonu ile çok yüksek sesle konuşmak, sesi çok açık olan bir bant kaydı dinlemek, sesli mesaj sistemine yetkisiz kişilerin erişim sağlaması, faks cihazını kullanarak faksın yanlış adrese gönderilmesi verilebilir. Ancak iletişim gereçleri kullanılamazsa, iş ilişkileri bozulabilir, bilgi yanlış değerlendirilebilir. Bu nedenle, ses, faks ve video iletişiminde kullanılırken takip edilecek prosedürlerin açık bir şekilde ifade edilmesine gerek vardır [91].

3.1.7 Erişim Denetimi

Bilişim güvenliğinde en önemli konularda biri, kaynaklara kimin nasıl eriştiğini kontrol etmek, bu sayede bilgi üzerinde yetkisiz değiştirme ve açığa çıkarma olaylarını engellemektir. Bu amaçla yapılan faaliyetlere genel olarak erişim denetimi denir. Bir kullanıcı bilgisayarından ağ üzerindeki bir dizine ulaşmak istediğinde ona kullanıcı adı ve parola soran bir ekranla karşılaşması, erişim denetimine örnek olarak verilebilir.

Erişim denetimi, yazılım ve donanım tabanlı olarak sağlanabilir [89].

Bilgiye erişim denetim yöntemleri, yeni kullanıcıların kayıt başlangıçlarından, bilgi sistemlerine ve hizmetlerine erişim gereksinimi artık kalmamış kullanıcıların son kayıttan çıkışlarına kadar olan, kullanıcıların tüm yaşam döngüsü basamaklarını kapsamalıdır. Sadece gerekli olan personele, gerektiği kadar erişim yetkisi sağlanmalı, erişim kontrolü kuralları ve süreçleri belirlenmelidir. Kullanıcı kayıt, kullanıcıya tanınan ayrıcalık özellikleri, kullanıcı şifre yönetimi, erişim haklarının gözden geçirilmesi

gibi işlemler için detaylı talimatlar oluşturulmalı, her bir konuya ilişkin isterler/kurallar politika dökümanına yansıtılmış olmalıdır. Kullanıcılar erişim hakları ile bu konuda kendi sorumluluk ve yükümlülükleri hakkında bilgilendirilmiş, bilinçlendirilmiş olmalıdır [95].

Erişim kontrolü, bir kaynağa erişimin ve o kaynağın kullanımının kişilere yetkiler vererek ve kısıtlamalar getirerek sınırlanmasıdır. Örnek olarak, hassas bilgiler içeren kurumsal programlara erişimlerin uygun şekilde düzenlenmesi ve kullanıcıların uymaya zorlanması, veritabanı ve sistem yönetim araçlarına ilgili BS personeli dışında erişimin engellenmesi ve sistem odasına sadece yetkili personelin girebilmesi verilebilir. Örneklerden de anlaşılabileceği gibi erişim kontrolleri bilgi güvenliğinin ana bileşenleri olan gizlilik, bütünlük ve erişilebilirliğin üçünün de sağlanmasına katkıda

bulunmaktadır.

Bilgi güvenliğinin sağlanmasında yüksek derecede önem taşıyan erişim kontrolleri, uluslararası standartlar ve yerel düzenlemelerde yoğun şekilde referanslanmaktadır. Erişim kontrollerine ilişkin maddeler içeren dökümanlardan bazıları aşağıda listelenmiştir [96].

- ISO 27002 Bilgi Güvenliği Yönetimi için Uygulama Prensipleri Standardı dökümanında

7 başlık altında 25 kontrol hedefi,

- COBIT 4.1 dökümanında 3 ana başlık altında 7 kontrol hedefi,

- PCI DSS dökümanının 12 gerekliliğinden 3 tanesi,

- BDDK Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ'de 3 madde,

- Ülkemizde pek çok kurumun uyum gerekliliği olan Sarbanes-Oxley yasasının 404. bölümü.

Erişim denetim yöntemleri:

- Kullanıcı sorumluluğu,

- Ağ erişimi denetimi,

- İşletim sistemi erişim denetimi,

- Uygulama erişimi denetimi,

- Sistem erişiminin gözlenmesi ve kullanımı,

- Mobil bilgi işlem ve uzaktan çalışma,

olmak üzere toplam altı başlık altında aşağıda sunulmuştur:

Kullanıcı sorumluluğu: Etkin bir güvenlik için yetkili kullanıcıların işbirliği çok önemlidir. Kullanıcılar, etkin erişim denetimlerini, özelliklede parolaların kullanımı ve kullanıcı teçhizatlarının güvenliği ile ilişkili olarak, sağlamak için sorumlulukları hakkında bilgilendirilmelidir. Kullanıcılar parolaların seçimi ve kullanımında doğru güvenlik uygulamalarını izlemelilerdir.

Ağ erişimi denetimi: Ağ oluşturulmuş hizmetlerin korunması için, dahili ve harici kurulmuş ağların her ikisine de erişim denetlenmelidir. Bu, ağlara ve ağ hizmetlerine erişimi olan kullanıcıların, ağ hizmetlerinin güvenliğini tehlikeye atmadıklarından emin olmak gereklidir.

İşletim sistemi erişim denetimi: Yetkisiz bilgisayar erişiminin engellenmesi için, işletim sistemi düzeyinde güvenlik Araçları, bilgisayar kaynaklarına erişimi engellemek için kullanılmalıdır. Tüm kullanıcılar (işlemciler, ağ yöneticileri, sistem programcıları ve veritabanı yöneticileri gibi teknik destek personelleri dahil), yapılan işlemlerin sonradan sorumlu bireyler kapsamında izlenebilmesi için, kişisel ve tek kullanımlara ilişkin özel birer tanımlayıcıya (kullanıcı kimliği) sahip olmalıdırlar. Ayrıca tanımlanmış bir çalışmazlık (etkinsizlik) süresinden sonra erişim hizmetini kapatılması için, terminal zaman aşımı ve yüksek riskli uygulamalarda bağlantı süresi sınırlaması dikkate alınmalıdır.

Uygulama erişimi denetimi: Uygulama sistemleri içersinde erişimi kısıtlamak için güvenlik araçları kullanılmalıdır. Yazılım ve bilgiye mantıksal erişim, yetkili kullanıcılarla kısıtlanmalıdır.

Sistem erişiminin gözlenmesi ve kullanımı: Erişim denetim politikasından sapmaları tespit etmek için sistemler gözlenmeli ve güvenlik arızalarının çıkması ihtimaline karşı bulgu sağlayabilmek için gözlenebilir olayları kaydedilmelidir. Sistemin gözlenmesi, kabul edilmiş (benimsenmiş) denetimlerin etkinliğinin kontrol edilmesine ve erişim

politikası modeline uygunluğunun teyit edilmesine izin verir.

Mobil bilgi işlem ve uzaktan çalışma: Mobil bilgi işlem kullanıldığında, korunmasız çevrelerde çalışmaya ait riskler dikkate alınmalı ve uygun koruma yöntemleri uygulanmalıdır. Uzaktan çalışma gerektiğinde, işletme çalışılan alana uygun koruma sağlamalı ve bu çalışma şekilleri için uygun düzenlemelerin yapıldığını temin etmelidir.

3.1.8 Sistem Geliştirme ve Bakım

Sistem geliştirme ve bakım süreçlerinde güvenliğin ele alınması ve mevcut uygulamaların güvenli olarak bakımının sağlanması beklentilerini içerir.

Bilgi işlem sistemlerinin geliştirilmesinden önce, güvenlik gerekleri belirlenmeli ve bu konuda uzlaşmaya varılmalıdır. Güvenlik gerekleri ve kontroller ilgili bilgi desteklerinin ve güvenlikteki bir aksaklıktan ya da güvenlik yoksunluğundan doğabilecek muhtemel iş kaybının iş açısından değerini yansıtmalıdır. Güvenlik gereklerini incelemeye ve bunları karşılayacak olan kontrolleri belirlemeye ilişkin altyapı risk değerlendirmesi ve risk denetimidir. Tasarım aşamasında yürütülen kontrollerin kurulması ve bakımı, kurulum sırasında ya da kurulumdan sonra dahil edilenlere göre, belirgin ölçüde daha ucuzdur.

Sistem geliştirme ve bakım süreçlerini aşağıdaki başlıklar altında açıklamaya çalışalım:

- Uygulama sistemlerinde güvenlik,

- Şifreleme kontrolleri,

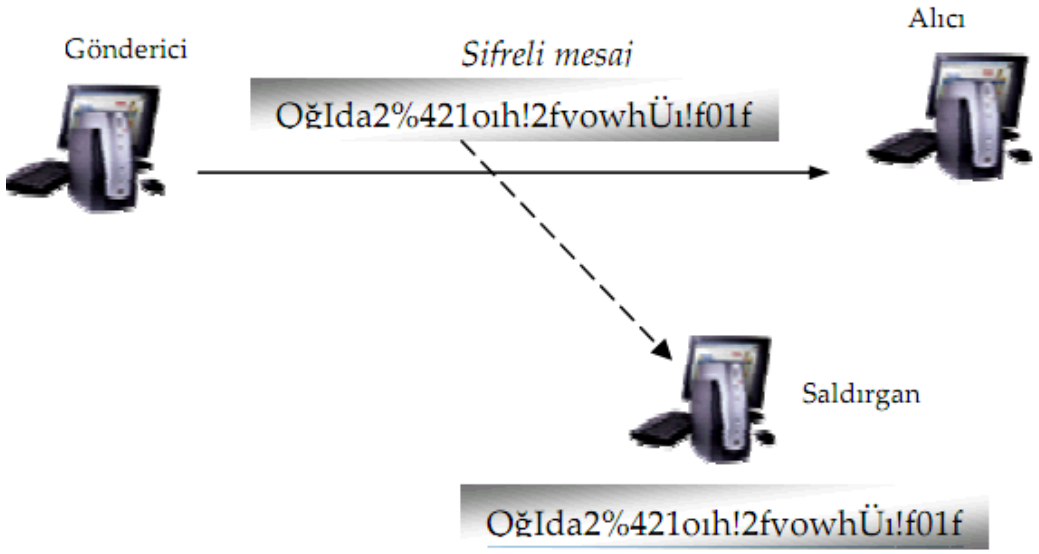
- Sistem dosyalarının güvenliği,

- Geliştirme ve destek süreçlerinde güvenlik.

Uygulama sistemlerinde güvenlik: Uygulama istemlerindeki kullanıcı verilerinin kaybedilmesini, değişmesini ya da hatalı kullanımının önlenmesi amacı ile, kullanıcı yazılı uygulamaları da dahil olmak üzere, uygun kontroller ve kontrol zincirleri ya da etkinlik kayıtları tasarlanmalıdır. Bunlar arasında, girilen verilerin, iç işleyişin ve son verilerin geçerli kılınması yer almalıdır.

Şifreleme kontrolleri: Bilginin gizliliği, aslına uygunluğu ya da bütünlüğünün korunması için şifreleme sistemler ve teknikler kullanılmalıdır. Şifrelemenin bir çözümün uygun

olup olmadığı konusunda bir karar vermek risklerin değerlendirilmesi ve kontrollerin seçilmesi yolundaki daha geniş bir işlemin bir parçası olarak görülmelidir. Bilginin verilmesi gereken seviyesinin belirlenmesi için bir risk değerlendirmesi yapılmalıdır. Daha sonra bu değerlendirme, şifrelemenin uygun olup olmadığını, ne tür ve hangi amaçla ve hangi iş etkinlikleri için bir kontrol uygulanması gerektiğini belirlemek için kullanılabilir. Şekil 26'da bir saldırganın hattı dinleyerek mesajı ele geçirmesi gösterilmiştir. Ancak saldırgan mesaja sahip olsa bile, mesaj kriptolu olduğundan içeriği konusunda bilgi sahibi olamaz.



Şekil 3.3 Hattı Dinleyen Bir Saldırgana Karşı Şifrelemenin Kullanılışı

Sistem dosyalarının güvenliği: İşletim sistemlerinin bozulma riskini asgariye indirmek için bazı kontroller yapılması gerekir. Bu kontroller şu şekilde değinilebilir:

- İşletim programları kütüphanesinin güncellenmesi yalnız uygun yönetim yetkilendirmesi ile tayin edilen kitaplık görevlisi tarafından gerçekleştirilebilir.

- Mümkünse, işletim sistemleri yalnız makine kodu taşımalıdır.

- Başarılı testlere ve kullanıcı onayına ilişkin kanıtlar elde edilinceye ve karşılık gelen program kaynak belgelikleri güncelleninceye kadar, makine kodu bir işletim sistemi üzerine yerleştirilmemelidir.

- İşletim belgeliklerine uygulanan tüm güncellemelerini içeren bir kontrol kaydı tutulmalıdır.

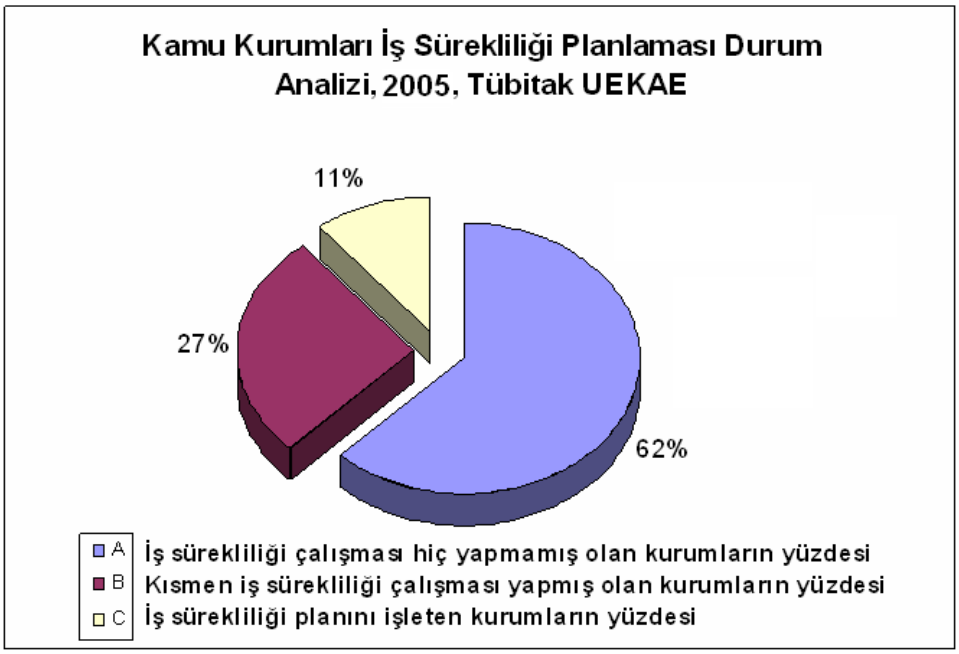
- Beklenmedik durum önlemi olarak yazılımın önceki versiyonları saklanmalıdır. Geliştirme ve destek süreçlerinde güvenlik: Uygulama sistemlerinden sorumlu yöneticiler projenin ve destek ortamının güvenliğinden de sorumlu olmalıdırlar. Sistemin ya da işletim ortamının güvenliğini bozmadığından emin olmak için, planlanan tüm sistem değişikliklerinin gözden geçirilmesini temin etmelidirler.

3.1.9 İş Devamlılığı Yönetimi

İş devamlılık yönetimi; felaketler ve güvenlik başarısızlıkları (örneğin, doğal felaketler, kazalar, araç gereç başarısızlıkları ve kasıtlı hareketlerin sonuçları olabilir)

nedeniyle oluşan bozulmayı, koruyucu ve yenileyici kontrollerin birleşmesi ile, kabul edilebilir bir seviyeye indirmek için uygulanmalıdır [91].

2006 yılında ABD'de ve Kanada'da bulunan 261 orta ve büyük ölçekli kurum üzerinde yapılan bir araştırma sonucuna göre kurumların %52'si iş sürekliliği planına sahiptir. Bu kurumlardan %26'sı iş sürekliliği planını kurum çapında yaygınlaştıramamış veya güncelleyememiştir. Dolayısıyla kurumların sadece %39'u planı uygun biçimde işletmektedir [99]. Ülkemizde ise TÜBİTAK UEKAE tarafından 2005 yılında yapılan bir araştırmanın sonucuna göre kurumların sadece %11'i iş sürekliliği planı işletmektedir. Bu çalışma kapsamında 37 kamu kurumu ile görüşmeler yapılmıştır. Ülkemizde bilgi güvenliği bilincinin artması ve finans sektöründe getirilen düzenlemeler ile birlikte son yıllarda iş sürekliliğinin ön plana çıktığını görmekteyiz. Bu kılavuz iş sürekliliği yönetim sistemi kurmayı planlayan kurumlara yol göstererek ülkemizde bu oranın artmasına katkı sağlamayı amaçlamaktadır.



Şekil 3.4 TÜBİTAK UEKAE Kamu Kurumları İş Sürekliliği Planlaması Araştırma Sonucu

İş devamlılık ve olağanüstü durum yönetimi, tüm dünyada son yıllarda, özellikle de terör saldırılarının artmasıyla birlikte, üzerinde daha da önemle durulan bir konu haline gelmiştir. Bu kapsamda, kurumlar kendi içlerinde olağanüstü durum organizasyonları oluştururken, tüm ülke boyutuna ulaşan kapsamlı hazırlık ve çalışmalar da gündeme gelmiştir [97].

İş sürekliliğinin sağlanmasında bilgi teknolojilerinin rolünün yüksek olmasından dolayı çalışmaların BT bölümü tarafından yapılması ve sorumluluğunun da BT bölümünde olması gerektiği inanışı yaygındır. İstatistikler iş sürekliliği çalışmalarına BT bölümünün katılımının diğer birimlerden fazla olduğunu göstermektedir. Öbür yandan iş sürekliliğinin sorumluluğunun çok yüksek oranda üst yönetim, yönetim kurulu veya iş sürekliliği takımında olduğu görünmektedir [99].

Felaketlerin, güvenlik başarısızlıklarının ve servis kayıplarının sonuçları incelenmelidir. Ticari işlemlerin gereken zaman aralıklarında düzeltilebilmesinin devamlılığının sağlanması için olası planlar geliştirmelidir ve uygulanmalıdır. Bu planların diğer bütün ticari işlemlerin bağlantılı bir parçası olması için sürekliliğinin ve pratikliliğinin sağlanması gereklidir. İş devamlılık yönetimi, riskleri tanımlamak ve en aza indirgemek, gelen zararların sonuçlarını sınırlandırmak için kontroller içermelidir ve operasyonlar için zaman sağlanmalıdır. İş devamlılık planlama işlemleri aşağıdakileri ele almalıdır:

- Tüm sorumluluk ve olağan üstü durumlarda yapılacak işlemlerinin belirlenmesi ve karar verilmesi,

- Gerekli zaman aralığında yenilenmenin yapılmasını sağlamak için ilkyardım işlemlerinin uygulanması,

- Karar verilen işlemler ve işlem sıralarının belgelerinin hazırlanması,

- Personele, olağan üstü durumlarda yapılmasına karar verilen işlemlerin ve işlem sıralarının, sorun durumundaki yönetimi de içeren uygun bir eğitimin verilmesi,

- Planların test edilmesi ve güncellenmesidir.

İş birimleri iş devamlılığına yönelik olarak, işlemlerini ikincil merkezden yürütmeyi B Planı olarak ele almışlarsa, bilişim hizmetleri olmaksızın da iş sürekliliğini ne şekilde sağlayabileceklerini bir C Planı çerçevesinde ele almalıdırlar. Bu süreç, işlerin daha çok kağıt ortamında nasıl takip edileceğine yöneliktir. İş birimleri, işin kağıt ortamında nasıl gerçekleştirilebileceğini ifade eden genel bir döküman hazırlamış olmalıdırlar. Tüm planlara ilişkin dökümanların bir kopyası ikincil yerleşmede korumalı bir şekilde hazır tutulmalıdır. Ayrıca, bu yerleşmede ihtiyaç duyulacak her türlü ekipman (bilgisayar, yazıcı, toner, kağıt, telefon, faks, teleks, kırtasiye malzemeleri v.b.) yedek olarak hazır bulundurulmalıdır. Yedek merkezden hizmet verilmesi ile ilgili olarak bilgisayar firmalarıyla yapılacak servis ve destek hizmetleriyle ilgili sözleşmelerde ikinci yerleşmede alınacak hizmetlerle ilgili maddeler bulunmalı ve alınacak hizmetlerin kapsamı doğru ve detaylı olarak tarif edilmelidir [97].

Tavsiye edilen İSYS kurulum aşamaları Çizelge 3.1' de yer almaktadır [98],[99].

Çizelge 3.1 İş Sürekliliği Kurulum Aşamaları

AŞAMA 1 - Proje Başlangıç Aşaması
Proje grubunun oluşturulması
Üst yönetim bilinçlendirmesi
Proje Planının hazırlanması
AŞAMA 2 – İş Etki ve Risk Analizi
İş Etki Analizi
Risk Analizi
AŞAMA 3: İş Sürekliliği Yönetim Sistemi Kurulumu
İş Sürekliliği Organizasyonunun Oluşturulması
İş Sürekliliği Yönetim Sistemi Dökümantasyonu
AŞAMA 4: İş Sürekliliği Yönetim Sisteminin Hayata Geçirilmesi
İş Sürekliliği Eğitim ve Bilinçlendirme Faaliyetleri
İş Sürekliliği Tatbikat İşlemleri

3.1.10 Uyumluluk

Bilgi sistemlerinin şekli, operasyonu ve kullanımı herhangi bir güvenlik gereksinimi için, yasal, düzenleyici ve kurucu yaptırımların konusu olabilir. Belirli bir kanuni gereksinim hakkındaki öneriler, organizasyonun kanuni tavsiyecileri tarafından verilmelidir. Kanuni gereksinimler ülkeden ülkeye çeşitlilik gösterir ve bilgilerin bir ülkeden diğer ülkeye geçiş vardır (geçiş köprüsü veri akışı).

Bütün uygun yasal, düzenleyici ve kurucu gereksinimler her bilgi sistemi için kesin olarak tanımlanmalı ve dökümantasyonu yapılmalıdır. Bu gereksinimlerle çakışan belirli kontroller ve bireylerin sorumluluklarının da aynı şekilde tanımının yapılması ve dökümantasyonunun sağlanması gereklidir.

Yasal kısıtlamalara uyulması açısından kopya hakkı, düzenleme hakkı, ticari marka gibi hakların kullanılmasında uygun işlemler yürürlülüğe sokulmalıdır. Kopya hakkının ihlal edilmesi bir suçtur [91].

3.2 TS ISO/IEC 27001 BİLGİ GÜVENLİK YÖNETİM SİSTEMİ (BGYS) (MD.4)

BGYS, bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası olarak adlandırılabilir.

Bir işletme için BGYS'nin benimsenmesi stratejik bir karar olmalıdır. Bir kuruluşun BGYS tasarımı ve gerçekleştirmesi, ticari ihtiyaçlar ve amaçlardan doğan güvenlik gereksinimlerinden, kullanılan süreçlerden ve kuruluşun büyüklüğü ve yapısından etkilenir. Bunların ve destekleyici sistemlerinin zaman içinde değişmesi beklenir. Basit durumların basit BGYS çözümlerini gerektireceği beklenir.

İşletme etkin bir şekilde işlev görmesi için, bir çok faaliyetini tanımlamalı ve yönetmek durumundadır. Kaynakları kullanan ve girdilerin çıktılara dönüştürülebilmesi için yönetilen her faaliyet, bir süreç olarak düşünülebilir. Çoğunlukla, bir sürecin çıktısı doğrudan bunu izleyen diğer sürecin girdisini oluşturur. Kuruluş içerisinde, tanımları ve bunların etkileşimi ve yönetimleriyle birlikte süreçlerin oluşturduğu bir sistem uygulaması "süreç yaklaşımı" olarak tanımlanabilir [4],[100].

3.2.1 BGYS'de Süreç Yaklaşımı

İlk iş olarak şunu vurgulayalım: ISO 27001 standardı BGYS'nin süreçlerden oluşan bir sistem olarak algılanması gerektiğini vurgulamaktadır. Buna ilave olarak, BGYS'nin kendisi de bir süreçtir [100].

ISO 27001 standardına göre "Girdileri çıktıya çevirmek için kaynak kullanan ve yönetilen faaliyetler süreç sayılır". Dolayısıyla sürecin ;

- Girdisi,
- Çıktısı,
- Girdiyi çıktıya dönüştürmekte kullandığı bilgisi ve yöntemi

olacaktır. Bunlara ilave olarak süreç çalışırken kaynak kullanacaktır. Peki standart "yönetilen faaliyet" ifadesi ile ne demek istemektedir? Biz bu ifade ile

- Yönetim tarafından tanımlanmış faaliyetin
- Yönetim tarafından atanmış sorumlular ve belirlenmiş roller uyarınca

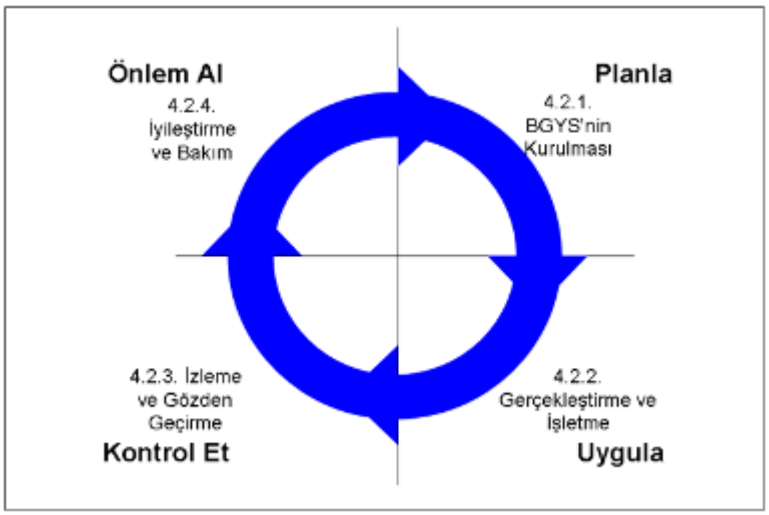
gerçekleştirilmesini anlıyoruz. Her iki konu ISO 27001 ve ISO/IEC 27002:2005 standardında açıkça vurgulanmaktadır.

BGYS sürecinin girdisi "Bilgi güvenliği ihtiyaç ve beklentileri", çıktısı "Yönetilen bilgi

güvenliği"dir.

3.2.2 Planla – Uygula – Kontrol Et – Önlem Al

Süreci meydana getiren faaliyetler dört adım altında toplanabilir. Bu dört adım PUKÖ (Planla-Uygula-Kontrol Et-Önlem Al) döngüsünü oluşturmaktadır. Bu adımlar ve standardın ilgili başlıkları aşağıdaki Şekil 3.5 ve Çizelge 3.2' de görülmektedir.



Şekil 3.5 PUKÖ adımları ve BGYS döngüsü

Çizelge 3.2 PUKÖ adımlarının standart alt başlıkları ile ilişkisi

Adım	Standardın ilgili başlığı
Planla	4.2.1 BGYS'nin kurulması
Uygula	4.2.2 BGYS'nin gerçekleştirilmesi ve işletilmesi
Kontrol Et	4.2.3 BGYS'nin izlenmesi ve gözden geçirilmesi
Önlem Al	4.2.4 BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi

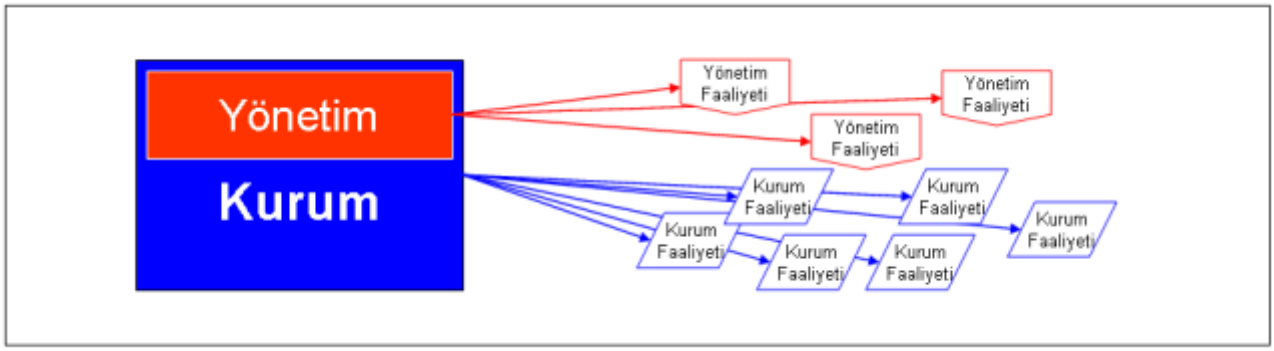
Bu dört adımın gerçekleştirilmesi ile PUKÖ döngüsü tamamlanmış olmaktadır.

4.2 başlığı altında BGYS döngüsünün çok yoğun bir özeti yapılmaktadır. Bu başlık altından standardın "dökümantasyon gereksinimleri", "yönetim sorumluluğu", "iç tetkik", hatta ISO 27002 kontrollerinin özetlendiği "Ek A. Kontrol Amaçları ve

Kontroller" bölümlerine göndermeler yapılmaktadır. Bu bölümlerde de PUKÖ döngüsü altında bahsi geçen faaliyetler daha detaylı olarak açıklanmaktadır [100].

3.2.3 İcracılar: Kurum ve Yönetim

Yönetim kurumun dışında yer alan bir unsur olamayacağına göre "Yönetim" ifadesinden "Sadece Yönetim", "Kurum" ifadesinden ise "Kurum içinde yönetim tarafından görevlendirilmiş birimler ve gerekiyorsa yönetim temsilcisi" anlaşılmalıdır.



Şekil 3.6 BGYS faaliyetleri, "Kurum" ve "Yönetim"

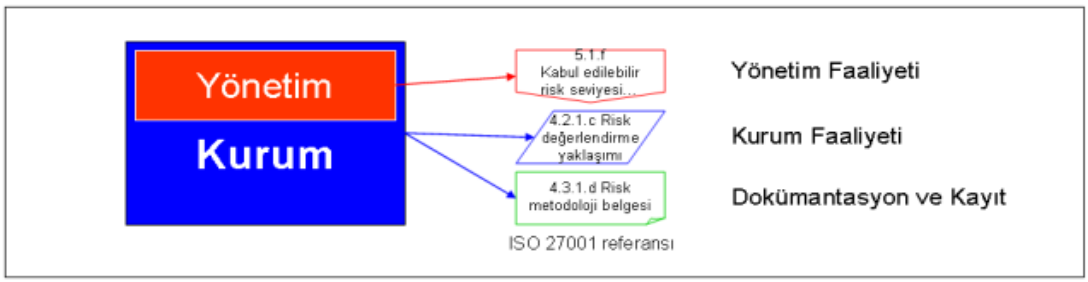
Özetle Şekil 3.6' da "Yönetim", tüm süreç boyunca devrede kalmakta, çeşitli adımlarda faaliyetler icra ederek veya kaynak sağlayarak BGYS sürecine katkıda bulunmaktadır.

"Kurum" ve "Yönetim" faaliyetlerine ilave olarak standartta dikkat çeken bir faaliyet türü de dökümantasyon ve kayıt çalışmalarıdır. Bu konu "4.3 Dökümantasyon ihtiyaçları" başlığı altında işlenmektedir. Bu başlık altında üretilmesi zorunlu olan dökümanların PUKÖ döngüsünün hangi faaliyetleri ile ilişkili olarak geliştirileceği ve dökümanlarla ilgili olarak yönetimin üstüne düşenler açıklanmaktadır.

3.2.4 Kurum, Yönetim ve Dökümantasyon faaliyetleri

PUKÖ döngüsünde mevcut herhangi bir kurum faaliyeti için bu faaliyete paralel olarak gerçekleştirilmesi gereken bir yönetim faaliyeti ve faaliyetlerin çoğu için oluşturulması gereken döküman veya kayıtlar mevcuttur. Örnek olarak "4.2.1.c Risk değerlendirme yaklaşımının tanımlanması" faaliyetini inceleyelim. Bu faaliyet ile ilgili olarak yönetimin 5.1.f başlığında belirtilen "Riskleri kabul etme ölçütlerini ve kabul edilebilir risk seviyelerini belirleme" faaliyetini gerçekleştirmesi beklenmektedir. Aynı faaliyetle ilgili

olarak 4.3.1.d başlığında “Risk değerlendirme metodolojisi tanımı”nın döküman olarak oluşturulması gerektiği belirtilmektedir [100]. (Şekil 3.7)



Şekil 3.7 4.2.1.c faaliyeti, eşlik eden yönetim faaliyeti ve dökümantasyon

3.2.5 Yönetim ve dökümantasyonun oluşturduğu paralel döngüler

Standardın “4.2 BGYS’nin kurulması ve yönetilmesi” başlığı, esasen “PUKÖ döngüsü”nün tamamını içermekte, BGYS süreci çerçevesinde gerçekleştirilecek kurum faaliyetlerine değinirken yönetim faaliyetlerine ve dökümantasyona da göndermeler yapmaktadır. (Kurum faaliyetlerinin bir kısmı ise - “6 İç tetkik” ve “8 BGYS’nin iyileştirilmesi”-daha-sonra-detaylandırılmıştır.)

Ardından gelen 4.3 başlığı süreç boyunca üretilecek dökümanlara değinmekte, 5 ve 7 numaralı başlıklar ise yönetim faaliyetlerini açıklamaktadır.

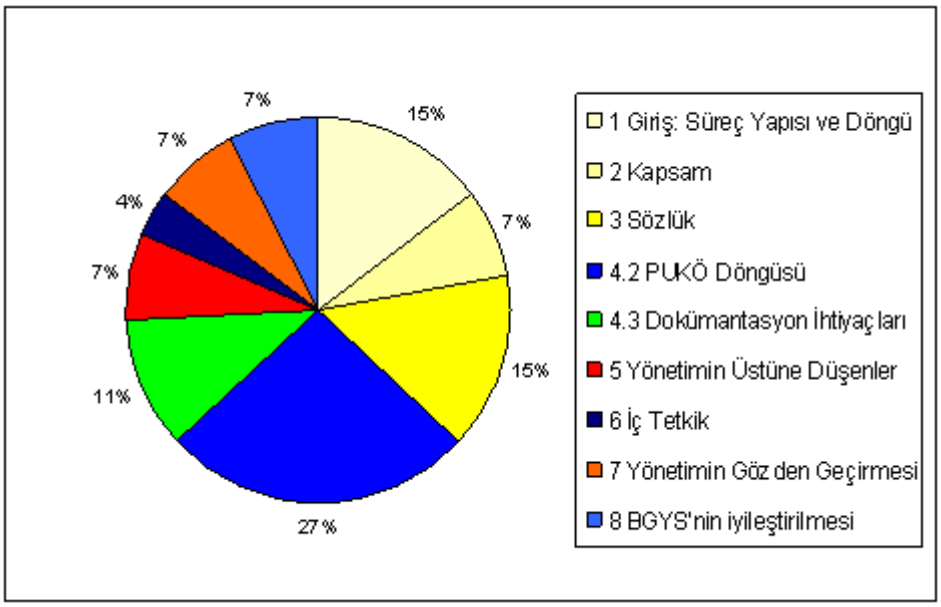
Bu bölümlerin içerikleri PUKÖ döngüsüne eşlik eden yönetim ve dökümantasyon döngülerini tanımlamaktadır. Bu üç paralel döngünün bir araya gelmesiyle çok katmanlı BGYS süreci oluşmaktadır (Şekil 3.8).

Şekil 3.8 Üç katmanlı BGYS döngüsü

Şekil 3.8'de de görüldüğü gibi

- Yönetim faaliyetleri üst katmanı,
- Kurum faaliyetleri orta katmanı,
- Dökümantasyon ve kayıtlar ise alt katmanı oluşturmaktadır.

Bu aşamada ekleri hariç 13 sayfadan ibaret olan ISO 27001 standardının hangi katmana ne kadar yer ayırdığına ve bunların sırasına da bir göz atalım. (Şekil 3.9 ve Çizelge 3.3) Daha detaylı bilgi için bu makalenin ekinde bulunan ISO 27001 standardının "İçindekiler" bölümünü inceleyebilirsiniz.



Şekil 3.9 Sıra ve sayfa sayısına göre ISO 27001 başlıkları

Çizelge 3.3 Kurum faaliyetleri, yönetim faaliyetleri ve dökümantasyonun standart alt başlıkları ile ilişkisi

ISO 27001 Referansı	İçerik	Sayfa Adedi	Ağırlık
4.2, 6 ve 8	Kurum faaliyetleri	5	%38
5 ve 7	Yönetim faaliyetleri	2	%14
4.3	Dökümantasyon ve kayıt	1.5	%11

Yukarıdaki şekilde kırmızı ve turuncu tonlarla belirtilen bölümler yönetim, mavinin tonlarıyla belirtilen bölümler kurum, yeşil bölümler ise dökümantasyon katmanına ait faaliyetlere değinmektedir.

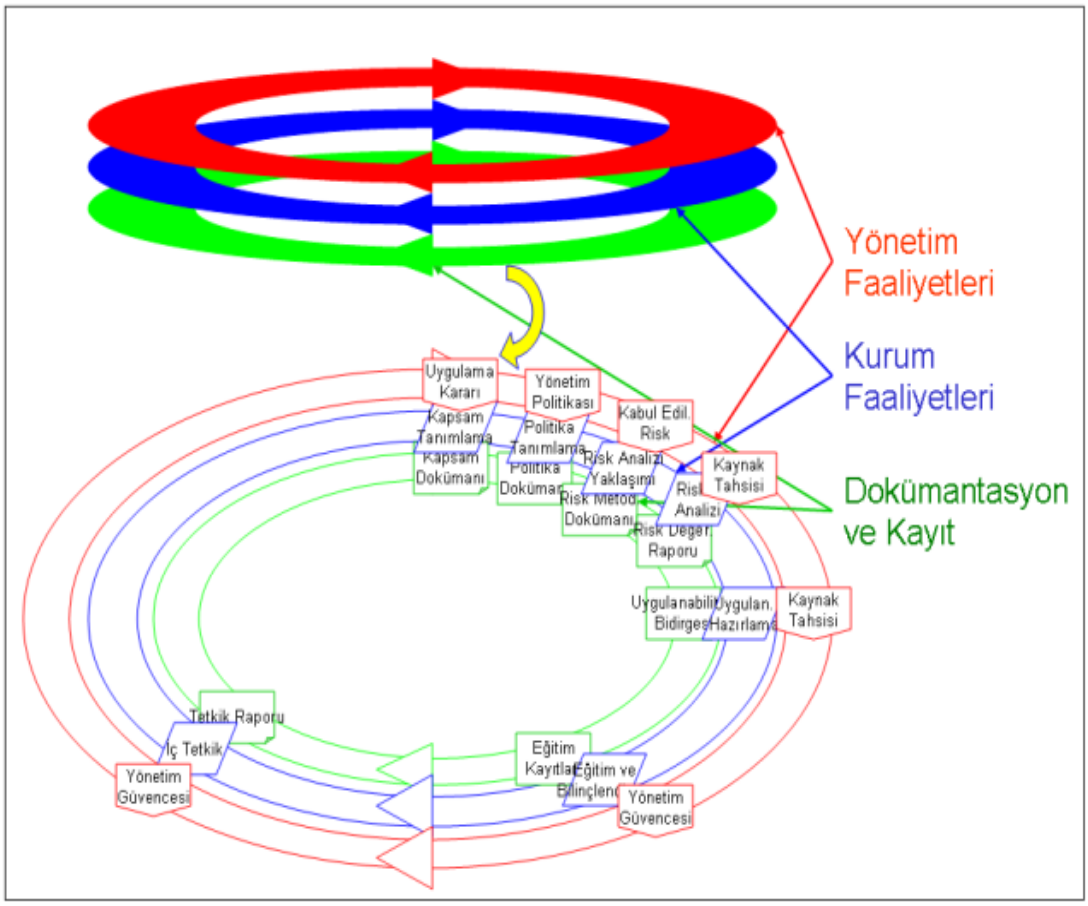
BGYS sürecinin her aşamasında üç katmanda birden faaliyet yürütüldüğünü söylemek mümkün olmasa da çoğunlukla mümkündür. Örneğin yönetim katmanının katkısının bazı aşamalarda kaynak tedarik etmekten ibaret olduğunu, diğer bazı aşamalar için ise standardın döküman talep etmediğini söylemek mümkündür. Buna rağmen sürecin tamamınında her üç katmanda da yerine getirilmesi gereken sorumlulukların bulunduğu, dolayısıyla Şekil 3.8 'de resmedilen çok katmanlı BGYS döngüsünün bilgi güvenliği sürecine ilişkin hayli gerçekçi bir model oluşturduğu kabul edilebilir.

Çok katmanlı yapıların hemen hepsinde olduğu gibi burada da üst katmanın çıktısı bir alttaki katmanın girdisini oluşturmakta, kurum faaliyetlerinin sonucunda oluşan dökümantasyon ise çoğunlukla sürecin bir sonraki faaliyeti için girdi olmaktadır.

Örnek olarak tekrar Şekil-3.5' e dönecek olursak; Bir yönetim faaliyeti olan kabul edilebilir risk seviyesinin belirlenmesi (5.1.f), kurum faaliyeti olan risk değerlendirme yaklaşımının belirlenmesine (4.2.1.c) girdi oluşturmakta, bu faaliyet sonucunda dökümantasyon katmanında yer alan risk metodoloji belgesi (4.3.1.d) üretilmektedir. Bu döküman, sürecin bir sonraki faaliyeti olan risk analizi çalışmaları (4.2.1.d-f) için girdi oluşturmaktadır.

