TC
YILDIZ TEKNİK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANA BİLİM DALI
İŞLETME YÖNETİMİ YÜKSEK LİSANS PROGRAMI

YÜKSEK LİSANS TEZİ

BİLGİ TEKNOLOJİLERİ DENETİMİNİN ESASLARI VE TÜRK BANKACILIK SEKTÖRÜNDEKİ UYGULAMALARI

Mustafa Cem Akocak
06713019

TEZ DANIŞMANI
Prof. Dr. SALİH DURER

İSTANBUL
2009

TC
YILDIZ TEKNİK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANA BİLİM DALI
İŞLETME YÖNETİMİ YÜKSEK LİSANS PROGRAMI

YÜKSEK LİSANS TEZİ

BİLGİ TEKNOLOJİLERİ DENETİMİNİN ESASLARI VE TÜRK BANKACILIK SEKTÖRÜNDEKİ UYGULAMALARI

Mustafa Cem Akocak
06713019

TEZ DANIŞMANI
Prof. Dr. SALİH DURER

İSTANBUL
2009

TC
YILDIZ TEKNİK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANA BİLİM DALI
İŞLETME YÖNETİMİ YÜKSEK LİSANS PROGRAMI

YÜKSEK LİSANS TEZİ

BİLGİ TEKNOLOJİLERİ DENETİMİNİN ESASLARI VE TÜRK BANKACILIK SEKTÖRÜNDEKİ UYGULAMALARI

Mustafa Cem Akocak
06713019

Tezin Enstitüye Verildiği Tarih: …….
Tezin Savunulduğu Tarih: ……...

Tez Oy birliği / Oy çokluğu ile başarılı bulunmuştur.

	Unvan Ad Soyad	İmza
Tez Danışmanı :	Prof. Dr. Salih DURER	
Jüri Üyeleri :	Prof Dr. Güler ARAS	
	Öğr. Gör. Halil Emre AKBAŞ	

İSTANBUL
Haziran 2009

ÖZ

Bilgi Teknolojileri Denetiminin Esasları ve Türk Bankacılık Sektöründeki Uygulamaları
Mustafa Cem Akocak
Haziran, 2009

Araştırma çalışmamızın temel amacı bağımsız finansal denetim amaçları ile bankacılık sektöründeki bilgi sistemleri denetim faaliyetleri kapsamındaki bilgi sistemleri denetim sonuçlarının nasıl bir arada değerlendirebileceğini ortaya koymaktır. Bunun yanında bilgi sistemleri denetiminin ve bilgisayar destekli denetim araçlarının kullanımının günümüz teknoloji çağında denetim sürecini bütünüyle etkilediği ve değiştirdiğini ortaya koymaktır.

Çeşitli bilgisayar destekli denetim araçlarından da yararlanarak bilgi sistemleri denetimi kapsamı altında Türk Bankacılık Sektörü üzerinde bilgi sistemleri denetimi kapsamında uygulama örnekleri verilerek bilgi sistemleri denetiminin dahil olduğu entegre denetimin gerekliliği ortaya konmuştur.

Bilgi sistemleri denetimi kapsamında gerçekleştirilen uygulama kontrolleri alanı denetimi finansal denetim ile ilişkilendirilerek bankaların teknoloji yoğun iş süreçlerini ve iç kontrol ortamını değerlendirmek için gerekli noktaları kapatmakta ve günümüz gereği olan entegre denetimin gerçekleşmesini sağlamaktadır. Ancak uygulama kontrolleri alanının denetimi bilgi sistemleri denetiminin başarılı olarak tamamlanması, diğer bir ifadeyle finansal denetim amaçlarının bilgi sistemleri denetim amaçları ile eksiksiz olarak desteklenmesi anlamına gelmemektedir. Bu kapsamda bilgi teknolojileri genel kontrol alanlarının da denetiminin gerçekleştirilmesi gerekmektedir. Bankalar tarafından kullanılan uygulamalar üzerinde tasarlanan kontroller etkin bir bilgi teknolojileri genel kontrol ortamı üzerinde çalışma gereği duymaktadırlar.

Sonuç olarak banka sektörü gibi veri miktarının yüksek ve bilgi sistemleri kullanımının yoğun olduğu sektörlerde bilgi sistemleri denetimi, bağımsız finansal denetim amaçlarının desteklenmesi açısında çok önemli bir yere sahip olduğu sonucu çıkmaktadır.

Anahtar Kelimeler : Bilgi Teknolojileri Denetimi, Uygulama Kontrolleri, Bilgi Teknolojileri Genel Kontrol Alanları, Bilgisayar Destekli Denetim Araçları, Bankalarda Bilgi Teknolojileri Denetimi

ABSTRACT

Basics of Information Technology Audit and Its Implementation on Banking Sector in Turkey
Mustafa Cem Akocak
June, 2009

The main purpose of this thesis is to explain how to relate and evaluate the financial audit objectives and results of information technology audit ("IT Audit") for banking sector in Turkey. Furthermore, its other purpose is to prove that IT audit and use of computer aided audit technologies/tools have great impact on classical audit process and they change the process of classical audit via supporting integrated audit.

By using various computer aided audit technologies/tools, IT audit process is explained and implemented with some examples to show necessity of integrated audit.

In scope of information technology audit, application controls audit process collaborates with the financial audit process to support evaluation of highly technology dependent business processes of banks and to meet integrated audit purposes. However, completion of application controls audit process does not mean to succeed integrated audit process via aligning financial audit and information technology audit objectives. Therefore, audit process of general information technology controls has to be completed to support operating effectiveness of application controls which are established in general information technology environment. Effectiveness of application controls depends on effectiveness of general information technology controls, because these application controls are designed on general information technology environment.

It was concluded that IT audit and use of computer aided audit technologies/tools have important role to support financial audit objectives in technology driven, highly transactional and financial sector including banking sector.

Keywords : Information Technology Audit, Application Controls, General Information Technology Controls, Computer Aided Audit Tools, IT Audit in Banks

ÖNSÖZ

Bağımsız finansal denetim kapsamında, bağımsız denetim kuruluşlarının ana amacı bağımsızlık ilkesine bağlı olarak finansal tabloların doğruluğu, tutarlılığı ve tam olarak açıklanmış olması adına makul bir güvence sağlamak için görüş verilmesidir. Bu açıdan değerlendirildiğinde bilgi sistemlerinin yoğun olarak kullanıldığı bankacılık sektöründe, finansal veri üretiminde bilgi sistemlerinin önemi göz önüne çıkmaktadır. Bu sebeple bağımsız finansal denetim faaliyetleri kapsamında bilgi sistemleri denetimi ile entegre olarak denetim faaliyetlerinin yürütülebilmesi günümüz teknolojik gelişmelerine ve bankacılık sektörünün yapısına bağlı olarak kaçınılmaz boyuta gelmiştir. Çalışmamızda bilgi sistemleri denetiminin ve bilgisayar destekli denetim araçların kullanımının teknoloji yoğun Türk Bankacılık Sektörü kapsamında denetim süreci üzerindeki etkileri uygulamalar ile ortaya konmuştur. Uygulama kapsamında Genel Muhasebe Süreci uygulama kontrolleri alanı ile DS5: Sistem Güvenliğinin Sağlanması genel kontrol alanı kapsamında örneklere yer verilmiş olup bilgi sistemleri denetiminin bankaların iç kontrol ortamının değerlendirilmesindeki ve finansal denetim amaçlarının desteklenmesindeki gerekliliği ortaya konmuştur.

Bu çalışmayı sonuçlandırmamda görüşleri ile katkıda bulunan değerli hocam Prof. Dr. Salih Durer ve KPMG Türkiye'ye çok teşekkür eder, çalışmanın tüm ilgililere yararlı olmasını dilerim.

İstanbul; Haziran, 2009 **Mustafa Cem Akocak**

İÇİNDEKİLER

ÖZ ..... **iii**
ABSTRACT ..... **iv**
ÖNSÖZ ..... **v**
İÇİNDEKİLER **1**
TABLOLAR LİSTESİ **4**
ŞEKİLLER LİSTESİ **5**
KISALTMALAR **7**