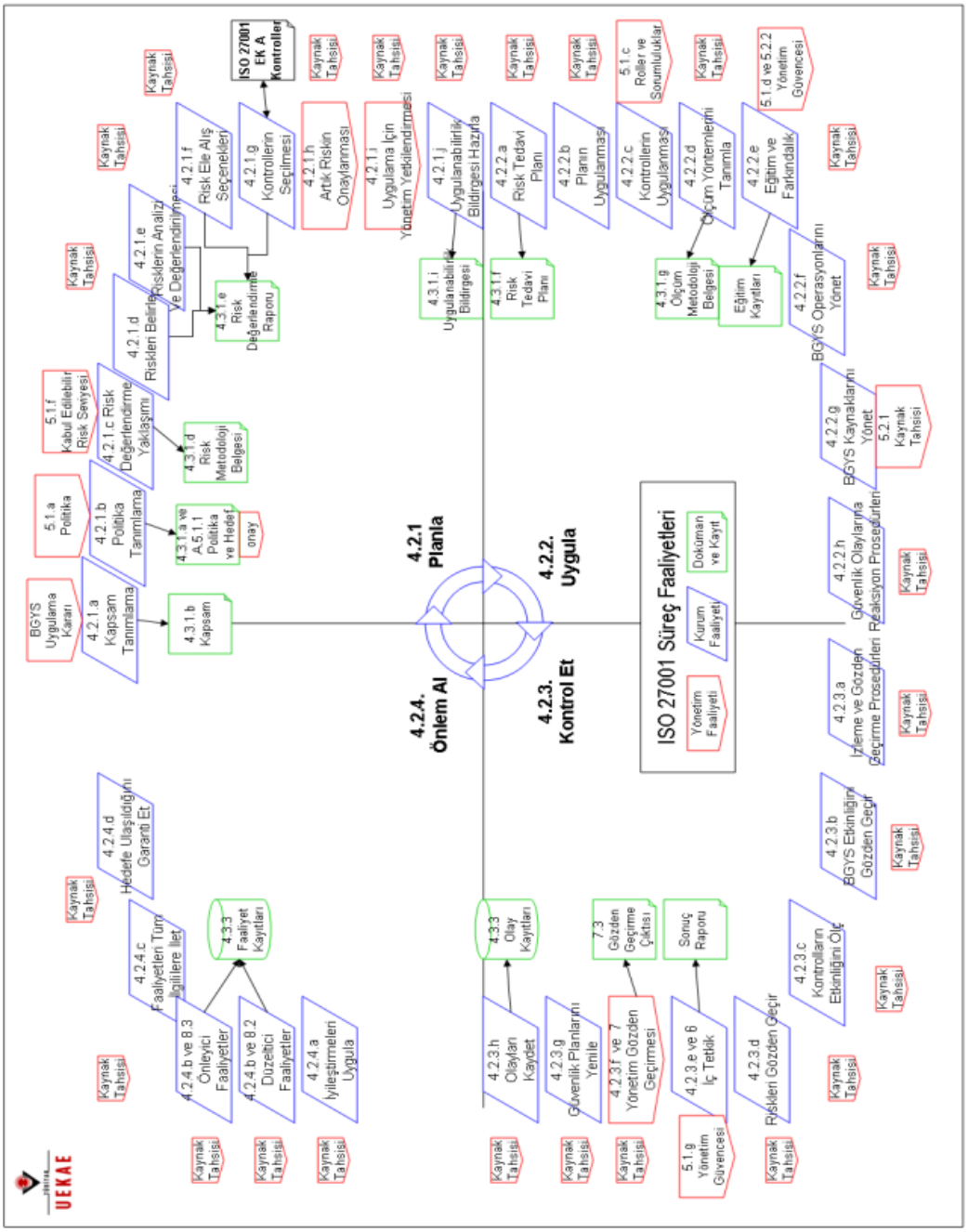
3.2.6 Katmanlar arası senkronizasyon ve BGYS süreç özeti

Standartta bulunan tüm göndermelerin incelenmesi ile farklı katmanlardaki faaliyetlerin ilişkilendirilmesi ve katmanlar arası senkronizasyonun sağlanması mümkün olabilir. Böylece Şekil 3.9 ve Çizelge 3.3' de görüldüğü üzere standartta karışık olarak yer alan BGYS sürecinin tüm katman ve faaliyetlerini tek şekilde özetlemek mümkün olacaktır. (Bu özet Şekil 3.10' da gösterilmiştir.)



Şekil 3.10 Çok katmanlı BGYS döngüsünün detaylandırılması

Standartta yer alan tüm faaliyetlerin detaylı BGYS döngüsüne yerleştirilmesi ile hem süreçte yer alan faaliyetlerin tamamı, hem de bu faaliyetler arasındaki ilişkiler gözler önüne serilmektedir [100]. (Şekil 3.11)



Şekil 3.11Detaylandırılmış üç katmanlı BGYS süreci

ISO 27001 standardı, bir kuruluşun BGYS'sini kurmak, gerçekleştirmek, işletmek, izlemek, bakımını yapmak ve etkinliğini arttırmak için bir süreç yaklaşımının benimsenmesini özendirir. BGYS kurulumuna yönelik gereksinimleri, aşağıdaki toplam yedi başlık altında açıklanacaktır.Bunlar:

- Genel gereksinimler,

- BGYS'nin kurulması ve yönetilmesi,

- Dökümantasyon gereksinimleri,

- Yönetim sorumluluğu,

- BGYS iç denetimleri,

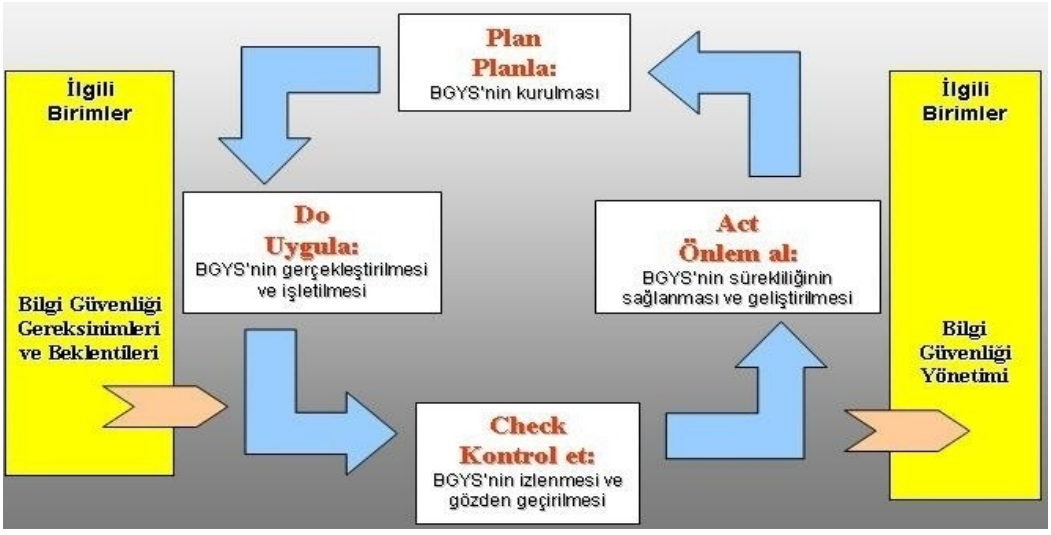
- BGYS'yi yönetimin gözden geçirmesi,

- BGYS iyileştirme, başlıkları olacaktır [100].

3.2.7 Genel Gereksinimler (Md.4.1)

Kuruluş, yazılı hale getirilmiş bir BGYS'yi, kuruluşun tüm ticari faaliyetleri ve riskleri bağlamında, geliştirir gerçekleştirir, sürdürür ve sürekli ilerletir. Bu standardın bir gereği olarak, kullanılan süreç, PUKÖ modeline dayanır [4],[101].

"Planla – Uygula - Kontrol Et - Önlem Al" (PUKÖ) modeli olarak bilinen model, bu standart'ta benimsenen tüm BGYS süreçlerine uygulanabilir. Şekil 3.11'de bir BGYS'nin bilgi güvenlik gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve süreçler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını (örneğin, yönetilen bilgi güvenliği) nasıl ürettiğini gösterir.



Şekil 3.12 BGYS Süreçlerine Uygulanan PUKÖ Modeli

3.2.8 BGYS'nin Kurulması ve Yönetilmesi (Md.4.2)

ISO 27001 standardına uygun olarak BGYS kurulması sürecinin aşamaları Şekil 3.12'de gösterilmektedir. BGYS'nin kurulumuna ilişkin bu adımların detayları söz konusu standarda göre 2.2.1. numaralı başlık altında sunulmuştur.

Şekil 3.13 ISO 27001 Sürecinin Aşamaları

3.2.8.1 BGYS'nin Kurulması (Md.4.2.1)

İşletmeler, BGYS kurmak için temel olarak aşağıdaki faaliyetleri gerçekleştirmek durumundadırlar. Bunlar:

- İşin, kuruluşun, yerleşim yerinin, varlıklarının ve teknolojisinin özelliklerine göre BGYS kapsamı ve sınırlarının tanımlanması gerekmektedir.

- İşletme özelliklerine göre aşağıdaki özelliklere sahip bir BGYS politikası tanımlaması gereklidir. Bu politika oluşturulurken aşağıdaki hususlara dikkat edilmelidir. Dolayısı ile politikalar:

• Amaçlarını ortaya koymak için bir çerçeve içeren ve bilgi güvenliğine ilişkin bir eylem için kapsamlı bir yön kavramı ve prensipleri içermeli,

• İş ve yasal ya da düzenleyici gereksinimleri ve sözleşmeye ilişkin güvenlik yükümlülüklerini dikkate almalı,

• BGYS kurulumu ve sürdürülmesinin yer alacağı stratejik kurumsal ve risk yönetimi bağlamını düzenlemeli,

• Risk değerlendirme yapısının tanımlanacağı kriterleri kurmalı,

• Yönetim tarafından kabul edilmiş, olmalıdır.

- Risk değerlendirmesine ilişkin sistematik bir yaklaşım tanımlanmalıdır. İşletmeler, BGYS'ye ve tanımlanmış iş bilgisi güvenliğine, yasal ve düzenleyici gereksinimlere uygun bir risk değerlendirme yöntemini tanımlanmalıdır. Riskleri kabul edilebilir bir seviyeye indirmek için, BGYS politika ve amaçlarını ortaya koymalı ve kabul edilebilir riskler için seviye ve kriterler belirlenmelidir.

- Kuruluşlar tarafından riskler tanımlanmalıdır. Bunlar kısaca:

• BGYS kapsamındaki varlıkları ve bu varlıkların sorumluları tanımlanmalı,

• Bu varlıklar için var olan tehditleri tanımlanmalı,

• Tehditlerin fayda sağlayabileceği açıklıklar belirlenmeli,

• Gizlilik, bütünlük ve kullanılabilirlik kayıplarının varlıklar üzerinde olabilecek etkileri tanımlanmalıdır.

- Riskler çözümlenmeli ve derecelendirilmelidir. İkinci bölümde anlatılan risk değerlendirme yöntemleri göz önüne alınarak:

• Varlıkların gizliliğine, bütünlüğüne ya da kullanılabilirliğine ilişkin oluşan kayıpların olası sonuçlarını dikkate alarak, bir güvenlik başarısızlığından kaynaklanabilecek iş hasarlarını neler olabileceği belirlenmeli,

• Mevcut tehditler, açıklıklar ve bu varlıklarla ilişkili tesirler ışığında oluşan bu gibi güvenlik başarısızlıklarının gerçekçi olasılığını ve gerçekleştirilen mevcut kontroller değerlendirilmeli,

• Risk seviyelerinin tahmin edilmeli

• Riskin kabul edilebilir mi olduğunu yoksa risk değerlendirme maddesinde saptanan

kriterler kullanılarak iyileştirme mi gerektirdiğine karar verilmesi gereklidir.

- Risk iyileştirmesi için seçenekler tanımlanmalı ve değerlendirilmelidir. Olası eylemler aşağıdakileri içermektedir:

• Uygun kontrollerin uygulanması,

• Kuruluşun politikasını ve risk kabul kriterlerini açıkça karşılaması şartıyla, bilerek ve nesnel olarak risklerin kabul edilmesi,

• Risklerden kaçınma,

• Bağlı iş risklerini diğer taraflara, örneğin, sigorta şirketlerine, tedarikçilere aktarmaktır.

- Risk iyileştirmesi için kontrol amaçları ve kontroller seçilmelidir. Uygun kontrol amaçları ve kontroller, risk değerlendirme ve risk iyileştirme süreçlerinde tanımlanan gereksinimleri karşılamak için seçilmeli ve gerçekleştirilmelidir.

- Sunulan artık risklere ilişkin yönetim onayı alınmalıdır.

- BGYS'yi gerçekleştirmek ve işletmek için yönetim yetkilendirmesi alınmalıdır.

- Uygulanabilirlik Bildirgesi hazırlanmalıdır. Seçilen kontrol amaçları ve kontroller ve bunların seçilme nedenleri Uygulanabilirlik Bildirgesi dökümanında yer almalıdır. Aynı şekilde seçilmeyen kontrollere ilişkin seçilmeme nedenlerine de yer verilmelidir.

3.2.8.2 BGYS'nin Gerçekleştirilmesi ve İşletilmesi (Md.4.2.2)

Kuruluşların, BGYS'yi gerçekleştirebilmek ve işletebilmek için gerekli faaliyetleri şu şekilde sıralanabilir:

- Bilgi güvenlik risklerini yönetmek için uygun yönetim eylem, sorumluluklar ve öncelikleri tanımlayan bir risk iyileştirme planı hazırlamalı,

- Finansman değerlendirmesi, roller ve sorumlulukların tahsisini içeren, tanımlanan kontrol amaçlarına ulaşmak için risk iyileştirme planı uygulanmalı,

- Kontrol amaçlarını karşılamak için seçilen kontroller uygulanmalı,

- Seçilen kontrollerin etkinliğinin nasıl ölçüleceği ve daha sonra bu ölçüm sonuçlarının nasıl kullanılacağı tanımlanmalı,

- Eğitim ve farkında olma programları gerçekleştirilmeli,

- BGYS'nin işleyişini yönetmeli,

- BGYS'nin kaynaklarını yönetmeli,

- Güvenlik olaylarını anında saptayabilme ve yanıt verebilme kabiliyetine sahip prosedür ve kontroller gerçekleştirilmelidir.

3.2.8.3 BGYS'nin İzlenmesi ve Gözden Geçirilmesi (Md.4.2.3)

Kuruluşlar BGYS'ni izlenmesi ve gözden geçirilmesi için aşağıdakileri gerçekleştirmek durumundadır:

- İzleme prosedürlerini ve diğer kontrolleri aşağıda belirtilen amaçlara ulaşmak için yürütülmelidir. Bunlar:

• İşleme sonuçlarındaki hataları anında saptamak,

• Denenen ve başarılı olan güvenlik kırılmalarını ve ihlal olaylarını anında tanımlamak,

• Yönetimin, kişilere devredilen ya da bilgi teknolojisince gerçekleştirilen güvenlik faaliyetlerinin beklenen biçimde çalışıp çalışmadığını belirleyebilmesini sağlamak,

• Güvenlik olaylarını saptama ve belirteçler kullanarak güvenlik ihlal olaylarını engellemeye yardım etmek,

• Bir güvenlik kırılmasını çözmek için alınan önlemlerin etkili olup olmadığını karar vermektir.

- Güvenlik denetimlerinin, olaylarının, önerilerinin sonuçlarını ve tüm ilgili taraflardan geri bildirimleri dikkate alarak BGYS'nin (güvenlik politikaları ve amaçlarını karşılama, ve güvenlik kontrollerini gözden geçirme dahil) etkinliği düzenli olarak gözden geçirilmelidir.

- Güvenlik gereksinimlerinin karşılandığını doğrulamak için kontrollerin etkinliğini ölçülmelidir.

- Oluşacak değişiklikleri dikkate alarak, artık risklerin ve kabul edilebilir risklerin seviyesi gözden geçirilmelidir.

- Planlanan aralıklarda iç BGYS denetimleri gerçekleştirilmelidir.

- BGYS'nin yönetim tarafından düzenli olarak gözden geçirilmesi üstlenilmelidir.

- İzleme ve gözden geçirme faaliyetlerindeki bulgular dikkate alınarak güvenlik planları güncelleştirilmelidir.

- BGYS etkinliğinde ya da performansında bir etkisi olabilecek eylemleri ve olayları kaydedilmelidir.

3.2.8.4 BGYS'nin Sürekliliği ve İyileştirilmesi (Md.4.2.4)

İşletmeler, süreklilik sağlama ve iyileştirme amacı ile belirli aralıklarla aşağıdaki faaliyetleri yapmak durumundadırlar:

- BGYS'deki tanımlanan gelişmeleri gerçekleştirmelidirler.

- Uygun düzeltici ve engelleyici önlemler alınmalıdır. Diğer kuruluşların ve kendisine ait güvenlik deneyimlerinden alınan dersler uygulanmalıdır.

- Sonuçları ve eylemleri bildirilmeli ve ilgili tüm taraflarla mutabık kalınmalıdır.

- İyileştirmelerin tasarlanan amaçlara ulaşması sağlanmalıdır.

3.2.9 Dökümantasyon Gereksinimleri (Md.4.3)

Dökümantasyon yönetim kararlarının kayıtlarını içermeli, eylemlerin yönetim kararları ve politikalarına izlenebilir olmasını ve kaydedilen sonuçların yeniden üretilebilir olması sağlanmalıdır. Tüm dökümantasyon BGYS politikası gereğince kullanılabilir yapılmalıdır. BGYS dökümantasyonu aşağıdakileri kapsamalıdır:

- BGYS politikası ve kontrol amaçlarının dökümante edilmiş ifadeleri,

- BGYS kapsamını,

- BGYS'yi destekleyici prosedür ve kontrolleri,

- Risk değerlendirme metodolojisinin bir tanımı,

- Risk değerlendirme raporu,

- Risk iyileştirme planı,

- Kuruluş tarafından, bilgi güvenliği süreçlerinin etkin planlanlanmasını, işlemesini ve

kontrolünü sağlamak için gereksinim duyulan dökümante edilmiş prosedürleri,

- İhtiyaç duyulan kayıtları,

- Uygulanabilirlik Bildirgesi.

3.2.9.1 Dökümanların Kontrolü (Md.4.3.2)

BGYS tarafından talep edilen dökümanlar korunur ve kontrol edilir. Dökümante edilmiş bir prosedür, aşağıdakilere ihtiyaç duyan yönetim eylemlerini belirlemek için kurulmalıdır:

- Yayınlanmadan önce dökümanları uygunluk açısından onaylama,

- Gerektiğinde dökümanları gözden geçirme, güncelleme ve tekrar onaylama,

- Döküman değişikliklerinin ve mevcut revizyon durumunun tanınmasını sağlama,

- İlgili dökümanların en son sürümlerinin kullanım noktalarında kullanılabilir olmasını sağlama,

- Dökümanların okunaklı ve hazır olarak tanınabilir olmasını sağlama,

- Dış kaynaklı dökümanların tanınmasını sağlama,

- Döküman dağıtımının kontrol edilmesini sağlama,

- Yürürlükte olmayan dökümanların istenmeden kullanımını engelleme,

- Eğer herhangi bir amaç için tutuluyorsa, bu dökümanlara uygun bir kimlik uygulanmasını kapsar.

3.2.9.2 Kayıtların Kontrolü (Md.4.3.3)

Kayıtlar, gereksinimlere uygun olduğuna ve BGYS'nin etkin işlediğine dair kanıtlar sağlamak için kurulmalı ve sürdürülmelidir. Kayıtlar korunmalı ve kontrol edilmelidir. BGYS, ilgili her yasal gereksinimi dikkate alır. Kayıtlar, okunabilir, hazır olarak tanınabilir ve geri alınabilir halde tutulur. Kayıtların tanınması, saklanması, korunması, geri alınması, tutulma ve düzenleme zamanları için gereken kontroller yazılı hale getirilmelidir. Kayıtlar, süreç performansına ve BGYS ile ilgili tüm güvenlik ihlal

olaylarının oluşumlarına ilişkin tutulmalıdır. Kayıtlara ilişkin örnek olarak, ziyaretçi defterleri, denetim kayıtları ve erişim yetkilendirme formları verilebilir [4],[101].

3.2.10 Yönetim Sorumluluğu (Md.5)

Yönetim desteği bilgi güvenliği programının olmazsa olmaz unsurudur. Güvenlik mesajlarının etkili olabilmeleri için en yukarıdan desteklenmeleri gereklidir. Pek çok yönetici bu tür çalışmalar konusunda desteğini dile getirse de, desteğin gerçekleşmesi söylemek kadar kolay olmamaktadır. Bu durum yöneticilerin kendi iş ve sorumluluklarının bulunmasından kaynaklanmaktadır [102].

BGYS kurulumunda yönetim sorumluluğu, yönetimin bağlılığı ve kaynak yönetim başlıkları altında açıklanmaya çalışılacaktır.

3.2.10.1 Yönetimin Bağlılığı (Md.5.1)

Yönetim BGYS'nin kurulumuna, gerçekleştirilmesine, işletimine, izlenmesine, gözden geçirilmesine, sürdürülebilirliğine ve iyileştirilmesine olan bağlılığını aşağıdaki faaliyetleri gerçekleştirerek kanıtlamalıdır:

- Bir bilgi güvenlik politikası kurarak,

- Bilgi güvenlik amaçlarının ve planlarının kurulmasını sağlayarak,

- Bilgi güvenliği için rolleri ve sorumlulukları kurarak,

- Kuruluşa, bilgi güvenlik amaçlarını karşılamanın ve bilgi güvenlik politikalarına uyumun önemini, yasaya karşı sorumluluklarını ve sürekli iyileştirmeye olan gereksinimi bildirerek,

- BGYS'yi geliştirmek, gerçekleştirmek, işletmek ve bakımını yapmak için yeterli kaynak sağlayarak,

- Kabul edilebilir risk seviyesini belirleyerek,

- İç BGYS denetimlerini sağlayarak,

- Yönetimin BGYS incelemelerini yürüterek.

3.2.10.2 Kaynak Yönetimi (Md.5.2)

BGYS gerçekleştirmede yönetim sorumluluğu kapsamında yer alan kaynak yönetim kapsamını, kaynakların belirlenmesi, sağlanması ve uygun yeterlilikte personel için gereken faaliyetleri içermektedir. Bu faaliyetleri sırası ile inceleyecek olursak :

Kaynakların Sağlanması (Md.5.2.1.): Kuruluş, BGYS faaliyetlerinin planlandığı şekilde sürdürülmesine yönelik aşağıdaki faaliyetler için gereken kaynaklara karar vermeli ve bunları yürütmelidir.

- Bir BGYS kurmak, gerçekleştirmek, işletmek, sürdürmek ve iyileştirmek,

- Bilgi güvenlik prosedürlerinin iş gereksinimlerini desteklemesini sağlamak,

- Yasal ve düzenleyici gereksinimleri ve sözleşmeden doğan güvenlik yükümlülüklerini tanımlamak ve ifade etmek,

- Gerçekleştirilen tüm kontrollerin doğru uygulamalarıyla, uygun güvenliği sürdürmek,

- Gerektiğinde incelemeleri yürütmek ve bu gözden geçirme sonuçlarına uygun olarak hareket etmek,

- İhtiyaç olduğunda, BGYS etkinliğini geliştirmektir.

Eğitim, Farkında Olma ve Yeterlilik (Md.5.2.2.): İşletmeler, ilgili tüm personelin bilgi güvenliği faaliyetlerinin yarar ve öneminin ve BGYS amaçlarına ulaşılmasına nasıl katkı sağlayacağının farkında olmasını sağlamalıdır. Bu amaçla kuruluşlar;

- BGYS'yi etkileyecek işleri gerçekleştiren personel için gerekli yeterlilikleri belirlemeli,

- Yeterli eğitimi sağlama ve, gerekirse, bu ihtiyaçları karşılamak üzere yeterli personel istihdam etmeli,

- Alınan önlemlerin etkinliğini değerlendirmeli,

- Eğitime, öğretime, becerilere, deneyime ve niteliklere ilişkin kayıtları tutmalıdır.

3.2.11 BGYS İç Denetimleri (Md.6)

Kuruluş, BGYS kontrol amaçlarının, kontrollerinin ve prosedürlerinin standardın gereklerine, tanımlanan bilgi güvenliği gereksinmelerine uyup uymadığını belirlemek için, planlanan aralıklarla iç denetimler yürütmelidir.

Bir denetleme programı, bir önceki denetim sonuçlarının yanı sıra denetlenecek süreçlerin ve alanların durumu ve önemi dikkate alınarak planlanmalıdır. Denetim kriterleri, kapsamı, sıklık ve yöntemler tanımlanmalıdır. Denetmenlerin seçiminde ve denetimlerin gerçekleştirilmesinde, denetim sürecinin nesnel ve tarafsız olarak işlemesi sağlanmalıdır. Denetmenler kendi çalışmalarını denetlememelidirler.

Denetimlerin planlanması ve yürütülmesinde ki ve sonuçların raporlanması ve kayıtların tutulmasında ki sorumluluklar ve gereksinimler, yazılı hale getirilmiş bir prosedür içinde tanımlanır.

Denetlenen alandan sorumlu olan yönetim, saptanan uygunsuzlukların ve bunların nedenlerinin giderilmesi için, gereksiz gecikmeler olmaksızın önlemlerin alınmasını sağlamalıdır. İzleme faaliyetleri, alınan önlemlerin doğrulanmasını ve doğrulama sonuçlarının raporlanmasını içermelidir.

3.2.12 BGYS'yi Yönetimin Gözden Geçirmesi (Md.7)

Yönetim, kuruluşun BGYS'sini planlanan aralıklarla, sürekli uygunluğunu, doğruluğunu ve etkinliğini sağlamak için gözden geçirmelidir. Bu gözden geçirme, güvenlik politikası ve güvenlik amaçları dahil BGYS'nin iyileştirilmesi ve gereken değişikliklerin yapılması için fırsatların değerlendirilmesini de içermelidir. Gözden geçirme sonuçları açıkça yazılı hale getirilmeli ve kayıtlar tutulup saklanmalıdır. Bu nedenden dolayı, gözden geçirme faaliyetlerinin kapsamı gözden geçirme girdisi ve gözden geçirme çıktısı başlıkları altında incelenecektir.

3.2.12.1 Gözden Geçirme Girdisi (Md.7.2)

BGYS kapsamında gerçekleştirilecek yönetimin gözden geçirme faaliyetleri için gerekli girdiler, aşağıdakileri içermelidir. Bunlar:

- BGYS denetimleri ve gözden geçirmelerinin sonuçları,

- İlgili taraflardan edinilen geri bildirimler,

- Kuruluşta BGYS'nin performansını ve etkinliği artırmak için kullanılabilecek teknikler, ürünler ya da prosedürler,

- Önleyici ve düzeltici faaliyetlerin durumu,

- Etkinlik ölçümlerinin sonuçları,

- Önceki risk değerlendirilmesinde uygun olarak ifade edilmeyen açıklıklar ya da tehditler,

- Önceki yönetim gözden geçirmelerinden izleme eylemleri,

- BGYS'yi etkileyebilecek herhangi bir değişiklik,

- İyileştirme için önerilerden, oluşmaktadır.

3.2.12.2 Gözden Geçirme Çıktısı (Md.7.3)

Bir BGYS yönetim gözden geçirme çıktıları, aşağıdakilerle ilgili her kararı ve eylemi içermelidir.

- BGYS etkinliğini iyileştirmek,

- Risk değerlendirme ve risk işleme planını güncelleştirmek,

- Gerektiğinde, BGYS üzerinde etkisi olabilecek iç ya da dış olaylara karşılık vermek için bilgi güvenliğini etkileyen prosedür ve kontrol değişiklikleri,

- Kaynak ihtiyaçları,

- Kontrollerin etkinliğinin ölçümünde iyileşme faaliyetleridir.

3.2.13 BGYS İyileştirme (Md.8)

BGYS süreçlerine uygulanan PUKÖ modelinin "Önlem Al" kapsamında, BGYS'nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici eylemlerin gerçekleştirilmesi gerekmektedir.

3.2.13.1 Sürekli İyileştirme (Md.8.1)

Kuruluş, bilgi güvenlik politikasını, güvenlik amaçların, denetim sonuçlarını, izlenen olayların analizini, düzeltici ve önleyici faaliyetleri ve yönetim gözden geçirmelerini kullanarak BGYS etkinliğini sürekli iyileştirmelidir.

3.2.13.2 Düzeltici Faaliyetler (Md.8.2)

Kuruluş tekrarları engellemek için, BGYS gereksinimleriyle uygunsuzlukların nedenlerini gidermek üzere önlemler almalıdır. Düzeltici faaliyetler için yazılı hale getirilmiş prosedür aşağıdaki gereksinimleri tanımlamalıdır:

- Uygunsuzlukları tanımlamak,

- Uygunsuzlukların nedenlerini belirlemek,

- Uygunsuzlukların tekrarlanmamasını sağlamak için ihtiyaç duyulan faaliyetleri değerlendirmek,

- Gereken düzeltici faaliyetleri belirlemek ve gerçekleştirmek,

- Gerçekleştirilen faaliyetlerin sonuçlarını kaydetmek,

- Gerçekleştirilen düzeltici faaliyetleri gözden geçirmek, olarak sıralanabilir.

3.2.13.3 Önleyici Faaliyetler (Md.8.3)

TS ISO/IEC 27001:2005 ‘ e göre ; Kuruluş tekrar ortaya çıkmalarını önlemek için, BGYS gereksinimleriyle olası uygunsuzlukların nedenlerini gidermek üzere alınacak önlemleri belirlemelidir. Gerçekleştirilen önleyici faaliyetler, olası sorunların yapacağı etkiye uygun olmalıdır. Önleyici faaliyetlerin önceliği, risk değerlendirme sonuçlarına bağlı olarak belirlenir. Önleyici faaliyetler için yazılı hale getirilmiş prosedür aşağıdaki gereksinimleri tanımlamaktadır:

- Olası uyumsuzlukları ve bunların nedenlerini belirlemek,

- İhtiyaç duyulan önleyici faaliyetleri belirlemek ve gerçekleştirmek,

- Gerçekleştirilen faaliyetlerin sonuçlarını kaydetmek,

- Gerçekleştirilen önleyici faaliyetleri gözden geçirmek,

- Değişen riskleri tanımlamak ve dikkatin önemli derecede değişen riskler üzerinde yoğunlaştıracak önleyici faaliyet gereksinimlerini, kapsamalıdır [4],[101].

BÖLÜM 4

ABC A.Ş' DE ISO/IEC 27001 STANDARDI ÇERÇEVESİNDE BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ UYGULAMASI

4.1 Uygulama Çalışmasının Amacı

Amaç uygulmanın gerçekleştirildiği ABC Grup bünyesinde bulunan, ABC şirketinin iç ve dış süreçlerinde şirkete özel olan, şirketin kurumsal hafızasını oluşturan ve diğer şirketlere karşı rekabet avantajı oluşturan arşivlerde saklanan, server'larda tutulan veya iletişim ağı gibi herhangi bir yerde saklanan her türlü bilginin korunmasıdır.

Bilgi ve veri'lerin bilgi sistemleri server'larında tutulması ve güvenliğinin sağlanması tek başına yeterli değildir. Bununla birlikte bu bilgilerin bulunduğu sunucuların bulunduğu ortamların güvenlik altında olması ve ortam yeterliliğinin gerektirdiği şartların sağlanması önemlidir. Bilgi Güvenliği Yönetim Sistemi kurulumu çalışması ile şirket çalışanlarını ve şirketin kendisini, bilerek yada bilmeyerek yasalara aykırı davranmaktan ya da zarar verici durumlardan korumak amaçlanmaktadır.

Bilgi güvenliğinin sağlanması amacı ile şirket varlıklarını tehdit eden risklerin belirlenmesi , risk derecelendirilmesinin ve risk sorumlularının belirlenmesi , önceden tanımlanmış veya tanımlanmamış riskler karşısında alınacak aksiyonların belirlenmesi önemlidir. Tüm bunları sağlamak amacıyla BGYS (Bilgi Güvenliği Yönetim Sistemi) aşağıdaki hedefler doğrultusunda tasarlanmalıdır.

-Her türlü bilgi, belge ve iletişimin yetkisiz kisilerin ve üçüncü şahısların ellerine

geçmesini engellemek amacıyla gizliliklerinin sağlanması,

-Kurumsal dokümanların ve bilgilerin personel hataları, virüsler, arka kapı solucanları ve

üçüncü şahıslar tarafından değiştirilmesi nedeniyle verilerin bütünlüklerinin bozulmasının engellenmesi,

-Kurumsal doküman ve bilgilere , doğal felaketler sırasında bile sorunsuz ve zamanında erişilebilmesi ,

-Uygun risk yönetim politiasının belirlenmesi ve risk izleme sisteminin kurulması , risk tedbirlerinin alınması.

Belirlenen bu hedeflere ulaşılabilmesi için ABC Şirketin'de organizasyonun önemli bir parçası olan Bilgi Teknolojileri bölümü içerisinde BGYS kurulumuna yönelik olarak bir BGYS ekibinin oluşturulması , araçları ve cihazları dahilinde tutulan bilgilerin güvenliğinin sağlanması için gerekli işlemlerin belirlenmesi, klavuz, bilgilendirme dokümanları ve prosedürleri oluşturulması ile üretilecek bilgi, yazılım kodları ve dökümanların güvenliği sağlanabilecektir.

Bu proje kapsamlında, kullanıcı istekleri doğrultusunda tanımlanan sistemin, tasarlanarak gerekli yazılım, donanım ve doküman üretimini hedeflemektedir.

Bu uygulamadan beklenen amaç, BGYS uygulama nedeni, risk yönetiminin şirketlere nasıl uygulanabileceği, BGYS'nin nelerden oluştuğu ve ISO 27001 standardının şirketler tarafından BGYS olarak seçilme nedenine yönelik dört temel araştırma sorularına cevap bulmak şeklinde özetlenebilir.

Bu çalışma ile ABC A.Ş' nin portföyünde yer alan kurumsal ve bireysel müşterilerine ait her türlü bilginin gizliliğini, bütünlüğünü ve erişilebilirliği sağlamak ve gelecekte ABC A.Ş. ve grup şirketlerinde ISO 27001 gereklerine uygun bir BGYS kurulumuna esas teşkil edecek olan altyapının kurulmasına yönelik hazırlıklar yapılmış olacaktır. Şirketin uluslar arası ortaklarının güvenlik denetim ilkelerinde gerekli koşul olarak istenilen ISO 27001 gerekleri sağlanmıs olacaktır, ilave olarak ABC A.Ş' nin portföyünde yer alan kurumsal ve bireysel müşterileri , kendilerine ait bilgilerin güvende tutulacağı konusundaki taahhütten dolayı kendilerini güvende hissedeceklerdir.

ABC A.Ş kurumsal değerlerini, yatırımlarını ve hedeflerini sürdürürken, sigorta sektöründe rekabet avantajı ve bilgi güvenliğini sağlayacak, bilgilerin korunabilmesi için ortaya konması gereken süreç ve kontrollerin şirket içinde yerleştirilmesi ve hayata

geçirilmesi sağlanacaktır.

4.2 Şirket Hakkında Genel Bilgiler

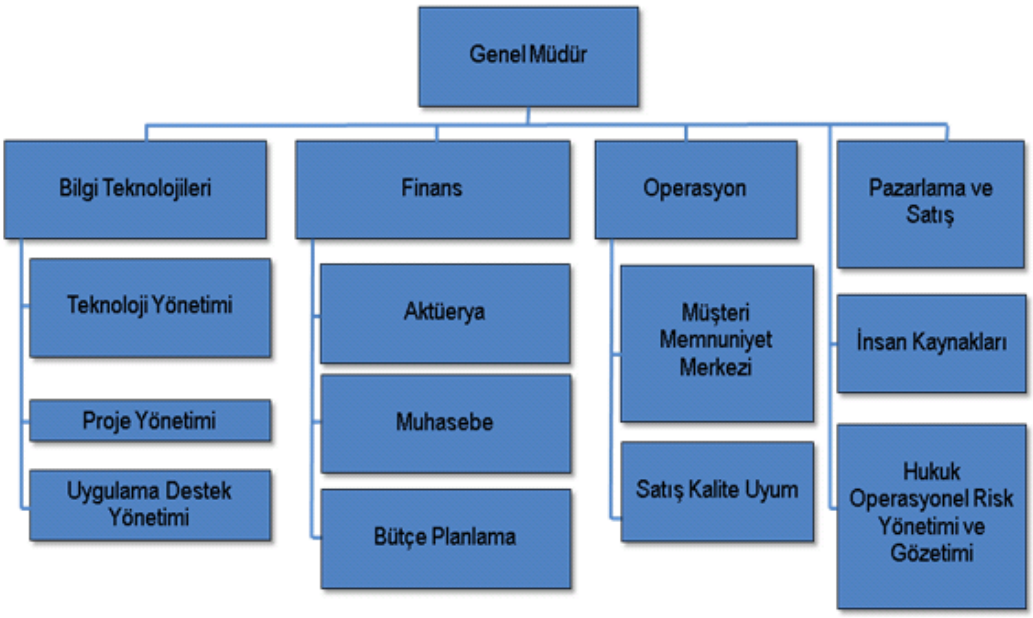
ABC A.Ş. %50 yurtdışı ortaklıkla kurulmuş olup finans ve sigorta sektöründe hizmet gösteren Türkiye'nin önde gelen ilk 5 sigorta şirketi arasında yer almaktadır. Türkiye'de çalışan sayısı 2000 kişidir. Ortalama 90 milyar dolar ciro ve 700 milyar dolardan fazla fon büyüklüğü ile ortaklarının güçlü sermaye yapısı ortakların dünya genelinde çalışan sayısının toplamda 100.000 kişiye yakın olması şirketin dünyadaki bilirliniğini arttırmaktadır ve markanın dünyadaki ilk 100 şirket arasında yer almasını sağlamaktadır.

380 kurum müşterisi ve yaklaşık 400 bin kadar bireysel müşterisi bulunan ABC A.Ş. , elementer sigorta, hayat sigortaları ve hayat dışı ürünler ile konusunda müşterilerine hizmet vermektedir.

4.2.1 Şirketin Vizyonu ve Misyonu

- Şirketin Vizyonu: Müşterilerimizin dinamik yatırım ve birkim ihtiyaçlarına etkin finansal çözümler üreten, güvenilir ve sektörün örnek alınan şirketi olmak.
- Şirketin Misyonu: Müşterilerimize kaliteli bir hizmet sunarak, müşterilerimiz ve çalışanlarımızın tercih ettiği güvenilir bir şirket olmak.

4.2.2 Şirketin Organizasyon Yapısı



Şekil 4.1 ABC A.Ş. Genel Organizasyon Yapısı

4.2.3 Kullanılan Standartlar

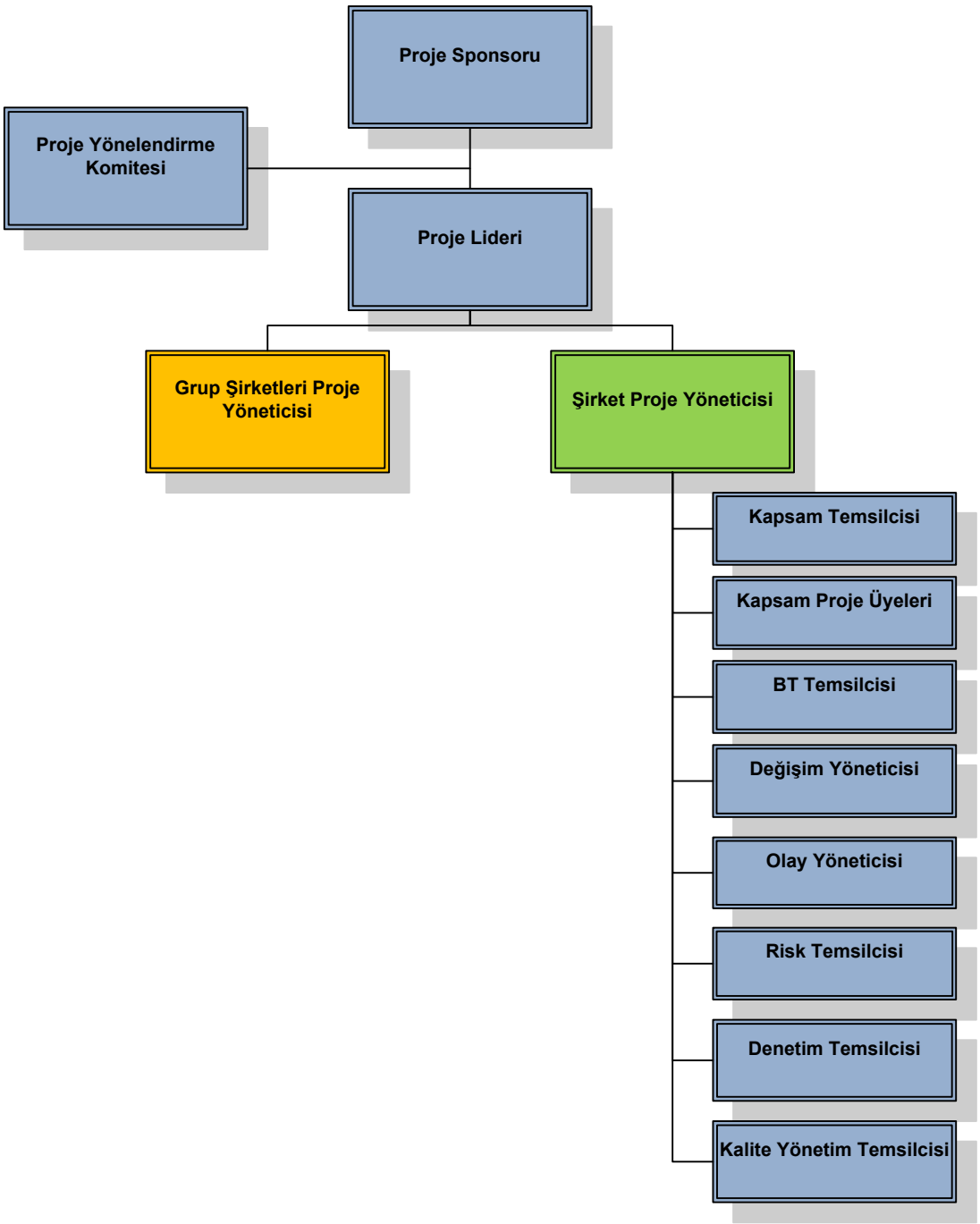
-TS-EN ISO 9001:2008 Üretim, Tesis ve Hizmette Kalite Güvencesi Modeli Kalite Sistem Standardı

-TS-EN ISO 10002 Müşteri Şikayetleri Yönetimi Kalite Sistem Standardı

4.3 Bilgi Güvenliği Yönetim Sistemi Uygulaması ve Yönetsel Faaliyetler

Proje kapsamında , varlıkların mevcut ve muhtemel tehditlere karsı güvenliğini sağlamak ve dış saldırılar, personel veya doğal nedenlerle ortaya çıkan risklerin gerçekleşmesi nedeniyle olusacak maddi ve manevi kayıpları en aza indirmek, yapılan yatırımların geri dönüşünü en üst seviyeye çıkarmak, temel güvenlik gereksinimleri olan Gizlilik, Bütünlük, Erişilebilirlik gereksinimlerinin proje kapsamında karşılanmasını garanti etmek ve mevcut tehditlerden kaynaklanan risklerin kabul edilebilir seviyede tutulmasını sağlamak amacıyla BGYS kurulumu ve en iyi uygulama pratikleri ile ilgili vurgulanan gereksinimleri karşılaması öngörülen aşağıda sıralanan yönetsel önlemler alınmıştır.