1. GİRİŞ **8**

2. BİLGİ SİSTEMLERİNİN YÖNETİMİ VE TEMEL KONTROL KAVRAMLARI **10**

2.1. Bilgi Sistemlerinin Temel Fonksiyonları 10
2.1.1. Veri Giriş Süreci 12
2.1.2. Veri İşleme Süreci 13
2.1.3. Veri Çıkış Süreci 15
2.2. Bilgi Teknolojileri Yönetimi 15
2.2.1. Sistem ve Alt Yapı Yönetimi 16
2.2.2. Bilgi Teknolojileri Servis Sunumu ve Destek 19
2.2.3. Bilgi Varlıklarının Korunması 21
2.2.4. İş Sürekliliği ve Felaketten Kurtarma Süreci 23
2.3. Bilgi Teknolojileri Kontrollerinin Kapsamlarına Göre Sınıflandırılması 26
2.3.1. Bilgi Teknolojileri Genel Kontrol Ortamı 26
2.3.2. Bilgi Teknolojileri Uygulama Kontrolleri 32
2.4. Uygulama Sistemleri ve Üzerindeki Kontrollere Yönelik Denetim Teknikleri 36

3. BİLGİ SİSTEMLERİ DENETİM SÜRECİ VE ESASLARI **41**

3.1. Denetimin Tanımı ve Amacı 41
3.2. Denetimin Türleri 43
3.2.1. Konusuna Göre Denetim Türleri 43
3.2.2. Denetçinin Durumuna Göre Denetim Türleri 44
3.3. Denetim Sürecinin Sınıflandırılması 45
3.3.1. Finansal Denetim 45
3.3.2. Operasyonel Denetim 46
3.3.3. Bilgi Sistemleri Denetimi 46
3.3.4. Entegre Denetim 46
3.3.5. Yönetsel Denetim 46
3.3.6. Adli denetim 46
3.3.7. Özel Amaçlı Denetim 47

3.4. Bilgi Sistemleri Denetiminin Amaçları 47
3.5. Bilgi Sistemleri Denetiminin Organizasyon İçindeki Yeri ve Önemi 48
3.6. Bilgi Sistemleri Denetiminin Finansal Denetim Üzerindeki Etkileri 49
3.7. Bilgi Sistemleri Denetim Standartları ve Prensipleri 53
3.8. Bilgi Sistemleri Denetiminde Risk Analizi 57
3.9. İç Kontrol Sistemi 63
3.9.1. İç Kontrol Sisteminin Tanımı ve Bankacılık Sektöründeki Yeri 63
3.9.2. İç Kontrol Sisteminin Amaçları 65
3.9.3. Bilgi Teknolojilerinin İç Kontrol Sistemi Üzerindeki Etkileri 67
3.10. Bilgi Sistemleri Denetim Süreci 69
3.10.1. Bilgi Sistemleri Denetim Hedefleri 70
3.10.2. Bilgi Sistemleri Denetim Metodolojisi 71
3.10.3. Bilgi Sistemleri Denetim Programları 73
3.10.4. Bilgi Sistemleri Denetim Riski ve Önemlilik Derecesi 74
3.10.5. Bilgi Sistemleri Risk Değerlendirme Teknikleri 77
3.10.6. Bilgi Sistemleri Denetimine Yönelik Testler 78
3.10.7. Örneklem Belirleme ve Kanıt Toplama 80
3.10.8. Bilgisayar Destekli Denetim Teknikleri 84
3.10.9. Bilgi Sistemleri Denetim Sonuçlarının Raporlanması 86

4. TÜRK BANKACILIK SEKTÖRÜNDE BİLGİ SİSTEMLERİ DENETİMİ VE YASAL MEVZUAT 90

4.1. Bankalarda Bilgi Sistemleri Denetiminin Amacı ve Kapsamı 90
4.2. Bankalarda Bilgi Sistemleri Denetiminde Yetkili Kuruluşlar ve Aranan Şartlar 92
4.3. Bilgi Sistemleri Denetimindeki Yükümlülükler 94
4.3.1. Denetlenen Bankaların Yükümlülükleri 94
4.3.2. Denetleyen Yetkili Denetim Kuruluşlarının Yükümlülükleri 96
4.4. Bilgi Teknolojilerine İlişkin Kontrol Hedefleri (CobiT) 98
4.5. Bilgi Teknolojileri Yönetimine İlişkin İlkeler ve Denetim Kapsamı 102
4.6. Uygulama Süreçlerinin Denetimi 108
4.6.1. Uygulama Kontrollerinin Türleri 109
4.6.2. Bankacılık Sektöründe Asgari Olarak Denetlenen Süreçler 112
4.7. Genel Kontrol Alanlarının Denetimi 114
4.7.1. Planlama ve Organizasyon Faaliyetlerinin Denetimi 115
4.7.2. Tedarik ve Uygulama Faaliyetlerinin Denetimi 119
4.7.3. Hizmet Sunumu ve Destek Faaliyetlerinin Denetimi 121
4.7.4. İzleme ve Değerlendirme Faaliyetlerinin Denetimi 127
4.8. Bankaların Bilgi Teknolojilerine Yönelik Destek Alım Faaliyetlerinin Denetimi 128
4.9. Bilgi Sistemleri Denetim Sonuçlarının Değerlendirilmesi ve Olgunluk Seviyesi 130
4.10. Bilgi Sistemleri Denetim Raporunun Oluşturulması 133