4.3.1 Bilgi Güvenliği Yönetim Sistemi Organizasyonu



Şekil 4.2 BGYS Proje Yönetimi Organizasyon Yapısı

4.3.1.1 Roller ve Sorumluluklar

- **Proje Sponsoru**

Rolün Sahibi , Şirkette yer alan en üst düzey yönetici

Sorumluluklar ,

- Proje için belirlenen hedeflere ulaşılmasını sağlamak amacıyla gerekli üst yönetim desteğini vermek
- Proje için gerekli kaynak düzenlemeleri onaylamak

➢ **Proje Yönlendirme Komitesi**

Rolün Sahibi, Şirket üst yönetiminden bir temsilci, kapsam dahilindeki en üst düzey yönetici, BT Yöneticisi, Grup Şirketleri Bilgi Güvenlik Ofis Yöneticisi ve Proje Yönetici'leri

Sorumluluklar ,

- BGYS'yi kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için yeterli kaynağı sağlamak
- Bilgi Güvenliği amaçlarını karşılamanın ve Bilgi Güvenliği politikalarına uyumun önemini, yasaya karşı sorumluluklarını ve sürekli iyileştirmeye olan gereksinimi bildirmek
- Riskleri kabul etme ölçütlerini ve kabul edilebilir risk seviyelerini belirlemek
- BGYS'nin yönetim gözden geçirmelerini gerçekleştirmek

➢ **Proje Lideri**

Rolün Sahibi, Şirket üst yönetiminde yer alan ve Bilgi Teknolojileri bölümünün bağlı olduğu en üst düzey yönetici

Sorumluluklar,

- Projeyi desteklemek ve projenin hedef ve amaçlarıyla örtüşen gelişmeleri ve yönetimin stratejik durum değerlendirmesini yapmak
- Projenin gelişimi ve belirlenen hedeflerin gerçekleştirilmesi amacıyla, planları ve metodları gözden geçirmek ve onaylamak
- Proje Yöneticisi ve ekibini liderlik ve koçluk açısından desteklemek
- Grup Şirketleri Bilgi Güvenlik Ofisi ile şirket arasında, projeye ait olan tüm

problemler ve riskler için ilk ve tek temas noktası olarak hareket etmek

- Projede yer alan tüm bölümler tarafından mutabık kalınan resmi proje planını gözden geçmek ve onaylamak
- Proje ile ilgili bütçe ve maliyeti yönetmek.

➢ **Grup Şirketleri Proje Yöneticisi**

Rolün Sahibi, Grup Şirketleri Bilgi Güvenliği Ofisi'nden bir kişi

Sorumluluklar,

- Şirket Proje Yöneticisi ile gerekli koordinasyonu sağlamak ve yönlendirmek
- Proje ile ilgili tüm bilgi ve birikimini ekip ile paylaşmak
- Proje için belirlenen çerçeve dokümanları, şirket proje ekibi ile paylaşmak
- Çerçeve dokümanların şirket içinde oluşturulmasını sağlamak ve bu konuda destek vermek
- Proje ile ilgili belirlenen raporlama ihtiyaçlarının giderilmesine destek olmak

➢ **Şirket Proje Yöneticisi**

Rolün Sahibi, Şirketin tüm süreçlerine hakim, iletişim becerisi yüksek, ekip yönetme kabiliyeti olan ve daha önce sistem kurma çalışmalarında bulunmuş, tercihen BT ve ISO standartları konusunda bilgi sahibi ve şirket BT Yöneticisi'ne raporlayan kişi

Sorumluluklar

- ABC Grup Şirketleri Proje Yöneticisi ile gerekli koordinasyonu sağlamak ve proje ekibini aktif olarak yönetmek
- Proje boyunca oluşturulması gereken tüm dokümanların (politika, prosedür vb.) yaratılması için gerekli koordinasyonu sağlamak
- Tüm oluşturulacak dokümanların ihtiyaçlarla aynı doğrultuda olduğunu temin etmek, kalite kontrolünün yapılmasını sağlamak
- Proje Lideri ve Proje Yönlendirme Komitesi ile gerekli iletişimi ve paylaşımı

sağlamak

- Gerekli raporları ve toplantı notlarını yaratmak ve ilgili tüm proje üyeleri ile vaktinde paylaşmak
- Proje boyunca oluşabilecek problemleri ve riskleri yönetmek, gerektiği durumlarda Proje Lideri'ni ve Proje Yönlendirme Komitesi'ni bilgilendirmek
- Proje planına göre gelişimi izlemek ve kontrol etmek
- Gelişmeyi (İlerlemeyi) yönetmek ve raporlamak
- Bilgi Güvenliği konusunda çalışanların farkındalığını arttırmaya yönelik faaliyetleri koordine etmek

➢ **Kapsam Temsilcisi**

Rolün Sahibi, Projenin yapılacağı kapsam içinde çalışan ve kapsam içindeki süreçlere hakim, iletişim ve koordinasyon becerisine sahip kişi

Sorumluluklar,

- Kapsam içinde yer alan süreç sahipleri ile haberleşmeyi koordine etmek ve Proje Yöneticisi'ne bu konuda destek olmak
- Proje planı hazırlanırken, kapsam dahilindeki kısıtları paylaşmak ve proje ekibini bu konuda güncel tutmak
- Kapsam alanı ile ilgili risk ve problemler için çözüm oluşturulmasına destek olmak
- İhtiyaç dahilinde kapsam için geliştirilecek dokümantasyonun oluşturulmasını sağlamak
- Gerektiği durumlarda kapsam içindeki en üst düzey yönetici ile bilgi paylaşımını sağlamak

➢ **Kapsam Proje Üyeleri**

Rolün Sahibi, Projenin yapılacağı kapsam içindeki süreç sahipleri ve bağlı çalışan kişi(ler)

Sorumluluklar,

- Belirlenen kapsam için onaylanmış proje planına uymak ve bunun için belirlenen çalışmalara katılmak
- Proje planını etkileyecek her türlü risk ve problemi Proje Yöneticisi ile zamanında paylaşmak
- Varlık ve Risk Değerlendirme seanslarına katılmak
- BGYS projesi ile ilgili farkındalık eğitimlerine katılmak

➢ **Bilgi Teknolojileri Temsilcisi**

Rolün Sahibi, Şirket BT süreçlerine hakim, BT bölümünden yönetici düzeyinde bir kişi

Sorumluluklar,

- Şirket BT yaklaşımını ve stratejisini proje ekibi ile paylaşmak
- BT ile ilgili yazılacak tüm dokümanların oluşturulmasını sağlamak
- Hızlı kazanımlar ve riskle ilgili aksiyonların gerçekleştirilmesi için BT yönetimi ile koordinasyonu sağlamak
- Proje planını etkileyecek her türlü risk ve problemi Proje Yöneticisi ile zamanında paylaşmak

➢ **Değişim Yöneticisi**

Rolün Sahibi, Şirket süreçlerine hakim ve şirket genelinde yapılacak değişiklikleri (Bilgi Güvenliği açısından) yönetecek, şirket yönetici seviyesinden bir kişi

Sorumluluklar,

- Değişim Yönetimi ile ilgili dokümanların / kayıtların oluşturulmasını ve bu konuda gerekli koordinasyonu sağlamak
- İlgili kişiler için, değişim yönetiminin farkındalığını arttırmak

- **Olay Yöneticisi**

Rolün Sahibi, Bilgi Güvenliği ile ilgili meydana gelen bir olayı, ilgili partiler ile birlikte yönetecek şirket yönetici seviyesinde bir kişi

Sorumluluklar,

- Olay Yönetimi ile ilgili dokümanların / kayıtların oluşturulmasını ve bu konuda gerekli koordinasyonu sağlamak
- İlgili kişiler için, Olay Yönetimi'nin farkındalığını arttırmak

- **Risk Temsilcisi**

Rolün Sahibi , Şirket içinde risk yönetiminden sorumlu kişi

Sorumluluklar ,

- Şirket için belirlenmiş risk yaklaşımını proje ekibi ile paylaşmak
- Bilgi Güvenliği kapsamında oluşturulacak tüm risk değerlendirme dokümanlarının geliştirilmesini ve denetlenmesini sağlamak
- Risk değerlendirme seanslarını desteklemek
- Risk ele alma planlarının yaratılmasını desteklemek

- **Denetim Temsilcisi**

Rolün Sahibi, Şirket içinde yürütülen iç denetim faaliyetinden sorumlu kişi

Sorumluluklar,

- Şirket içinde yürütülen iç denetim faaliyetleri hakkında proje ekibini bilgilendirmek
- Bilgi Güvenliği kapsamında denetim için oluşturulacak tüm dokümantasyonun geliştirilmesini ve kontrolünü sağlamak
- İç BGYS denetimi için kaynak sağlamak ve gerekli denetçi profilinin oluşturulmasını sağlamak

➢ **Kalite Yönetim Temsilcisi**

Rolün Sahibi , Şirketteki kalite sisteminin yönetiminden sorumlu olan ve yönetim temsilcisi olarak görev yapan kişi

Sorumluluklar ,

- Düzeltici ve Önleyici Faaliyetlerin Yönetimi (DÖFİ), Dokümantasyon Yönetimi ve Kayıt Yönetimi ile ilgili entegrasyonu ve uygunluğu sağlamak
- Şirket kalite yönetimi ile ilgili bilgi ve birikimini paylaşmak
- Şirketteki dokümantasyon yönetimine ilişkin destek vermek

4.3.2 Bilgi Güvenliği Politikası

Oluşturulan strateji doğrultusunda, ABC Şirketinde yürütülmekte olan tüm süreçlerin ve bu süreçlerde kullanılan kurumsal bilgilerin sağlam temelli bir yaklaşımla korunması amaçlanmıştır.

Üst yönetimin bilgi güvenliği ile ilgili kararlılığının göstergesi olarak kapsamlı bir bilgi güvenliği politikası hazırlanmıştır, şirket bilgilerine erişimi olan tüm çalışanlarla birlikte bilgi paylaşımında bulunulan tüm kuruluş/bireyler ile paylaşılacaktır.

Tüm süreçlerin Bilgi Güvenliği açısında gelişimlerinin destelenmesi amacıyla aşağıda belirtilen 18 alanda uygulama yapılması kararlaştırılmıştır.

- Bilgi güvenliği ve uyumluluk yönetimi
- Bilgi güvenliği varlık yönetimi
- Bilgi güvenliği risk yönetimi
- Bilgi güvenliği değişim yönetimi
- Bilgi güvenliği olay yönetimi
- İnsan kaynakları yönetimi
- Fiziksel güvenlik yönetimi
- Tedarik ve lojistik hizmetleri yönetimi

- Üçüncü kişilerle ilişkilerin yönetimi
- Kurumsal iletişim yönetimi
- Erişim yönetimi
- Mevzuata uyum
- İş sürekliliği yönetimi
- Bilgi sistemleri alım, geliştirme ve değ
- Bilgi sistemleri operasyon yönetimi
- Bilgi sistemleri uygulama geliştirme yöne
- Bilgi sistemleri ağ güvenliği yönetimi
- Taşınabilir ortam yönetimi

Bilgi güvenlik politikası şirket proje yöneticisinin sorumlulugunda proje grubu ile yapılan grup çalısmaları sonucunda asagıdaki sekilde olmasına Bilgi Güvenligi Onay Kurulu (Proje Yönelndirme Komitesi) tarafından karar verilmistir. Buna göre;

Teknoloji, bilgisayarlar, ağ ve iletişim sistemlerindeki değişikliklerin ivme kazanarak hızlanması, bilgiye olan ilginin ve sosyal bağımlılığın artması nedeniyle bilgi güvenliğini sağlamak ve tehditleri önlemek için kurulmuş kontrol sistem ve süreçlerin dinamik olarak bu hızlı değişiklikler ve dışarıdan gelebilecek taleplere paralel olarak yenilemesi ve güncellenmesi gerekmektedir.

Bilgi Güvenliği ve Uyumluluk Yönetimi ile ilişkili olan süreçlerin yönetim yaklaşımının, bu yaklaşımın organizasyona yayılımının ve değerlendirme kriterlerinin, geliştirilebilir ve sürdürülebilir bir yapıda ele alınması sağlanmaktadır.

Bilgi ve data, belirlenen otorizasyon seviyeleri dahilinde ulaşılabilir olmalıdır. Kötü niyet veya yanlışlıkla bilgi kötü amaçlarla kullanabilecek kişilerin ellerine geçmemelidir. Kötü niyet veya yanlışlıkla dataya ve bilgiye zarar verilmemeli, verilen zararın geri dönüşü uygulanabilmelidir.

İş süreçlerindeki bilgi güvenliği müşterilerin güvenli ve profesyonelce korunduklarını hissetmelerine izin vermelidir. Herhangi bir yanlış anlaşılmaya izin vermemek için ilave

dokümanlar oluşturulmalıdır. Bilgi yönetme politikası, risk analiz verilerine dayanarak, iç ve dış kullanıcı için stratejik bilgileri koruma yolları tanımlayacaktır. Şifre politikası şifre yaratmanın, saklamanın ve degistirmenin dogru yollarını tanımlayacaktır. Her çalısan gizlilik sözleşmesini imzalamalıdır ve bilgi güvenliği iş sorumluluklarının içine eklenmelidir. Bilgi Güvenliğinin elemanları tüm iş prosedürlerinin içine eklenmeli ve uymayanlar cezalandırılmalıdır.

Bu politikanın kapsamındaki her kişi tespit ettikleri ihlalleri sorumlu güvenlik temsilcisine rapor etmek zorundadır. Bilgi varlıklarının kullanılamaması, iş sürekliliğinin aksaması, ABC A.Ş. için o varlığın hasar görmesi kadar önemli bir problemdir. Bilgi varlıklarının kullanılamaz oldugu zamanlarda iş sürekliliğinin devam ettirebilmek için bir iş sürekliliği ve olağan üstü durum planlaması hazırlanacaktır. Yazılı hale getirilen ve yılda bir kez test ve tatbikatları gerçeklestirilecek bu planla, kaynak sahipleri tarafından kritik olarak değerlendirilmiş tüm bilgi varlıkları kapsanacaktır. Sistemi düzgün bir biçimde kurup çalısır halde tutması için bir kişi atanmalı ve tüm sonuçlardan sorumlu olmalıdır. Bu kişinin iletişim becerilerinin ve iş bilgisinin yüksek , teknik ve organizasyonel bir bakış açısın sahip olması gerekmektedir. Amaç sistemi gereksiz çatışmalardan kurtarmak ve her çalışanın da bu kişinin önerilerini dikkate almasını sağamaktır.

4.3.3 Bilgi Varlıkları ve Sorumluluklar

Bilgi varlıkları tespit edilirken sistem içerisinde iş sürekliliğinin sağlanmasında anahtar rol oynayan varlıklara yer verilecektir. Örneğin , bir projeksiyon cihazı şirket içerisinde yer alan bir varlıktır ancak bozulması durumunda, şirketin tüm web uygulamalarının üzerinde yer aldığı bir bilgisayar sunucusunun bozulması kadar soruna ve iş kesintisine neden olmazlar.

Çizelge 4.1 Varlık listesi ve varlık iş sürekliliği önem derecelendirmesi

Kategori No	Varlık Kategori	Sıra No	Varlıklar	X-Adet	Y-Oran (Adet / Toplam Adet)	Z-İş sürekliliği Puanı Önem 10 - Çok Önemli 1 - Az Önemli	W- Ağırlıklı Varlık Puanı (W=X*Z)	T-Ağırlıklı Varlık Oranı W/Toplam W	Sorumlu	Yeri	Güvenlik Sınıflandırması
1	Bilgi Varlıkları	1	Kullanıcı Veri Tabanı	4	0,12%	10	40	0,24%			
1	Bilgi Varlıkları	2	Yazılım Lisansları	25	0,73%	10	250	1,48%			
1	Bilgi Varlıkları	3	Bilgisayar Sistem Dokümantasyonu	1	0,03%	10	10	0,06%			
1	Bilgi Varlıkları	4	Sistem Dokümantasyonu	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	5	IBM AIX v. 4.3	3	0,09%	10	30	0,18%			
2	Yazılım Varlıkları	6	IBM eASy400	3	0,09%	10	30	0,18%			
2	Yazılım Varlıkları	7	Content Manager	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	8	FTP Server	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	9	Symantec Protection Antivirüs	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	10	SAP Business Objects R3.1	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	11	Windows NT 4.0 , XP , 7	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	12	Satış Uygulamaları (Web Sale)	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	13	Exchange Server 5.5	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	14	Microsoft Domain Name Server	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	15	Telnet Server	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	16	LAN Manager	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	17	Value Added Services Server	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	18	Çağrı Merkezi Uygulamaları (IVR, IVN, CRM)	1	0,03%	10	10	0,06%			
2	Yazılım Varlıkları	19	Oracle Financials	1	0,03%	10	10	0,06%			

3	1.SeviyeFizik sel Varlıklar	20	AIX Server	5	0,15%	10	50	0,30%			
3	1.SeviyeFizik sel Varlıklar	21	Content Management Server	1	0,03%	10	10	0,06%			
3	1.SeviyeFizik sel Varlıklar	22	Ağ Kartı	45	1,31%	10	450	2,66%			
4	2.SeviyeFizik sel Varlıklar	24	CD-Rom Sürücü	800	23,32 %	4	3200	18,92 %			
3	1.SeviyeFizik sel Varlıklar	25	NT Server (Sanal Serverlar Dahil)	200	5,83%	10	2000	11,83 %			
3	1.SeviyeFizik sel Varlıklar	26	Sabit Disk	30	0,87%	10	300	1,77%			
3	1.SeviyeFizik sel Varlıklar	28	Switch	46	1,34%	10	460	2,72%			
3	1.SeviyeFizik sel Varlıklar	29	Router Cisco 2600	10	0,29%	10	100	0,59%			
3	1.SeviyeFizik sel Varlıklar	30	Ağ Kabloları	1	0,03%	10	10	0,06%			
3	1.SeviyeFizik sel Varlıklar	31	Yazılım Yükleme Diskleri	20	0,58%	10	200	1,18%			
3	1.SeviyeFizik sel Varlıklar	32	Yedekleme Diskleri	20	0,58%	10	200	1,18%			
4	2.SeviyeFizik sel Varlıklar	33	Bilgisayarlar - (PC ve Notebook)	200 0	58,29 %	4	8000	47,31 %			
4	2.SeviyeFizik sel Varlıklar	34	Yazıcılar	200	5,83%	7	1400	8,28%			
5	Servisler	33	Elektrik	1	0,03%	10	10	0,06%			
5	Servisler	34	Su	1	0,03%	10	10	0,06%			
5	Servisler	35	Havalandırma	1	0,03%	10	10	0,06%			

Çizelge 4.1 de listelenen varlıklar iş sürekliliği ve bilgi güvenliği açısından 1 ile 10 arasında en az önemliden en çok önemliye göre puanlandırılmıştır. Şirketin toplam varlıklarının yani 3431 adet varlığının hepsini süreçlerde kontrolden geçirilmesini sağlamak uygulama sürecini karmaşıklaştıracaktır. Çizelge 4.1'den varlıkların önem puanına adetlerine göre basit ağırlıklı ortalamalar hesaplanarak varlıklar gruplanarak oran ve adet değerleri toplanıp sıralandığında Çizelge 4.2 deki sonuçlar elde edilmiştir.

Çizelge 4.2 Varlık listesi önem derecelendirmesi özet tablosu.

Kategori No	Varlık Kategori	Y- Adet / Toplam Adet	T- Ağırlıklı Oran (Adet*Önem Puanı / Ağırlıkşı Varlık Puanı Toplamı)	Z- İş sürekliliği Önem Puanı Toplamları 10 - Çok Önemli / 1 - Az Önemli	Z/ Toplam Z Ağırlıklı Önem Oranı
2	Yazılım Varlıkları	0,55%	1,12%	150	44,78%
3	1.SeviyeFiziksel Varlıklar	11,02%	22,35%	100	29,85%
1	Bilgi Varlıkları	0,90%	1,83%	40	11,94%
5	Servisler	0,09%	0,18%	30	8,96%
4	2.SeviyeFiziksel Varlıklar	87,44%	74,51%	15	4,48%
Toplam		100,00%	100,00%	335	100,00%

Çizelge 4.2 den çıkarılan sonuç, önemli kabul edilen varlıkların % 95 inin toplam varlıkların normal ortalamasına göre %13' ünü , ağırlıklı varlık ortalamasına göre yaklaşık %25 ini sistem için gerekli esas değerli varlıklar belirlenmiş olur.

Bu sonuçlar ışığında bilgi varlıkları , yazılım varlıkları, 1.seviye fiziksel varlıklar ve servisler iş sürekliliği bakış açısı ile öncelikli olarak değerlendirlecek varlıklardır.

Bilgi güvenliğine göre varlıkları ayrıca varlık etki puanı ile ağırlıklandırarak , bilgi güvenliği açısından bu değerlendirme risk yönetim prosedürü bölümünde yapılacaktır.

4.3.4 Bilgi Güvenliği Yönetim Sistemi Prosedürleri

Güvenlik süreçlerinin yönetimine yönelik olarak oluşturulan prosedürler Çizelge 4.3' te sunuşmuştur.

Çizelge 4.3 Oluşturulan Prosedürler.

Prosedür Adı
Bilgi güvenliği politikası
Bilgi güvenliği varlık yönetimi
Bilgi güvenliği risk yönetimi
Bilgi güvenliği değişim yönetimi
Bilgi güvenliği olay yönetimi
İnsan kaynakları yönetimi

Fiziksel güvenlik yönetimi
Tedarik ve lojistik hizmetleri yönetimi
Üçüncü kişilerle ilişkilerin yönetimi
Kurumsal iletişim yönetimi
Erişim yönetimi
Mevzuata uyum
İş sürekliliği yönetimi
Bilgi sistemleri alım, geliştirme ve değ
Bilgi sistemleri operasyon yönetimi
Bilgi sistemleri uygulama geliştirme yöne
Bilgi sistemleri ağ güvenliği yönetimi
Taşınabilir ortam yönetimi

4.3.4.1 Bilgi Güvenliği Politika Prosedürü

Yönetim net bir yönlendirmede bulunarak, kararlılığını göstererek, açıkça görevlendirme yaparak ve bilgi güvenliği sorumluluklarını kabul ederek şirket içinde bilgi güvenliği yaklaşımını destekler.

- **Yaklaşım**

  - Şirket, bilgi güvenliği ve uyumluluk standartlarına uygunluğu yeterli yetkiye sahip, üst yönetim organı eliyle yöneterek, bu konudaki kararlılığını gösterir,
  - Bilgi güvenliği hedeflerinin belirlenmesini, bu hedeflerin organizasyonel gereklilikleri karşılamasını ve ilgili süreçlere entegre edilmesini sağlar,
  - Bilgi güvenliği tanımı,
  - Bilgi güvenliğinin genel hedeflerinin açıklaması,
  - Bilgi paylaşımına yönelik bir altyapı oluşturma mekanizması olarak güvenliğin önemine dair bir tanım ,
  - ABC A.Ş.'nin ortaklarından olan grup şirketlerinin Bilgi Güvenliği Politikası ile uyumluluk ve bu politikaya atıfta bulunulması,
  - Kontrol hedeflerinin ve kontrollerin belirlenmesine yönelik bir çerçeve,
  - Risk değerlendirme ve risk yönetimi yapısı,

- Şirket açısından özel önem taşıyan; bilgi politikaları, ilkeleri ve standartları ile uygunluk gerekliliklerine dair kısa bir açıklama,
- Yasa, yönetmelik vb. mevzuata (bundan sonra "Mevzuat" olarak anılacaktır) ve sözleşmelerden doğan gerekliliklere uyulmasıyla ilgili beyanlar,
- İş sürekliliği yönetiminin kurallara uygunluğu,
- Bilgi güvenliği politikası ihlallerinin yaptırımları,
- Bilgi güvenliği yönetimiyle ilgili, bilgi güvenliği olaylarının raporlanması da dahil, genel ve belirli sorumlulukların tanımı ,
- Bilgi güvenliği ve uyumluluk çalışmaları, organizasyonun tümünü kapsayacak şekilde şirket tarafından belirlenmiş "Bilgi Güvenliği ve Uyumluluk Yönetimi Temsilcisi "tarafından ilgili bölümler ile birlikte koordine edilir, "ABC Grup Denetim Bölüm Başkanlığı – Bilgi Güvenliği ve Uyumluluk Yönetimi" ile iletişim sağlanır,
- Bilgi güvenliği ve uyumluluk çalışmalarının koordinasyonu ile standartlara uyumsuzluk durumuna göre alınacak aksiyonlar tanımlanır,
- Bilgi güvenliği ve uyumluluk çalışmalarının koordinasyonu ile varlık yönetimi, risk yönetimi, olay yönetimi ve değişim yönetimi gibi temel bilgi güvenliği süreçleri oluşturulur,
- Bilgi güvenliği ve uyumluluk çalışmalarının koordinasyonu ile bilgi güvenliği kontrollerinin yeterli olup olmadığı değerlendirilir ve bunların uygulanması koordine edilir

➢ **Dağıtım**

- Bilgi güvenliği politikası onaylanır ve yayınlanır
- Bilgi güvenliği politikası, tüm çalışanlarla birlikte ve bilgi paylaşımında bulunulan tüm kuruluş ve/veya bireyler ile paylaşılır
- Bilgi güvenliği ve uyumluluk çalışmalarının koordinasyonu için süreç sahipleri, risk yönetimi, yasal konular, insan kaynakları, fiziksel güvenlik,

denetim ve bilgi teknolojileri yönetimi gibi alanlarda uzmanlık sahibi olanların işbirliği ve birlikte çalışması planlanır.

- Bilgi güvenliği ve uyumluluk çalışmalarının koordinasyonu ile tüm şirketi kapsayacak şekilde bilgi güvenliği eğitim ve farkındalığı etkin bir şekilde teşvik edilir

➢ **Gözden Geçirme ve iyileştirme**

- Politikayla ilgili olarak, gözden geçirme takvimini ve sıklığını içeren süreç oluşturulur
- En az yılda 1 (bir) kez olmak kaydıyla planlanan aralıklarla ve/veya önemli değişiklikler olduğunda gözden geçirilerek bilgi güvenliği politikasının etkinliği ve sürdürülebilirliği sağlanır
- Bilgi güvenliği ve uyumluluk çalışmalarının koordinasyon sorumlulukları ve bu sorumluluklarla ilgili çıktılar en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir ve iyileştirme çalışmalarında kullanılır

4.3.5 Varlık Belirleme ve Sınıflandırma Prosedürleri

Şirkete değer yaratan her türlü fikri mülkiyet (fikir, konsept, know-how, teknik, kod, materyal, dokümantasyon ve diğer çalışma ürünleri), insan, teknoloji, bina ve donanım varlıkları ile kurumsal belleği oluşturan süreçler, varlık olarak açık ve net bir şekilde belirlenir, sahiplendirilir, sınıflandırılır, etiketlenir ve bir envanter hazırlanarak güncel tutulur.

➢ **Yaklaşım**

- Varlık yönetimine yönelik dokümante edilmiş bir süreç ve uygulama bulunur,
- Varlık envanterinde temel olarak, süreç adı, akışı, girdi ve çıktıları, sahibi, etiketleme değeri ve iş değeri yer alır,
- Sınıflandırma yapılırken bilgilerin gizliliği, bütünselliği ve erişilebilirliği dikkate alınır,

- İş değeri; bilginin izinsiz veya kaza ile açıklanması (gizlilik), hata, bozulma, çoğaltma, kısmen yanlışlık veya kasten silinme yoluyla hatalı ve/veya eksik bilgiye dönüşmesi (bütünsellik) ya da ihtiyaç duyulduğu anda ve yetki dahilinde erişilebilir durumda olmaması (erişilebilirlik) sonucunda iş üzerinde yaratacağı etki ile ilgilidir ve 4 ayrı seviyede ele alınır : Düşük, Orta, Yüksek, Kritik,
- Etiketleme değeri; bilginin izinsiz veya kaza ile açıklanması durumunda iş üzerinde yaratacağı etki ile ilgilidir, varlığın her türlü paylaşımı sırasında paylaşılan kişilere iletilir ve 4 ayrı seviyede ele alınır: Genel, Şirket İçi, Gizli, Çok Gizli,
- Yazıcı çıktısı alma, fotokopi ile çoğaltma, tarayıcı kullanımı, şirket içi/dışı sözel (sunum, toplantı, vb.), fiziksel (basılı kopya, vb.) ya da elektronik (e- posta, vb.) yöntemlerle paylaşma, saklama ve imha etme (basılı kopyaların imhası, taşınabilir medyadaki bilgilerin imhası, vb.) kuralları, etiket değerleri bazında belirlenir,

➢ **Dağıtım**

- Süreç sahiplerinin varlıklar ile ilgili sorumlulukları varlıkların sınıflandırılması, erişim sınırlamalarının ve sınıflandırmaların tanımlanmasını kapsar
- Topluluk içi şirketlerden gelen bilgilerin kullanımında etiketleme değerleri dikkate alınır,
- Bilgiler kullanılırken, basılı raporların, ekran görüntülerinin, kayıt ortamlarının (ör. bant, disk, CD), elektronik mesajların ve dosyaların taşıdığı etiketler dikkate alınır,
- Gerçek ve/veya tüzel kişiler ile bilgi paylaşımını içeren sözleşmeler, sınıflandırmanın belirlenmesine yönelik prosedürleri içerir,

➢ **Gözden Geçirme ve iyileştirme**

- Varlık yönetimine ilişkin süreç ve çıktıları düzenli olarak en az yılda 1 (bir) kez

olmak kaydıyla gözden geçirilir,

- Sürecin gözden geçirilen sonuçları iyileştirme çalışmalarında kullanılır,

4.3.6 Risk Yönetim Prosedürü

Şirkete değer yaratan her türlü fikri mülkiyet, insan, teknoloji, bina ve donanım varlıkları ile kurumsal belleği oluşturan süreçler için gizlilik, bütünsellik ve erişilebilirlik açısından risk değerlendirmesi yapılır, mevcut riskler belirlenir, kabul edilebilir risk seviyelerine göre gerekli aksiyonlar alınır,

➢ **Yaklaşım**

- Risk yönetimine yönelik dokümante edilmiş bir süreç ve uygulama bulunur,
- Risk değerlendirme yöntemi varlık esaslıdır, iş değeri açısından "Kritik" ve "Yüksek" değere sahip varlıklar mutlaka risk değerlendirme kapsamına alınır
- Risk değerlendirme yöntemiyle, varlıklar için geçerli olan tehditler saptanır, tehditlerin gerçekleşmesine sebep olabilecek zayıflıklar belirlenir ve ilgili varlıklar için mevcut kontroller değerlendirilir,
- Risklerin iş etkileri hizmet, marka değeri, Mevzuat'a uygunluk, tedarikçi, müşteri, çalışan, vb. boyutlardan, şirket stratejilerine uygun olanlar seçilir ve "Risk Etki Sınıflandırma Tablosu" şirket yönetim kurulunun görüş ve onayı alınarak oluşturulur,
- Riskin gerçekleşme olasılığı ve iş üzerindeki etkisi birlikte değerlendirilerek risk düzeyinin belirlenmesine yönelik ölçekler tanımlanır,
- Kabul edilebilir risk düzeylerine ilişkin kriterler, risk değerlendirme yönteminde tanımlanır,
- Kabul edilemez risk düzeyine sahip varlıklar için ilave kontroller ve sorumluların belirlendiği aksiyon planları hazırlanarak üst yönetimin onayına sunulur,

➢ **Dağıtım**

- Risk yönetimi ile ilgili sorumluluklar, olası tehdit ve zayıflıklar, mevcut kontroller ve risk etki / olasılık düzeyleri (Çizelge 4.4) varlıkların ait olduğu süreç sahipleri ile birlikte belirlenir

Çizelge 4.4 Olasılık değerleri

0	İmkansız	20 yılda 1
1	Muhtemel değil	5 yılda 1
2	Az olası	Yılda 1
3	Olası	Ayda 1
4	Sık sık	Günde 1
5	Devamlı	Günde 1'den fazla

- Risk değeri, varlık değeri ve olasılığın çarpımıdır. Çizelge 4.5' te risk değerlerinin alabileceği sınır değerler verilmiş olup, eğer risk değeri 8'e eşit veya daha yüksek ise veya varlık değeri 4 ise veya olasılık değeri 5 ise hemen önlem alınması gerekir. Güvenlik marjındaki bölgeler(4–6) güvenlik altına alınmalıdır ama düşük önceliklidir. Eğer risk değeri 3'ün altında ise güvenlik önlemine gerek yoktur ama sürekli kontrol, ani durum değişiklikleri için gereklidir.

Çizelge 4.5 Risk etki matrisi

		Olasılık değerleri					
		0	**1**	**2**	**3**	**4**	**5**
Varlık Değeri	**0**	0	0	0	0	0	0
	1	0	1	2	3	4	5
	2	0	2	4	6	**8**	**10**
	3	0	3	6	**9**	**12**	**15**
	4	0	4	**8**	**12**	**16**	**20**

- Kabul edilemez risk düzeyine sahip varlıklar için belirlenen ilave kontrollerin sorumlulukları, organizasyonun tümünü kapsayacak şekilde dağıtılır

➢ **Gözden Geçirme ve iyileştirme**

- Risk değerlendirmesi düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gerçekleştirilir
- Kabul edilemez risk düzeyine sahip varlıklar için belirlenen ilave kontrollerin gelişimi düzenli olarak en az yılda 4 (dört) kez olmak kaydıyla izlenir
- Kalıntı riskler tanımlanarak, düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla izlenir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.6.2 Risk Yönetimi

Proje kapsamındaki bilgi, yazılım, fiziksel varlıklar ve hizmetlerden oluşan varlıklar üzerinde Bölüm 3'te detayları verilen ve 4. Bölümün 3. maddesinde belirtilen Risk yönetim prosedürüne göre risk analiz sonuçları ve önerilen korumalar Çizelge 4.6' da verilmiştir.

Çizelge 4.6 Risk analiz sonuçları

Varlık No	Varlık Adı	Etki Değeri	Zayıflıkları	Tehditler	Olasılık	Risk	Önerilen Koruma
Bilgi Varlıkları							
V1	Kullanıcı Veri Tabanı	4	Erişim Gerektiriyor, Şifreler Süresiz, Kişiye özel bilgilerde kriptolama yapılmıyor	Silinebilir	4	12	Yönetici Tarafından Sahiplenmeli
				Değiştirilebilir	4	12	
				İçeriği Öğrenilebilir	4	12	Tek Yönlü Şifrelenmeli
				Kullanıcılar Bilgilerini Unutabilir	4	12	İş Süresince Yönetilmeli
V2	Yazılım Lisansları	3	Sistem Bakımında Gereklidir (online yardım, yükseltme, vs.)	Kaybetmek / Yok etmek	2	6	Özel Bir Yerde Saklanmalı Kopyaları Çıkarılmalı
V3	Bilgisayar Sistem Dokümantasyonu	3	Sistem Bakımında Gereklidir (sorun giderme, yükseltme, vs.)	Kaybetmek / Yok etmek	2	6	Özel Bir Yerde Saklanmalı Kopyaları Çıkarılmalı
V4	Sistem Dokümantasyonu	4	Sistemin Düzgün Çalışması İçin Gerekli	Kaybetmek / Yok etmek	3	12	Özel Bir Yerde Saklanmalı
				Uygun Olmayan Prosedürleri İzlemek	3	12	Kopyaları Çıkarılmalı
Yazılım Varlıkları							
V5	IBM AIX v. 4.3	4	Boot etmek	Yanlış Deamon/Program Yüklemesi	3	12	Kayıtları Analiz Etmeli
				Yanlış Bileşen Tanımlaması	3	12	
				Yanlış Aygıt Kontrolü	3	12	
			Kullanıcı Erişimi	Şifrenin açığa çıkması	4	16	Şifre Politikası Kullanmalı
						16	Her şifre kullanımı kayıtlanmalı
				Şifreyi Unutmak	4	16	Şifre Politikası Kullanmalı
				Uygun olmayan kullanıcı hakları	3	12	Erişim Listesi Kullanılmalı

				etc/bin/shadow	3	12	Root tarafından sahiplenilmeli
							"guest" ve "nobody" hesapları silinmeli
							hesapları yönetmek için "aduser" ve "rmuser" gibi sistem araçların kullanılmalı
			Uygunsuz Sistem Kapanışı	Uygunsuz Servis Sonlandırılması	3	12	Her zaman uygun komutları kullanılmalı (shutdown, reboot)
							Kesintisiz Güç Kaynağı kullanılmalı
			Başlangıç Skriptleri	Yanlış çok kullanıcı ayarı			Root tarafından sahiplenilmeli
							Kayıtlar Analiz Edilmeli
			Yetkilendirme standardı yok	Çok düşük veya çok yüksek erişim hakları	4	16	Gerekli Erişim Listesine göre gerçekten gerekli ise kullanmalı
			Sticky Bit komutu				Find komutu kullanmalı
			SUID&SGID komutu				Ps komutun kullanmalı
			Root komutu	Kazara sistem hasarı riski	3	12	Hesaba sadece yönetim için bağlanmalı
							Herhangi bir değişiklik yapmadan sistem yedeklenmeli
				Kök hesabın hacklenme riski	3	12	Gereksiz özellikler kullanım dışı bırakmalı
							Güncellemeler yüklenmeli
							Şifre kullanmalı
							Netstat komutunu sık kullan

			Netstat/ ps / df Komut kullanımları	Değiştirilebilirler ve yanlış bilgi verebilirler	5	20	Köke ayrıcalıklı silme ve değişiklik yapma yetkisi vermeli
							File control-sum'ı kontrol etmeli
			Find komutu	Değiştirilebilir ve yanlış bilgi verebilir	5	20	File control-sum'ı kontrol etmeli
							Köke ayrıcalıklı silme ve değişiklik yapma yetkisi vermeli
				Çok fazla disk zamanı kullanıyor	3	12	Yüklenmiş dosya sistemleri içinde bilinen dosyaları aramak için (s)locate komutunu kullanmalı
							Köke ayrıcalıklı silme ve değişiklik yapma yetkisi vermeli
V6	IBM eASy400	4	Şifre formatı güvenli değil, Şifre değişiklik prosedürü yok, Sistemde üst düzey yetkili kullanıcılar var,	Şifrenin açığa çıkması	2	8	IBM'in sağladığı WWTS (Worldwide Tool Set Version) password kontrol programıyla daha detaylı kontroller yapılabilir. BGYS Prosedürleri uygulanması gerekiyor.
				Bilgi sızıntısı	5	20	
				Kötüye kullanım	4	16	
V7	Symantec Protection Antivirüs	4	Kesinti	Uzak kök verme	5	20	Sürüm güncellemek gerekiyor
				Geçersiz ayar	5	20	Zone protection'i devreye al
			Pek çok TCP servis için gerekiyor (e-mail, WWW, chat, SMTP)	Eğer server devre dışı kalırsa tüm bu servisler devre dışı kalır	3	12	Uygun DNS server ayarları kullan
V8	FTP Server	2	Güvenli değil, kaynak kodunda hatalar mevcut	Bilgi transferini korumadan zayıf kimlik tespiti	5	10	Tüm dosyaları www üzerinden gönder
				Sık sunucu kök ayrıcalıklara sahip	5	10	

				Her “anonymous” kullanıcı bazı dosyaları alabilir	5	10	
				Bazen anonymous kullanıcı ayrıcalığı varmış gibi katalog yazabilir	4	8	
			Dosya alma ve gönderme	Yetkisiz dosya transferi	4	8	Netstat komutunu kullanmalı
				Kötü amaçlı dosyaların transferi	4	8	Bilgi Transfer Planı yapmalı
							Anti virüs yazılımı kurmalı ve sürekli güncel tutmalı
V9	Content Manager Server	2	Güvensiz	Mail iletme	5	10	Dahili çalıştırmalı
							8.12.1 sürümünü güncellemeli
							Yazılım değiştirmeli
				Kötü amaçlı dosyaların transferi	4	8	Anti virüs yazılımı kurmalı ve sürekli güncel tutmalı
							Bilgi Transfer Planı yapmalı
				Zayıf kimlik tespiti	3	6	Bilgi Transfer Planı yapmalı
			SUID	Yetkisiz kullanıcılara yetki verebilir	4	8	Dahili çalıştırmalı
							Yazılım değiştirilmeli
			Popüler Protokollerde (SMTP, POP3) tekst temizlemek	Bilgi sızıntısı	3	6	Dahili çalıştırmalı
							Program Değiştirilmeli
							Mesajları Şifrelenmeli
			Mesaj Güvenliği	Değiştirilebilir	3	6	e-imza kullanmalı
				İzinsiz okunabilir	3	6	Şifreleme yapılmalı
			Unix servis loglarını yollamak için SendMail	Diğer servisleri rahatsız edebilir	4	8	Tüm değişiklikler iki kez kontrol edilmeli
V10	SAP Business Objects R3.1	2	Universe tasarımındaki hatalar	Hatalı tablo ilişkileri nedeniyle	3	6	Universe tasarımının güncellenmesi gerekiyor

			Güvensiz	Buffer Taşması	5	10	Silinmeli
				Yetkisiz dosya transferi riski	4	8	Netstat komutu kullanmalı
				Sistem kesintisi riski	4	8	İndex çalışması yapılmalı
							İlişkisel veri modelinin iyileştirilmeli
			Tekst Temizleme	Veri Hackleme	3	6	KrediKartı ve Şifre bilgilerine maskeleme yapılmalı
				Bilgilere yetkisiz Ulaşım	3	6	Bilgi Transfer Politikası KurulmalıPerfo
							Kişi bazlı yetkilendirme çalışması yapılmalı
V11	Web Satış Uygulamaları (Web Sale)	4	Yavaşlık	Sistem kesintisi	3	12	Uygulama servere üzerinde performans çalışması yapılarak Java sürüm yükseltmek gerekiyor,
			Yetkilendirme	Bilgi sızıntısı	4	16	Müşteri bilgilerine erişim sağlayan personelin loglanması ve aktivitelerin izlenmesi ile ilgili
V12	Windows NT 4.0 , XP , 7	4	Kullanıcı Logini	Şifrenin açığa çıkması	4	16	Şifre Politikası Kullanmalı
				Şifreyi Unutmak	4	16	
				Uygun olmayan kullanıcı hakları	3	12	Erişim Listesi Kullanmalı
			Boot etmek	Yanlış sunucu / program kullanımı	3	12	NTFS Bölümlendirme kullanmalı
				Yanlış Bileşen Tanımlaması	3	12	
				Yanlış Aygıt Kontrolü	3	12	
			Uygunsuz Sistem Kapanışı	Uygunsuz Servis Sonlandırılması	2	8	Her zaman uygun komutları kullanmalı (shutdown, reboot)
				Bilgi Kaybı	2	8	Kesintisiz Güç Kaynağı kullanmalı
				Uç durumlarda insan desteksiz sistemi yeniden açamama	3	12	
			NetBios	Bilgi Yayınlanması	4	16	NetBios'u filtrelemeli

				Kaynaklara ulaşım verilmesi	4	16	
				Ağ üzerinden disk paylaşımı (güvenliği tam sağlanmamış, uygun olmayan erişimlere ve sistem kataloglanmasına izin veriyor olabilir)	4	16	İptal etmeli
			NTFS	Yanlış yedekleme	3	12	Tüm yedeklerin doğruluğunu kontrol etmeli
				Çok düşük veya çok yüksek erişim hakları vermek	3	12	Erişim Listesine gerekli hakları eklemeli
V13	Çağrı Merkezi Uygulamaları (IVR, IVN, CRM)Server	4	Kullanıcı yoğunluğu olduğunda yavaşlama ve kesinti	Çağrı merkezi ve iştirak satış sistemlerini durdurma riski	5	20	Uygulama gözden geçirilmeli , kullanılan SQL ler için performans çalışması yapılmalı
			Kullanıcı şifre zayıflığı	Bilgi sızıntısı	3	12	BGYS prosedürleri uygulnmalı , güçlü şifre algoritmaları ve prosedürleri
V14	Exchange Server 5.5	4	Mail Server	Bilgi sızıntısı	3	12	Şifrelemeli
							e-imza kullanmalı
				E-mektup iletimi	5	20	e-mektup iletimi devre dışı bırakmalı
			Sürekli disk dolumu	Sabit diskin dolum tehlikesi, program durması ve sistem tamirinin imkansızlığı	4	16	Disk alanını günlük olarak kontrol etmeli
							Artan şekilde yedekleme yapmalı
			Admin mod dışında çöp klasörünün silinmemesi	Sabit disk yerinin olmaması durumunda program çalışmayacak veya veri silmeyecek	4	16	Disk alanını günlük olarak kontrol etmeli
							Yedek sabit disk almalı
			Mailbox veri tabanı yönetimi	Veri tabanı bozulması	3	12	Yedeklemeli
				Ağ bağlantısı yok	3	12	Veri tabanını
				iken kullanıcıların mesajlarına ulaşamaması			birleştirmeli

				Veritabanının antivirüs programı ile taranması ile ilgili sorunlar	3	12	Workstation a anti virüs yazılımı kurmalı
			Mesaj güvenliği	Değiştirilebilir	3	12	E-imza kullanmalı
				İzinsiz okunabilir	3	12	Şifreleme yapılmalı
			Güvenlik modeli (OS parçası olarak ACL)	Kendi ayarları yanlış	4	16	ACL değiştirilmeli (erişim kontrol listesi)
				Büyük karışıklık, bir kısım işler Exchange bir kısım işler NT tarafından yapılmış			
V15	Microsoft Domain Name Server	4	Server restart edildiğinde Otomatikolarak aktif olmuyor.	Uzak noktaya root verme	5	20	v.8.2.5'den v.9.1.3'e geçilmeli
				Yanlış ayar	5	20	Zone transferi devre dışı bırakmalı
			Pek çok TCP servis için gerekiyor (e-mail, WWW, chat, SMTP)	Eğer server devre dışı kalırsa tüm bu servisler devre dışı kalır	3	12	Uygun DNS server ayarı kullanmalı
V16	Telnet Server	2	Kod hatası	Zayıf kimlik kontrolü	3	6	Yazılımı SSH v2 protokolü kullanarak kurmalı
			Güvensiz	Buffer taşması	5	10	Kaldırmalı
				İzinsiz dosya transferi riski	4	8	GUI'ye ulaşmak için terminal services (firewalldan geçmiş) kullanmalı
				Zararlı yazılım indirme riski	4	8	Anti virüs yazılımı kurmalı ve güncel tutmalı
							Bilgi Transfer Planı yapmalı
			Kontrolsüz olarak dosya siliyor	Verilere zarar verme	3	6	Şifrelemeli
				Bilgiye izinsiz erişim	3	6	Bilgi Transfer Planı yapmalı
							Uzaktan erişim için SSH destekli bir yazılım kullanmalı
V17	Oracle Financials	4	Uzaktan erişim	Bilgiye izinsiz erişim	3	12	Bilinen iyi bir çözümü yok
							Uzaktan erişimi devre dışı bırakmalı

			Zayıf şifre ile şifreleme	Şifre kırma	3	12	Syskey kurmalı
Fiziksel Varlıklar(Donanımlar , Server , Hub, PC, Switch, Network)							
V18	AIX Server	4	Fiziksel olarak ulaşılabilir	Yok etme / parça çalma	2	8	Yedek bir tane almalı
							Sigortalamalı
							Kısıtlı erişim sağlanmalı
							Acil durumda yeni bir tane almak için para ayrılmalı
				Bilgiye yetkisiz ulaşım	4	16	Şifre koruması sağlanmalı
							Kısıtlı erişim sağlanmalı
			Yok edilebilir	Bilgiye ulaşım yok	2	8	Yedeklenmeli
							Kısıtlı erişim sağlanmalı
			Çalınabilir	Bilgiye ulaşım yok	2	8	Şifreleme yapılmalı
				Bilgi sızıntısı	2	8	Kısıtlı erişim sağlanmalı
V19	Content Managemen t Server	4	Sınırlı Kapasite	Bilgi için yer yok	3	12	Disk alanını günlük gözden geçirmeli
							Bilgi Transferi
			Çalınabilir	Bilgi sızıntısı	2	8	Şifreleme yapılmalı
				Bilgiye ulaşım yok	2	8	Kısıtlı Erişim sağlanmalı
			Yok edilebilir	Bilgiye ulaşım yok	2	8	Sık yedekleme yapılmalı
							Kısıtlı Erişim sağlanmalı
V20	Ağ Kartı	2	Yok edilebilir	LAN ve Internet bağlantısı yok	2	4	Yedek bir tane almalı
V21	Bilgisayarlar -(PC ve Notebook)	1	Yok edilebilir	yedekleme ve geri yükleme imkanının olmaması	3	3	Yedeklenmeli
				Veri iletimi imkanının olmaması	3	3	

				Sistem bileşenlerinin yüklenmesini bölebilir	2	3	
			Veri Transferi için kullanılabilir	Bilgi çalmak için kullanılabilir	4	4	Erişim Listesi Kullanmalı
							Bilgi Transferi Politikası Kurmalı
V22	CD-Rom Sürücü	1	Yok edilebilir	Yedekleme ve geri yükleme imkanının olmaması	2	2	Yedek bir tane almalı
				Yazılım yüklemek imkansızlaşabilir	2	2	
			Yasal olmayan yazılım yüklemek için kullanılabilir	Lisans anlaşmasının bozulması	4	4	Bilgi Transferi Politikası Kurmalı
							CD'den yüklemeyi yasaklamalı, sadece yöneticiye izin vermeli
V23	NT Server	4	Fiziksel olarak erişilebilir	Yok etme / Parça çalma	2	8	Yedek bir tane almalı
							Sigortalamalı
							Kısıtlı Erişim sağlanmalı
							Acil durumda yenisini almak için para ayrılmalı
				Bilgiye Yetkisiz Ulaşım	3	12	Şifre ile korumalı
							Kısıtlı Erişim sağlanmalı
			Yok edilebilir	Bilgiye erişimin kesilmesi	2	8	Sık yedekleme yapmalı
							Kısıtlı Erişim
			Çalınabilir	Bilgiye erişimin kesilmesi	2	8	Şifreleme yapılmalı
				Bilgi Sızıntısı	2	8	Kısıtlı Erişim sağlanmalı
V24	Sabit Disk	4	Sınırlı Kapasite	Bilgi için yer yok	3	12	Disk alanını günlük gözden geçirmeli
							Bilgi Transferi Politikası Kurmalı
			Exchange 5.5 aktiviteleri	Değişimin bekletmesi	4	16	Disk alanını günlük gözden geçirmeli

			yüzünden dolabilir	Mail kutularına erişimin olmaması	4	16	Yedek bir disk alınmalı ve ağ ortamında düzenli olarak yedeklenmeli
				Dosyaları Boşaltma imkanının olmaması	4	16	
			Çalınabilir	Bilgi sızıntısı	2	8	Şifreleme yapılmalı
				Bilgiye ulaşım yok	2	8	Kısıtlı Erişim sağlanmalı
			Yok edilebilir	Bilgiye ulaşım yok	2	8	Sık yedekleme yapılmalı
							Kısıtlı Erişim sağlanmalı
V25	Yazıcılar	3	Şifre kontrolü yok	Önemlı çıktılar başkalarının eline geçebilir, Bilgi güvenliği riski	2	6	Yazıcılara kullanıcı bazlı şifre konulmalı
V26	Switch	4	Yok edilebilir	LAN veya internet erişimi yok	3	12	Yedek bir tane almalı
V27	Routers	4	Ağ trafiğini düzenler	Bilgilerin bozulması	3	12	Düzgün Router ayarı yapılmalı
			Zor düzgün ayarlar				
			Standart zayıf şifre	Şifre tahmini	3	12	Şifre güvenlik politikası uygulanmalı
			Yok edilebilir	LAN veya internet erişimi yok	2	8	Yedek bir tane almalı
V28	Ağ kabloları	2	Yok edilebilir	LAN veya internet erişimi yok	2	4	Düzgün yerleştirmeli
V29	Yazılım yükleme diskleri	3	Fiziksel olarak ulaşılabilir	Kaybetme /yok etme / çalınma	4	12	Erişimi kısıtlanmalı
			Yok edilebilir	Bilgisayar sistem bakımı için gerekebilir	4	12	Yedeklerini almalı
V30	Yedekleme diskleri	3	Fiziksel olarak ulaşılabilir	Kaybetme / yok etme / çalınma	4	12	Erişimi kısıtlanmalı
			Yok edilebilir	Bilgi sızıntısı	4	12	Erişimi kısıtlanmalı
							Şifrelenmeli
			Çalınabilir	Bilgisayar sistem bakımı için gerekebilir	4	12	Yedeklerini almalı
Hizmetler (Elektirk,Su ,Havalandırma sistemleri)							

V31	Elektrik	4	Kısa devre	Donanıma zarar verebilir	2	8	Kesintisiz Güç Kaynağı kullanmalı
			Kesinti	Önlem alınmamış bilgisayarların elektriğini kesebilir, sisteme zarar verebilir	3	12	Yedek güç kaynağı
							Kesintisiz Güç Kaynağı kullanmalı
				İş süreçlerini bloke edebilir	2	8	İş Devam Programı başlatmalı
			Yangın	Şirketi, tüm varlıkları ve bilgiyi yok edebilir	2	8	Yangın koruma sistemi kurmalı
							Çalışanları yangından koruma programı oluşturmalı ve eğitim vermeli
							Yedekler almalı
							Yedekleri düzün saklamalı
				Donanımı yok edebilir	2	8	Yangın koruma sistemi kurmalı
				Yazılımı yok edebilir	2	8	Yedekleri düzün saklamalı
				İş süreçlerini bloke edebilir	2	8	Yedek güç kaynağı kullanmalı
V32	Su	1	Sel	Donanımı yok edebilir	2	2	Donanımı ve kabloları yerden yükseğe yerleştirmeli
				Yazılımı yok edebilir	2	2	Kurulum disklerini düzgün yerleştirmeli
				Yedekleri yok edebilir	2	2	Yedekleri düzgün yerleştirmeli
				İş süreçlerini bloke edebilir	2	2	İş Devam Programı başlatmalı
V33	Havalandırma	1	Donanımın havalandırılması	Donanıma zarar verebilir	2	2	Server odalarının oğutulmasına dikkat etmeli
				Yangına neden olabilir	2	2	Düzgün kurulum yapmalı

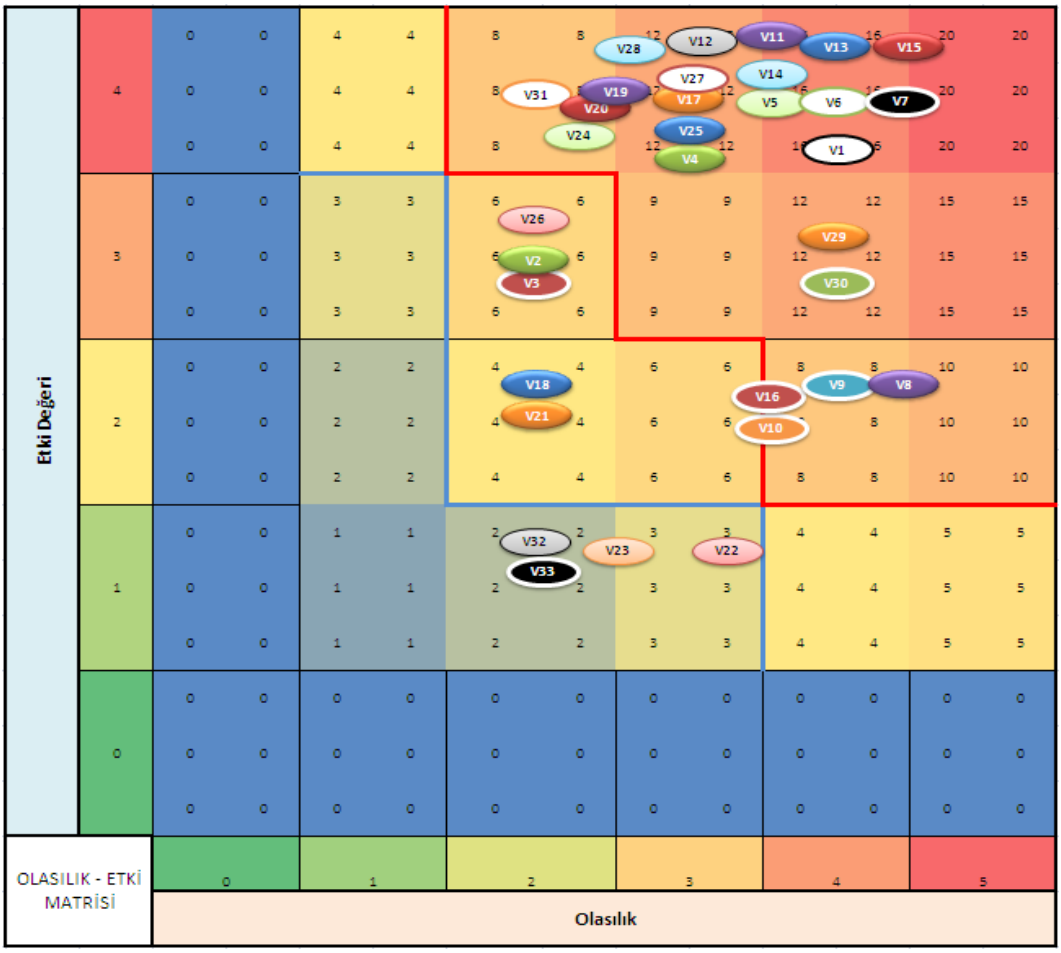
Varlık listesinde tespit edilen tehdit, etki ve olasılık değerleri dikkate alınarak ve açıklıklar sonucu meydana gelecek risklerin ortalamaları alınarak varlık bazında ortalama olasılık değerleri hesaplanarak aşağıdaki çizelge oluşturulmuştur.

Çizelge 4.7 Varlık Olasılık Etki Risk

VarlıkNo	Olasılık	Etki	Açıklık Adet	Ortalama Risk Puanı	Risk Toplamı
V2	2,00	3	1	6,00	6
V3	2,00	3	1	6,00	6
V18	2,00	2	1	4,00	4
V21	2,00	2	1	4,00	4
V26	2,00	3	1	6,00	6
V32	2,00	1	4	2,00	8
V33	2,00	1	2	2,00	4
V31	2,14	4	7	8,57	60
V24	2,20	4	5	8,80	44
V20	2,25	4	4	9,00	36
V19	2,40	4	5	9,60	48
V23	2,67	1	3	2,67	8
V28	2,67	4	3	10,67	32
V4	3,00	4	2	12,00	24
V17	3,00	4	2	12,00	24
V25	3,00	4	7	12,00	84
V27	3,00	4	1	12,00	12
V12	3,21	4	14	12,86	180
V22	3,25	1	4	3,25	13
V11	3,50	4	2	14,00	28
V5	3,67	4	15	14,67	220
V10	3,67	2	6	7,33	44
V16	3,67	2	6	7,33	44
V14	3,75	4	10	15,00	150
V1	4,00	4	4	16,00	64
V6	4,00	4	3	14,67	44
V13	4,00	4	2	16,00	32
V29	4,00	3	2	12,00	24
V30	4,00	3	3	12,00	36
V9	4,14	2	7	8,29	58
V7	4,33	4	3	17,33	52
V15	4,33	4	3	17,33	52
V8	4,50	2	6	9,00	54

Risk senaryosunun önem derecesi (Risk toplamı), gerçekleşme olasılığı ve etki değerlerinin çarpımı ile belirlenmiştir. Bir alandaki senaryonun genel önem derecesi belirlenirken, her varlık için farklı alt değerlendirmeler sonucu oluşan ortalama önem derecesinin değeri kullanılmıştır.

Bir alanın genel risk haritası her bir senaryo ile ilgili olasılık ve etkinin Şekil 4.3 'teki varlıkların grafik üzerinde yerleştirilmesi ile oluşturulmaktadır , bu kapsamda risk prosedüründe belirtilen maddeler ışığında güvenlik riski bulunan varlıklarla ilgili olarak şirketin risk prosedürleri ve risk önlemleri doğrultusunda uygulayacağı önleyici ve düzeltici bir takım aksiyon planları hazırlanacaktır. Kırmızı alandaki riskler en kritik senaryolardır, ancak toplam risk puanlarına göre ve maliyet ve iş kesici etkilerini de dikkate alarak, ABC A.Ş acil olarak senaryolar ile belirlenen riskler uygun kontroller ile kabul edilebilir düzeye indirilmelidir.



Şekil 4.3 Varlıkların olasılık etki matrisindeki dağılımı, genel risk haritası

- Risk listesi hazırlandıktan sonra niteliksel ve niceliksel analiz metodları kullanılarak riskler detaylı olarak tanımlanır.
- Riskler ile ilgili detaylı maliyet ve zaman planlanları hazırlanacaktır.
- Risklerin ve tehditlerin gerçekleşme olasılıklarına ve etkilerine göre risk yanıt planı hazırlanır. Yanıt planı staratejileri , riskten kaçınma, riski devir etme, riski azaltma, riski kabul etme şeklinde olabilir.

4.3.7 Değişim Yönetimi

Şirkete değer yaratan her türlü fikri mülkiyet, insan, teknoloji, bina ve donanım varlıkları ile kurumsal belleği oluşturan süreçler üzerinde olabilecek değişimler gizlilik, bütünsellik ve erişilebilirlik açısından değerlendirilerek yönetilir

➢ **Yaklaşım**

- Değişim yönetimine yönelik dokümante edilmiş bir süreç ve uygulama bulunur.
- Organizasyon içinde değişim yönetimi sürecine ilişkin sürecin sahibi ile görev ve sorumluluklar belirlenir.
- "Risk Etki Sınıflandırma Tablosu" dikkate alınarak, gerçekleştirilecek değişimlerin etki düzeyleri belirlenir, etki düzeylerine göre roller, onay ve sorumluluklar tanımlanır.
- "Risk Etki Sınıflandırma Tablosu"ndaki etki düzeyi en üst 2 (iki) seviyedeki değişimler için risk değerlendirmesi yapılır.
- Değişim yönetimi sürecinde temel olarak değişime yönelik ana adımlar / zamanlamaları / sorumluları, her bir adım için kabul kriterleri, değişimin başarısız olması durumunda geriye dönüş adımları, test planları ve başarı kriterleri tanımlanır

➢ **Dağıtım**

- Değişim, değişimi gerçekleştirecek, varlıkları değişimden etkilenecek ve değişim sonrası ortaya çıkabilecek aksiyonları devreye alacak ilgili tüm süreç sahiplerinin koordinasyonunda gerçekleştirilir

➢ **Gözden Geçirme ve iyileştirme**

- Değişimin sonuçları ile ilgili şirket içinde gerekli bilgilendirme ve başarı kriterlerinin gerçekleşme durumları değerlendirilir, sonuçlara göre değişim döngüsü tekrar çalıştırılır
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.8 Bilgi Güvenliği Olay Yönetimi

Şirkete değer yaratan her türlü fikri mülkiyet, insan, teknoloji, bina ve donanım varlıkları ile kurumsal belleği oluşturan süreçler ile ilgili oluşmuş veya oluşabilecek bilgi güvenliği olaylarının yönetilmesi ve benzer olayların tekrarlanmaması için çalışmalar yürütülür.

➢ **Yaklaşım**

- Olay yönetimine yönelik dokümante edilmiş bir süreç ve uygulama bulunur Süreçte, bilgi güvenliği olaylarının iç ve dış iletişim kuralları, düzeltici / önleyici aksiyonlar ve takip çalışmaları (eskalasyon, soruşturma, delil toplama, sınırlandırma ve bilgi güvenliği olayının nedeninin ortadan kaldırılması, vb.) tanımlanır
- Organizasyon içinde olay yönetimi sürecine ilişkin sürecin sahibi ile görev ve sorumluluklar belirlenir
- Olayların iş üzerindeki etkileri, olayların sonucundan bağımsız olarak “Risk Etki Sınıflandırma Tablosu” ile değerlendirilerek etki düzeyleri belirlenir, etki düzeylerine göre roller, onay ve sorumluluklar tanımlanır

- Bilgi güvenliği ihlali gerçekleştiğinde, bu ihlali gerçekleştirerek şirketi doğrudan ve/veya dolaylı olarak zarara uğratan kişi ve/veya kuruluş aleyhine hukuki yollara başvurulmasının söz konusu olduğu durumlarda kanıtlar, hukuka uygun ve gerektiği şekliyle toplanır, saklanır ve sunulur

➢ **Dağıtım**

- Bilgi güvenliği olayına konu olan çalışmalar, organizasyon içinden ve/veya dışından süreç sahiplerinin (ör. hukuk, kurumsal iletişim, insan kaynakları, emniyet organları, vb.) katılımı ile yürütülür
- Tüm çalışanlar, stajyerler, alt yükleniciler, danışmanlar ve diğer gerçek ve/veya tüzel kişiler, kendi başına hareket etmeden, her türlü bilgi güvenliği olayını ve/veya bilgi güvenliği zaafiyetini bildirmekten sorumlu oldukları konusunda bilgilendirilir
- Bilgi güvenliği olaylarının iş üzerindeki etkileri değerlendirilerek, güvenlik ihlalinde bulunan çalışan, stajyer, alt yüklenici, danışman veya diğer gerçek ve/veya tüzel kişilere ait kullanıcılarla ilgili yaptırımlar belirlenir ve paylaşılır

➢ **Gözden geçirme ve iyileştirme**

- Bilgi güvenliği olayları ile ilgili şirket içinde ve/veya dışında gerekli bilgilendirme yapılır
- Bilgi güvenliği olayları kök neden, etki, maliyet ve tekrarlama sıklığı boyutları göz önünde bulundurularak değerlendirilir, elde edilen sonuçlar olayların tekrarını ya da zaafiyetlerin oluşmasını önlemek amacıyla kullanılır
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.9 İnsan Kaynakları Yönetimi Prosedürü

Çalışan ve stajyerlerin bilgi güvenliği ile ilgili görev ve sorumlulukları, şirketin bilgi güvenliği yaklaşımına uygun olarak tanımlanır ve dokümante edilir

➢ **Yaklaşım**

Çalışan ve stajyerlerin;

- Bilgi güvenliğiyle ilgili görev ve sorumlulukları tanımlanır ve yönetim tarafından onaylanır
- İşe alım sürecinde görev ve sorumlulukları, kendi faaliyetleri ile ilgili sorumluluğunun kendisine ait olduğu açıkça anlatılır
- Bilgi güvenliğiyle ilgili görev ve sorumluluklar, şirketin bilgi güvenliği politikalarına uygun davranılmasını, varlıkların korunmasını ve diğer dokümante edilmiş (politika, prosedür, taahhütname, vb.) sorumlulukları kapsar
- Bilgi güvenliği sorumlulukları, sadece çalışma saatleri ve şirket ortamıyla sınırlı olmayıp istihdam sona erdikten sonra da devam eder

➢ **Dağıtım**

Çalışan ve stajyerlerin bilgi güvenliği ile ilgili görev ve sorumluluklarının gerek kendilerince ve gerekse birlikte çalışacakları şirket çalışanlarınca bilinirliliği garanti altına alınır

➢ **Gözden geçirme ve iyileştirme**

- Görev ve sorumluluklar düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.9.2 Referans Kontrol Prosedürü

- Çalışan ve stajyer adayları için, öz geçmişlerini doğrulayıcı reefrans kontrolleri, ilgili kanun / yönetmelik ve etik kurallara uygun olarak yapılır
- Referans incelemesine yönelik süreç, doğrulama amaçlı kontrollerle ilgili kriter ve sınırlamaları içerir ve incelemeyi yapabilecek kişiler tanımlanır

- İstihdam öncesinde doğrulama kontrolleri yapılır
- İncelemelerde en az 2 (ikreferans kontrolü yapılır ve kayıt altına alınır
- Adayın bitirdiği eğitim kurumuna ait diplomanın aslı veya noter onaylı kopyası talep edilir ve eğitim kurumu ile doğrulama yapılarak adayın özlük dosyasında saklanır
- Adayın adli sicil kayıt belgesi talep edilir
- Adayın kişisel profil analizi yapılır
- Referans inceleme çalışmalarına ait bilgilerin nasıl elde edileceği ve kullanılacağı ile ilgili süreç tanımlanır ve bu süreç, kişisel verilerin korunmasına ilişkin yasal düzenlemelere, gizlilikle ilgili kanunlara ve diğer ilgili mevzuata uygun yürütülür
- Adaylara, inceleme çalışmaları hakkında önceden bilgi verilir
- Kişisel verilerin korunmasına ilişkin yasal düzenlemeler ve diğer ilgili mevzuat takip edilerek ilgili süreç güncel tutulur
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.9.3 İşe Alım Prosedürü

- İş akdi/hizmet sözleşmesinin bir parçası olarak çalışan ve stajyerler, şirketin bilgi güvenliği yaklaşımını da içeren, işe alma şartlarını kabul ederek imzalarlar
- Çalışan ve stajyerlerin imzaladığı iş akdi/hizmet sözleşmesi şirketin bilgi güvenliği yaklaşımını içerecek şekilde hazırlanır
- İş akdi/hizmet sözleşmesi içeriğinde şirket varlıklarının gizliliği, bütünselliği ve erişilebilirliğinin korunmasına yönelik maddeler bulunur
- İş akdi/hizmet sözleşmesi içeriğinde işini gerçekleştirmesi için şirket tarafından kendisine sağlanan şirket kaynaklarının, sadece iş amaçlı kullanılacağına yönelik maddeler bulunur

- Gerektiği durumlarda imzalatılmak üzere, ek bir gizlilik anlaşması veya bilgi güvenliği taahhütnamesi hazırlanır
- İş akdi/hizmet sözleşmesi içeriğinde, şirketin tabi olduğu Mevzuat'la birlikte ABC Grup politika ve prosedürleri kapsamındaki sorumluluk ve haklar da yer alır
- İş akdi/hizmet sözleşmesi içinde yer alan sorumluluklar, şirketin tesisleri ve normal mesai saatleri dışında da geçerlidir
- İş akdi/hizmet sözleşmesi, istihdamın sona ermesinden sonra, çalışılan süre içinde doğrudan veya dolaylı olarak edinilen ve şirketin faaliyet alanına giren, açıklanmasında sakınca görülmesi nedeniyle korunması gereken ve Gizli Bilgilerin Korunması Politikası çerçevesindeki her türlü ticari, mesleki, teknik bilgi ve sırlar, bilgi birikimi (know-how), işyerinde geliştirilmiş bilgi ve teknikler, şirketin yazılı izni dışında hiç bir surette resmi, özel kişilere, kurum ve kuruluşlara, görsel ve yazılı medyaya ifşa edilmemesi, herhangi bir ticari veya gayri ticari amaçla kullanılmamasına yönelik maddeleri içerir
- Bilgi güvenliği farkındalığını artırmak amacıyla düzenlenen eğitim, oryantasyon programının bir parçası olarak ele alınır
- Farkındalık uygulamaları, şirketin bilgi güvenliği yaklaşımını içerecek şekilde oluşturulur
- Farkındalık uygulamaları, yürürlükte olan bilgi güvenliği ile ilgili politika ve prosedürlerinin tanıtımını ve uygulama adımlarını kapsar
- Farkındalık uygulamaları, bilgi güvenliği temel süreçleri olan varlık yönetimi, risk yönetimi, değişim yönetimi, olay yönetimi ile ilgili çalışan, stajyer, alt yüklenici, danışman veya diğer gerçek ve/veya tüzel kişilerle ilgili personelin sorumluluklarını kapsayacak şekilde hazırlanır
- Farkındalık uygulamaları, gizlilik, bütünsellik ve erişilebilirlik açısından olası tehdit, zayıflık, riskler ve bunları önlemeye yönelik alınabilecek kontrollerle ilgili bilgileri kapsar

- Çalışan, stajyer, alt yüklenici, danışman veya diğer gerçek ve/veya tüzel kişilerin görevine, sorumluluklarına ve becerilerine uygun olarak, gerektiği durumlarda ek bilgi güvenliği farkındalık eğitimleri planlanır
- Farkındalık eğitimi tüm çalışan, stajyer, alt yüklenici, danışman veya diğer gerçek ve/veya tüzel kişiler için uygulanır
- Bilgi güvenliği farkındalığının şirket genelinde oluşturulması amacıyla çeşitli iletişim kanalları kullanılır (e-öğrenme uygulamaları, ekran koruyucu uygulamaları, posterler, bilgilendirme e-postaları, toplantı odası kuralları, vb.)
- İş akdi/hizmet sözleşmesi, sözleşme içeriğinde yer alan kayıt ve koşullara aykırı davranılması halinde izlenecek disiplin sürecini de kapsar
- İşe alım sürecinde, işe alınanın üstleneceği iş ve pozisyonuna bağlı olarak sahip olunması gereken fiziksel ve elektronik erişim hakları tanımlanır
- İş akdi/hizmet sözleşmesi çalışan ve stajyere imzalatılır
- Şirketin tabi olduğu Mevzuat' la birlikte ABC Grup politika ve prosedürleri kapsamı takip edilerek ilgili süreç güncel tutulur
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır
- Farkındalığı artırmaya yönelik uygulamaların etkinliği ölçülür
- Bilgi güvenliği farkındalığıyla ilgili uygulamalar, bilgi güvenliği yaklaşımındaki değişikliklere göre en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir ve güncellenir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır
- Çalışan ve stajyerlere yaptırım uygulanması gereken durumlar ve uygulanacak yaptırımlar belirlenir
- Disiplin sürecine yönelik dokümante edilmiş bir süreç ve uygulama bulunur

- Disiplin süreci, bilgi güvenliği ihlal durumlarını ve bu ihlal durumlarında uygulanacak yaptırımları kapsar
- Disiplin süreci, bilgi güvenliği ihlalinde bulunduğundan şüphe edilen çalışanlara doğru ve adil davranılmasını sağlar
- Disiplin süreci, gerektiği durumlarda personelin erişim haklarının ve yetkilerinin derhal geri alınarak refakatçi eşliğinde tesis dışına çıkarılmasını kapsar
- Bilgi güvenliği ihlallerinin oluşması sonucunda uygulanacak disiplin süreci hakkında çalışan, stajyer, alt yüklenici, danışman veya diğer gerçek ve/veya tüzel kişiler düzenli olarak bilgilendirilir
- Şirketin tabi olduğu Mevzuat' la birlikte ABC politika ve prosedürleri kapsamı takip edilerek ilgili süreç güncel tutulur
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

İstihdamın sona ermesi (istifa, işten çıkarma, emeklilik durumlarveya görev değişikliği ile ilgili olarak uygulanması gereken bilgi güvenliği sorumlulukları tanımlanır.

- İstihdamın sona ermesi veya görev değişikliği yapılmasıyla ilgili olarak rol ve sorumlulukların yer aldığı bir süreç ve uygulama bulunur
- İstifa eden personel ve/veya şirket tarafından ihbar önelini kullandırmak suretiyle İş akdi/hizmet sözleşmesi sona erdirilen personel ile ilgili ihbar süresinin kullanımı ve bu sürede sahip olacağı erişim yetkilerinin düzenlemesine yönelik kurallar belirlenir
- İstihdamı sona eren personelin, iş amacıyla kullandığı elektronik ve fiziksel varlıkları (blackberry/iphone/pda, dizüstü bilgisayar, kredi kartı, giriş-çıkış kartı, vb.) iade etmesine yönelik kurallar belirlenir
- İstihdamı sona eren personelin, şirketi temsilen yürütmekte olduğu abonelik, üyelik, vb. temsil sorumlulukları sonlandırılır

- İstihdamı sona eren personelin, sona erme öncesinde elinde mevcut işlerin görevlendirilen kişiye devrine yönelik sorumlulukları tanımlanır
- İstihdamın sona ermesi veya görev değişikliği durumunda, sahip olunan fiziksel ve elektronik erişim haklarının kaldırılması veya değiştirilmesiyle ilgili koşullar ve sorumluluklar tanımlanır
- İstihdamı sona eren personel, her türlü grup erişim ve iletişim listesinden çıkarılır
- İstihdamın sona ermesi veya görev değişikliği olması durumunda en fazla 1 saat içerisinde erişim hakları kaldırılır
- Şirketin tabi olduğu Mevzuat' la birlikte ABC Grup politika ve prosedürleri kapsamı takip edilerek ilgili süreç güncel tutulur
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.10 Fiziksel Güvenlik Yönetimi Prosedürü

Çalışma ortamı ve tesisler sadece yetkili kişilerin kullanımına izin verecek şekilde yapılandırılmış güvenlik sistemleri ile korunur.

➢ **Yaklaşım**

- Çalışma ortamı ve tesislerin güvenliği ile ilgili rol ve sorumlulukların yer aldığı bir süreç ve uygulama bulunur
- Çalışma ortamı ve tesislerin kullanımına yönelik yetki ve her biri için farklı giriş yetki tanımlaması yapılabilecek şekilde ayrıştırılmış lokasyon bilgileri tanımlanır
- Çalışma ortamı ve tesislerin (teslimat ve yükleme alanları dahikorunması için uygun minimum 2 (ardıl elektronik alt güvenlik sistemleri (x-ray, bariyer, kartlı geçiş sistemi, kapı ve pencere kontakları, CCTV, vb.) belirlenir, alınan tüm önlemler bir noktaya adreslenir, izlenir

- İlave fiziksel güvenlik gereksinimleri olan lokasyonlar açıkça tanımlanır (arşiv, sistem odası, laboratuar, güvenli alanlar, ofis alanı, vb.) ve gerekli ilave kontroller belirlenir
- Bina veya tesis perimetresi, fiziksel alt güvenlik tedbirleri çerçevesinde sağlam ve uygun nitelikte beton duvar üstü tel örgü/dikenli tel ile çevrilir
- Çalışma ortamı veya tesis kapıları, dıştan içe doğru olmak üzere kademeli bir şekilde fiziksel dayanımı yüksek ve minimum 2 (ik tedbirle desteklenmek suretiyle koruma altında tutulur
- Binada yüksekliği 6 m. den aşağ ıda olan pencereler, fiziksel veya elektronik önlem ile ayrıca denetim altında bulundurulur
- Dış kapılarda ve erişilebilen pencerelerde takılı olan izinsiz giriş saptama sistemleri eş zamanlı olarak izlenir ve müdahale edilir
- Çalışma ortamı veya tesislere girişte, görevli kişinin bulunduğu bir resepsiyon alanı veya girişin kontrol edilmesini sağlayan bir uygulama bulunur
- Çalışma ortamı veya tesisler genelinde haftanın 7 günü, günün 24 saati aktif olan insanlı alt güvenlik sistemi bulunur
- Çalışma ortamı veya tesisin insanlı alt güvenlik sistemi, "5188 sayılı Özel Güvenlik Hizmetlerine Dair Kanun" esaslarına göre yürütülmekle birlikte, onaylı bir koruma planı bulunur
- Çalışma ortamı veya tesisin duvar ve yangın çıkış kapıları "Binaların Yangından Korunması Hakkındaki Yönetmelik"te belirtilen standartlara uygundur, yangın kaçış hacimlerinden çalışma ofislerine geçiş, sınırlı ve elektronik tedbir denetimi altında tutulur
- Çalışan, stajyer, alt yüklenici, danışman veya diğer gerçek ve/veya tüzel kişiler ve ziyaretçiler kimliklerini tanımlayan kartlarını kolayca görünür şekilde taşırlar

- Personel tarafından ziyaretçi bilgisi, araç bilgisi, lokasyon, zamanlama ve görüşülecek kişiler detayında fiziksel güvenlik yönetimine yazılı olarak iletilir ve uygun giriş izni tanımlanır
- Ziyaretçiler refakatçi eşliğinde çalışma ortamı ve tesislere alınarak kişisel bilgileri, geliş ve ayrılış bilgileri kaydedilir
- Ziyaretçilerin bilgi güvenliği ile ilgili olarak uyması gereken kurallar belirlenir ve ziyaret başlamadan önce paylaşılır
- Çalışma ortamı ve tesislerde güvenlik risk analiziyle tespit edilen kritik alanlar kamera sistemleri ile sürekli gözetim altında tutulur ve kayıtları en az 30 (otuz) gün süre ile saklanır
- Prosedürel koruma tedbirleri çerçevesinde tutulan tüm manuel kayıtlar ve mevcutsa giriş kontrol sistemine ait tanıtım kartı personel trafik verileri minimum 2 (iki) yıl saklanır
- Fiziksel erişim yetkisi, bu yetkiye artık ihtiyaç kalmadığında derhal iptal edilir
- Çalışma ortamları ve tesisler için genel ve iş sağlığı ve güvenliği ile ilgili Mevzuat' a uyulur

➢ **Dağıtım**

- Çalışma ortamı ve tesislerin güvenliği ile ilgili olarak sorumluluklar ve uygulamalar tüm personel ile paylaşılır
- Çalışma ortamı ve tesis güvenliğini tehdide yönelik şüpheli belirtiler ve bu durumda yapılması gerekenler konusunda çalışanların farkındalığını artırmak üzere eğitim, etkinlik, vb. paylaşımlar düzenlenir

➢ **Gözden geçirme ve iyileştirme**

- Sadece yetkisi olan kişilere fiziksel erişim yetkisi verilmesini sağlamak amacıyla, fiziksel erişim kayıtları düzenli olarak en az haftada 1 (bir) kez gözden geçirilir

- Güvenlik sistemi dış denetim kapsamında yetkisiz giriş denemeleri de dahil olmak üzere drıll uygulamaları en az 3 (üç) ayda bir kez gerçekleştirilir
- Yangın için kullanılan alarm sistemleri haftalık bina zemininde bulunan yangın çıkış kapı alarm ve kilitleri gün lük periyodlar ile test edilir
- Fiziksel güvenlik kamera sistemlerinin verileri kayıt kalitesi ve süresi açısından hafta lık olarak kontrol ve test edilir
- Şirketin tabi olduğu Mevzuat' la birlikte ABC Grup politika ve prosedürleri kapsamı takip edilerek ilgili süreç güncel tutulur
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

Yangın, sel, deprem, patlama, terör veya diğer doğal/insan kaynaklı felaketler ile oluşan hasara karşı fiziksel koruma, Sivil Savunma planlarına ve ilgili Mevzuat'a göre tasarlanır ve uygulanır

- Çalışma ortamı ve tesislerin dış ve çevresel tehditlere karşı fiziksel koruması ile ilgili olarak sorumlulukların da yer aldığı bir Sivil Savunma planı bulunur
- Tehlikeli veya patlayıcı maddeler, çalışma ortamı ve tesislerin dışında güvenli bir mesafede depolanır, şirket içi kullanıma konu olan tehlikeli ve patlayıcı madde, kimyasal madde, vb. maddeler için uygun standartlar ve korunma yöntemleri geliştirilir
- Çalışma ortamı ve tesisler, gazlı ve otomatik söndürme sistemi ile 200 metrekare taban alan için ve her bağımsız kapalı bölüm için en az 1 (bir) adet yangın söndürme tüpü ile korunur
- Bilgi işlem alanlarında gazlı yangın söndürme sistemi olarak FM200 veya benzeri temiz maddeler kullanılır, otomatik fıskiyeler veya diğer su bazlı otomatik söndürme sistemleri devre dışı bırakılır

- Bilgi işlem alanları ile belirlenmiş diğer kritik noktalar toz, ısı, duman, nem ve su sızıntısına karşı dedektör koruması altında olup, bu noktalar 7 gün 24 saat kesintisiz izlenerek kontrol altında tutulur
- Yangın güvenlik sistemi ve alt üniteleri ile sahada kullanılan yangın söndürme tüpü, dahili anons panelleri dahil olmak üzere hydrant vb. sistem uzantılarının bakımı, periyodik bakım programlarına uygun olarak yapılır
- Çalışma ortamı ve tesisler yürürlükteki deprem yönetmeliklerine göre inşa edilir veya gerekli güçlendirmeler yapılır
- Çalışma ortamı ve tesislerin deprem riski gözönüne alınarak belirlenen cihazlar, deprem riskine karşı ilave kontrollerle sabitlenir (kabinet taban ağırlıkları, kayışlarla tavana sabitleme, vb.)
- Komşu tesislerden kaynaklanan tehditler değerlendirilir
- Tesisler, yıldırımlara karşı uygun paratoner sistemleri ile korunur
- Acil durumlara karşı tatbikat senaryoları hazırlanır, acil durumlarda görev alacak ekipler ve bu ekipler ile ilgili rol ve sorumluluklar belirlenir
- Seçilmiş personele, yangın söndürme cihazlarının kullanımıyla ilgili düzenli eğitim verilir
- Acil durumlara karşı bilinçlendirme eğitimleri, belirlenen düzenli aralıklarla tüm personele verilir (tahliye planları, yangın çıkışları, vb.)
- Acil durumlara karşı hazırlanmış olan tatbikat senaryoları belirlenen düzenli aralıklarla tüm personelin katılımı ile gerçekleştirilir, sonuçları organizasyonun ilgili bölümleri ile paylaşılır
- Algılayıcıların kontrol panelleri ve oluşturduğu alarmlar haftan ın 7 günü , günün 24 saat i izlenir ve kritik alarmlar sorumlu personele gönderilir
- Cihazların (algılayıcılar, detektörler, kontrol panelleri, vb.), iklimlendiriciler ve yangın söndürme sistemleri ve portatif cihazlar düzenli olarak kalibre edilir, kullanılabilirliği test edilir ve raporlanarak kayıt altına alınır

- Şirketin tabi olduğu Mevzuat' la birlikte ABC Grup politika ve prosedürleri kapsamı takip edilerek ilgili süreç güncel tutulur
- Paratoner sistemi ve topraklama uçların bakımı en a z yılda 1 (bir) kez olmak kaydıyla düzenli olarak yapılır
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.11 Tedarik,Destek ve Lojistik Hizmetler Yönetimi

Destek ekipmanları (iklimlendirme cihazları, nemlendirme cihazları, jeneratörler, kesintisiz güç kaynakları (UPS), sigorta panelleri, vb.), kesintisiz hizmet vermek amacıyla uygun koşullarda konumlandırılır ve korunur.