5. UYGULAMA 139

5.1. Uygulamanın Problemi 139
5.2. Uygulamanın Amacı 140
5.3. Uygulamanın Önemi 140

5.4. Uygulamanın Kapsamı ve Kısıtları 141
5.5. Kullanılan Araçlar 142
5.6. Uygulamanın Yapılması ve Sonuçları 143
5.6.1. Uygulama Kontrollerinin Denetimi ve Raporlaması: Genel Muhasebe Kontrolleri Süreci 143
5.6.2. Genel Kontrol Alanı Denetimi ve Raporlaması: Sistem Güvenliğinin Sağlanması (DS5) 168

6. SONUÇ 193

KAYNAKÇA 196

EKLER 199

Ek 1. CobiT Olgunluk Seviyesi Değerlendirme Aracı 199

ÖZGEÇMİŞ 203

TABLOLAR LİSTESİ

Sayfa No

Tablo 1 : Genel Kontrol Alanlarına Yönelik Kontrol Hedefi Sayısı..... 130
Tablo 2 : CobiT Olgunluk Seviyeleri ve Açıklamaları 132
Tablo 3 : Test Edilen Kontrol Kapsamında Uygulama Kontrol Listesi 1 155
Tablo 4 : Test Edilen Kontrol Kapsamında Bulgu İfadesi 1 155
Tablo 5 : Test Edilen Kontrol Kapsamında Uygulama Kontrol Listesi 2 159
Tablo 6 : Test Edilen Kontrol Kapsamında Bulgu İfadesi 2 160
Tablo 7 : Test Edilen Kontrol Kapsamında Uygulama Kontrol Listesi 3 164
Tablo 8 : Olgunluk Seviyesi "0" için Anket Soruları..... 190
Tablo 9 : Olgunluk Seviyesinin Hesaplanma Yöntemi 191

ŞEKİLLER LİSTESİ

Sayfa No

Şekil 1 : Bilgi Sisteminin İşleyişi 11
Şekil 2 : Zayıf BT Genel Kontrol Ortamı 27
Şekil 3 : Güçlü BT Genel Kontrol Ortamı 27
Şekil 4 : BT Kontrol Ortamları 28
Şekil 5 : Denetim Riski 75
Şekil 6 : Denetim Faaliyetleri ile İlgili Risk Noktalarının Yerleri 76
Şekil 7 : CobiT Model Bileşenleri Arasındaki İlişkiler 99
Şekil 8 : CobiT Temel Prensipleri 100
Şekil 9 : CobiT Kontrol Başlıkları Arası İlişkiler 101
Şekil 10 : Olgunluk Seviyesi Grafiği 131
Şekil 11 : Bankalarda Entegre Denetim 140
Şekil 12 : IDEA Veri Girişi 1 145
Şekil 13 : IDEA Veri Girişi 2 145
Şekil 14 : IDEA Veri Girişi 3 146
Şekil 15 : IDEA Veri Girişi 4 147
Şekil 16 : IDEA Veri Girişi 5 147
Şekil 17 : IDEA'ya Transfer Edilen Verinin Görünümü 148
Şekil 18 : IDEA İstatistiksel Özel Bilgi 149
Şekil 19 : IDEA Sıralama İşlemi 149
Şekil 20 : IDEA "Field Summarization" İşlemi 150
Şekil 21 : IDEA "Field Summarization" İşleminde İlgili Kolonların Seçimi 150
Şekil 22 : IDEA "Field Summarization" İşleminin Sonucu 1 151
Şekil 23 : IDEA "Field Summarization" İşleminin Sonucu 2 151
Şekil 24 : IDEA "Field Summarization" İşleminde Gruplanan Kayıtların Detayı 152
Şekil 25 : IDEA "Field Summarization" İşleminde Fiş Sırası ve Kayıt Miktarları 153
Şekil 26 : IDEA Borç-Alacak Dengesi Analiz Sonucu 154
Şekil 27 : IDEA "Gap-Detection" Analizi 157
Şekil 28 : IDEA "Gap-Detection" Analizinde Fiş Kolonunun Seçilmesi 157
Şekil 29 : IDEA "Gap-Detection" Analiz Sonucu 1 158
Şekil 30 : IDEA "Gap-Detection" Analiz Sonucu 2 158
Şekil 31 : IDEA "Gap-Detection" Analiz Sonucu 3 159
Şekil 32 : IDEA "Field Summarization" Analizi 161
Şekil 33 : IDEA "Field Summarization" Analizi Kullanıcı-Fiş Kolonlarının Seçimi 162
Şekil 34 : IDEA "Field Summarization" Kullanıcı-Fiş Girişi Analiz Sonucu 162
Şekil 35 : IDEA Kullanıcı-Fiş Girişi Analiz Sonucunun Grafiksel Gösterimi 163
Şekil 36 : IDEA Kullanıcı-Fiş Girişi Grafiği 163
Şekil 37 : Bilgisayar Destekli Denetim Araçlarının Kullanım Amaçları 165
Şekil 38 : Bilgisayar Destekli Denetim Araçlarının Sınıflandırılması 166
Şekil 39 : Bilgisayar Destekli Denetim Araçlarının Kullanım Dağılımı 167
Şekil 40 : Bilgi Sistemleri Güvenlik Ortamı Değerlendirme Aracı ("MSAT") Profil Girişi 169
Şekil 41 : MSAT Genel Bilgi Girişi 169
Şekil 42 : MSAT Banka Risk Profili Girişi 1 170
Şekil 43 : MSAT Banka Risk Profili Girişi 2 170