➢ **Yaklaşım**

- Destek ekipmanları, çalışma ortamlarına gereksiz girişi en aza indirecek şekilde konumlandırılır
- Tek bir noktadaki arızanın sistemin tümünü etkilemesinden kaçınmak için birden fazla elektrik besleme noktasının devrede olması sağlanır
- Klimaların, nemlendirme cihazlarının ve yangın söndürme sistemlerinin ihtiyaç duyabileceği kaynaklar, kritiklik seviyesine göre yedeklenir
- Acil durum elektrik kesme anahtarları, ekipman odalarındaki acil çıkışların yakınında yer alır
- Ana elektrik arızası olması halinde acil durum aydınlatması sağlanır
- Kesintisiz güç kaynağı (UPS) vardır, fiziksel güvenlik kontrollerinin elektronik altyapısı dahil kritik iş süreçlerini destekler
- Bilgi sistemleri ve kritik altyapıları destekleyen yedeklenmiş (redundant) bir UPS sistemi bulunur
- Uzun süreli elektrik kesintileri için bir jeneratör bulunur ve yeterli yakıt stoğu tutulur

- Ekipmanların bakım periyodlarına uygun olarak bakımı yapılır, bakım kayıtları tutulur
- Bakımlar sadece yetkili bakım personeli tarafından yapılır
- Kritik iş operasyonlarını destekleyen çalışma ortamları için klima sistemleri yedeklenir
- Destek ekipmanlarının bulundukları ortamlar, gerekli fiziksel güvenlik önlemlerini içerecek şekilde konumlandırılır
- Uygun görülen destek ekipmanları sigorta kapsamında değerlendirilir ve yapılan tüm bakım çalışmaları sigorta poliçelerine uygun yürütülür
- Enerji ve veri kabloları, hizmet sürekliliğinin sağlanması amacıyla korunur.
- Enerji ve veri kabloları yerleşimi (dağıtım panosu bileşenleri dahiile ilgili şemalar oluşturulur, güncellenir ve korunur
- Enerji ve veri kabloları, yetkisiz kişilerce ele geçirilmeye veya iç/dış hasara karşı kablo kanalı/tepsisi kullanarak, herkese açık yerlerden geçen
- rotalardan kaçınarak, vb. korunur
- Yüksek akım/yüksek gerilim kabloları ile veri kabloları, ayrı kanal/tepsi içerisinde konumlanır
- Kablolar ve dağıtım panoları net bir şekilde etiketlenir, bu etiketler güncel tutulur
- Kabloların fiziksel dış etkenlere karşı korunmasına yönelik kontroller uygulanır
- Dağıtım panolarına ve kablo odalarına erişim kontrol edilir (kilitli dolaplar, kilitli odalar, vb.)

➢ **Dağıtım**

- Destek ekipmanlarının kullanımına yönelik dokümantasyon hazırlanır ve gerekli personelin kolay erişilebileceği şekilde konumlandırılır
- Destek ekipmanlarının kullanımına yönelik olarak, bulundukları çalışma ortamlarındaki personel eğitilir
- Enerji ve veri kablolarına yönelik yapılacak her türlü çalışma için, iş sistemlerinin sürekliliği açısından organizasyondaki ilgili süreç sahipleri bilgilendirilir

➢ **Gözden geçirme ve iyileştirme**

- Tüm destek ekipmanları üretici tavsiyelerine göre düzenli olarak test edilir Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.12 Üçüncü Kişilerle İlişkilerin Yönetimi

- Şirket dışı gerçek ve/veya tüzel kişilerce ("Üçüncü Kişi/ler") erişilen, işlenen, paylaşılan veya yönetilen şirket bilgileri ve bilgilerin bulunduğu ortamların kullanım kuralları belirlenir.
- Üçüncü Kişiler'le yapılan çalışmaları konu alan her türlü sözleşme (gizlilik, bilgi paylaşımı, hizmet/servis sözleşmeleri, vb.), şirketin bilgi güvenliği yaklaşımını destekleyecek şekilde oluşturulur

➢ **Yaklaşım**

- Üçüncü Kişiler tarafından erişilen, işlenen, paylaşılan veya yönetilen şirket bilgilerinin ve bilgi işlem olanaklarının kullanım kuralları ve bu kuralların uygulama sorumluluklarını içeren dokümante edilmiş bir süreç ve uygulama bulunur

- Üçüncü Kişiler'le çalışmaya başlamadan önce üçüncü kişiyle hüküm ve şartları tanımlayan bir sözleşme imzalanır
- Üçüncü Kişiler'in şirket bilgilerine erişim ve bu bilgileri kullanımında işletme standart ve talimatları ile tüm güvenlik kuralları ve gereklilikleri ayrıntılı
- olarak belirtilir
- Üçüncü Kişiler tarafından yürütülecek çalışmalar, şirketin tabi olduğu Mevzuat dikkate alınarak değerlendirilir
- Üçüncü Kişiler kendi çalışanlarına, hizmet verdikleri şirketlerin bilgi güvenliği kurallarına uygun davranmaları konusundaki kişisel
- sorumluluklarını bildirir ve bu sorumluluklara uyumu garanti altına alır
- Üçüncü Kişiler, büyük çaplı hizmet kesintileri sonrasında, kararlaştırılan hizmet sürekliliği düzeylerinin sürdürülmesini sağlamak üzere tasarlanan uygulanabilir planlarla birlikte yeterli hizmet yetkinliğini devam ettirmesini sağlar
- Üçüncü Kişiler'in, hizmet verdikleri şirkete ait bilgi ortamlarını kullanarak şirketin bilgi güvenliği politikalarına aykırı şekilde davranması ve şirket
- itibarının tehlikeye düşürülmesinin önüne geçmek için sözleşmesel veya fiili her türlü tedbir alınır
- Üçüncü Kişiler'in hizmetlerini sağlamak amacıyla çalıştırdığı alt yüklenici firmaların, Üçüncü Kişinin uymakla yükümlü olduğu tüm işletme standart
- ve talimatları ile güvenlik kurallarına uygun hareket etmesini temin etmesi sağlanır
- Üçüncü Kişiler tarafından gerçekleştirilen elektronik veri akışı, elektronik ticaret ve elektronik haberleşme için ticari ve yasal yükümlülükler ile
- gerekli kontroller belirlenir
- Şirketin risk değerlendirme yaklaşımı, Üçüncü Kişilerin etkileyebileceği iş süreçleriyle bağlantılı risklerin değerlendirilmesini kapsar

- Üçüncü Kişiler' in erişmesi gereken bilgilere, bilgi işlem olanaklarına ve bu olanaklara kimlerin, ne tür erişim sağlayacağı (fiziksel, mantıksal, ağ bağlantısallığı, lokasyondan/ lokasyon dışından) belirlenir
- Erişim ile ilgili uygun kontroller hayata geçirilene kadar Üçüncü Kişilerin bilgi ve bilgi ortamlarına erişimi engellenir
- Üçüncü Kişiler'le yapılan çalışmaları konu alan her türlü sözleşme için tür, içerik, akış, onay, değişiklik, takip vb. konuları içeren süreç ve sorumluluklar belirlenir
- Sözleşmelerde, Üçüncü Kişiler'in faaliyetlerini denetleme hakkı, fikri mülkiyet haklarının kime ait olduğu ve olacağı, fikri mülkiyet haklarının kullanılma esasları ile gizlilik prensipleri diğer sözleşme hükümlerinin yanısıra mutlaka yer alır
- Sözleşmeler ile şirkete ait bilgiler gizlilik, bütünsellik ve erişilebilirlik açısından korunur ve sözleşme taraflarına, bilgileri sorumluluk bilinci içinde ve izin verilen şekillerde koruma, kullanma ve açıklama sorumlulukları bildirilir
- Üçüncü Kişiler'le, şirketin çalışma ortamı dışında elektronik veya fiziksel yollarla bilgi paylaşımına konu olan güvenlik kuralları belirlenir, sözleşme içerisinde ele alınır
- Sözleşmeler Üçüncü Kişi kullanıcı faaliyetini izleme ve iptal etme hakkı konularını kapsar
- Sözleşmelerde izlenebilirliği sağlayan ve inkar etmeyi olanak dışı bırakan kontroller belirlenir
- Sözleşmeler şirketin bilgi güvenliği yaklaşımının farkındalığına yönelik gereklilikleri kapsar
- Gizlilik sözleşmeleri Üçüncü Kişiler'in çalışmaları başlamadan önce yapılır
- Gizlilik sözleşmelerinde korunacak bilgilerin tanımı yapılır
- Gizlilik sözleşmelerinin süresi, paylaşılan bilgi ve bilgi ortamlarının hassasiyeti göz önüne alınarak belirlenir

- Gizlilik sözleşmelerinde, sözleşmenin feshedilmesi veya sona ermesi durumunda paylaşılan bilgilere uygulanacak prensipler belirtilir
- Gizlilik sözleşmelerinde, sözleşme hükümlerine aykırı davranış halinde takip edilecek prosedür belirlenir

➢ **Dağıtım**

- Şirketin bilgi güvenliği yaklaşımı ilişkide bulunulan Üçüncü Kişiler'le paylaşılır
- Üçüncü Kişiler'in erişim sağlayacağı bilgi ve bilgi işlem olanakları ile erişim yolları ve bu erişim yollarını kullanacak dış personelin bilgileri, güncel olarak organizasyonun ilgili bölümleriyle paylaşılır
- Organizasyon içerisinde Üçüncü Kişiler'le çalışma yapacak her personel, sözleşme yönetimi konusunda bilgilendirilir

➢ **Gözden geçirme ve iyileştirme**

- Üçüncü Kişiler'le yapılan çalışmaları konu alan her türlü sözleşme (gizlilik, bilgi paylaşımı, hizmet/servis sözleşmeleri, vb.), şirketin bilgi güvenliği yaklaşımını destekleyecek şekilde oluşturulur
- Sözleşme gereklilikleri, belirli aralıklarla ve bunları etkileyen değişiklikler olduğunda gözden geçirilir
- Üçüncü Kişiler'den alınan hizmetler izlenir, gözden geçirilir ve yapılan sözleşmelerdeki bilgi güvenliği koşullarına uyumu kontrol edilir
- Üçüncü Kişiler'den alınan hizmetlere ilişkin denetim ve güvenlik durumlarıyla ilgili kayıtlar, operasyonel sorunlar, arızalar, sunulan hizmetle ilgili hata ve kesintiler izlenir, sözleşmeye uygunluğu kontrol edilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.13 Kurumsal İletişim Yönetimi

Sosyal paydaşlarla iletişime konu olan bilgi doğruluk, şeffaflık ve güven prensipleriyle gizlilik, bütünsellik ve erişilebilirlik açısından korunarak yönetilir

- **Yaklaşım**

  - Sosyal paydaşlarla iletişime konu olan bilgiler, kurumsal iletişim süreçleri dahilinde paylaşılmadan önce gerekli onay sürecinden geçirilir
  - Herkesin erişimine açık bilgiler yayınlanmadan önce bu bilgilerin kişisel verilerin korunması, fikri mülkiyetin korunması, Mevzuat'a uygunluk kapsamında değerlendirilmesini sağlayacak bir süreç ve sonrasında da güncel olmasını ve yanıltıcı nitelikte öğelerden arındırılmasını sağlayacak bir süreç tanımlanır
  - Herkesin erişimine açık bilgilerin yayınlandığı sistemlerde, bilgilerin bütünselliği ve erişilebilirliği uygun yöntemlerle korunur
  - Kurumsal iletişim süreçleri kapsamındaki bilgiler “ABC Topluluğu İletişim Rehberi” ve “ABC Grup Bilgilendirme Politikası” esaslarına uygun nitelik taşır
  - Kurumsal iletişim süreçleri kapsamındaki bilgiler kurum kimliği esaslarına uygunluk açısından iç onay süreçlerinden geçirilir
  - Şirket tarafından oluşturulan yıllık stratejik iletişim planları, “ABC Topluluğu İletişim Rehberi”nde belirtilen esaslar çerçevesinde hazırlanır
  - Medya ilişkileri süreci, Topluluk genelinde aşağıdaki rol dağılımlarına uygun şekilde doğru bilgi, şeffaflık ve güven prensipleriyle yönetilir:

-ABC Şirketi Yönetim Kurulu Başkanı: Topluluk vizyon, misyon ve yönetim felsefesi, politik değerlendirmeler

- ABC Şirketi CEO'su: Hedefler, makroekonomik değerlendirmeler, önemli satın almalar, birleşmeler, yeni pazarlara

giriş veya çıkış, Topluluğun faaliyet alanlarına ilişkin strateji, yaklaşım ve hedefleri

- Grup Başkanları: İlgili sektör-fonksiyona ilişkin strateji ve hedefleri ilgili sektör-fonksiyona ilişkin makro değerlendirmeler (pazar

bilgileri, sorunlar ve gelecek projeksiyonları), ilgili sektördeki yeni yatırımlar ve yeni kategoriler

- Genel Müdürler ve Yetkilendirilmiş Genel Müdür Yardımcıları/Direktörler: Şirketin içinde bulunduğu pazara ilişkin değerlendirmeler, şirket ve ürünleri ilgili stratejiler ve büyüme planları, şirketin ciro, kar ve üretim rakamları, uzmanlık alanlarıyla ilgili gelişmeler ve görüşler

- Grup Sözcüsü: Kriz döneminde yapılacak açıklamalar

- ABC şirketi yurtdışı lokasyonları, genel merkezlerinin koordinasyonunda, ABC Topluluğu Kurumsal İletişim Direktörlüğü'nün görüşlerini de alarak iletişim faaliyetlerini hayata geçirir
- ABC Topluluğu şirketleri ve yönetilen markalarının konumlanma ve online mecralara yönelik iletişim çalışmaları ile ilgili stratejisi belirlenir, şirketler bu doğrultuda ilgili mecralarda markasını yönetir ve etkisini ölçümler
- ABC Topluluğu şirketleri kriz yönetimi prensipleri çerçevesinde, kendi kriz iletişim planlarını oluşturur ve ABC Topluluğu Kurumsal İletişim Direktörlüğü ile paylaşır
- ABC Topluluğu şirketleri, iş akışı içerisinde ortaya çıkan etkinliklerini, planlama aşamasında ABC Topluluğu Kurumsal İletişim Direktörlüğü'nü bilgilendirerek, ABC marka değerlerine ve topluluk ilkelerine uygun şekilde kurgular
- ABC Topluluğu şirketleri, kuruluşundan itibaren tüm arşivsel doküman, görüntü ve fotoğrafı uygun koşullarda, yetkisiz erişim ve kullanıma yönelik kontrolleri alarak saklar
- Herkesin erişimine açık bilgilerin yayınlandığı sistemler için açıklıklara ve tehditlere karşı düzenli olarak zaafiyet tarama ve sızma testleri yapılır

- Yüksek bütünlük gerektiren ve herkesin erişimine açık bilgilerin yayınlandığı sistemlerde kullanıma açılan yazılımlar, veriler ve diğer bilgiler uygun mekanizmalarla korunur
- Şirketin yönetiminde olan online mecralar, bilgilerin her türlü veri koruma mevzuatına uygun olarak toplanma, işlenme, paylaşım ve depolanma sırasında hassas bilgilerin korunmasını sağlamak üzere özenle kontrol edilir

➢ **Dağıtım**

- Medyanın çeşitli birimleri ile farklı ortam ve zamanlarda sürekli iletişim halinde olan yöneticiler, göreve geldiklerinde ABC Topluluğu Medya Eğitimi'ni alırlar
- Şirketler gerekli durumlarda çalıştıkları üçüncü partileri de, bu süreçle ilgili bilgilendirirler

➢ **Gözden geçirme ve iyileştirme**

- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.14 Erişim Yönetimi Prosedürü

Erişimle ilgili gereklilikler değerlendirilerek fiziksel ve elektronik erişim kontrolleri yönetilir.

Kullanıcı erişim yönetimi, kullanıcı kaydı yaratma/değişiklik/silme, doğrulama, vb. unsurlar, yetkili kullanıcıların görevlerini yapabilmeleri amacıyla yeterli ve fakat yetki sınırlarını aşmalarına izin verilmeyecek şekilde yapılandırılır.

Ayrıcalık yönetimi, erişim ayrıcalıkları sunulan kullanıcıların erişim hakları, güvenlik gereklilikleri dikkate alınarak yönetilir.

- **Yaklaşım**

  - Organizasyonel rol ve sorumluluklara göre, erişim kontrol tablosu hazırlanarak erişim hakları açıkça belirtilir
  - Erişim kontrol tablosu görevler ayrılığı ilkesi göz önüne alınarak hazırlanır, görev ayrılığı yapılamaması durumlarında, faaliyetlerin izlenmesi, ayrıntılı geçmiş bilgileri ve yönetimin gözetimi gibi kontroller uygulanır
  - Erişim kontrol tablosu hazırlanırken gereken roller için fiziksel ve elektronik erişim kontrolleri birlikte dikkate alınır
  - Erişim talebi, erişim haklarının belirlenmesi, erişim yetkisi verilmesi/kaldırılması birbirinden ayrı ele alınır
  - İş uygulamalarının ve ağların (test ortamlarının bulunduğu ağ, kritik iş sistemlerinin bulunduğu ağ, vb.) güvenlik gereklilikleri erişim kontrolü açısından dikkate alınır
  - Erişim hakları tanımlanırken ilgili politikalar ve yetkiler dikkate alınır ("bilmesi gerekenler" ilkesi ve güvenlik düzeyleri, bilgilerin sınıflandırması, vb.)
  - Kullanıcı bilgisayarlarında tutulan iş bilgileri özel bir dizin altında ve yetkisiz erişime karşı uygun şifreleme yöntemleriyle korunur
  - Bilgilere veya hizmetlere erişimin korunmasıyla ilgili Mevzuat ve her türlü sözleşmesel yükümlülük dikkate alınır
  - Kullanıcı erişim yönetimi (kullanıcı kaydı yaratma/değişiklik/silme, doğrulama, vb.) ile ilgili olarak sorumlulukların da yer aldığı bir süreç ve uygulama bulunur
  - Kullanıcıların, yaptıkları işlemlerle bağlantılarının kurulabilmesi ve bunlardan sorumlu tutulabilmeleri için benzersiz kullanıcı kimlikleri kullanılır
  - Kullanıcı kaydı yaratma/değişiklik/silme, doğrulama, ayrıcalık ve parola yönetimi süreçleri şirketin bilgi güvenliği politikası ile tutarlı olması sağlanır
  - Erişim haklarının verilmesi, değiştirilmesi ve kaldırılması ile ilgili bir kimlik ve erişim yönetimi çözümü kullanılır

- Kullanıcı erişim yönetimi, verilen erişim yetkilerinin görevler ayrılığına ilkelerine uygun olarak verildiğinin kontrol edilmesini kapsar
- Yetkilendirme süreci tamamlanana kadar kullanıcı kaydının kullanıma açılmaması sağlanır
- Görevleri veya işleri değişen veya şirketten ayrılan kullanıcıların erişim hakları en fazla 1 (bir) saat içer is inde kaldırılır
- Geçmişte kullanılmış olan kullanıcı kimliklerinin, başka kullanıcılara verilmemesi sağlanır
- Yetkisiz erişim denemelerinde bulunulması halinde uygulanacak yaptırımlar belirlenir ve yaptırımlar iş akdi/hizmet sözleşmesinde yer alır
- Erişilecek bilgilerin hassasiyeti açısından daha güçlü kimlik doğrulama gereken durumlarda şifreleme araçları, akıllı kartlar, şifre üreten araçlar veya biyometrik çözümler gibi alternatifler yöntemler değerlendirilir ve uygulanır
- Her bir sistem/uygulama bağlantılı erişim ayrıcalıkları belirlenir
- Ayrıcalıklar, erişim kontrolü yaklaşımı doğrultusunda, rol ve sorumluluk bazında belirlenir, onaylanır ve verilen ayrıcalıkların kaydı güncel olarak tutulur
- Ayrıcalıkların verilmesi durumunda oluşabilecek riskler değerlendirilerek ilave kontroller sağlanır
- Kullanıcılarının ve bilgi işlem personelinin erişim ayrıcalıkları, ilgili süreç sahipleri tarafından onaylanır
- Yetkilendirme süreci tamamlanana kadar ayrıcalıkların devreye alınmaması sağlanır
- Kullanıcılara ayrıcalık tanımak gereğinden kaçınmak için sistem rutinlerinin geliştirilmesi ve kullanımı özendirilir
- Sistem yöneticiliği ayrıcalıklarının uygunsuz kullanımı (bir bilgi sisteminin, kullanıcının, sistem veya uygulama kontrollerini geçersiz kılabilmesini sağlayan her türlü özelliği veya olanağı kontrol edilir ve izlenir

- İzne çıkan ayrıcalıklı kullanıcının erişim hakları pasif hale getirilir
- Görevleri veya işleri değişen veya şirketten ayrılan, ayrıcalıklı kullanıcının erişimi olan tüm sistemler üzerindeki kimlik doğrulama bilgileri, araçları ve erişim hakları en fazla 1 (bir) saat içerisinde iptal edilir
- Ayrıcalıklı kullanıcıların erişim haklarıyla ilgili erişim koşulları ve sorumluluklarına yönelik farkındalıkları artırılır

➢ **Dağıtım**

- Erişim kontrol tablosu, erişelecek bilginin sahibi olan şirket süreç sahipleri ile oluşturulur, organizasyonun ilgili bölümleri ile paylaşılır
- Hassas bilgilere erişecek kullanıcıların erişim haklarıyla ilgili erişim koşulları ve sorumluluklarına yönelik farkındalıkları artırılır
- Kullanıcıların erişim hakları terfi, değişiklik veya işten çıkma/çıkarılma gibi her türlü durumdan sonra gözden geçirilir
- Kullanıcı erişim yönetimi verilen erişim yetkilerinin, görevler ayrılığıilkelerine uygun olarak verildiği kontrol edilir
- Artık kullanılmayan kullanıcı kimlikleri ve hesapları belirli aralıklarla gözden geçirilerek kaldırılır
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır
- Ayrıcalıklı kullanıcıların erişim haklarıyla ilgili erişim koşulları ve sorumluluklarına yönelik farkındalıkları artırılır

➢ **Gözden geçirme ve iyileştirme**

- Erişim kontrol tablosu en az yılda 2 (iki) kez olmak kaydıyla gözden geçirilir

- Erişim kontrol tablosu ve bu tabloya ilişkin erişim kayıtları en az yılda 2 (iki) kez olmak kaydıyla karşılaştırılarak, varsa başarılı/başarısız yetkisiz erişim denemeleri incelenir
- Personelin görev ve sorumluluklarındaki değişikliklerin, görevler ayrılığı ilkesine uygun olup olmadığı değerlendirilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır
- Yetkisiz ayrıcalıkların elde edilmemesi için ayrıcalık dağıtımları, düzenli aralıklarla kontrol edilir
- Ayrıcalıklı hesaplardaki değişiklikler, belirli aralıklarla gözden geçirilmesi için kayıt altına alınır
- Ayrıcalıklı erişim yetkilerinin, görevler ayrılığı ilkelerine uygun olarak verildiği kontrol edilir
- Personelin şirket veya Topluluk içinde görev değişikliği yapması durumunda kullanıcının ayrıcalıklı erişim hakları gözden geçirilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.14.1 Parola Yönetimi Prosedürü

Bilginin gizlilik, bütünsellik ve erişilebilirlik açısından korunması amacıyla uygun parola yönetim çözümleri uygulanır

➢ **Yaklaşım**

- Şirketin bilgi güvenliği yaklaşımına paralel olarak parola yönetimi ile ilgili bir politika oluşturulur
- Bilgi sistemlerinde kullanıcı kimliğinin belirlenmesi ve gerçeklenmesi için güçlü parola, iki faktörlü doğrulama yöntemleri veya akıllı kartlar gibi donanımsal şifre üreten cihazlar, vb. kullanılır

- Kullanıcılar, iş amaçlı olarak kendilerine verilen kişisel parolaları korur
- Parolaların en az 3 (üç) ayda bir kez olmak kaydıyla düzenli olarak değiştirmesini zorunlu kılan bir parola yönetim sistemi kullanılır
- Kullanıcılara başlangıçta güvenli bir geçici parola verilir, bu parolanın sisteme ilk girildiğinde değiştirilmesi zorunlu kılınır
- Geçici parolalar kullanıcılara güvenli bir şekilde iletilir
- Geçici parolalar bireye özel ve benzersiz olup tahmin edilemez özellikte seçilir
- Parolaların bilgisayar sistemleri, dokümanlar, vb. ortamlarda gerekli koruma önlemleri alınmadan tutulmaması sağlanır
- Tüm varsayılan (sistemle/yazılımla gelen) parolalar, sistemlerin veya yazılımların kurulması ile birlikte sisteme ilk girildiğinde değiştirilir
- Tüm kullanıcıların nitelikli (güçlü) parolalar kullanmasını zorunlu kılan bir parola yönetim sistemi kullanılır
- Parolalar rakamlar, özel karakterler ve hem büyük hem küçük harflerden seçilir ve en az 8 karakter uzunluğunda oluşturulur
- Parolalarda, başka kişilerin kolayca tahmin edebileceği veya kişiyle bağlantılı bilgileri kullanarak elde edebileceği herhangi bir şeyin (ör. ad, soyad, çocuğunun adı ve doğum tarihleri vb.) kullanılmaması sağlanır En az son 3 (üç) kullanılan parolanın seçilmesi önlenir
- Ayrıcalıklı hesaplara ait parolalar, en az 30 (otuz) günde b ir olmak kaydıyla değiştirilir
- Bir parola değişikliğinden sonra kullanıcılar, parolayı en az 1 (bir) gün boyunca tekrar değiştiremezler (min password age)
- Tüm kullanıcılar, parolalarının geçerliğini kaybetmesinden en az 10 (on) gün önce uyarılmaya başlanır

- Parola yönetim sistemi, kullanıcıların kendi parolalarını seçmelerine ve değiştirmelerine izin verir

➢ **Dağıtım**

- Tüm kullanıcılar, parolaların gizli tutulması konusunda bilgilendirilir
- İş amaçlı şirket içi veya dışından erişilen her türlü sistem/uygulama için "beni hatırla (save password)" opsiyonun işaretlenmemesi konusunda kullanıcılar bilgilendirilir
- Tüm kullanıcılar, aynı parolayı hem iş hem iş dışı amaçlarla kullanmamaları konusunda bilgilendirilir

➢ **Gözden geçirme ve iyileştirme**

- Parola yönetim sisteminin aktivite ve sistem kayıtları en az 1 (bir) ay süre ile tutulur ve olağan dışı durumlar değerlendirilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.14.2 Sistem Kullanıcı Şifrelerine İlişkin Teknik Ayarlar Uygulama

- Sistem Kullanıcı Şifresi geçerlilik süresi 90 gündür. Bu süre sonunda sistem sizden şifrenizi değiştirmenizi isteyecektir. (İşletim sistemi dışındaki program ve uygulamalar 'force' etmiyor ve otomatik değiştirme istemiyor ise bu durumda kullanıcılar bir mesaj ile uyarılarak manual olarak şifrelerinin değiştirilmesi istenecektir. Mesaj, Bilgi Sistemleri ve İş Geliştirme adresinden ayda bir kez periyodik olarak gönderilir.)
- Minimum 8 karakter uzunluğunda şifre belirlenmesi gerekmektedir. Ayrıca şifrenizin kompleks şifre standartını kapsaması gerekir. Verilecek şifrenin aşağıdaki listede yer alan kriterlerden en az üç tanesini kapsıyor olması gerekmektedir.

  - Büyük Harf (A - Z)

- Küçük hart (a - z)
- Basit Sayı (0 - 9)
- Özel Karakter (!, $, #, %,... v.b.)

- Ek olarak yeni şifreniz içerisinde kullanıcı adınızda yer alan ardışık 3 ya da daha fazla karakterin kullanılmasına izin verilmemektedir.

  Örnek :

  - Kullanıcı Adı: BahadırKandemirli
  - BaK12Gd? (Kullanıcı adında yer alan 3 karakter ardışık olarak kullanıldığı için şifre complex password policy'e uygun değil.)
  - asdfg123 (Şifre içerisinde en az 3 kriter kullanılmadığından dolayı şifre complex password policy'e uygun değil.)
  - gHr&34r (Şifrenin en az 8 karakter karakter olması gerekmektedir.)
  - AwE4p54s (4 Kriterden en az 3 tanesini kapsadığından şifre complex password policy'e uygun.)
  - gky7u8?e (4 Kriterden en az 3 tanesini kapsadığından şifre complex password policy'e uygun.)

- **Not:** Şifrelerinizi belirlerken, şifre içerisinde Türkçe karakter olmaması önerilir. Türkçe karakterler kullanılması farklı dil seçenekleri (İngilizce, Türkçe klavye) olan bilgisayarlarda hatalı şifre girilmesi nedeni ile hesabınızın kilitlenmesi (account lock) problemine neden olabilecektir.
- Şifre değiştirirken son 12 şifrenin kullanılamaması
- Şifrenin 5 defa yanlış yazılmasında Account Lock (kullanıcı hesabı kilitlenmesi) Daha önce kullanmış olduğunuz şifreyi tekrar kullanamazsınız. Bu durumda sistem 10 dakika sonra tekrar şifrenizi denemenize izin verir. Bu durumda da hatırlayamaz iseniz lütfen servicedesk'e başvurunuz.

4.3.14.3 Güvenli Oturum Açma/Kapama Prosedürü

Yetkisiz kullanıcıların, herhangi bir bilgiye veya sisteme erişimleri güvenli oturum açma/kapama yöntemleri ile önlenir

- **Yaklaşım**

  - Yetkisiz erişim olasılıklarını en aza düşürecek şekilde güvenli oturum açma / kapama süreci tasarlanır
  - Kullanıcıların erişim yetkisi olmayan bir sistemde oturum açması ile ilgili kontroller (sistemin versiyon ve uygulanan son yama numaralarını görüntülenmemesi, erişim için girilen bilgilerin hangi kısmının doğru veya hatalı olduğunu belirtilmemesi, vb.) uygulanır
  - Ulaşılmak istenen sistem veya uygulama ile ilgili sistem veya uygulamaları tanımlayıcı bilgilerin, güvenli giriş tamamlanıncaya kadar ekranda görünmemesi sağlanır
  - Oturum açma sırasında, sistemlere sadece yetkili kullanıcıların girmesi gerektiğine dair genel bir uyarı görüntülenir
  - En fazla 5 (beş) denemeye kadar başarısız oturum açma denemesine izin verilir
  - İzin verilen başarısız deneme sayısına ulaşıldıktan sonra veri bağlantıları kesilir, sistem sorumlularına bir alarm mesajı gönderilir
  - Belirli yetkilendirme olmaksızın başka oturum açma denemesine izin verilmeden veya başka deneme yapılması reddedilmeden önce en fazla 30 (otuz) dakika beklemeye mecbur bırakılır
  - Oturum açma mekanizması, kullanıcılara (oturum açma işlemi başarılı olduğund son başarılı oturum açma tarihini/saatini ve en son başarılı oturum açışından sonraki tüm başarısız oturum açma denemeleriyle ilgili bilgi verecek şekilde yapılandırılır
  - Parolaların, ağ üzerinden gönderilmesi ile ilgili kontroller (şifrelenmiş metin, vb.) belirlenir

- Sistemler ve uygulamalar için açılan oturumların süresi sınırlıdır, en fazla 1 (bir) saat boyunca hareket olmamasının ardından oturumu kapatan bir zaman aşımı özelliği vardır
- En fazla 2 (ik saat boyunca hareket olmamasının ardından hem uygulamayı hem ağ oturumlarını kapatan bir zaman aşımı özelliği vardır
- Çalışma ortamı dışında kalan halka açık veya dış alanlar gibi yüksek riskli yerlerden yapılan bağlantılarda, hassas uygulamalar için bağlantı süresi kontrolleri değerlendirilir ve uygulanır

➢ **Dağıtım**

- Hassas bilgiye ve sistemlere erişen kullanıcılar güvenli oturum açma/kapama yaklaşımları ile ilgili bilgilendirilir

➢ **Gözden geçirme ve iyileştirme**

- Başarılı ve başarısız denemeler kaydedilir ve düzenli olarak gözden geçirilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.14.4 Ekran ve Masa Üstü Temizliği Prosedürü

Fiziksel çalışma ortamında yer alan bilgilerin gizlilik, bütünsellik ve erişilebilirlik açısından korunması sağlanır

➢ **Yaklaşım**

- Fiziksel (temiz mas ve elektronik (temiz ekran) çalışma ortamında yer alan bilgilerin gizlilik, bütünsellik ve erişilebilirlik açısından korunmasına yönelik bir politika oluşturulur

- Basılı hassas evraklar ve hassas elektronik bilgi barındıran depolama ortamları (dizüstü bilgisayar, harici disk, flash memory,vb.), gerekli olmadıkları zamanlarda güvenli ortamlarda tutulur
- Toplantı odası, konferans salonu, vb. alanların bilgi güvenliği açısından kullanım kuralları belirlenir
- Çalışma ortamından kısa süreli ayrılırken, bilgisayarlarda oturum kapatılır (log-off)
- Mesai saatleri dışında çalışma ortamlarında ve güvenli koşullarda bırakılan bilgisayarlar kapatılır (shut-down)
- Şirket içindeki gelen ve giden evrakların dağıtımı sırasında uygulanması gereken kontroller belirlenir
- Yazıcı, fotokopi makinesi ve tarayıcı cihazların yetkisiz kullanımı önlenir
- Kullanıcı oturumları için, parola korumalı ekran koruyucular devreye alınır
- Taşınabilir haberleşme cihazlarında yetkisiz erişimi önlemek için gerekli şifreleme teknikleri kullanılır

➢ **Dağıtım**

- Fiziksel (temiz masve elektronik (temiz ekran) çalışma ortamındaki bilgilerin gizlilik, bütünsellik ve erişilebilirlik açısından korunması ile ilgili farkındalığı artıracak uygulamalar (toplantı odaları kullanım kuralları, kağıt öğütücülerin kullanımı, yazıcı kullanımı, vb.) devreye alınır
- Şirketin temiz masa ve temiz ekran kuralları, kullanıcılarla paylaşılır

➢ **Gözden geçirme ve iyileştirme**

- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.14.5 Uzatan Erişim (Remote Access) Prosedürü

Uzaktan bağlanan kullanıcıların güvenli erişim sağlamaları amacıyla uygun koruma yöntemleri uygulanır

- **Yaklaşım**

  - Uzaktan erişim yapmaya yetkili kullanıcılar ile yetkili oldukları sistem/uygulamalar belirlenir
  - Üçüncü Kişiler'in canlı sistemlere dış bağlantıları için iş ve ağ sahibi tarafından ihtiyaç belirlenir, riski değerlendirilir, gerektiği durumlarda ilave kontroller uygulanır
  - Uzaktan erişim için kullanabilecek cihaz türleri (dizüstü bilgisayarlar, akıllı telefonlar vb.) ve kullanacak kişiler belirlenir
  - Uzaktan erişim yetkisi kalktığında yetkinin ve erişim haklarının iptaline ve cihazların iadesine yönelik bir süreç uygulanır
  - Uzaktan erişim sağlayan kullanıcıların erişimini kontrol etmeye yönelik kimlik doğrulama yöntemleri değerlendirilerek uygun yöntem kullanılır (şifrelemeye dayanan bir teknik / donanımsal parola üretme araçları / bir sorgulama - yanıt protokolü olan bir sanal özel ağ (VPN), vb.)
  - Uzaktan erişim sağlayan kullanıcılara, güvenli bir ağa erişinceye kadar geçtikleri her bir ağ bileşeninde (düğümd kimlik doğrulaması yapılır
  - Ağa gelen tüm dış erişimler belirlenerek kontrol edilir, onaylanır, izlenir ve şirketin belirleyeceği süre boyunca saklanır
  - Uzaktan erişim için kullanıcı kayıt ve silme süreci, “Bölüm 9 - Kullanıcı Erişim Yönetimi” bölümüne uygun olarak yapılır
  - Ağ tasarımı, dışarıdan gelen trafiği, sadece ağın belirli kısımlarıyla sınırlandıracak ve tanımlı giriş noktalarına yönlendirecek şekilde yapılandırılır
  - Yetkisiz dış bağlantılar, “ağ yönetimi” ve “tanı” araçları kullanılarak (port probları ve ağ keşif / haritalama araçları, vb.) saptanır

- Uzaktan erişim, güvenilir ve eksiksiz bir kimlik doğrulama yöntemi ile sağlanır

➢ **Dağıtım**

- Uzaktan erişim ihtiyacı olan kullanıcılar süreç hakkında bilgilendirilir
- Üçüncü Kişiler'in uzaktan erişim ihtiyaçları için organizasyonun tümünü kapsayacak şekilde ilgili kişiler bilgilendirilir

➢ **Gözden geçirme ve iyileştirme**

- Yetkisiz dış bağlantılara ait kayıtlar o luştukça ve düzenli aralıklarla en az ayda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Uzaktan erişim kayıtları (başlangıç / bitiş zamanı, süresi, giriş yapılan sistemler,kullanıcı izleme bilgileri, vb.) ve düzenli aralıklarla en az 3 (üç) ayda bir kez olmak kaydıyla gözden geçirilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.15 Mevzuata Uyum

Bilgi güvenliğini etkileyen Mevzuat ve sözleşmeler ile ilgili tüm gereklilikler belirlenir, uyulur ve izlenir.

Bireylerle ilgili kişisel verilerin uygunsuz ve kontrolsüz kullanımı önlenir, ilgili Mevzuat'tan doğan gerekliliklere uyulur.

➢ **Yaklaşım**

- Bilgi güvenliğini etkileyen ve şirketin uymakla yükümlü olduğu (faaliyet gösterilen ülke yasaları dahiyasa ve yönetmelikler belirlenir
- Bilgi güvenliğini etkileyen Mevzuat ve/veya sözleşmelerden doğan gereklilikler, yönetim, iş sahipleri, bilgi güvenliği ve diğer ilgili fonksiyonların (hukuk, operasyonel risk, denetim, iletişim, insan kaynakları, fiziksel

güvenlik, bilgi sistemleri, vb.) süreç sahipleri ile etkileri ve yaptırımları açısından değerlendirilir

- Bilgi güvenliğiyle ilgili Mevzuat güncel haliyle takip edilir
- Bilgi güvenliğiyle ilgili Mevzuat'a, sözleşme hükümlerine, sektör standartlarına ve şirket politikalarına göre saptanan uyumluluk gereklilikleri, risk değerlendirme çalışmalarında dikkate alınır
- İş süreçleri tasarlanırken ve yürütülürken Mevzuat ve/veya sözleşmelerden doğan bilgi güvenliği gereklilikleri dikkate alınır
- Organizasyonel kayıtlar(muhasebe kayıtları, fatura, sözleşme, işlem kayıtları (log), denetim kayıtları (log), vb.), Mevzuat, sözleşme ve ticari gerekliliklere uygun sürelerle kaybolmaya, imha edilmeye veya değiştirilmeye karşı korunur
- Kişisel verilerin korunması ile ilgili çalışmalar, kişisel verileri söz konusu olan gerçek ve/veya tüzel kişilerin dokunulmazlığı, maddi ve manevi varlığı ile temel hak ve özgürlükleri korunması amacıyla oluşturulan ve kişisel verileri işleyen kişilerin uyacakları esas ve usulleri düzenleyen Mevzuat'tan kaynaklanan gereklilikleri dikkate alır
- Kişisel verilerin kaybolmaya, bozulmaya, izinsiz erişilmeye, kullanıma, değiştirilmeye, ifşa edilmeye veya herhangi başka bir yanlış kullanıma karşı korunmasına yönelik olarak şirket dışı üçüncü kişileri de kapsayacak şekilde uygun teknik ve organizasyonel önlemler alınır
- Kişisel verilerin bulunduğu ortamlar, beyanı, verilerin elde edilme yöntemleri, bu verilerin kullanımı ve doğruluğuna yönelik kriterler belirlenir
- Kişisel verilerin gizli tutulması, hukuka ve dürüstlük kurallarına uygun olarak işlenmesi, belirli, açık ve meşru amaçlar için toplanması ve bu amaçlara aykırı olarak yeniden işlenmemesi, toplandıkları amaçla bağlantılı, yeterli ve orantılı olması, doğru olması ve gerektiğinde güncellenmesi, gerekli olduğu süre kadar muhafaza edilmesi sağlanır

- Kişisel verilerin kaydedildikleri ve yeniden işlenme amaçlarının ortadan kalkması durumunda, bu verilerin silinme veya yok edilmesinin kriterleri belirlenir, kişisel veri sahibi bilgilendirilir
- Kişisel verileri kaydedilen ve/veya yeniden işlenen kişilerin, bu bilgiler toplanmadan, depolanmadan, işlenmeden veya üçüncü şahıslara açıklanmadan önce onayı alınır ve bu kişiler kullanım amaçları konusunda bilgilendirilirler
- Üçüncü Kişiler'le yapılan sözleşmeler, kişisel verilerin korunmasına yönelik adımları içerir

➢ **Dağıtım**

- Bilgi güvenliğini etkileyen Mevzuat ve/veya sözleşmelerden doğan gereklilikler, ilgili tüm fonksiyonlarla (hukuk, operasyonel risk, denetim, iletişim, insan kaynakları, fiziksel güvenlik, bilgi sistemleri, vb.) paylaşılır
- Bilgi güvenliğiyle ilgili Mevzuat güncel haliyle ilgili tüm fonksiyonlarla bilgi paylaşılır
- Şirket, personelin ve Üçüncü Kişiler'in, kişisel verilerin gizliliğinin ve korunmasının öneminin farkında olmasını sağlar
- Kişisel veriye erişim sağlayacak tüm personel, stajyer, şirketle iş ilişkisine giren Üçüncü Kişiler vb., kişisel verilerin korunması için bilgilendirilir

➢ **Gözden geçirme ve iyileştirme**

- Bilgi güvenliğini etkileyen Mevzuat gerekliliklerine uyum, Mevzuat'ta değişiklik meydana gelmesi halinde Mevzuat'ın güncel haline göre bahse konu uyumun yeniden oluşturulması için gerekli gözden geçirmeler ile gerçekleştirilir
- Mevzuat değişikliklerine uyumun sağlanmasının ardından, süreçler gerekli her türlü değişikliği barındıracak şekilde güncellenir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir

- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.16 İş Sürekliliği Prosedürü

Süreçler analiz edilerek iş sürekliliği stratejisi belirlenir, kapsam, gereksinim ve planlar oluşturulur.

İş sürekliliği planları, güncel ve etkili olmalarının sağlanması amacıyla düzenli olarak test edilir ve güncellenir.