Şekil 44 : MSAT Banka Risk Profili Girişi 3 171
Şekil 45 : MSAT Banka Risk Profili Girişi 4 172
Şekil 46 : MSAT Banka Risk Profili Girişi 5 172
Şekil 47 : MSAT Banka Güvenlik Değerlendirme Tanımlaması 173
Şekil 48 : MSAT Banka Güvenlik Değerlendirme 1 174
Şekil 49 : MSAT Banka Güvenlik Değerlendirme 2 174
Şekil 50 : MSAT Banka Güvenlik Değerlendirme 3 175
Şekil 51 : MSAT Banka Güvenlik Değerlendirme 4 175
Şekil 52 : MSAT Banka Güvenlik Değerlendirme 5 176
Şekil 53 : MSAT Banka Güvenlik Değerlendirme 6 176
Şekil 54 : MSAT Banka Güvenlik Değerlendirme 7 177
Şekil 55 : MSAT Banka Güvenlik Değerlendirme 8 178
Şekil 56 : MSAT Banka Güvenlik Değerlendirme 9 178
Şekil 57 : MSAT Banka Güvenlik Değerlendirme 10 179
Şekil 58 : MSAT Banka Güvenlik Değerlendirme 11 179
Şekil 59 : MSAT Banka Güvenlik Değerlendirme 12 180
Şekil 60 : MSAT Banka Güvenlik Değerlendirme 13 181
Şekil 61 : MSAT Banka Güvenlik Değerlendirme Raporlaması 181
Şekil 62 : MSAT Banka Güvenlik Değerlendirme Özet Rapor 182
Şekil 63 : MSAT Banka Güvenlik Değerlendirme Detay Rapor 182
Şekil 64 : MSAT Banka Güvenlik Değerlendirme Detay Rapor: Karne Gösterimi 183
Şekil 65 : MSAT Banka Güvenlik Değerlendirme Detay Rapor: Tavsiyeler 184
Şekil 66 : MSAT Banka Güvenlik Değerlendirme Karşılaştırmalı Rapor 1 184
Şekil 67 : MSAT Banka Güvenlik Değerlendirme Karşılaştırmalı Rapor 2 185

KISALTMALAR

AICPA : Amerikan Sertifikalı Muhasebeciler Enstitüsü / Uluslararası Muhasebe Uzmanları Federasyonu (American Institute of Certified Public Accountants)

ISACA : Bilgi Sistemleri Denetimi ve Kontrolü Derneği (Information System Auditing Control Association)

BDDK : Bankacılık Düzenleme ve Denetleme Kurulu

TCMB : Türkiye Cumhuriyeti Merkez Bankası

COBIT : Bilgi Teknolojileri Kontrol Hedefleri (Control Objectives for Information and related Technology)