➢ **Yaklaşım**

- İş sürekliliği yönetimi, ürünlerin, servislerin ve iş süreçlerinin devamlılığını sağlamak üzere gerekli planları, potansiyel iş kesintileri göz önünde bulundurularak yönetim tarafından onaylanmış kurtarma stratejilerini, rol ve sorumlulukları içerir
- Şirket içinde yürütülen çalışmaları kapsayan süreçler ve birbirleriyle olan etkileşimleri belirlenir
- İş etki analiz (Business Impact Analysis – BI çalışmaları gerçekleştirilerek kritik iş süreçleri belirlenir ve önceliklendirilir
- Kritik iş süreçleriyle ilgili tüm bileşenler insan, süreç, teknoloji açısından değerlendirilerek saptanır ve her bileşen için kurtarma zaman hedefi (RTO) ve kabul edilebilir veri kaybı hedefi (RPO) belirlenir
- Şirket iş süreçlerinde kesintilere yol açabilecek tüm durumlar saptanır
- Şirket içi ve dışı ticari bağımlılıklar ve yürürlükteki sözleşmeler ile etkileri değerlendirilir
- Kesintilerin olasılıklarının ve zaman, hasar ölçeği ve normale dönme süresi açısından etkilerinin değerlendirilmesi için risk analizi yapılır
- İş sürekliliği risk analizinde riskler, kritik kaynaklar, kesintilerin etkileri, kabul edilebilir hizmet dışı kalma süreleri ve normale dönme öncelikleri de

- dahil olmak üzere, şirketle ilgili kriterler ve hedeflerle karşılaştırılarak saptanır, sayıya dökülür ve önceliklendirilir
- İş etki analizi ve risk analizi sonuçlarına göre, şirketin iş sürekliliği yaklaşımını yansıtan iş sürekliliği stratejisi oluşturulur
- Kritik iş süreçleriyle ilgili değerlendirilen bileşenlere yönelik, iş sürekliliği planları oluşturulur
- İş sürekliliği planlarında senaryo, hedef başarı kriterleri, alternatif lokasyon, yeterli maddi, organizasyonel, teknik ve çevresel kaynaklar, iletişim planları, bilgi güvenliği gereklilikleri, acil durum planı, eskalasyon planı ve devreye alınma koşulları, izlenecek geçici operasyonel prosedürler, geri dönüş planları ve sorumluluklar belirlenir
- İş sürekliliği planlarında Üçüncü Kişiler'in sorumlulukları açık ve net bir şekilde tanımlanır
- İş sürekliliği planlarının kopyaları ile planların gerçekleştirilmesi sırasında gerekecek diğer materyaller, ana lokasyondaki bir felaketten etkilenmemesi için yeterli mesafedeki uzak bir lokasyonda saklanır
- İş sürekliliği planlarının kopyaları günceldir ve aynen ana lokasyonda uygulanan güvenlik düzeyinde korunur
- İş sürekliliği planlarının testleri takvimlendirilir ve yılda en az 1 (bir) kez olmak kaydıyla gerçekleştirilir
- İş sürekliliği planının her bir unsuruna ait test adımları, yöntemi, zamanlaması ve katılacak personel belirlenir
- İş sürekliliği planının test edilmesinde masaüstü testleri, simülasyonlar, teknik normale dönüş testleri, eksiksiz provalar, yedek lokasyonda normale dönüş testi gibi çeşitli teknikler dikkate alınır
- Test sonuçları kaydedilir ve planlanan hedeflere göre gerçekleşmeler raporlanır

- Organizasyonda, süreçlerde ve teknolojilerde değişiklik olduğunda, iş sürekliliği planları güncellenir
- Test planlarının uygulandığı alternatif geçici lokasyonlarda uygulanan güvenlik kontrollerinin düzeyinin, ana lokasyondakine denk olması sağlanır

➢ **Dağıtım**

- İş etki analizi ve risk değerlendirme çalışmaları iş süreç sahiplerinin tam katılımıyla gerçekleştirilir
- İş sürekliliği yönetiminin anlaşılması için farkındalık faaliyetleri planlanır ve yürütülür
- İş sürekliliği planlarının testleri için kapsam ve bu kapsama yönelik ilgili personel ile rol ve sorumlulukları paylaşılır
- Gerçekleşen iş sürekliliği planlarının test çalışmaları hakkında ilgili personelden geri bildirim alınır

➢ **Gözden geçirme ve iyileştirme**

- İş sürekliliğinin yönetimi, şirket stratejisi ve organizasyonun gelişimi doğrultusunda sürekli gözden geçirilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.17 Bilgi Sistemleri Geliştirme ve Değişklik

Şirket bilgi sistemlerine yönelik her türlü geliştirme, değişiklik vb. çalışmalar iş ve güvenlik ihtiyaçları doğrultusunda ve belirlenen test senaryolarıa uygun olarak gerçekleştirilir

➢ **Yaklaşım**

- Şirket bilgi sistemleri ile ilgili her türlü alım, geliştirme ve değişiklik çalışmalarının iş ihtiyaçlarına uygun yürütülmesine yönelik bir süreç geliştirilir
- Alım, geliştirme veya değişiklik sonrasında oluşan sistemlerin, belirlenen iş ihtiyaçlarına uygunluğunu değerlendirme yöntemleri belirlenir
- İş ihtiyaçları iş süreç sahiplerinin onayı ile dokümante edilir
- İş ihtiyaçları, sistem kapasitesi, sistem sürekliliği, sistem esnekliği, sistem entegrasyonu, sistem uyumluluğu, destek koşulları, vb. Gereksinimleri kapsayacak şekilde oluşturulur
- İş ihtiyaçları sözleşme, yasa ve düzenlemelerden kaynaklanan yükümlülüklere uyuma dikkat eder
- İş ihtiyaçları, kullanıcı türlerinin (şirket kullanıcıları, destek personeli, üçüncü şahıslar, vb.) belirli yerlerden (ev, ofis, şirket dışı lokasyondan, vb.) ve belirli bilgi türlerine (şirkete ait bilgiler, kredi kartı bilgileri, kişisel bilgiler, ticari sırlar, verişimiyle ilgili gereklilikleri kapsar
- İş ihtiyaçları tek arıza noktalarının (single point of failur oluşmamasını sağlayacak şekilde tasarlanır
- İş ihtiyaçları, mevcut bilgi güvenliği politikaları, standartları, prosedürleri ve talimatları, vb. dokümanlarını dikkate alır
- Alım, geliştirme veya değişiklik çalışmalarına konu olan bilgi sistemleri (işletim sistemleri, altyapı, iş uygulamaları, hazır ürünler, hizmetler ve kullanıcı tarafından geliştirilen uygulamalar, vb.) için güvenlik ihtiyaçları belirlenir ve iş süreçleri sahipleri ile uzlaşılır
- Alım, geliştirme veya değişiklik sonrasında oluşan sistemlerin, belirlenen güvenlik ihtiyaçlarına uygunluğunu değerlendirme yöntemleri belirlenir

- Şirket bilgi sistemleri ile ilgili her türlü alım, geliştirme ve değişiklik çalışmaları, bilgi güvenliği açısından risk yönetimi süreçlerine uygun olarak analiz edilir, gerektiği durumlarda ilave güvenlik kontrolleri uygulanır
- Alım, geliştirme veya değişiklik çalışmalarını gerçekleştiren Üçüncü Kişiler'le yapılan sözleşmelerde, çalışmalara yönelik uygulanması gereken güvenlik gereklilikleri yansıtılır
- Sistemlerin, şirket bilgi güvenliği politikasına, standartlara, prosedürlere, yasal ve düzenleme gerekliliklerine ve güvenlikle ilgili belirli iş gerekliliklerine uygun olacak şekilde geliştirilmesini sağlayan bir sistem geliştirme yöntemi vardır
- Kritik güvenlik faaliyetleri, sistem geliştirme aşamaları sırasında kalite güvencesine tabi tutulur (sistem geliştirme yöntemlerine uygunluğunu garanti etmek için kontroller, yeni personelin veya kritik faaliyetlerin denetimsel incelemesi, vb.)

➢ **Dağıtım**

- Şirket bilgi sistemleri ile ilgili her türlü alım, geliştirme ve değişiklik çalışmalarına konu olacak iş süreçlerinin sahipleri, süreç hakkında bilgilendirilir

➢ **Gözden geçirme ve iyileştirme**

- Alım, geliştirme veya değişiklik sonrasında, sistemlerin belirlenen iş ihtiyaçlarına uygunluğu değerlendirilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır
- Şirket bilgi sistemlerine yönelik her türlü alım, geliştirme, değişiklik vb. çalışmaları (donanım, yazılım ve hizmetler dahil), belirlenen test senaryolarına uygun testler gerçekleştirilir

4.3.17.2 Test Prosedürleri

- **Yaklaşım**

  - Şirket bilgi sistemlerine yönelik her türlü alım, geliştirme, değişiklik vb. çalışmaları için test senaryoları (ağa sızma, erişim kontrolü, performans, stres, kapasite, uygunluk ve işlevsellik, son kullanıcı, kabul, kurtarma, bütünlük, vb.) oluşturulur
  - Geliştirme, test ve canlı sistemin kullanımına yönelik süreç, rol ve sorumluluklar oluşturulur
  - Test sistemleri, canlı ortamlardan ya da geliştirme ortamlarından farklı sistemler ve farklı etki alanlarında (domain) çalıştırılır
  - Test senaryoları ile ilgili başarı kriterleri belirlenir
  - Test senaryoları, iş gerekliliklerinin işlevselliğini, normal ve istisnai iş koşulları altında kullanımını, hata durumlarını, diğer sistemlerle etkileşimlerini, ilgili iş istasyonu konfigürasyonlarıyla uyumluluğunu kapsar
  - Test senaryoları, teknik zayıflık testleri de dahil olmak üzere güvenlik kontrollerini ve etkinliğini kapsar
  - Test senaryoları, herhangi bir problem durumunda bir önceki çalışır duruma dönüş koşullarını içerir
  - Test senaryolarının hazırlanması ve test çalışmaları donanım, yazılım ve hizmetler ile bu hizmetleri kullanacak son kullanıcıların katılımıyla gerçekleştirilir
  - Test sonuçları kayıt altına alınır, beklenen sonuçlarla karşılaştırılarak kontrol edilir, kullanıcılar ve süreç sahibi tarafından onaylanır
  - Uygun olan durumlarda test sürecinin gerçekleştirilmesi (sistem arayüzlerinin geçerliliğinin kontrol edilmesi, birden fazla kullanıcıdan yükleme yapılmasının simüle edilmesi, işletim sistemi ve yama seviyelerinin

aynı olması ile mümkünse canlı ortam ile benzer özelliklere sahip donanım temin edilmesi vb.) için otomatik araçlar kullanılır

- Test sürecinde saptanan hataların tutarlı bir şekilde çözümlenmeleri için, saptanan hataların ayrıntılı olarak kaydedilmesi, bağlantılı risklerin değerlendirilmesi, önlemlerin uygulanması ve uygulamanın yeniden test edilmesi vb. adımlar içerilir Tüm yeni sistemler için kabul testleri, hem geliştirme ortamından hem de canlı ortamdan ayrı bir ortamda ve sistem geliştirme personelinden bağımsız olarak gerçekleştirilir
- Canlı sistemlerdeki bilgilerin test sistemlerine kopyalanması için izlenecek yöntem, rol ve sorumluluklar belirlenir
- Test sırasında sistem kusurlarının veya zaafiyetlerinin saptanması için özel olarak tasarlanmış test verileri kullanılır
- Test verileri dikkatle seçilir ve korunur, kontrol edilir
- Eğer kişisel veya diğer nedenlerle hassas bilgiler test amacıyla kullanılırsa tüm hassas ayrıntılar ve içerikler kullanım öncesinde kaldırılır veya tanınmayacak şekilde değiştirilir (maskelenir)
- Canlı uygulama sistemlerine uygulanan erişim kontrol prosedürleri test sistemlerine de uygulanır

➢ **Dağıtım**

- Test senaryoları çalışmalarındaki son kullanıcı rol ve sorumlulukları organizasyondaki ilgili çalışanlarla paylaşılır

➢ **Gözden geçirme ve iyileştirme**

- Gerçekleştirilen test senaryolarının belirlenen başarı kriterlerine uygunluğu değerlendirilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.18 Bilgi Sistemleri Operasyon Yönetimi Prosedürü

4.3.18.1 Bilgi Sistemleri İşletim Yönetimi Prosedürü

Bilgi sistemleri işletimine yönelik süreçler belirlenir, şirketin bilgi güvenliği yaklaşımına paralel olarak tasarlanır ve yönetilir

- **Yaklaşım**

  - Bilgi sistemleri operasyonları ile ilgili tüm süreçler (işletim, yedekleme ve kurtarma, yama yönetimi, sistem izleme, kayıt (loyönetimi, kötü niyetli kodlara karşı kontrollerin yönetimi, sürüm yönetimi, sistem kabulü, donanım yönetimi, bakım ve destek yönetimi, yardım masası yönetimi, sistem odası çevre koşulları ve güvenlik yönetimi, dış kaynak hizmet yönetimi, değişiklik yönetimi, kapasite yönetimi, vb.) , roller (sistem admin, sistem operatörü, yardım masası ekibi, veritabanı yöneticisi, vb.) ve sorumluluklar belirlenir, dokümante edilir ve kayıt altına alınır
  - Sistemlerin üzerinde tutulan bilgilerin gizliliği, bütünselliği ve erişilebilirliğinin korunması göz önünde bulundurulur
  - Sistemlerin yönetimi ile ilgili güvenlik kontrolleri, yapılan risk değerlendirme çalışmaları doğrultusunda uygulanır
  - Operasyonel veya teknik konularda bakım ve destek için bağlantı noktaları belirlenir
  - Şirketin bilgi güvenliği yaklaşımına paralel olarak, şirket içinde kullanılacak uygulamalar belirlenir, yeni uygulama ihtiyacı olduğu durumlarda süreç sahipleri tarafından iş ihtiyacına uygunluğu dikkate alınarak değerlendirilir
  - Şirketin bilgi güvenliği yaklaşımına paralel olarak, iş sistemleri üzerinde bulundurulabilecek bilgi içeren dosya türleri belirlenir
  - İşletim yönetimi sorumluluğuna sahip personelin, canlı (production) ortamlardaki uygulamalara ve içerdiği bilgilere, sistem izleme kayıtlarına erişmemesine yönelik kontroller uygulanır

- Test sistemi ortamı, canlı ortama mümkün olduğunca benzer konfigürasyonda seçilir
- Test ortamlarına erişim yetkili kullanıcılarla sınırlandırılır
- Bilgi sistemleri ekipleri koordinasyonunda iş süreçleri sahipleri tarafından, canlı ortamdaki hassas bilgiler belirlenir
- Hassas bilgilerin canlı ortamdan test ortamına kopyalanmamasına yönelik kontroller (maskeleme, filtreleme, gerçek dışı veri ile değiştirme, loglama vb.) uygulanır
- Yeni sistemlerin kabul edilmesiyle ilgili gereklilikler ve kriterler belirlenir, yeni bilgi sistemleri, sürüm yükseltimleri ve yeni sürümler, resmi kabul (yazılı kabul onayı, dokümanı, vb.) alındıktan sonra canlı ortama taşınır
- Yeni bilgi sistemleri, sürüm yükseltimleri ve yeni sürümler, planlı bakım çalışmaları, vb. durumlarda, iş süreçlerinin etkilenmemesi için süreç sahipleri ile zamanlama konusunda uzlaşılır
- Tüm sistemler, uluslararası geçerliliği olan tutarlı, doğru ve ortak bir tarih ve saat sistemi kullanacak şekilde ayarlanır
- Kritik donanım ve işletim sistemi bileşenleri, teknik uygunluk ve zaafiyetlerinin/ açıklıklarının değerlendirilmesi amacıyla, bağımsız ve güvenilir şirket dışı taraflarca en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir ve raporlanır

➢ **Dağıtım**

- Operasyonel veya teknik konularda bakım ve destek için bağlantı noktaları organizasyon içindeki ilgili kişilerle paylaşılır
- Organizasyon içindeki ilgili kişilere sistemlerin kullanımına yönelik gerekli eğitimler verilir

➢ **Gözden geçirme ve iyileştirme**

- Sistemlerin yönetimi ile ilgili yapılan risk değerlendirme çalışmaları düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gerçekleştirilir
- Sistemlerdeki zayıflıkların denetlenmesine yönelik çalışma sonuçları değerlendirilerek gerekli ilave kontroller devreye alınır
- Organizasyonel değişiklikler olduğunda, bilgi sistemlerine yönelik süreçler, rol ve sorumluluklar gözden geçirilir
- İş sistemleri üzerinde bulunan uygulamalar ve bilgi içeren dosya türleri, şirket politikalarına uygunluk açısından düzenli olarak gözden geçirilir
- Sistem saatleri belirli aralıklarla kontrol edilerek, farklılık olması durumunda düzeltilir
- Teknik uygunluk ve zaafiyetlerin/açıklıkların değerlendirme rapor çıktıları gözden geçirilerek, uygun düzeltici/önleyici aksiyonlar planlanır
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.18.2 Bilgi Sistemleri Zararlı Yazılımlara Karşı Koyma

Kötü niyetli yazılımlara ve zararlı/mobil kodlara karşı korunmak amacıyla saptama, önleme ve kurtarma kontrolleri uygulanır

➢ **Yaklaşım**

- Kötü niyetli yazılım ve zararlı/mobil kodlara karşı korumak amacıyla gerekli güvenlik kontrolleri belirlenir
- Sunucular, ağ geçitleri, masaüstü ve dizüstü bilgisayarlar, vb. tüm sistemlere, kötü niyetli yazılım ve zararlı/mobil kodlara karşı koruma sağlayan uygulamalar kurulur

- Kötü niyetli yazılım ve zararlı/mobil kodlara karşı koruma sağlayan uygulamaların (anti-virus, anti-spyware, anti-malware, vb.) konfigürasyonları belirlenir ve değiştirilmemesine yönelik kontroller uygulanır
- Sistemlerin, kötü niyetli yazılımlara ve zararlı/mobil kodlara maruz kalmaları riskinin azaltılması için kullanılan uygulamaların güncellemeleri, otomatik olarak ve belirlenmiş olan zaman aralıklarında dağıtılır
- Taşınabilir bilgi depolama ortamlarında (cd/dvd, flash bellek, harici disk, vb.) veya ortam aracılığıyla (web browser, vb.) dosya ve/veya yazılım elde edilmesiyle oluşabilecek kötü niyetli yazılımlar ve zararlı/mobil kodlara karşı güvenlik kontrolleri (kurulum konfigürasyonları dahiuygulanır
- Kötü niyetli yazılımlar ve zararlı/mobil kodlara karşı koruma sağlayan uygulamalar, kurumsal ağa gelebilecek ve kurumsal ağdan çıkabilecek ağ trafiği ile iç ve dış veri depolama ortamlarını taramak üzere yapılandırılır
- Tüm bilgisayarlar ve ortamlar, belirlenmiş zaman aralıklarında otomatik olarak taranır
- Kötü niyetli yazılım ve zararlı/mobil kod içerebilecek dosya türleri ve dosya türlerini barındıran kaynaklar sınırlanır, internet üzerinden indirilmesi önlenir (bazı ActiveX kontrolleri, JavaScript ve Tarayıcı Yardımcı Nesneleri) gibi bilinen hassasiyetlerle bağlantılı olanlar, vb.)

➢ **Dağıtım**

- Kullanıcı farkındalığını artırmak amacıyla, kötü niyetli yazılımlar, zararlı/mobil kodlar ve bunlara yönelik uygulamalar hakkında bilgi paylaşılır
- Kullanıcılar, kötü niyetli yazılımların yaygın belirtileri konusunda bilgilendirilir (sistem performansının kötüleşmesi, uygulamalarda beklenmedik davranışlar, bir uygulamanın aniden kapanması, vb.)
- Kullanıcılar, yeni kötü niyetli yazılımlarla bağlantılı riskler hakkında derhal bilgilendirilir (e-posta, intranet aracılığıyla, vb.)

- Kullanıcılar, güvenmedikleri kaynaklardan yazılım yüklememeleri ve güvenmedikleri ekleri açmamaları konusunda bilgilendirilir

➢ **Gözden geçirme ve iyileştirme**

- Kötü niyetli yazılımlara ve zararlı/mobil kodlara karşı koruma sağlayan uygulamaların konfigürasyonu düzenli aralıklarla gözden geçirilir
- Güncellemelerin tanımlı süreler içinde uygulandığından emin olunması için düzenli gözden geçirme çalışmaları yapılır
- Otomatik olarak yapılan taramaların gerçekleşme durumları düzenli olarak takip edilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.18.3 Bilgi Sistemleri Yedekleme ve Kurtarma

Hizmet sürekliliğinin sağlanması için bilgiler yedeklenir, korunur ve gerektiği durumda geri dönülmesine yönelik çalışmalar yürütülür

➢ **Yaklaşım**

- Şirket içerisinde kullanıcı bilgisayarları dahil olmak üzere kullanılan bilgilerin yedeklenmesine yönelik kriterler (bilgi türleri, yedekleme yapılacak ortam, yedekleme döngüsü {sıklık, sayı}, kopya sayısı, yedekleme yöntemleri {online-offline, full-transactional, snapshot, snapclone, vb.}, kurtarma süresi, etiketleme, depolama, arşivleme, vb.) ve kurtarma senaryoları iş süreç sahipleri ile birlikte belirlenir
- Yedeklenen bilgilerin her türlü yetkisiz erişime, kaybolma, hasar görme, üzerine yazma gibi durumlara karşı korunmasına yönelik elektronik, fiziksel ve çevresel güvenlik kontrolleri belirlenir

- Yedekleme düzenlemeleri tüm sistemlerin kurtarılması için gereken bütün konfigürasyon bilgilerini, erişim yetkilerini, içerdikleri uygulamaları ve iş süreçlerine ait bilgileri kapsar
- Yedekleme ve kurtarma süreçlerinin gerçekleştirilmesi için uygun teknolojik altyapılar kullanılır
- Yedekleme ve kurtarma süreçleri iş sürekliliği planlarına uygun hazırlanır
- Yedekleme ve kurtarma süreçleri şirketin uymakla yükümlü olduğu Mevzuat, standart ve sözleşmelerden doğan yükümlülüklere uygun hazırlanır
- Yedekleme ortamları kullanılırken üretici tavsiyelerine (depolama şartları, azami raf ömrü, azami kullanım sayısı, vb.) uyulur
- Yedekleme işlemleri sonucunda, yedeklemenin başarısı ve alınan yedeklerin içeriklerinin yedekleme planı ile olan uyumluluğu doğrulanır
- Yedekleme ortamlarına yazılan hassas bilgiler, yetkisiz erişime karşı uygun şifreleme yöntemleriyle korunur
- Yedekleme yapılan lokasyon dışındaki yerlere giden veya lokasyon dışından gelen nakil halindeki yedeklerin güvenliğinin sağlanması amacıyla, şifreleme yöntemleri, güvenilir kuryeler ve koruyucu ambalajlar kullanılır
- Yedekleme ortamları ve kurtarma senaryoları düzenli olarak test edilir

➢ **Dağıtım**

- Yedeklemelerin tutulduğu her lokasyondaki ilgili personel, yedekleme ve kurtarma süreçleri hakkında bilgilendirilir
- Yedeklenen bilgilerin kurtarılması ile ilgili yürütülen çalışmalar için iş süreçleri sahipleri bilgilendirilir
- Şirket içerisinde kullanılan bilgilerin yedeklenmesi ile ilgili kriterler iş sürekliliğini destekleyecek şekilde süreç sahipleri ile birlikte oluşturulur ve güncel tutulur

➢ **Gözden geçirme ve iyileştirme**

- Düzenli olarak test edilen yedekleme ortamları ve kurtarma işlemleri ile elde edilen sonuçlara göre, yedekleme ve kurtarma süreçleri en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.18.4 Bilgi Sistemleri Interner Erişimi ve Elektronik Mesajlaşma

İnternet erişimi, elektronik ve anlık mesajlaşma servisleri, iletilen bilgilerin gizlilik, bütünsellik ve erişilebilirliği korunarak sağlanır

➢ **Yaklaşım**

- İnternet erişimi (filtreleme, zamanlama, yetkilendirme, vb.), elektronik ve anlık mesajlaşma kullanım kuralları şirketin bilgi güvenliği yaklaşımı dikkate alınarak belirlenir
- Kullanıcılar, şirket tarafından sunulmuş olan internet erişim, elektronik ve anlık mesajlaşma hizmetini şirketin belirlediği politikalar uyarınca kullanırlar
- Kullanıcılar, internet erişimini sadece yönetimi şirkete ait olan, erişim ve içerik inceleme/engelleme/yönlendirme/loglama cihazları üzerinden gerçekleştirmekle sorumludur
- İnternet erişimi, elektronik ve anlık mesajlaşma yoluyla genel olarak iş ile ilgili bilgi ihtiyacı duyulan araştırmalarda, güncel konuların takibi ve iletişim amacıyla kullanılır
- İnternet erişimi, elektronik ve anlık mesajlaşma yoluyla elde edilen bilgiler, geçerliliği, güvenilirliği, güncelliği ve doğruluğu kontrol edilerek kullanılır
- İnternet erişimi, elektronik ve anlık mesajlaşma yoluyla elde edilen verilerin kullanımında, fikri mülkiyet hakkı kısıtlamalarına, kişisel verilerin korunması ilkelerine, gizlilik esaslarına, kullanım şartlarına ve Mevzuat hükümlerine uygun davranılır

- Şirkete ait internete erişebilen cihazlar ile başka şirket ve/veya kişilere ait ağlara, o ağların yöneticilerinden izinsiz olarak erişim yapılması engellenir
- Kanunun emredici hükümlerine, ahlaka, kamu düzenine ve Etik kurallarına aykırı zararlı içerik barındıran (intihara yönlendirici, çocukların cinsel istismarı, uyuşturucu ve uyarıcı madde kullanımını kolaylaştırma, sağlık için tehlikeli madde temini, müstehcenlik, kumar oynanması için imkan sağlayıc("Zararlı İçerik") sitelere erişim engellenir
- E-posta sunucuları, mesajların ve kullanıcı posta kutularının büyüklüğünü sınırlandırarak, sıkıştırma işlemleri uygulayarak, vb. mesajlaşma sisteminin fazla yüklenmesini önleyecek şekilde yapılandırılır
- E-posta ve anlık ileti (office communicator, msn, gtalk, vb.) hizmetlerinin kullanımı, iş ihtiyacı dikkate alınarak yetkilendirilir
- E-postaya erişim sağlanan kurumsal dış ortamların (web-mail, blackberry, iphone, vb.) organizasyon içerisinde kullanım yetkisi ve kuralları belirlenir
- Kişisel ortamlardan (ev bilgisayarı, blackberry, iphone, vb.) şirket e-posta sistemlerine erişimin sağlanmasına yönelik kurallar belirlenir
- Sosyal paylaşım sitelerine erişim konusu, şirketin bilgi güvenliği yaklaşımına paralel olarak ve iş ihtiyaçları doğrultusunda değerlendirilir
- Dış ağlardan elektronik mesajlaşma sistemlerine erişim sağlanırken şifrelenmiş haberleşme yöntemleri (SSL, VPN, vb.) kullanılır
- E-postaların şirket dışı e-posta adreslerine yönlendirilmemesi sağlanır
- E-postalar, otomatik olarak sorumsuzluk (disclaimer) mesajı içerecek şekilde yapılandırılır

➢ **Dağıtım**

- İnternet erişimi, elektronik ve anlık mesajlaşma kullanım kuralları, tüm çalışanlarla paylaşılır
- Kullanıcılar, internet erişimi, elektronik ve anlık mesajlaşma sistemleri

- kullanarak, Zararlı İçerik paylaşmaması konusunda bilgilendirilir

➢ **Gözden geçirme ve iyileştirme**

- İş ihtiyaçları kapsamında internet erişimi, elektronik ve anlık mesajlaşma kullanım kuralları gözden geçirilir
- İstihdamın sona ermesi durumunda, kullanıcıya ait internet erişimi, e-posta, anlık mesajlaşma, vb. yetkilerinin kaldırılmasına yönelik kayıtlar gözden geçirilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.18.5 Bilgi Sistemleri Kapasite Yönetimi

Bilgi sistemleri kaynaklarının (insan, süreç, teknolojverimliliği ve sürekliliğinin sağlanması amacıyla kapasite yönetimi yapılır

➢ **Yaklaşım**

- Bilgi sistemleri kaynaklarının verimlilik ve sürekliliğinin sağlanmasına yönelik hedef kriterler; insan, süreç ve teknolojik açılardan belirlenir, izlenir, performans sonuçlarına göre değerlendirilir
- Belirlenen kriterlere göre oluşan problemlerin zamanında tespit edilmesine yönelik kontroller devreye alınır
- Her yeni ve devam eden bilgi sistemleri kaynakları kapasite yönetimi açısından değerlendirilir
- İş süreçleri stratejileri doğrultusunda, gelecekte oluşacak bilgi sistemleri altyapıları kapasite ihtiyaçları için tahminler hazırlanır
- Kapasite izleme çalışmalarında RAM, CPU, depolama alanları, disk G/Ç (I/O-input/output), yedekleme alanları, kayıt alanları, WAN/LAN bant genişlikleri, vb. dikkate alınır

➢ **Dağıtım**

- Bilgi sistemleri süreç sahipleri, doğru ve etkin kapasite yönetimi yapabilmek adına iş süreçleri sahipleri ile düzenli olarak değerlendirme çalışmaları gerçekleştirir
- İş süreçleri sahipleri, bilgi sistemleri kaynaklarını etkilebilecek stratejik/operasyonel değişiklikleri, kapasite yönetimi kapsamında ele alınması amacıyla ilgili bilgi sistemleri süreç sahipleriyle paylaşır

➢ **Gözden geçirme ve iyileştirme**

- Sistemlerin performansını etkileyen darboğazlar / aşırı yüklenmeler araştırılarak izlenir Süreç düzenli olarak en az yılda 2 (ikkez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.18.6 Bilgi Sistemleri İzleme Kayıt Yönetimi

Sistemler, planlı ve düzenli izleme aktiviteleri ile gözlemlenir

➢ **Yaklaşım**

- Her bir sistem için gereken izlenecek bilgi (yetkisiz erişim denemeleri, sistem uyarıları/arızaları, ağ yönetimi alarmları vb.), izleme düzeyi, izleme sıklığı, kayıt süresi, olağandışı durum kriterleri, bu kriterler için uygulanacak kontroller ve sorumluluklar belirlenir ve izlenir
- İzleme faaliyetleri yürütülürken tüm yasal gerekliliklere uyulur Kritik sistemlerle ilgili, yüksek seviyeli kullanıcılar (supervisor, administrator, root) gibi ayrıcalıklı hesapların kullanılması, sistemin başlatılması ve durdurulması, cihaz bağlanması/sökülmesi gibi tüm ayrıcalıklı işlemler izlenir
- Sistem üzerindeki güvenlik ayarları ve kontrollerindeki değişiklikler veya değişiklik teşebbüsleri izlenir

- Saldırı tespit ve önleme (IDP, vb.) mekanizmaları kullanılarak bilinen saldırı özellikleri tespit edilir, bu sistemler yeni veya güncellenmiş saldırı özelliklerini belirli aralıklarla bünyesine dahil eder ve şüpheli bir aktivite tespit edildiğinde uyarı verir
- Kayıtlar temel olarak kullanıcı kimliği, tarih, saat, uçbirim kimliği, lokasyon, ağ adreslerini ve protokollerini kapsar
- Sistem yöneticilerinin, kendi faaliyetlerine ait kayıtları (log silememeleri veya devre dışı bırakamamaları sağlanır
- Kayıtlar yedeklenir ve yetkisiz erişimden korunacak şekilde arşivlenir
- Kayıtların gizliliğinin sağlanması için uygun koruma yöntemleri (şifreleme, erişim kontrolü vb.) kullanılır
- Kayıtların anlaşılır bir şekilde izlenebilmesine yönelik olarak uygun çözümler geliştirilir

➢ **Dağıtım**

- Süreç sahipleri tarafından izleme ve kayıt altına alınacak bilgiler, kayıtların saklanma süreleri (olası adli soruşturmalarda yasa, yönetmelik ve iş gerekliliklerinin karşılanması amaçlı, vb.) ve imha yöntemleri belirlenir, bilgi sistemleri süreç sahipleri ile paylaşılır

➢ **Gözden geçirme ve iyileştirme**

- İzleme çalışmalarının sonuçları, süreçlerin kritiklik düzeylerine bağlı olarak belirlenen aralıklarla gözden geçirilir
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.19 Bilgi Sistemleri Uygulama Geliştirme Prosedürü

Uygulamalar şirket bilgi güvenliği yaklaşımına uygun olarak geliştirilir

➢ **Yaklaşım**

- Uygulama geliştirme yönetimi ile ilgili bir süreç oluşturulur ve bu sürece ilişkin rol ve sorumluluklar tanımlanır
- Uygulama geliştirme süreci iş süreç sahipleri ile iletişimi, iş ve güvenlik ihtiyaçlarına yönelik analizi, dokümantasyon, performans kriterleri, risk değerlendirme, test, eğitim, güncelleme, vb. aşamaları kapsar
- Uygulama geliştirme çalışmaları yapılırken, şirket bilgi sistemleri standartlarını karşılayan teknoloji, donanım, yazılım, güvenlik, vb. diğer bileşenler dikkate alınır
- Uygulama geliştirme çalışmaları tasarım, geliştirme, test, canlıya alım, değerlendirme aşamalarından oluşur
- Tasarım aşamasında iş ihtiyacına yönelik analiz çıktıları (yazılım standartları dokümanı, yazılım tasarımı dokümanı, teknik mimari tasarım dokümanı, vb.) oluşturulur ve iş süreç sahipleri ile üzerinde mutabık kalınır
- Geliştirilen uygulama, canlıya alınmadan önce iş süreç sahipleri tarafından, planlanan ortamlarda testler gerçekleştirilir ve bu test sonuçlarına kabul onayı verilir
- Kabul onayı verilen uygulamalar için eğitim planlaması yapılır
- Değerlendirme aşaması tamamlandıktan sonra, gerekli dokümantasyon ile birlikte bakım/destek çalışmalarını yürütmek üzere devredilir
- Uygulama geliştirme çalışmalarında girdi/çıktı verileri ile mesajların doğrulanması sağlanır
- Kredi limitleri, banka hesap numaraları, kişisel bilgiler, maaş bilgileri, satış fiyatları, maliyet bilgileri gibi önemli veri alanlarının giriş, değişiklik, silme işlemleri denetlenir, bu veriler veritabanlarında ve mümkünse giriş arayüzlerinde maskelenir
- Hata mesajlarında uygulamanın kendine özgü bilgilerinin görünmesi önlenir

- Canlı sistemlerde sadece onaylanmış çalıştırılabilir kod (exe, dll, vb.) bulunur, tüm güncellemelerin denetim kaydı (lotutulur
- Sistem dokümantasyonunun yanı sıra tüm uygulanan yazılımları denetim altında tutmak için bir konfigürasyon kontrol ve arşiv sistemi kullanılır
- Güncellemelerin uygulamaya konması öncesinde bir geri dönüş stratejisi belirlenir
- Canlı ortama fiziksel veya mantıksal erişim, gerektiğinde sadece destek amacıyla ve yönetim onayıyla sağlanır, izlenir
- Program kaynak koduna ve bağlantılı bileşenlere (tasarım, spesifikasyon, dokümantasyon vb.) kontrollü erişim sağlanır, bakımı/güncel tutulması ve kopyalanması izlenir
- Program kaynak kodunun, programı geliştiren iç/dış kaynağın lokal bilgisayarı yerine merkezi bir şekilde "program kodu kitaplıklarında" depolanması sağlanır, "program kodu kitaplıkları"nın canlı sistemlerde bulunması engellenir
- Üçüncü Kişiler'den sağlanan uygulamalara ait kodun bir kopyası, güvenilen ve tarafların üzerinde uzlaştığı bir üçüncü şahısa (avukat, yeddi emin, vb.) emanet edilir ve güncelliği sağlanır
- Üçüncü Kişiler'den sağlanan uygulamalara ait lisans düzenlemeleri, kod sahipliği ve fikri hakların mülkiyeti konuları dikkate alınır
- Üçüncü Kişiler'den sağlanan uygulama geliştirme çalışmalarında varsa kötü niyetli kodların saptanması amacıyla içerik ve doğruluk kontrolü yapılır
- Üçüncü Kişiler'in (bir felaket / ihtilaf dolayısıyla, vb.) hizmet sunamaz hale gelmesi durumunda izlenecek alternatif çalışmalar belirlenir
- Kritik uygulamaların bileşenleri, teknik uygunluk ve zaafiyetlerinin/açıklıklarının değerlendirilmesi amacıyla, bağımsız ve güvenilir şirket dışı taraflarca en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir ve raporlanır

➢ **Dağıtım**

- Uygulama geliştirme sürecinin her aşamasında iş süreç sahipleri ile iletişim sağlanır ve bu iletişime konu olan tüm raporlar zamanında ve eksiksiz olarak paylaşılır

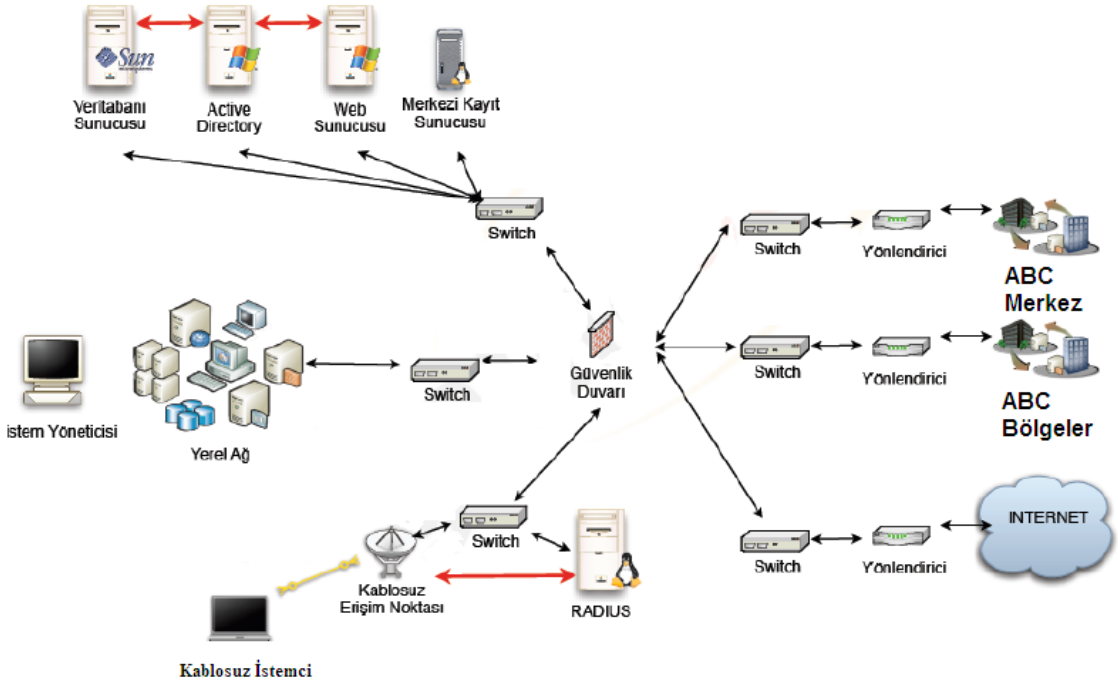
➢ **Gözden geçirme ve iyileştirme**

- Uygulama geliştirme sürecinin tamamlanıp devreye alınmasından sonra düzenli olarak uygulamayı kullanan iş süreçleri ile değerlendirme ve iyileştirme çalışmaları gerçekleştirilir
- Uygulama geliştirme sürecine yönelik belirlenen performans kriterlerine uyum değerlendirilir
- Teknik uygunluk ve zaafiyetlerin/açıklıkların değerlendirme rapor çıktıları gözden geçirilerek, uygun düzeltici/önleyici aksiyonlar planlanır
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.20 Bilgi Sistemleri Ağ Güvenliği Prosedürü

Şirket iç/dış ve kablolu/kablosuz ağ hizmetlerinin, güvenlik özellikleri, hizmet düzeyleri ve yönetim gereklilikleri saptanır, uygun kontrollerle yönetilir.

Şekil 4.3 Güvenli Ağ Yapısı



➢ **Yaklaşım**

- Şirket iç/dış ve kablolu/kablosuz ağlarının yönetimine ilişkin güvenlik kontrolleri, yönlendirme tablolarındaki ve ağ cihazlarının ayarlarındaki değişiklikler ve hizmet seviyeleri ile bu seviyelerle ilgili izleme faaliyetleri yönetilir
- Şirkete ait her türlü lokasyondaki (kullanıcı alanlarındaki ekipmanlar dahiağ hizmet ve ekipmanlarının yönetimiyle ilgili rol ve sorumluluklar tanımlanır
- iç/dış ve kablolu/kablosuz ağ ve ağ bağlantılı hizmetlere erişim ve yetkilendirme, iş süreçleri ihtiyaçları kapsamında belirlenir
- Ağlarla ilgili operasyonel sorumluluk, uygun durumlarda bilgi sistemleri işletim operasyonlarından ayrı tutulur
- Şirketin yönetiminde olmayan halka açık ağlar üzerinden yürütülen çalışmalarda bilgilerin gizlilik ve bütünselliğinin korunması için özel kontroller uygulanır

- Üçüncü Kişilerden sağlanan ağ hizmetleri ile ilgili denetleme çalışmaları yürütülür
- Şirket dışı personel ve/veya ziyaretçilerin ağ hizmetlerinden belirlenmiş güvenlik kontrolleri ve onay sonrasında yararlanması sağlanır
- Uygun durumlarda, ekipmanın ağa bağlanma izni olup olmadığının belirlenmesi için 802.1x gibi uygulamalar kullanılır
- Ağ cihazları (router, hub, bridge, switch ve güvenlik duvarı, vb.) ile ilgili tanı ve yapılandırma portlarına sadece yetkili personel erişimi, gerekli erişim yöntem (SSH2, vb.) ve kontrolleriyle (parola veya fiziksel kilitler, vb.) sağlanır
- Bir bilgisayar veya ağ sistemi üzerinde kurulu olan ve işin yapılabilmesi için gerekli olan portlar, hizmetler (RPC, rlogin, rsh, rexec, NetBIOS, vb.) ve benzeri sistemler belirlenir, bunların haricindekiler devre dışı bırakılır veya kaldırılır
- Bir hizmet kesintisinin toplam etkisinin azaltılması için ağ içinde depolanan veya işlenen bilgilerin iş değeri, sınıflandırması veya iş kolları temel alınarak ayrı mantıksal ağ etki alanları (canlı ortam ağı, test ağı, DMZ, vb.) tasarlanır
- Ağ etki alanları arasında güvenlik duvarları kullanılır
- Ağ, ağ isimleri ve topolojileri şirket dışı taraflarca anlaşılamayacak şekilde (ör. ikili veya ayrık (split) ağ dizinleri / isim sunucuları kullanılarak) tasarlanır
- Ağ cihazları, yapılandırma bilgilerini ayrı sistemlere yedekleyecek şekilde yapılandırılır
- Ağ cihazları, üretici tarafından sağlanan varsayılan parolalar ve parametreler (SNMP adı, vb.) değiştirmek üzere yapılandırılır
- Ağ cihazları, parola gibi hassas bilgilerin düz (şifrelenmemiş) metin biçiminde gönderilmemesini sağlayacak şekilde yapılandırılır
- Yönlendiriciler (yönlendirme yapan ağ cihazları dahil), yönlendirme güncellemelerinin kaynağı ve hedefini teyit ederek (en kısa açık yol algoritması (OSPF) veya yönlendirilmiş internet protokolü (RIP) gibi

teknikler kullanılarak, vb.) yetkisiz veya hatalı güncellemeleri önlemek üzere yapılandırılır

- Kablosuz erişim noktaları (kablosuz ağ ile kablolu ağ arasında arayüz işlevi gören donanımlar) yapılandırılır
- Kablosuz erişim standardında bilgilerin korunması için WPA2 veya daha güçlü güncel şifreleme yöntemleri kullanılır
- Kablosuz erişim noktaları şifreleme anahtarları düzenli olarak değiştirilir
- Kritik kablosuz erişim bağlantıları için sanal özel ağlar (VPN) gibi ek güvenlik kontrolleri uygulanır
- Ağlar güvenlik duvarları, IDP, vb. teknolojilerle korunur
- Güvenlik duvarları, bağlantılı haberleşmelerin durumu, kullanıcıların durumu ve bir ağ hizmetinin geçerliliğini kontrol etmek için kullanılır
- Güvenlik duvarları, suistimale açık iletişim protokollerini (DNS, FTP, NNTP, RIP, SMTP, Telnet, UUCP, vb.) korumak üzere yapılandırılır
- Güvenlik duvarları saldırıları yürütmek için kullanılan ağ paketlerini bloke etmek üzere yapılandırılır (ICMP Echo, UDP ve TCP Echo, Chargen ve Discard, vb.)
- Güvenlik duvarları, kaynak adresin „yanıltıcı' hale getirildiğinin bilindiği durumlarda (kaynak adresin ağa ait olduğu ama ağ içinden/dışından başladığı durumlarda, vb.) gelen trafiği reddedecek şekilde yapılandırılır
- Güvenlik duvarları, belirli kaynak / hedef adresleri (belirli bir IP adresine, vb.) temel alan iletişimleri bloke edecek veya başka şekilde kısıtlayacak şekilde yapılandırılır
- Kritik ağ bileşenleri ve hizmetleri, teknik uygunluk ve zaafiyetlerinin / açıklıklarının değerlendirilmesi amacıyla, bağımsız ve güvenilir şirket dışı taraflarca en az yılda bir kez olmak kaydıyla gözden geçirilir ve raporlanır

➢ **Dağıtım**

- Kullanıcılar şirket dışındaki ağ hizmetlerinden (ev, otel, havaalanı, vb.) yararlanırken oluşabilecek bilgi güvenliği riskleri konusunda düzenli olarak bilgilendirilir
- Kullanıcılar ağ hizmetlerinin kullanımı sırasında olağan dışı bir durum gözlediğinde, bilgi sistemleri sorumlularına bilgi vermeleri konusunda bilinçlendirilir

➢ **Gözden geçirme ve iyileştirme**

- Ağ cihazları, yapılandırma ayarlarının (yönlendirme tabloları ve parametreleri, vb.) doğruluğunun kontrolü için düzenli olarak gözden geçirilir
- Ağ cihazları, ağ cihazı üzerinden yapılan aktivitelerin değerlendirilmesi için düzenli olarak gözden geçirilir
- Teknik uygunluk ve zaafiyetlerin/açıklıkların değerlendirme rapor çıktıları gözden geçirilerek, uygun düzeltici/önleyici aksiyonlar planlanır
- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.3.21 Taşınabilir Ortam Yönetimi Prosedürü

Taşınabilir bilgi depolama (dizüstü bilgisayar, harici sabit disk, flash bellek, yedekleme kartuşu, cd/dvd, vb.) ve haberleşme cihazlarının (blackberry, iPhone, pda, vb.) kullanımına yönelik bilgi güvenliği kuralları uygulanır.

Taşınabilir bilgi depolama (dizüstü bilgisayar, harici sabit disk, flash bellek, yedekleme kartuşu, cd/dvd, vb.) ve haberleşme cihazlarının (blackberry, iPhone, pda, vb.) gerekliliklerin ortadan kalkması veya yeniden kullanılması durumunda, güvenli yöntemler uygulanarak imha edilir veya yeniden kullanıma sunulur.

➢ **Yaklaşım**

- Haberleşme cihazları ve iş bilgilerinin depolanmasına izin verilen taşınabilir depolama cihaz türleri ve özellikleri belirlenir
- Taşınabilir bilgi depolama ve haberleşme cihazlarının kullanımına yönelik bilgi güvenliği ile ilgili kurallar belirlenir
- Dizüstü bilgisayar, akıllı telefon gibi taşınabilir bilgi depolama ve haberleşme cihazları ile kritik bilgi paylaşılırken dikkat edilir
- Taşınabilir bilgi depolama ve haberleşme cihazlarına yönelik fiziksel koruma, erişim kontrolleri, şifreleme teknikleri, yedekleme, virüs ve kötü niyetli yazılımlara karşı koruma vb. gibi kontroller sağlanır
- Taşınabilir bilgi depolama ve haberleşme cihazları, özellikle arabada veya başka bir taşıtta, otel odasında, alışveriş merkezinde, kongre merkezlerinde ve toplantı yerlerinde bırakıldığında hırsızlığa karşı fiziksel olarak da korunması sağlanır
- Taşınabilir bilgi depolama cihazlarının korunması için cihazda (cihaza bağlı her türlü flash bellek dahi saklanan bilgilerin korunması için şifreleme yazılımları kullanılır
- Tekrar kullanılabilen ortamlardan bilgilerin silinmesi için geri dönüşe imkan tanımayan yöntemler kullanılır ve gerekli durumlarda bu işlemler, uzaktan müdahale ile gerçekleştirilir
- Taşınabilir ortam sürücülerinin (usb portları, cd/dvd writer, vb.) iş ihtiyaçları göz önüne alınarak kullanım durumları belirlenir
- Taşınabilir bilgi depolama ve haberleşme cihazlarının bakım/onarım faaliyetleri için şirket dışına gönderilmesi durumunda, organizasyon
- içerisindeki ilgili kişiler bilgilendirilir, gönderilme ve teslim alınma kayıtları tutulur
- Taşınabilir bilgi depolama ve haberleşme cihazlarının taşınmasında şirket tarafından onaylanmış güvenilir ulaşım yolları veya kuryeler kullanılır

- Taşınabilir bilgi depolama ve haberleşme cihazları için koruyucu ambalaj ve yöntemler (kilitli, sağlam kutular, manyetik alan koruyucuları, elden teslim, vb.) kullanılır
- Taşınabilir bilgi depolama (dizüstü bilgisayar, harici sabit disk, flash bellek, vb.) ve haberleşme cihazlarının (BlackBerry, iPhone, PDA, vb.) gerekliliklerin ortadan kalkması veya yeniden kullanılması durumunda uygulanması gereken imha ve yeniden kullanım kuralları ve bu kurallara yönelik sorumluluklar belirlenir
- İmha veya yeniden kullanıma hazırlama aşamalarında taşınabilir bilgi depolama ve haberleşme cihazlarında bulunabilecek hassas bilgiler, yetkisiz erişime karşı korunur
- İmha edilmesi gereken taşınabilir bilgi depolama ve haberleşme cihazları ve güvenli imha yöntemleri (yakma, kırma, delme, hurda satışı, vb.) belirlenir
- Hurda satışına konu olan taşınabilir bilgi depolama ve haberleşme cihazlarının üzerindeki bilgiler, güvenli temizleme yöntemleri ile erişilemez hale getirilir
- Yeniden kullanılması durumunda taşınabilir bilgi depolama ve haberleşme cihazlarının üzerindeki bilgiler, güvenli temizleme yöntemleri ile silinir
- Hibe yöntemi ile yeniden kullanıma sunulan taşınabilir bilgi depolama ve haberleşme cihazları üzerindeki şirkete ait lisanslı yazılımlar kaldırılır
- Taşınabilir bilgi depolama ve haberleşme cihazlarının imhası için bir alt yüklenici seçilirse, bu alt yüklenicinin güvenli imha yöntemlerine uygun hareket etmesi sağlanır
- Taşınabilir bilgi depolama ve haberleşme cihazlarının imhası bir tutanak yoluyla kayıt altına alınır

➢ **Dağıtım**

- Taşınabilir bilgi depolama ve haberleşme cihazlarının çalışma ortamı dışındaki halka açık yerler, toplantı odaları ve diğer korumasız yerlerde kullanımı sırasında kullanıcılar, özellikle dikkat etmeleri konusunda bilgilendirilirler
- Taşınabilir bilgi depolama ve haberleşme cihazları halka açık yerlerde kullanılırken, yetkisiz kişilerin cihaz ekranındakileri görme riskine karşı, kullanıcılar bilgilendirilir
- Taşınabilir bilgi depolama ve haberleşme cihazlarının çalınması veya kaybolmasına yönelik yasal gereklilikleri, sigorta gereklilikleri ve şirketin diğer güvenlik gereklilikleri hakkında kullanıcılar bilgilendirilir
- Kişisel taşınabilir bilgi depolama cihazlarının iş amaçlı kullanılmamasına yönelik farkındalık artırılır
- Şirket tarafından sağlanan taşınabilir bilgi depolama cihazlarının kişisel amaçlarla kullanılmamasına yönelik farkındalık artırılır
- Taşınabilir bilgi depolama ve haberleşme cihazlarının gerekliliklerin ortadan kalkması veya yeniden kullanılması durumunda uygulanması gereken kurallar kullanıcılarla paylaşılır

➢ **Gözden geçirme ve iyileştirme**

- Süreç düzenli olarak en az yılda 1 (bir) kez olmak kaydıyla gözden geçirilir
- Sürecin gözden geçirilen sonuçları, iyileştirme çalışmalarında kullanılır

4.4 Uygulama Denetimi

Prosedürlerin uygulanması sırasında/sonrasında denetimlerde kullanılacak kontrol listeleri, TS ISO 27001 standardının Ek-A'sında uygun olanların ve Cobit Kontrol Hedefleri çerçevesinde ilgili kontrol hedeflerinin belirlenip, uygulamaya konulması ile sağlanmaktadır. Söz konusu ekte, işletmeler için yaygın şekilde uygun oldugu düşünülen kapsamlı bir kontrol amaçları ve kontroller listesi içerir. Bu standardın

kullanıcıları, hiçbir önemli kontrol seçeneginin gözden kaçmamasını sağlamak amacıyla kontrol seçimi için bir başlangıç noktası olarak Ek-A'yı ve mümkünse Cobit kontrol hedeflerini incelemelidirler. Eğer kapsam yeterli gelmiyorsa kapsamı genişletilebilir. 11 temel konu başlığı altında toplam 39 adet kontrol amacı içeren ISO27001 listesi ve bu kontrol amaçlarını kapsayan Cobit Kontrol Alanları ve Hedefleri Çizelge 4.7 da yeralmaktadır.

Çizelge 4.6 ISO27001 ve Cobit kontrolleri eşleştirmesi

ISO 27001		**COBIT**
Kontrol Başlığı	**Kontrol Amacı**	**Kontrol Hedefleri**
A.5 Güvenlik politikası		
	A.5.1 Bilgi güvenliği politikası	Planlama ve Organizasyon - PO1 Stratejik bir BT Planı Tanımlama - PO4 BT Süreçleri, Organizasyon ve İlişkilerini Tanımlama - PO6 Yönetim Hedefleri ve Yönünü Bildirme - PO7 BT İnsan Kaynaklarını Yönetme
A.6 Bilgi güvenliği organizasyonu		
	A.6.1 İç organizasyon	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.6.2 Dış taraflar	Planlama ve Organizasyon - PO8 Kaliteyi Yönetme Servis ve Destek - DS1 Servis Düzeyi Yönetimi - DS2 Üçüncü Taraf Hizmetlerin Yönetilmesi - DS5 Sistem Güvenliğinin Sağlanması
A.7 Varlık yönetimi		
	A.7.1 Varlıkların sorumlulugu	Planlama ve Organizasyon - PO4 BT Süreçleri, Organizasyon ve İlişkilerini Tanımlama

	A.7.2 Bilgi sınıflandırması	Planlama ve Organizasyon - PO2 Bilgi Mimarisini Tanımlama - PO9 BT Risklerini Değerlendirerek Yönetme Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
A.8 İnsan kaynakları güvenliği		
	A.8.1 İstihdam öncesi	Planlama ve Organizasyon - PO7 BT İnsan Kaynaklarını Yönetme Servis ve Destek - DS12 Fiziksel Ortamların Yönetimi
	A.8.2 Çalısma esnasında	Planlama ve Organizasyon - PO7 BT İnsan Kaynaklarını Yönetme Servis ve Destek - DS7 Kullanıcıların Eğitimi ve Öğretimi
	A.8.3 İstihdamın sonlandırılması veya degiştirilmesi	Planlama ve Organizasyon - PO4 BT Süreçleri, Organizasyon ve İlişkilerini Tanımlama - PO7 BT İnsan Kaynaklarını Yönetme
A.9 Fiziksel ve çevresel güvenlik		
	A.9.1 Güvenli alanlar	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması - DS11 Veri Yönetimi - DS12 Fiziksel Ortamların Yönetimi
	A.9.2 Teçhizat güvenliği	Servis ve Destek - DS3 Performans ve Kapasite Yönetimi - DS4 Sürekli Hizmetin Sağlanması
A.10 Haberleşme ve işletim yönetimi		
	A.10.1 Operasyonel prosedürler ve sorumluluklar	Planlama ve Organizasyon - PO4 BT Süreçleri, Organizasyon ve İlişkilerini Tanımlama Temin Etme ve Uygulama - AI6 Değişiklikleri Yönetme Servis ve Destek - DS4 Sürekli Hizmetin Sağlanması - DS13 Operasyonların Yönetimi

	A.10.2 Üçüncü taraf hizmet saglama yönetimi	Planlama ve Organizasyon - PO4 BT Süreçleri, Organizasyon ve İlişkilerini Tanımlama - PO8 Kaliteyi Yönetme - PO10 Projeleri Yönetme Servis ve Destek - DS1 Servis Düzeyi Yönetimi - DS2 Üçüncü taraf Hizmetlerin Yönetilmesi
	A.10.3 Sistem planlama ve kabul	Servis ve Destek - DS3 Performans ve Kapasite Yönetimi - DS4 Sürekli Hizmetin Sağlanması
	A.10.4 Kötü niyetli ve mobil koda karsı koruma	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması - DS8 Hizmet Masası ve Olaylar Yönetimi - DS9 Konfigürasyon Yönetimi - DS10 Sorun Yönetimi
	A.10.5 Yedekleme	Servis ve Destek - DS4 Sürekli Hizmetin Sağlanması - DS11 Veri Yönetimi
	A.10.6 Ag güvenliği yönetimi	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.10.7 Ortam işleme	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.10.8 Bilgi degişimi	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.10.9 Elektronik ticaret hizmetleri	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.10.10 İzleme	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması Gözlem ve Değerlendirme - ME1 BT Performansının Gözlemi ve Değerlendirmesi - ME2 İç Kontrol Gözlemi ve Değerlendirmesi

A.11 Erişim kontrolü		
	A.11.1 Erişim kontrolü için iş gereksinimi	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.11.2 Kullanıcı erişim yönetimi	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.11.3 Kullanıcı sorumlulukları	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.11.4 Ağ erişim kontrolü	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.11.5 işletim sistemi erişim kontrolü	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.11.6 Uygulama ve bilgi erişim kontrolü	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.11.7 Mobil bilgi işleme ve uzaktan çalısma	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
A.12 Bilgi sistemleri edinim, geliştirme ve bakımı		
	A.12.1 Bilgi sistemlerinin güvenlik gereksinimleri	Temin Etme ve Uygulama - AI2 Uygulama Yazılımını Geliştirilmesi ve Bakımı - AI3 Teknoloji Altyapısının Oluşturulması ve Bakımı
	A.12.2 Uygulamalarda dogru isleme	Temin Etme ve Uygulama - AI2 Uygulama Yazılımını Geliştirilmesi ve Bakımı

	A.12.3 Şifreleme kontrolleri	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.12.4 Sistem dosyalarının güvenliği	Temin Etme ve Uygulama - AI6 Değişiklikleri Yönetme Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.12.5 Gelistirme ve destekleme süreçlerinde güvenlik	Temin Etme ve Uygulama - AI6 Değişiklikleri Yönetme Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması
	A.12.6 Teknik açıklık yönetimi	Planlama ve Organizasyon - PO9 BT Risklerini Değerlendirerek Yönetme Servis ve Destek - DS2 Üçüncü taraf Hizmetlerin Yönetilmesi - DS4 Sürekli Hizmetin Sağlanması - DS5 Sistem Güvenliğinin Sağlanması - DS9 Konfigürasyon Yönetimi Gözlem ve Değerlendirme - ME1 BT Performansının Gözlemi ve Değerlendirmesi
A.13 Bilgi güvenliği ihlal olayı yönetimi		
	A.13.1 Bilgi güvenliği olayları ve zayıflıklarının rapor edilmesi	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması - DS8 Hizmet Masası ve Olaylar Yönetimi - DS10 Sorun Yönetimi Gözlem ve Değerlendirme - ME1 BT Performansının Gözlemi ve Değerlendirmesi - ME2 İç Kontrol Gözlemi ve Değerlendirmesi
	A.13.2 Bilgi güvenliği ihlal olayları ve iyilestirmelerin yönetilmesi	Servis ve Destek - DS5 Sistem Güvenliğinin Sağlanması - DS8 Hizmet Masası ve Olaylar Yönetimi - DS10 Sorun Yönetimi Gözlem ve Değerlendirme - ME1 BT Performansının Gözlemi ve Değerlendirmesi - ME2 İç Kontrol Gözlemi ve Değerlendirmesi

A.14 İş sürekliliği yönetimi		
	A.14.1 İş sürekliliği yönetiminin bilgi güvenliği hususları	Servis ve Destek - DS4 Sürekli Hizmetin Sağlanması - DS10 Sorun Yönetimi - DS11 Veri Yönetimi
A.15 Uyum		
	A.15.1 Yasal gereksinimlerle uyum	Gözlem ve Değerlendirme - ME3 Yönetmeliklere Uyumluluğun Sağlanması - ME4 BT Yönetimi Sağlanması
	A.15.2 Güvenlik politikaları,standartlarla teknik uyum	Temin Etme ve Uygulama - AI7 Çözüm ve Değişikliklerin Kurulması ve Akreditasyonu Gözlem ve Değerlendirme - ME1 BT Performansının Gözlemi ve Değerlendirmesi - ME2 İç Kontrol Gözlemi ve Değerlendirmesi - ME4 BT Yönetimi Sağlanması
	A.15.3 Bilgi sistemleri denetim hususları	Gözlem ve Değerlendirme - ME1 BT Performansının Gözlemi ve Değerlendirmesi - ME2 İç Kontrol Gözlemi ve Değerlendirmesi - ME4 BT Yönetimi Sağlanması

4.5 ABC A.Ş.'de BGYS Uygulamasının Değerlendirilmesi

Söz konusu proje kapsamında üretilen bilgi kaynaklarının güvenliğinin sağlanmasında ve mevcut bilgisayar sistemi ile beraber dinamik ve sağlıklı bir Bilgi Güvenlik Sistemi yapılandırılması için altyapı oluşturulmuştur.Proje ile şirketin daha önce bilgi güvenlik yaklaşımlarını uyguladığı ancak herhangi bir standart ve sistem yaklaşımı içerisinde bu konunun üzerine eğilmediği tespit edilmiştir. Tez, bilgi güvenliği politikası, bilgi güvenlik süreçleri ve risk yönetim yaklaşımı oluşturulmasına katkıda bulunmuştur. Bu uygulamadan sonra gerek yurt içi gerek ise yurtdışı şirketlerin yaptıkları şekilde ISO 27001 sertifikası için gerekli hazırlıklar gözden geçirilip, sertifikasyona yönelik başvuru yapılmalıdır.

Bu tez sonucunda, Bilgi Güvenliği Yönetim Sistemi gereksiniminin nedeni, risk yönetiminin yaklaşımının nasıl belirleneceği ve uygulanacağı, BGYS' i oluşturan parçaların neler olduğu ve Bilgi Güvenliği Yönetim Sistemi olarak ISO 27001 standardının seçilme nedenlerine yönelik dört temel araştırma sorusu yanıtlanabilmiştir.

ISO 27001 standardı, güvenlik saldırılarını uygun noktada tutmak için gerekli yönetimsel faaliyetleri içermesi, daha etkili teknik koruma sağlaması ve uluslararası geçerliliğinin olmasından dolayı seçilmiştir. Bölüm üçte bu tür bir sistemin ana fikirleri ve bölüm dörtte nasıl yapılması ile ilgili bilgiler yer almaktadır. Tüm süreçler tam olarak uygulanır ve yönetilirse, şirket genelinde tehdit ve açıklıların yönetilerek risklerin azaltırlmasına ve şirketi geleceğe hazırlamaya yardımcı olur. ISO 27001 uluslararası bir standart olmasının getirdiği yüksek tanınmışlık seviyesi ve organizasyona sağladığı faydalar nedeniyle saygı görümektedir.

Oluşturulan BGYS yapısal olarak çok esnektir ve güncellemeler mümkün olduğu kadar basit yapılabilmektedir. Blok yapısından dolayı yeni elemanlar eklemek, varolanları yenilemek veya kaldırmak çok kolaydır. Analiz sonuçları göstermiştir ki, ABC A.Ş. iki konu üzerinde yoğunlaşmalıdır, tüm yazılımları, eski güvenlik açıklarından zarar görmemek için güncel tutmalı ve sistemlere erişimde kullanılan şifreler daha güvenli hale getirlerek, kullanıcı bazlı erişim şifre prosedürleri uygulamalıdır.

Prosedürler uygulanarak süreçler iyileştirildikten sonra yeniden bir risk analizi yapılarak zayıflıklar ,tehdit ve açıklar tespit edilerek risk durumundaki iyileşme seviyesi ölçülmelidir.

ABC A.Ş. en basit risk analiz yöntemini, varlık değeri ve tehdit oranı ile nitel bir ölçek kullanarak benimsemiştir. Süreçleri basit hale getirmek amacı ile ilk aşamada risk analizi safhasında tehdit ve risklerle ilgili maliyet etkileri dikkate alınmamıştır. Kurulmuş olan risk analiz prosedürü maliyet unsurlarıda dikkate alınarak zaman içerisinde geliştirilecektir. Analize yeni elemanlar ekleyerek örneğin korumaların bedeli ve potansiyel kayıplar gibi değerlerin karşılaştırılacağı şekle gelecektir. Şu anda tamamlanan prosedür sistemin önemli parçalarına odaklanmalı ve ABC A.Ş. 'e sistemi güncel tutmasına fırsat verilmelidir.

Risk yönetim politikası, şifre politikası, bilgi güvenlik politikası ve gizlilik antlaşması gibi dokümanlar şirket içerisinde kullanılmaya başlamış olup günlük iş sürecinin parçası olmuştur. ISO 27001 bazlı sistem ABC A.Ş. organizasyonuna BGYS stratejisini kullanmayı öğreterek, yüksek rekabet ortamında global ekonominin içinde varolmak için etkili bir risk yönetim yaklaşımı ile bilgi kaynaklarının koruma ve güvence altına alma konusunda ne kadar başarılı olduğunu gösterecektir.

BÖLÜM 5

SONUÇ VE ÖNERİLER

5.1 COBIT, ITIL ve ISO 27001 kavramlarının değerlendirilmesi ve karşılaştırılması

Tez kapsamında BTYS-Bilgi Teknolojileri Yönetim Sistemleri uygulamalarına değinilerek COBIT , ISO 20000 ve ITIL Bilgi Teknolojileri Hizmet Yönetim Sistemleri konularında Bilgi Güvenliği Yönetim Sistemi-BGYS kurulumuna rehberlik eden ya da BGYS kurulumunu değişik açılardan (bilgi güvenliği, BT hizmet sürekliliği, BT Yönetişimi vb.) destekleyen COBIT, ITIL, 27001/2 standard ve çerçeveleri Risk Yönetimi ve BGYS bakış açısıyla incelenmiştir.

ISO 27001/ISO 27002 standartları COBIT ve ITIL standartlarından oldukça farklıdır , ISO 27001/ISO 27002 standartları bilgi güvenliği konusunu dar bir çerçevede derinlemesine incelerken , geniş bir perspektiften bilgi teknolojilerini bilgi güvenliğini dahil bir çok bilgi teknolojileri sürecini ele alan ancak bilgi güvenliği konusunda ISO 27001 standardı kadar derinleşmeyen COBIT ve ITIL standartlarıyla karşılaştırmak zordur.

Basit ve yüksek seviyede bu standartların birbirleri ile Fonksiyon, Alan, İlgili, Uygulama, Danışmanlık , Sertifikasyon, Kullanılabilirlik v.d. bilgilerine göre karşılaştırılması Şekil 5.1’ de yer almaktadır.

ALAN	COBIT 4.1	ITIL® v.3	ISO 27K 1/2
Fonksiyon	BT Yönetimi ve Süreçleri	BT Hizmet Seviyesi Yönetimi Çerçevesi	Bilgi Güvenliği
Bilgi Alanı	4 Domain ve 34 Süreç	5 Domain 29 Süreç	Risk Yönetimi + 11 Domain
İlgili Kurum	ISACA / IT Governance Institute	United Kingdom Department of Commerce (OGC The Office of Government Commerce)	ISO Board of Directors
Amaç ve Uygulama	Bilgi Sistemleri Denetimi ABD'de yaygındır Bilgi teknolojisi tabanlı hizmetlerin kapsamlı ve yüksek kaliteli yönetimi ve teslimatı için çerçeve sağlar. Süreçlere değer kazandıran en iyi uygulamaları belirler	Hizmet Seviyesi Yönetimi Avrupa'da yaygındır. Uluslararası kamu ve özel sektörler için oluşturulmuş bir en iyi uygulamarı içeren bir çerçeve sunar.	Uyum güvenlik standardı Tüm dünyada yaygındır 27001 BGYS, 27002 En iyi uygulamalar, 27005 Güvenlik riskleri 27006 denetim ve sertifikasyon için bilgi.
Eşleşen bilgi güvenliği kriterleri	**11 Domain** (Security Policy .. Compliance etc.)	**11 Domain** (Security Policy .. Compliance etc.)	**11 Domain** (Security Policy .. Compliance etc.)
Bilgi Güvenliği Yaklaşımı	**Genele odaklanır**	**Genele odaklanır**	**Derinlemesine odaklanır**
Danışmanlık	Muhasebe Bürosu, Bilişim Danışmanlık Firması	BT Danışmanlık firması	IT Danışmanlık firması, Güvenlik Bürosu, Ağ Danışmanı
Sertifikasyon	Bireysel Sertifika	Bireysel Sertifika	Kurumsal Sertifika
Kuruluş Tarihi	1996	1980'ler	23 Şubat 1947
Bilinirlik	**160 ülke**	**50 uluslararası bölge**	**Dünya çapında 203 ülkede , 163 ulusal üye ülke**
Maliyet	Denetim Bütçesi	BT Bütçesi	BT Bütçesi
Uygulanabilirlik	Modüler olarak uygulanması zor	Aşamalı olarak uygulanması kolay	Modüler olarak uygulanması zor
Yaklaşım	"Kontrol" odaklı	"Süreç" odaklı	"Süreç ve Kontrol" odaklı

Şekil 5.1 Yüksek seviye COBIT,ITIL ve ISO27001 karşılaştırmaları

Tez kapsamında bilgi güvenliğinin sağlayabilmek için incelenen standartlardan hangisinin uygulanması gerektiği cevaplanması zor bir soru olup kesin bir cevabı yoktur. Bu sorunun cevabı şirketin stratejileri , gereksinimleri ve politikaları doğrultusunda değişiklik göstermektedir. Bu standartların bir birinden farklılaştıkları pek çok nokta olduğu gibi özellikle bilgi güvenliği alanında ortak noktalarıda fazladır (Bknz EK-A). EK-A da COBIT, ITIL ve ISO27001 yaklaşımlarının bilgi güvenliği konusunda ait birbirine karşılık gelen süreç ve kontrol hedefleri verilmiştir.

Ancak genel olarak bu standardın geniş bir çerçeveden bilgi teknolojileri süreçlerinin tamamını kapsamakta ve kontrol etmekte olması nedeniyle şirketler ilk önce COBIT standardını uygulamasını tercih etmektedirler. Sonrasında ise genellikle en iyi uygulama pratiklerini içeren ITIL veya ISO 27001/ISO 27002 standartları ile ilgili uygulamalar gelmektedir.

Seçim kriterinde diğer belirleyici unsurlar ise bütçe ve yetkilerdir. COBIT uygulamaları genellikle denetim bütçesinden sağlananan kaynaklarla hayata geçirilir , ITIL ve ISO 27001/ISO 27002 uygulamalarında ise genellikle BT bütçesinden faydalanılır. Bu nedenle hangi standartın ilk önce uygulanacağını yönetim politikası belirleyecektir.

İncelenen standartlar ile ilgili akla gelen diğer bir soruda hangi standartın uygulamasının diğerlerine göre daha kolay olacağıdır. Bu sorunun cevabı, ITIL uygulama süreçlerinin hayata geçirilmesi bir birinden ayrı şekilde farklı zamanlarda gerçekleştirilebilmesi nedeniyle parçalı bir şekilde uygulanması oldukça zor olan COBIT ve ISO 27001/ISO 27002 süreçlerine çok göre daha kolaydır.

Pazar payının artırılması vb. motivasyonlarla uyumluluk iddiaları gün geçtikçe artan ve yasal düzenlemelerle de zaman geçtikçe değişik sektörlerde zorunlu hale gelmesini beklediğimiz bu kaynakların BTYS ve BGYS kurulum/uygulama çalışmalarında en baştan göz önünde bulundurulması, kurumlarda yersiz harcamaların yapılmasının önüne geçecektir. Kurum iş stratejileriyle hizalanmış bir BT stratejisi ve iş sürekliliği stratejisinin belirlenmesi, genellikle çalışmaları birbirinden bağımsız olarak başlatılan kalite yönetim sistemleri, BT yönetişim süreçleri, BTYS, BGYS, İSYS-İş Sürekliliği Yönetim Sistemi gibi yönetim sistemlerinin birbirleriyle entegre şekilde tek bir yönetim sistemi çatısı altında uyumlu olarak çalışmasını sağlayacaktır ve bilgi kaynaklarını korumak için

geliştirilmiş olan BGYS'nin daha etkin bir şekilde kullanılmasını mümkün kılacaktır. Bu konu ile ilgili değişik yaklaşımlar mevcuttur fakat hepsinin ortak bazı özellikleri vardır. Tüm bu yaklaşımlarda risklerin doğru şekilde analiz edilerek, planlanarak ve önceliklendirilerek kurgulanan risk yönetim modeline göre hareket edilmesiyle başarılabilecek olan etkin risk yönetiminin değerini vurgulamaktadır. Ayrıca bu yaklaşımların hepsi süreç başlangıcında kurum içerisinde organizasyonel değişiklikleri gerektirir. Risk Analizine bağlı olarak önerilen özel korumaları ile ISO-27002/ISO17799 ve ISO 27001 gelişmiş en iyi sistemlerden birisidir. Uluslararası bir standart olduğundan dünya çapında tanınmış ve kabul görmüştür. Bu standardı uygulayan firmalar geçmişe göre çok daha az dahili problem yaşadıklarını vurgulamışlardır.

Sonuç olarak ; ISO standartlarına üye olan ülke sayısının dünya çapındaki toplam ülke sayısının %80'inin oluşturması, BGYS kurulum aşamasında, mevcut ISO standartları ile uyumluluğu ve bilgi güvenliğini derinlemesine irdelemesi diğer standart ve yaklaşımlar arasından, tercih edilecek global bir standart olarak ISO27001'i ön plana çıkarmaktadır.

5.2 ISO 27001 çerçevesinde BGYS kurulum sürecinin değerlendirilmesi

Sunulan tez kapsamı hem ISO 27002/ISO 17799 hem de ISO 27001 düzenleme tabanlıdır. Bilgi güvenliği süreç yapısını kullanarak, uygun BGYS gerçekleştirmesini sağlamaktadır. BGYS gerçekleştirilmesi süreçleri dört ana unsurdan oluşur. Başlatılması zordur, sürekli ve sabit analiz gerektirir ve hatasız kesin bir şekilde yapılmalıdır. Yönetim desteği ve dökümantasyon ISO 27001 standardında tarif edilen BGYS sürecinin olmazsa olmazlarındandır. Süreci oluşturan faaliyetlerin yönetim ve dökümantasyon boyutlarının da sürece paralel ve vazgeçilmez katmanlar olarak algılanması BGYS'nin başarı ile uygulanma şansını arttıracaktır.

Bu metindeki fikirler bunların altını çizmek ve uygun uygulamalarının metotlarını vermek üzerinedir. ISO 27001 daha önceki kullanıcıların deneyimlerine göre bazı kritik başarı faktörler listelenebilir. Bunlar:

- İş amaçlarını yansıtan Güvenlik Politikası, amaçları ve aktiviteleri,

- Firma kültürü ile uyumlu bir güvenlik gerçekleştirme yaklaşımı,

- Yönetimden görülen destek ve sorumluluk,

- Güvenlik gereksinimlerinin, risk değerlendirmelerinin ve risk yönetiminin iyi algılanması,

- Tüm yönetici ve çalışanlara güvenliğin pazarlanması,

- Tüm çalışanlara ve yüklenicilere bilgi güvenlik politikası kılavuzunun dağıtımı,

- Uygun eğitim ve bilginin sağlanması,

- Bilgi güvenlik yönetimindeki performansı ölçen dengeli ve ayrıntılı ölçme sistemi ve iyileştirme için geri besleme, olarak vurgulanabilir.

Bu liste göstermektedir ki şirket yapısındaki değişiklikler fiziksel güvenlik önlemlerinden daha önemlidir. Yöneticiler, çalışanlarını, tüm sistemin anlaşılmasına hazırlamalıdırlar. Her şey sıra düzen içinde en üstten başlamalı ve çevre ile birlikte geliştirilmelidir. Her şeyin nasıl gözükeceği üst düzey yönetimin bir hareketine bağlıdır.

ISO 27001 tabanlı bir Bilgi Güvenli Sistemi oluşturmanın kendine özgü güçlü ve zayıf yönleri vardır. Güçlü yönleri, sistem düzgün bir şekilde uygulamaya geçince yönetiminin çok kolay olmasıdır. Yerleşik kontroller sayesinde tüm bilgi sistemini kapsayacaktır. Başka bir avantajı ise ISO 27001 kontrolleri tüm sistemi kapsar, hata için alan bırakmaz ve standart çok detaylı değildir. Kontroller bazı işlemler gerektirse de uygun ve kesin çözüm için çok fazla serbest alan bırakır.

Zayıf noktası ise bu konuda çok fazla yayın, sık kullanılan yöntemleri tanımlayan ve bazı durumlarda yapılması gerekenleri anlatan, olmamasıdır. Bazı durumlarda genelleme seviyesi çok yüksektir ve bu durum firma içinde uzun sürecek tartışmalara yol açabilir.

Özellikle Risk Analizi göstermiştir ki, bu faaliyetin pek çok yöntemi vardır. Analizin formunu ve kontrol edecek değerleri seçerken pek çok problem çıkabilir. Bu tez içinde vurgulanan ana noktaları taban alarak, bir BGYS sistemini uygulanırken dikkate alınması gereken, üç ana sonuca varan bir liste oluşturulmuştur.

- Risk Analizi mümkün olduğu kadar kesin yapılmalıdır: İyi yapılmış bir Risk Analizi sistemin ve kendisini çevreleyen ortam ile ilişkilerin anlaşılmasına izin verir. Varlıkların tam listesi, düzgün şekilde analiz edildiğinde, gelecek olayların getireceklerini ve bunlara karşı yapılacak hazırlıkları yüksek doğrulukla verir.

- Sistem süreçlerin devamlılığını sağlamalıdır: Her organizasyon çevresi ile birlikte gelişmektedir ve sistem bu değişimlere ayak uydurabilmesi için güncellenmelidir. Bu kısmın atlanması görevlerini verimli olarak yerine getiremeyen eski korumalara yol açacaktır.

-Hiçbir BGYS sürekli olarak %100 güvenliği garanti etmez ve korunamaz: Günümüzde bilgisayar sistemlerinde %100 güvenlik sağlamak imkansızdır. Bu sistemlerin karmaşıklığı ve BGYS'nin ele alması gereken mevcut olasılıkların fazlalığı uzun bir sürede sistemin güvenliğini imkansız kılar. Bu tip bir toplam güvenliğin maliyeti de çok yüksek olacaktır, sistemin kendi maliyetini bile aşabilir.

Bu gerçeklere rağmen, bilgi güvenliği yatırım için uygun bir alandır. Bilgi varlıkları çok önemlidir ve bir önlem alınmalıdır. Bilgi güvenliği bütçesi ve planlamaya uygun olursa dengeli ve iyi organize olmuş bir firmada başarı ile yürütülebilir.

Tüm bunlardan çıkan sonuç; Bilgi Güvenliği'nin bir teknoloji sorunu olmadığı, bunun bir iş yönetimi sorunu olduğudur. Bu nedenle günümüzün rekabet ortamında global ekonominin içinde varolmak için bilgi kaynaklarının koruma ve güvence altına alma, bunu bir yönetim sistemi yaklaşımı içinde kurumsal düzeyde yaygınlaştırma mecburiyeti kurumları Bilgi Güvenliği Yönetim Sistemi kurmaya ve kullanmaya zorlayacaktır.

KAYNAKLAR

[1] DeNardis L., (2007). The History of Information Security: A coprehensive handbook, Elsevier

[2] Brendan P. Kehoe, Zen and Art of the Internet: CERT Advisory CA-90:01, Sun sendmail vulnerability http://www.cs.indiana.edu/docproject/zen/zen-1.0_10.html#SEC91, 9 Mayıs 2010.

[3] Cisco Systems, IP Next Generation Networks for Service Providers, http://www.cisco.com/en/US/solutions/collateral/ns341/ns524/ns562/ns583/net_implementation_white_paper0900aecd803fcbbe.pdf, 10 Mayıs 2010.

[4] ISO/IEC27001:2005,(2005) Information Technology, Security techniques, Information security management systems requirements.

[5] System Security Engineering Capability Maturity Model V 3.0 http://www.sse-cmm.org/docs/ssecmmv3final.pdf , 10 Mayıs 2010.

[6] Skordas T., (2006),"Evolution and Policy considerations", OECD Foresight Forum Next Generation Networks, February 2007, Budapest

[7] Richardson, R., CSI Computer Crime and Security Survey 2008, http://www.gocsi.com/forms/csi_survey.jhtml, 11 Mayıs 2010.

[8] Burke, B., Christiansen C., Insider Risk Management: A Framework Approach to Internal Security, http://www.rsa.com/solutions/business/insider_risk/wp/10388_219105.pdf , 11 Mayıs 2010.

[9] Salem M., Shlomo Hershkop S. ve Stolfo S.,(2008) , A Survey of Insider Attack Detection Research, Insider Attack and Cyber Security, 39: 69-90

[10] Honepots C., (2003), "Catching the Insider Threat", Computer Security Applications Conference, December 2003.

[11] Prathaben Kanagasingham P., Bambenek J. C. C., Data Loss Prevention, 2011, http://www.sans.org/reading_room/whitepapers/dlp/data_loss_prevention_32883?show=32883.php&cat=dlp,13 Mayıs 2010.

[12] Alparslan E., Veri Kaçağı Önleme (DLP) ve Veri Madenciliği, https://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/veri-kacagi-onleme-dlp-ve-veri-madenciligi.html?Itemid=6, 13 Mayıs 2010.

[13] Spiekermann S. ve Lorrie Faith C.,(2009), "Engineering Privacy," IEEE Transactions on Software Engineering, 35:67-82.

[14] Fung, B., Wang C K., Chen R. Ve Yu P. S.,(2009), Privacy-Preserving Data Publishing: A Survey on Recent Developments, In ACM Computing Surveys,14:1-52.

[15] Sweeney.L.,(2002), k-anonymity: A model for protecting privacy. Int'l Journal on Uncertainty, Fuziness, and Knowledge-based Systems, 10(5):557-570.

[16] Beydağlı E., Kara M., Bahşi H. ve Alparslan E., Güvenli Yazılım Geliştirme Modelleri ve Ortak Kriterler Standardı, Ulusal Yazılım Mühendisliği Sempozyumu, 8 Ekim 2009.

[17] Microsoft Security Lifecycle (SDL) Version 3.2, http://msdn.microsoft.com/en-us/library/cc307748.aspx,27 Nisan 2010.

[18] Software Assurance Maturity Model, A Guide to Building Security into Software Development Version. 1.0, http://www.opensamm.org, 16 Mayıs 2010.

[19] IBM Internet Security Systems, X-Force 2008 Trend & Risk Report, January 2009, http://www-935.ibm.com/services/us/iss/xforce/trendreports/xforce-2008-annual-report.pdf, 15 Nisan 2010

[20] Walters, j.P., Liang Z., Shi, W. ve Chaudhary V.,(2006) Wireless Sensor Network Security: A Survey, Security in Distributed, Grid, and Pervasive Computing , CRC Press.

[21] U.S.-South Korea Cyberattack: Lessons Learned, http://www.networkworld.com/news/2009/070909-us-south-korea-cyberattack-lessons.html?page=1, 24 Nisan 2010

[22] Igure V., Laughter S. veWilliams R.,(2009), "Security Issues in Scada Networks" Computer&Security, 496-506.

[23] Mehmet K., Hayretdin B., TÜBİTAK UEKAE, Bilgi sistemleri güvenliği araştırmalarının yönü, http://www.bilgiguvenligi.gov.tr/guvenlik-teknolojileri/bilisim-sistemleri-guvenligi-arastirmalarinin-yonu.html,24 Haziran 2010

[24] Sunay, K., (2006). Yönetimde Bilgi Güvenlik Sisteminin Yapısı İşleyişi ve Aselsan A.Ş'de Uygulanması, Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimleri Enstitüsü, Eskişehir.

[25] Şerif Ş., Yönetim ve Organizasyon, Konya: Günay Ofset, 2002, 410.

[26] TIWANA, A., Bilginin Yönetimi, Dışbank, 2003, Çeviren:Elif ÖZSAYAR. İstanbul: Dışbank, 76,87,97,110

[27] T.C. Resmi Gazete, 2005/05 No'lu e-Dönüşüm Türkiye Projesi 2005 Eylem Planı konulu Yüksek Planlama Kurulu Kararı. (25578), 01.04.2005, 24.

[28] ISO/IEC 20000-1:2005, (2005), International standard for IT service management,ISO,Switzerland.

[29] ISO/IEC 13335-1, (2004), Guidelines for the management of IT Security Part 1: Concepts and models for IT Security, ISO, Switzerland.

[30] ISO/IEC 17799:2005,ISO/IEC 27002:2005,(2005), Information Technology – Code of practice for information security management, ISO,Switzerland..

[31] Mustafa B.,(2006). Bankalarda Teknoloji Riski ve Yönetimi ,Yüksek Lisans Tezi, Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü,İstanbul.

[33] Bünyamin Y.,(2007). Bilgi Güvenliği ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması,Gebze Yüksek Teknoloji Enstitüsü Sosyal Bilimler Enstitüsü, Gebze.

[34] Calder, Alan, Bon, Jan Van, "Implementing Information Security based on ISO 27001/ISO 17799 - A Management Guide", Van Haren Publishing, 2006, ISBN: 9789077212783.

[35] ISO/IEC 27000:2009, (2009), Information technology – Security techniques – Information security management systems – Overview and vocabulary, First Edition, ISO, Switzerland..

[36] ISO/IEC 27001:2005, (2005) Information technology – Security techniques – Information security management systems – Requirements, First Edition, , ISO, Switzerland.

[37] Bilgi Güvenliği, UEKAE BGYS0001-Bilgi Güvenliği Yönetim Sistemi Kurulumu, http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0001-bilgi-guvenligi-yonetim-sistemi-kurulumu/download.html, 25 Nisan 2010.

[38] ITIL Hizmetleri,Information Technologies Infrastructure Library, http://www.infratech.com.tr, 12 Mayıs 2010.

[39] IT Governance Institute, (2005), COBIT 4.0 Control Objectives Management Guidelines Maturity Models, 33,78,162.

[40] Wikipedia, Bilgi teknolojileri için kontrol hedefleri, http://tr.wikipedia.org/wiki/Cobit#COBIT_Versiyon_4.1, 23 Mayıs 2010.

[41] Information Technologies Infrastructure Library, Cobit Owerview, http://www.itil.org/en/zumkoennen/cobit/index.php,2 Haziran 2010.

[42] BDDK, IT_Audit_BDDK_Yaklasimi,www.bddk.org.tr/turkce/yayinlarveraporlar/sunumlar/IT_Audit_BDDK_Yaklasimi_20_4_2006.ppt, 3 Haziran 2010.

[43] IT Governance Institute, COBIT 4.1 Control Objectives Management Guidelines Maturity Models,2007, http://www.isaca-bogota.net/Metodologias/COBIT/COBIT4.1.pdf,17, 4 Haziran 2010.

[44] ISACA, (2000), Control Objectives for Informaion Technologies, 13, Illinois.

[45] COBIT Nedir? , İlker TUTU, http://www.cozumpark.com/blogs/cobit-itil/archive/2010/11/21/cobit-nedir.aspx, 4 Haziran 2010.

[46] PWC, COBIT, http://www.pwc.com/tr/tr/service/it-services/cobit-bes, 4 Şubat 2011.

[47] Hadi Gökçen, (2002), Yönetim Bilgi Sistemleri , 13, EPİ yayıncılık,Ankara.

[48] Şimsek, Ş., (2002), Yönetim ve Organizasyon, 408, Günay Ofset, Konya.

[49] ISO17799-Danışmanlığı,(2006), http://www.innova.com.tr/04Hizmetler/detayli_bilgi02.htm,4 Haziran 2010.

[50] Alpay, B., (2008). ITIL (Information Technology Infrastracture Library) Güvenlik Yönetimi Süreçlerinin Orta/Büyük Şirketlerde Uygulanması , Yüksek Lisans Tezi, Haliç Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

[51] TS ISO/IEC 17799, (2002), Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri, TSE-Türk Standardları Enstitüsü, Ankara.

[52] Accountability, National Information Assurance, http://staff.washington.edu/dittrich/center/4009.pdf, 4 Haziran 2010.

[53] CANBEK G. , SAĞIROĞLU Ş. .(2007).,Bilgisayar Sistemlerinde Yapılan Saldırılar ve Türleri , Erciyes Üniversitesi Fen Bilimleri Enstitüsü Dergisi 23 (1-2) 1 - 12 (2007) , http://fbe.erciyes.edu.tr/mka-2005/Dergi/2007-vol23-no-1-2/01-2007-vol23-no-1-2.pdf, 6 Haziran 2010.

[54] 2004 Web Server Intrusion Statistics, Zone-H, http://www.zone-h.org/files/82/ZoneHorg2004statisticsfinal.pdf, 4 Haziran 2010.

[55] Hamelink, C. H., The Ethics of Cyberspace, Sage Publications Inc, 32-34, 2001.

[56] Klein, A., Cross Site Scripting Explained, Sanctum Security Group, http://crypto.stanford.edu/cs155/CSS.pdf, 4 Haziran 2010.

[57] Bilişim Sistemleri Güvenliği El Kitabı, (2003), Türkiye Bilişim Derneği, Ankara.

[58] B. Preneel ve P. C. van Oorschot, (1996), "On the Security of Two MAC Algorithms", Advances in Cryptography- EUROCRYPT '96, Saragosa, Spain.

[59] Whitfield Diffie ve Martin Hellman, http://en.wikipedia.org/wiki/Diffie%E2%80%93Hellman_key_exchange,4 Haziran 2010.

[60] What are the advantages and disadvantages of public-key cryptography compared with secret-key cryptography?, http://www.rsa.com/rsalabs/node.asp?id=2167, 4 Haziran 2010.

[61] KALAYCI T., (2003), Bilgi Teknolojilerinde Güvenlik ve Kriptografi, Lisans Tezi, EGE Üniversitesi Bilgisayar Mühendisliği Bölümü , İzmir. yzgrafik.ege.edu.tr/~tekrei/dosyalar/yayinlar/LisansTez.pdf

[62] ISO27001 Bilgi Güvenliği Yönetim Standardı, http://www.isokalitebelgesi.com/iso_belgeleri_egitim_danismanlik/ISO_27001_ISO_27000_22057/bilgi_guvenligi_belgesi_1.php, 7 Haziran 2010.

[63] An Introduction Information Security and ISO27001, www.itgovernance.co.uk/files/Infosec_101v1.1.pdf, 2 Ekim 2010.

[64] TSE 17799, (2002), Bilgi Teknolojisi - Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri,TSE ,Ankara.

[65] Bisson J. ve Saint-Germain R., (2006), The BS 7799 / ISO 17799 Standard, White Paper, https://www.callio.com/files/wp_iso_en.pdf, 15 Ekim 2010.

[66] ISO27001 sertifikasyonuna sahip organizasyonlar, ,http://www.iso27001certificates.com/ , 15 Haziran 2011.

[67] UEKAE BGYS0004 – BGYS Risk Yönetim Süreci, http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys0004-bgys-risk-yonetim-sureci-kilavuzu/download.html, 20 Şubat 2011.

[68] Karacan A.,(2000) Bankacılık Ve Kriz ,19, Creative Yayıncılık, İstanbul.

[69] Arman T. ve Gürman T., (1997), Bankalarda Finansal Yönetime Giriş, 203:2, TBB Yayını, İstanbul,

[70] Fıkırkoca M., (2003) Bütünsel Risk Yönetimi, 142, Pozitif Matbaacılık, Ankara

[71] Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme, www.emo.org.tr/ekler/cf1d15d2fe95ac4_ek.pdf, 22 Mart 2011.

[72] ISO 27005, (2011), Information Technology Risk Management, ISO, Switzerland.

[73] Cobra, http://www.riskworld.net/benefits.htm, 24 Mart 2011.

[74] CCTA Risk Analysis and Management Method, http://en.wikipedia.org/wiki/CRAMM , 24 Mart 2011.

[75] CRAMM CCTA Risk Analysis and Management Method, (1996), Central Computing and Telecommunications Agency CCTA, United Kingdom.

[76] Octave Criteria V2, www.cert.org/archive/pdf/01tr016.pdf,14 Nisan 2011.

[77] Ebios, http://en.wikipedia.org/wiki/EBIOS, 15 Nisan 2011.

[78] Isamm, http://rm-inv.enisa.europa.eu/methods_tools/m_isamm.html, 16 Nisan 2011.

[79] Art Of Risk, http://www.aexis.de/index.php?site=static&staticID=4 , 17 Nisan 2011.

[80] RealISMS, http://www.realismssoftware.com/, 18 Nisan 2011.

[81] ISMart, http://www.biznet.com.tr/ismart_faq.htm, 8 Mayıs 2011.

[82] RiskWatch, http://rminv.enisa.europa.eu/methods_tools/t_riskwatch.html, 17 Mayıs 2011.

[83] Proteus, http://rm-inv.enisa.europa.eu/methods_tools/t_proteus.html, 21 Mayıs 2011.

[84] Callio, http://www.callio.com/PDF/Calio_Secura17799.pdf, 22 Mayıs 2011.

[85] ISMS-RAT, http://www.brothersoft.com/isms-rat-74927.html, 22 Mayıs 2011.

[86] Sommer P., (1994), Industrial espionage: analysing the risk, Computers & Security, 13-7:558-563

[87] Kurumsal Bilgi Güvenliğinde Risk Analizi, http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/kurumsal-bilgi-guvenliginde-etkin-risk-analizi.html, 19 Haziran 2011.

[88] UEKAE BGYS-0004 BGYS Risk Yönetim Süreci Kılavuzu , SÜRÜM 1.00 17.08.2007, http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0004-bgys-risk-yonetim-sureci-kilavuzu.html, 19 Haziran 2011.

[89] Oracle Türkiye ve Pro-G, (2003), Bilişim Güvenliği, http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf , 23 Haziran 2011.

[90] Türkiye Bilişim Derneği, (2006), Bilişim Sistemleri Güvenliği El Kitabı Sürüm 1.0, 29-30., Türkiye Bilişim Derneği, Ankara.

[91] TS ISO/IEC 27002 – 17799 , (2005), Bilgi Teknolojisi-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri, Türk Standardları Enstitüsü, Ankara.

[92] NAZLI M., http://www.bilgiguvenligi.gov.tr/kurumsal-guvenlik/fiziksel-ve-cevresel-guvenlik.html, 29 Haziran 2011.

[93] ERGUN A., (2006), Fiziksel Güvenliğinizden Emin misiniz?, http://www.acemiler.net/pc_guvenlik.phtml,1 Temmuz 2011.

[94] Karaarslan E., Ağ Cihazlarının Güvenliğinin Sağlanma Yöntemleri, http://csirt.ulakbim.gov.tr/dokumanlar/NwCihazGuvenligi2002.pdf, 12 Temmuz 2011.

[95] Küçükoğlu Ş., Uygun Güvenlik Çözümüne Yolculuk, (2006), http://www.infosecurenet.com/macroscope/macroscope6.pdf,14 Temmuz 2011.

[96] Rol-Tabanlı-Erişim-Kontrolü_BurakÖzgirgin http://www.denetimnet.net/UserFiles/Documents/Makaleler/Rol-Tabanl%C4%B1-Eri%C5%9Fim-Kontrol%C3%BC_Burak%20%C3%96zgirgin.pdf, 17 Temmuz 2011.

[97] Okay M., Pekel A., Yaman O., Soyar D.,Kuleyın N. ve Mete A., (2006), "Bilişim Teknolojilerinde Risk Yönetimi", Kamu Bilişim Platformu, http://kamubib.tbd.org.tr/dokumanlar/cg2.doc, 16 Temmuz 2011.

[98] BS 25999-1:2006, (2006) Code of Practice for BCM, BSI, United Kingdom

[99] UEKAE BGYS-0009 İş Sürekliliği Yönetim Sistemi Kurulum Kılavuzu, http://www.bilgiguvenligi.gov.tr/dokuman-yukle/bgys/uekae-bgys-0009-is-surekliligi-yonetim-sistemi-kurulum-kilavuzu/download.html, 19 Temmuz 2011.

[100] Ottekin F., (2008), TÜBİTAK-UEKAE , Çok Katmanlı ISO 27001 Süreci , http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/cok-katmanli-iso-27001-sureci.html, 21 Temmuz 2011.

[101] TS ISO/IEC 27001, (2006), Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenliği Yönetim Sistemleri, Gereksinimler, TSE, Ankara.

[102] Emiral F., (2006), Bilgi Güvenliği Bilincinin Genele Yayılması, http://www.deloitte.com/dtt/article/0,1002,sid%253D8497%2526cid%253D53205,00.html, 27 Temmuz 2011

[103] Esener H.,(2005) Hizmet Yönetim Sistemi, Yüksek Lisans Tezi, Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul.

[104] Işıkçı Ç., (2011), COBIT Denetimleri Açısından Bilgi Güvenliği, http://www.bilgiguvenligi.gov.tr/bt-guv.-standartlari/cobit-denetimleri-acisindan-bilgi-guvenligi.html, 27 Temmuz 2011

[105] Clinch J., (2009), ITIL V3 and Information Security, http://www.best-managementpractice.com/gempdf/ITILV3_and_Information_Security_White_Paper_May09.pdf , 27 Temmuz 2011.

EK-A

IS0 27001, ITIL, COBIT EŞLEŞTİRME TABLOSU

EK-A başlığı altında verilen aşağıda yer alan çizelge COBIT, ITIL ve ISO27001 arasındaki ilişkiyi göstermektedir. Verilen tablodaki bilgiler kesin kurallar değildir , ilgili dökümanlardaki ana başlıkları referans etmektedir , rehber olarak kullanılması amacı ile oluşturulmuştur.

Güvenlik Maddesi	**COBIT 4.1**	**ISO 27001:2005**	**ISO 20000:2005 /ITIL Referans**
I. Güvenlik Politikası	PO6 İletişim Yönetimi Amaçları ve Yönelimi PO4.14 Sözleşmeli Personel Politikaları ve Prosedürleri	5.1 Bilgi Güvenliği Politikası	6.6 Bilgi Güvenliği Yönetimi
I. Güvenlik Politikası	PO6 İletişim Yönetimi Amaçları ve Yönelimi PO4.14 Sözleşmeli Personel Politikaları ve Prosedürleri	5.1 Bilgi Güvenliği Politikası	6.6 Bilgi Güvenliği Yönetimi
I. Güvenlik Politikası	M1 Proseslerin İzlenmesi 1.1 İzleme Verisinin Toplanması 1.2 Performansın Değerlendirilmesi 1.3 Müşteri Memnuniyetinin Değerlendirilmesi 1.4 Yönetim Raporlama M2 Kontrol Etkinliğinin Değerlendirilmesi 2.1 Kontrollerin İç Denetimi	5.1.2 Bilgi Güvenliği Politikasının Gözden Geçirilmesi	6.6 Bilgi Güvenliği Yönetimi

I. Güvenlik Politikası	M1 Proseslerin İzlenmesi 1.1 İzleme Verisinin Toplanması 1.2 Performansın Değerlendirilmesi 1.3 Müşteri Memnuniyetinin Değerlendirilmesi 1.4 Yönetim Raporlama M2 Kontrol Etkinliğinin Değerlendirilmesi 2.1 Kontrollerin İç Denetimi	5.1.2 Bilgi Güvenliği Politikasının Gözden Geçirilmesi	6.6 Bilgi Güvenliği Yönetimi
I. Güvenlik Politikası	M1 Proseslerin İzlenmesi 1.1 İzleme Verisinin Toplanması 1.2 Performansın Değerlendirilmesi 1.3 Müşteri Memnuniyetinin Değerlendirilmesi 1.4 Yönetim Raporlama M2 Kontrol Etkinliğinin Değerlendirilmesi 2.1 Kontrollerin İç Denetimi	5.1.2 Bilgi Güvenliği Politikasının Gözden Geçirilmesi	6.6 Bilgi Güvenliği Yönetimi
I. Güvenlik Politikası	M1 Proseslerin İzlenmesi 1.1 İzleme Verisinin Toplanması 1.2 Performansın Değerlendirilmesi 1.3 Müşteri Memnuniyetinin Değerlendirilmesi 1.4 Yönetim Raporlama M2 Kontrol Etkinliğinin Değerlendirilmesi 2.1 Kontrollerin İç Denetimi	5.1.2 Bilgi Güvenliği Politikasının Gözden Geçirilmesi	6.6 Bilgi Güvenliği Yönetimi
I. Güvenlik Politikası	11.18 Kullanımdan Çıkartılmış Hassas Bilgilerin Korunması, 11.26 Arşivleme	7.2.2 Bilgi Etiketleme ve İşleme	6.6 Bilgi Güvenliği Yönetimi
I. Güvenlik Politikası	11.27 Hassas Mesajların Korunması	5 Güvenlik Politikası 8.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi	6.6 Bilgi Güvenliği Yönetimi
II. Organizasyonel Güvenlik	PO1 Bir Stratejik IT Planının Yapılması PO4.11 IT Çalışanları		4 Servis Yönetiminin Planlanması ve Uygulanması

II. Organizasyonel Güvenlik	4.2 IT Fonksiyonunun Organizasyondaki Yeri 4.4 Roller ve Sorumluluklar 4.6 Fikri ve Fiziksel Güvenlik Sorumlulukları	6.1.3 Bilgi Güvenliği Sorumluluklarının Tahsisi 8.1.1 Roller ve Sorumluluklar	6.6 Bilgi Güvenliği Yönetimi
II. Organizasyonel Güvenlik	PO7 İnsan Kaynakları Yönetimi 7.1 Personel İşe Alımı ve Terfisi 7.2 Personel Yetkinlikleri 7.5 Çapraz Eğitim veya Çalışanların Yedeklerinin Tutulması 7.6 Personel İş Sonlandırma Prosedürleri	A 8 İnsan Kaynakları Güvenliği	3.3 Yetkinlik, Bilinç ve Eğitim
II. Organizasyonel Güvenlik	PO7 İnsan Kaynakları Yönetimi 7.1 Personel İşe Alımı ve Terfisi 7.2 Personel Yetkinlikleri 7.5 Çapraz Eğitim veya Çalışanların Yedeklerinin Tutulması 7.6 Personel İş Sonlandırma Prosedürleri	A 8 İnsan Kaynakları Güvenliği	3.3 Yetkinlik, Bilinç ve Eğitim
II. Organizasyonel Güvenlik	PO7 İnsan Kaynakları Yönetimi 7.1 Personel İşe Alımı ve Terfisi 7.2 Personel Yetkinlikleri	A 8 İnsan Kaynakları Güvenliği	6.6 Bilgi Güvenliği Yönetimi
II. Organizasyonel Güvenlik	DS2 Üçüncü Taraf Servislerin Yönetilmesi 2.4 Üçüncü Tarafların Nitelikleri 2.5 Dış Kaynak Sözleşmeleri	A 6.2 Dış Taraflar 6.2.3 Üçüncü taraf anlaşmalarında güvenliği ifade etme	7.3 Tedarikçi Yönetimi
II. Organizasyonel Güvenlik	DS2 Üçüncü Taraf Servislerin Yönetilmesi 2.6 Servislerin Sürekliliği 2.7 Güvenlik İlişkileri	A 6.2 Dış Taraflar 6.2.3 Üçüncü taraf anlaşmalarında güvenliği ifade etme	7.3 Tedarikçi Yönetimi
II. Organizasyonel Güvenlik	DS5 Sistem Güvenliğinin Sağlanması 5.13 Karşı tarafa Güven	6.2.3 Üçüncü taraf anlaşmalarında güvenliği ifade etme A 6.2 Dış Taraflar	7 İlişki Prosesi 7.3 Tedarikçi Yönetimi 7.3 Tedarikçi Yönetimi

III. Varlık Sınıflandırma ve Kontrolü	PO2.3 Veri sınıflandırma Şeması PO4.7 Sahiplik ve Kullanıcısı PO4.8 Veri ve Sistem Sahipliği	6.1.1 Sınıflandırma Kılavuzu	6.6 Bilgi Güvenliği Yönetimi
III. Varlık Sınıflandırma ve Kontrolü	PO2.3 Veri Sınıflandırma Şeması	6.1.1 Sınıflandırma Kılavuzu	6.6 Bilgi Güvenliği Yönetimi
III. Varlık Sınıflandırma ve Kontrolü	PO4.8 Veri ve Sistem Sahipliği	5 Güvenlik Politikası 9.2.5 Kuruluş dışındaki teçhizatın güvenliği 10.8.3 Aktarılan fiziksel ortam 11.7.1 Mobil bilgi işleme ve iletişim	6.6 Bilgi Güvenliği Yönetimi
III. Varlık Sınıflandırma ve Kontrolü	PO8 Dış Gerekliliklere Uyum Sağlandığından Emin Olunması 8.4 Gizlilik, Fikri Mülkiyet ve Veri Akışı	5 Güvenlik Politikası 9.2.5 Kuruluş dışındaki teçhizatın güvenliği 10.8.3 Aktarılan fiziksel ortam 11.7.1 Mobil bilgi işleme ve iletişim	6.6 Bilgi Güvenliği Yönetimi
III. Varlık Sınıflandırma ve Kontrolü	PO7 İnsan Kaynakları Yönetimi 7.8 Görev Değişikliği ve Sonlandırma PO4.8 Veri ve Sistem Sahipliği	9.2.5 Kuruluş dışındaki teçhizatın güvenliği 10.8.3 Aktarılan fiziksel ortam 11.7.1 Mobil bilgi işleme ve iletişim	6.6 Bilgi Güvenliği Yönetimi
III. Varlık Sınıflandırma ve Kontrolü	DS9 Konfigürasyon Yönetimi 9.1 Konfigürasyon Kaydı 9.3 Durum Muhasebesi 9.4 Konfigürasyon Kontrolü 9.8 Yazılımın Güvenilirliği	12.4.1 Operasyonel yazılımın kontrolü 12.5.2 İşletim sistemindeki değişikliklerden sonra teknik gözden geçirme 9.2 Ekipman Güvenliği	9.1 Konfigürasyon Yönetimi

IX. Erişim Kontrolü	DS5 Sistem Güvenliğinin Sağlanması 5.3 Veriye Çevrimiçi Erişim Güvenliği 5.4 Kullanıcı Hesap Yönetimi	11.1 Erişim kontrolü için iş gereksinimi 11.1.1 Erişim Kontrol Politikası 11.2 Kullanıcı Erişim Yönetimi 11.6 Uygulama ve bilgi erişim kontrolü 11.6.1 Bilgi Erişim Kısıtlaması	6.6 Bilgi Güvenliği Yönetimi
IX. Erişim Kontrolü	DS5 Sistem Güvenliğinin Sağlanması 5.4 Kullanıcı Hesap Yönetimi 5.5 Kullanıcı Hesaplarının Yönetim Gözden Geçirmesi 5.21 Elektronik Değerlerin Korunması	11.2 Kullanıcı Erişim Yönetimi 11.2.1 Kullanıcı Kaydı 11.2.4 Kullanıcı erişim haklarının gözden geçirilmesi	6.6 Bilgi Güvenliği Yönetimi
IX. Erişim Kontrolü	DS5 Sistem Güvenliğinin Sağlanması 5.2 Tanımlama, Kimlik DOğrulama ve Erişim 5.4 Kullanıcı Hesap Yönetimi 5.5 Kullanıcı Hesaplarının Yönetim Gözden Geçirmesi 5.6 Kullanıcı Hesaplarının Kullanıcılar Tarafından Gözden Geçirilmesi	11.2.3 Kullanıcı Parola Yönetimi	6.6 Bilgi Güvenliği Yönetimi
IX. Erişim Kontrolü	DS5 Sistem Güvenliğinin Sağlanması 5.2 Tanımlama, Kimlik Doğrulama ve Erişim 5.4 Kullanıcı Hesap Yönetimi 5.5 Kullanıcı Hesaplarının Yönetim Gözden Geçirmesi 5.6 Kullanıcı Hesaplarının Kullanıcılar Tarafından Gözden Geçirilmesi	11.2.3 Kullanıcı Parola Yönetimi	6.6 Bilgi Güvenliği Yönetimi
IX. Erişim Kontrolü	DS5 Sistem Güvenliğinin Sağlanması 5.2 Tanımlama, Kimlik Doğrulama ve Erişim 5.4 Kullanıcı Hesap Yönetimi 5.5 Kullanıcı Hesaplarının Yönetim Gözden Geçirmesi 5.6 Kullanıcı Hesaplarının Kullanıcılar Tarafından Gözden Geçirilmesi	7.2.2 Bilgi Etiketleme ve İşleme 11.2 Kullanıcı Erişim Yönetimi	6.6 Bilgi Güvenliği Yönetimi

IX. Erişim Kontrolü	DS5 Sistem Güvenliğinin Sağlanması 5.2 Tanımlama, Kimlik Doğrulama ve Erişim 5.4 Kullanıcı Hesap Yönetimi 5.5 Kullanıcı Hesaplarının Yönetim Gözden Geçirmesi 5.6 Kullanıcı Hesaplarının Kullanıcılar Tarafından Gözden Geçirilmesi	7.2.2 Bilgi Etiketleme ve İşleme 11.2 Kullanıcı Erişim Yönetimi	6.6 Bilgi Güvenliği Yönetimi
V. Fiziksel ve Çevresel Güvenlik	DS12 Tesis Yönetimi 12.1 Fiziksel Güvenlik	9.1 Güvenli Alanlar 9.2 Ekipman Güvenliği	6.6 Bilgi Güvenliği Yönetimi
VI. Ekipman Güvenliği	PO6 İletişim Yönetimi Amaçları ve Yönelimi 6.3 Organizasyon Politikalarının Etkileşimi 6.6 Politika, Prosedür ve Standartlara Uyum 6.11 IT Güvenlik Bilincinin İletişimi PO8 Dış Gerekliliklere Uyum Sağlandığından Emin Olunması 8.4 Gizlilik, Fikri Mülkiyet ve Veri Akışı DS7 Kullanıcı Eğitimi ve Bilinçlendirmesi	11.7.1 Mobil bilgi işleme ve iletişim	6.6 Bilgi Güvenliği Yönetimi
VII. Genel Kontroller	PO9 Risklerin Değerlendirilmesi 9.1 İş Risk Değerlendirme 9.3 Risk Tanımlama DS5 Sistem Güvenliğinin Sağlanması 5.8 Veri Sınıflandırma	6.2.1 Dış taraflarla ilgili riskleri tanımlama 15.3.2 Bilgi sistemleri denetim araçlarının korunması 15.3.1 Bilgi sistemleri denetim kontrolleri	6.6 Bilgi Güvenliği Yönetimi

VII. Genel Kontroller	PO9 Risklerin Değerlendirilmesi 9.5 Risk Aksiyon Planı AI1 Otomasyon Çözümlerinin Tanımlanması 1.9 Maliyet Açısından Etkin Güvenlik Kontrolleri DS7 Kullanıcı Eğitimi ve Bilinçlendirmesi 7.3 Güvenlik Prensipleri ve Bilinçlendirme Eğitimi	6.2.1 Dış taraflarla ilgili riskleri tanımlama 15.3.2 Bilgi sistemleri denetim araçlarının korunması 15.3.1 Bilgi sistemleri denetim kontrolleri	6.6 Bilgi Güvenliği Yönetimi
VII. Genel Kontroller	AI1 Otomasyon Çözümlerinin Tanımlanması 1.1 Bilgi Gerekliliklerinin Tanımlanması	ISO 27001'de direkt bir karşılığı yoktur.	6.6 Bilgi Güvenliği Yönetimi
VII. Genel Kontroller	DS11 Veri Yönetimi 11.1 Veri Hazırlama Prosedürleri 11.2 Kaynak Doküman Yetkilendirme Prosedürleri 11.3 Kaynak Doküman Veri Toplama 11.4 Kaynak Dokümanı Hata İşleme 11.7 Doğruluk, Tam Olma ve Yetkilendirme Kontrolleri 11.8 Giriş Verisi Hata İşleme 11.9 Veri İşleme Bütünlüğü 11.10 Veri İşleme Geçerleme ve Düzenleme 11.11 Veri İşleme Hata	10.9.1 E - Ticaret 12.2 Uygulamalarda doğru işleme 12.3 Kriptografik Kontroller	9.1 Konfigürasyon Yönetimi 10.1 Sürüm Yönetimi Süreci
VII. Genel Kontroller	M1 Proseslerin İzlenmesi 1.1 İzleme Verisinin Toplanması 1.2 Performansın Değerlendirilmesi 1.3 Müşteri Memnuniyetinin Değerlendirilmesi 1.4 Yönetim Raporlama M2 Kontrol Etkinliğinin Değerlendirilmesi 2.1 Kontrollerin İç Denetimi	5.1.2 Bilgi Güvenliği Politikasının Gözden Geçirilmesi	6.6 Bilgi Güvenliği Yönetimi

VII. Genel Kontroller	M3 Bağımsız Gözden Geçirme 3.3 IT Hizmetlerinin Bağımsız Etkinlik Gözden Geçirmesi 3.4 3. Taraf Servis Sağlayıcıların Etkinliklerinin Bağımsız Gözden Geçirilmesi 3.5 Yasalara ve düzenlemelere, gerekliliklere ve sözleşme gerekliliklerine uyum 3.6 3. Taraf Servis Sağlayıcıların Yasalara,	İlgili madde yoktur.	6.6 Bilgi Güvenliği Yönetimi
VII. Genel Kontroller	11.18 Kullanımdan Çıkartılmış Hassas Bilgilerin Korunması	7.2.2 Bilgi Etiketleme ve İşleme	6.6 Bilgi Güvenliği Yönetimi
VII. Genel Kontroller	11.18 Kullanımdan Çıkartılmış Hassas Bilgilerin Korunması	7.2.2 Bilgi Etiketleme ve İşleme	6.6 Bilgi Güvenliği Yönetimi
VII. Genel Kontroller	11.26 Arşivleme, 11.27 Hassas Mesajların Korunması	10.8.4 Elektronik Mesajlaşma	6.6 Bilgi Güvenliği Yönetimi
VII. Genel Kontroller	11.26 Arşivleme, 11.27 Hassas Mesajların Korunması	10.8.4 Elektronik Mesajlaşma	6.6 Bilgi Güvenliği Yönetimi
VIII. Haberleşme ve İşletim Yönetimi	PO9 Risklerin Değerlendirilmesi AI3-3.6 Teknoloji Altyapısının Edinim ve Bakımı PO11 Kalite Yönetimi	12 Sistem Edinim, Geliştirme ve Bakımı 10.1.4 Geliştirme, test ve işletim olanaklarının ayrımı	6.6 Bilgi Güvenliği Yönetimi
VIII. Haberleşme ve İşletim Yönetimi	AI4 Prosedürlerin Geliştirilmesi ve Bakımı 4.2 Kullanıcı Prosedürleri El Kitabı 4.3 Operasyon El Kitabı 4.4 Eğitim Malzemeleri DS7 Kullanıcı Eğitimi ve Bilinçlendirmesi 7.1 Eğitim İhtiyaçlarının Belirlenmesi	8.2.2 Bilgi güvenliği farkındalığı, eğitim ve öğretimi	3.3 Yetkinlik, Bilinç ve Eğitim

VIII. Haberleşme ve İşletim Yönetimi	DS5 Sistem Güvenliğinin Sağlanması 5.19 Kötü Niyetli Yazılımın Engellenmesi, Belirlenmesi ve Düzeltilmesi	10.4 Kötü niyetli ve mobil koda karşı koruma	6.6 Bilgi Güvenliği Yönetimi
VIII. Haberleşme ve İşletim Yönetimi	DS5 Sistem Güvenliğinin Sağlanması 5.19 Kötü Niyetli Yazılımın Engellenmesi, Belirlenmesi ve Düzeltilmesi	10.4 Kötü niyetli ve mobil koda karşı koruma	6.6 Bilgi Güvenliği Yönetimi
X. Sistem Geliştirme ve Bakımı	AI3 Teknoloji Altyapı Edinim ve Bakımı 3.1 Yeni Donanım ve Yazılımın Değerlendirilmesi DS8 Müşterilere Yardım Edilmesi ve Öneride Bulunulması PO11 Kalite Yönetimi 11.9 Teknoloji Altyapısı İçin Edinim ve Bakım Çerçevesi	12.1 Bilgi sistemlerinin güvenlik gereksinimleri 12.1.1 Güvenlik gereksinimleri analizi ve belirtimi	7.3 Tedarikçi Yönetimi
X. Sistem Geliştirme ve Bakımı	PO9 Risklerin Değerlendirilmesi 9.1 İş Risk Değerlendirme 9.3 Risk Tanımlama AI3-3.6 Teknoloji Altyapısının Edinim ve Bakımı 11.9 Teknoloji Altyapısı İçin Edinim ve Bakım Çerçevesi	10.1.2 Değişim yönetimi 12.5.1 Değişim kontrol prosedürleri 12.1 Bilgi sistemlerinin güvenlik gereksinimleri 12.1.1 Güvenlik gereksinimleri analizi ve belirtimi 15.3.1 Bilgi sistemleri denetim kontrolleri	
X. Sistem Geliştirme ve Bakımı	PO9 Risklerin Değerlendirilmesi AI3-3.6 Teknoloji Altyapısının Edinim ve Bakımı PO11 Kalite Yönetimi	12 Sistem Edinim, Geliştirme ve Bakımı	6.6 Bilgi Güvenliği Yönetimi

X. Sistem Geliştirme ve Bakımı	AI5 Sistem Kurulumu ve Akreditasyonu 5.7 Değişikliklerin Test Edilmesi 5.11 Operasyonel Test 5.12 Üretime Geçiş	10.3 Sistem Planlama ve Kabul 10.1.4 Geliştirme, test ve işletim olanaklarının ayrımı	10 Sürüm Süreci
X. Sistem Geliştirme ve Bakımı	AI5 Sistem Kurulumu ve Akreditasyonu 5.9 Son Kabul Testi 5.13 Kullanıcı Gerekliliklerinin Yerine Getirilmesinin Değerlendirilmesi 5.14 Uygulama Sonrası Yönetim Gözden Geçirmesi	10.3.2 Sistem Kabulü	10 Sürüm Süreci
X. Sistem Geliştirme ve Bakımı	AI5 Sistem Kurulumu ve Akreditasyonu 5.7 Değişikliklerin Test Edilmesi AI6 Değişiklik Yönetimi 6.4 Acil Değişiklikler	10.1.2 Değişim Yönetimi 12.5 Geliştirme ve destekleme proseslerinde güvenlik 12.5.1 Değişim kontrol prosedürleri 12.5.2 İşletim sistemindeki değişikliklerden sonra teknik gözden geçirme 12.5.3 Yazılım paketlerindeki değişikliklerdeki kısıtlamalar	10 Sürüm Süreci 9.2 Değişiklik Yönetimi
X. Sistem Geliştirme ve Bakımı	AI5 Sistem Kurulumu ve Akreditasyonu 5.7 Değişikliklerin Test Edilmesi AI6 Değişiklik Yönetimi 6.4 Acil Değişiklikler	10.1.2 Değişim Yönetimi 12.5 Geliştirme ve destekleme proseslerinde güvenlik 12.5.1 Değişim kontrol prosedürleri 12.5.2 İşletim sistemindeki değişikliklerden sonra teknik gözden geçirme 12.5.3 Yazılım paketlerindeki değişikliklerdeki kısıtlamalar	9.2 Değişiklik Yönetimi

XI. İş Sürekliliği	DS4 Servis Sürekliliğinin Sağlanması 4.2 IT Süreklilik Plan Stratejisi ve Felsefesi 4.4 IT Süreklilik Gerekliliklerinin Minimize Edilmesi 4.10 Kritik IT Kaynakları DS10 Problem ve Olayların Yönetilmesi 10.1 Problem Yönetim Sistemi 10.2 Problem Eskalasyon Yöntemi DS12 Tesis Yönetimi 12.6 Uninterruptible Power	14 İş Sürekliliği Yönetimi 14.1.2 İş sürekliliği ve risk değerlendirme	6.3 Servis Sürekliliği ve Erişilebilirliği Yönetimi
XI. İş Sürekliliği	DS4 Servis Sürekliliğinin Sağlanması 4.2 IT Süreklilik Plan Stratejisi ve Felsefesi 4.4 IT Süreklilik Gerekliliklerinin Minimize Edilmesi 4.10 Kritik IT Kaynakları DS10 Problem ve Olayların Yönetilmesi 10.1 Problem Yönetim Sistemi 10.2 Problem Eskalasyon Yöntemi DS12 Tesis Yönetimi 12.6 Uninterruptible Power	14 İş Sürekliliği Yönetimi 14.1.3 Bilgi güvenliğini içeren süreklilik planlarını geliştirme ve gerçekleştirme 14.1.4 İş sürekliliği planlama çerçevesi	6.3 Servis Sürekliliği ve Erişilebilirliği Yönetimi 6.3.4 Servis Sürekliliği Planlama ve Test
XI. İş Sürekliliği	DS4 Servis Sürekliliğinin Sağlanması 4.3 IT Süreklilik Plan İçeriği 4.9 Kullanıcı Departmanı Alternatif Bilgi İşleme Yedekleme Prosedürleri	14 İş Sürekliliği Yönetimi 14.1.3 Bilgi güvenliğini içeren süreklilik planlarını geliştirme ve gerçekleştirme	6.3 Servis Sürekliliği ve Erişilebilirliği Yönetimi
XI. İş Sürekliliği	DS4 Servis Sürekliliğinin Sağlanması 4.2 IT Süreklilik Plan Stratejisi ve Felsefesi 4.10 Kritik IT Kaynakları DS10 Problem ve Olayların Yönetilmesi 10.1 Problem Yönetim Sistemi 10.2 Problem Eskalasyon Yöntemi	14.1 İş sürekliliği yönetiminin bilgi güvenliği hususları 14.1.3 Bilgi güvenliğini içeren süreklilik planlarını geliştirme ve gerçekleştirme	6.3 Servis Sürekliliği ve Erişilebilirliği Yönetimi

XI. İş Sürekliliği	DS4 Servis Sürekliliğinin Sağlanması 4.3 BT Süreklilik Plan İçeriği 4.9 Kullanıcı Departmanı Alternatif Bilgi İşleme Yedekleme Prosedürleri	14.1 İş sürekliliği yönetiminin bilgi güvenliği hususları 14.1.5 İş sürekliliği planlarını test etme, sürdürme ve yeniden değerlendirme	6.3 Servis Sürekliliği ve Erişilebilirliği Yönetimi
XI. İş Sürekliliği	DS4 Servis Sürekliliğinin Sağlanması 4.6 IT Süreklilik Planının Test Edilmesi 4.12 Saha Dışında Yedekleme DS11 Veri Yönetimi 11.23 Yedekleme ve Geri Dönüş 11.24 Yedekleme Görevleri 11.25 Yedek Depolama	10.5 Yedekleme 10.5.1 Bilgi Yedekleme 14.1 İş sürekliliği yönetiminin bilgi güvenliği hususları	6.3 Servis Sürekliliği ve Erişilebilirliği Yönetimi
XII. Uyum	PO8 Dış Gerekliliklere Uyum Sağlandığından Emin Olunması 8.1 Dış Gerekliliklerin Gözden Geçirilmesi 8.2 Dış Gerekliliklere Uyum Sağlama İçin Gereken Uygulama ve Prosedürler 8.3 Güvenlik ve Ergonomik Uyum 8.4 Gizlilik, Fikri Mülkiyet ve Veri Akışı 8.5 Elektronik Ticaret 8.6 Sigorta Sözleşmelerine Uyum	15.1 Yasal gereksinimlerle uyum	6.6 Bilgi Güvenliği Yönetimi
XII. Uyum	DS5 Sistem Güvenliğinin Sağlanması 5.7 Güvenlik Takibi 5.11 Olay Yönetimi	15.1 Yasal gereksinimlerle uyum 15.3.2 Bilgi sistemleri denetim araçlarının korunması 10.10.2 Sistem kullanımını izleme 15.2.1 Güvenlik politikaları ve standardlarla uyum 15.2.2 Teknik uyum kontrolü 6.3 Güvenlik olayları ve arızalara yanıt verilmesi	

XII. Uyum	DS9 Konfigürasyon Yönetimi 9.5 Lisanssız Yazılım 9.8 Yazılımın Güvenilirliği	5.1.1 Varlık Envanteri 15.1 Yasal gereksinimlerle uyum 12.1.2 Fikri mülkiyet hakları	9.1 Konfigürasyon Yönetimi
XII. Uyum	DS11 Veri Yönetimi 11.5 Kaynak Dokümanların Muhafazası 11.19 Depolama Yönetimi 11.20 Muhafaza Süreleri ve Depolama Koşulları 11.26 Arşivleme	8.6 Ortam yönetimi ve Güvenlik 12 Uyum 12.1.3 Organizasyonel kayıtların korunması 12.1.4 Verilerin korunması ve kşisel bilgilerin gizliliği	6.6 Bilgi Güvenliği Yönetimi

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı	**:**Bahadır Murat KANDEMİRLİ
Doğum Tarihi ve Yeri	**:**29.11.2981 - Gaziantep
Yabancı Dili	**:**İngilizce
E-posta	**:**muratkandemirli@gmail.com

ÖĞRENİM DURUMU

Derece	**Alan**	**Okul/Üniversite**	**Mezuniyet Yılı**
Lisans	Endüstri Mühendisliği	Erciyes Üniversitesi	2004
Lise	Fen ve Matematik Bilimleri	Bayraktar Lisesi	1998

İŞ TECRÜBESİ

Yıl	**Firma/Kurum**	**Görevi**
2008	Abc	BT Proje Yöneticisi,PMP
2007	Ceva Lojistik	Yazılım Kalite Güvence Uzmanı
2006	Fortis Emeklilik ve Hayat	Kıdemli Sistem Analisti
2005	Aksigorta	Uzman

Proje

1. Clementain verimadenciliği aracı ile müşteri tutundurma ve çapraz satış
2. SAP Business Objects R3.1 iş zekası ve raporlama ortamı için veritabanı tasarımı ve uygulama entegrasyonu
3. Çağrı merkezi IVR ve IVN sistemlerinin entegrasyonu
4. Ceva Lojistik - Ford Gölcük ERP sistemi ve Ceva lojistik depo yönetim sistemi entegrasyonu - Ceva Lojistik
5. Opel GM depo yönetim sistemi ve RFID entegrasyonu – Ceva Lojistik
6. Kurumsal internet şube tasarımı ve geliştirilmesi - Fortis Emeklilik
7. Oracle Hyperion Essbase iş zekası ve raporlama aracı entegrasyonu – Fortis Emeklilik
8. Aksigorta Vizyoneks ERP entegrasyon projesi - Aksigorta