BDDA : Bilgisayar Destekli Denetim Araçları

SAS70 : Servis Organizasyonları Tarafından Gerçekleştirilen İşlemlere Yönelik Bağımsız Denetim Raporu (Statement on Auditing Standard 70)

IIA : İç Denetim Derneği (The Institute of Internal Auditors)

CISA : Yetkili Bilgi Sistemleri Denetçisi (Certified Information System Auditor)

BT : Bilgi Teknolojileri

KYS : Kalite Yönetimi Sistemi

ITGI : Bilgi Teknolojileri Yönetişim Enstitüsü (The IT Governance Institute)

MSAT : Bilgi Sistemleri Güvenlik Ortamı Değerlendirme Aracı (Microsoft Security Assessment Tool)

EFT : Elektronik Fon Transferi

ATM : Automatic Teller Machine

IB : Internet Bankacılığı

BS : Bilgi Sistemleri

1. GİRİŞ

Yaşadığımız bilgi çağının ve küreselleşmenin bir sonucu olarak artan rekabet, bilginin önemini artırmıştır. İşletmeler bu rekabet ortamında ayakta kalabilmek ve koşullara olabildiğince çabuk tepki verebilmek için detaylı bilgi ve raporlama sistemlerine ihtiyaç duymaktadırlar. Bu ihtiyaç üzerindeki artış, günümüz çağındaki bilgi artışı ile bir araya geldiğinde, hemen hemen tüm kuruluşların muhasebe fonksiyonu da dahil olmak üzere iş süreçlerini bilgi sistemlerinin desteği ile yönettiklerini ortaya çıkmaktadır. Özellikle bankalar gibi teknoloji odaklı ve finansal işlem miktarı yoğun kuruluşlarda muhasebe ve finansal raporlama süreçlerinin bilgi sistemlerine dayandığı görülebilmektedir.

Muhasebe ve finansal raporlama süreçlerinde bilgi sistemlerinin kullanılması sürecin genel mantığını değiştirmese de finansal verilerin işlenmesini, saklanmasını, aktarılmasını doğrudan etkilemekte ve iç kontrol ortamının yapısını da değiştirmektedir. Dolayısıyla bu gelişmeler finansal denetimin kapsamı da etkilenmiş olup bilgi sistemleri denetimi ile beraber yürüyen finansal denetimin diğer adıyla entegre denetimin önemi artmıştır. Diğer bir ifadeyle, finansal denetimin nihai amacı ve kapsamında bir değişiklik olmasa da bilgi teknolojilerinin kullanımının artması faaliyetlerin yürütülme şeklini ve iş süreçlerinin üzerindeki kontrol noktalarını etkilediği gibi denetim sürecini de etkilemiş bulunmaktadır.

Bununla birlikte İmar Bankası kapsamında bilgi sistemleri üzerinden gerçekleştirilen hile ve usulsüzlüklerin de etkisiyle yasal merciler bilgi sistemlerinin iç kontrol ortamındaki önemini ve bağımsız bilgi sistemleri denetiminin gerekliliği bir kez daha görmüş ve Türk Bankacılık sektöründe bağımsız bilgi sistemleri denetimi zorunlu hale getirilmiştir.

Araştırmamız kapsamında bilgi sistemleri denetiminin esasları, Türk Bankacılık sektöründeki uygulamaları ve finansal denetim açısından önemi, dört bölüm üzerinden açıklanmaya çalışılacaktır. İlk bölüm kapsamında bilgi teknolojileri sistemlerinin yönetimi ve idame ettirilmesi ile birlikte süreç içerisindeki temel bilgi teknolojileri kontrollerinin açıklamalarına yer verilecektir.

İkinci bölümde ise bilgi sistemleri denetimi ile finansal denetim arasındaki ilişki, bilgi teknolojilerinin denetim sürecine etkileri, bilgi sistemleri denetim alanında uygulanan modeller ve uluslararası standartların açıklamalarına yer verilecektir.

Üçüncü bölümde ise bankacılık sektöründe bilgi sistemleri denetiminin kapsamı ve ülkemizde uygulanan yasal mevzuat ile birlikte açıklanmasına ve değerlendirilmesine yer verilecektir.

Son olarak dördüncü bölümde ise bankacılık sektöründe bilgi sistemleri denetimi kapsamında uygulama denetimine ve genel kontrol alanlarına yönelik seçilen süreçler kapsamında bilgi sistemleri denetiminin nasıl gerçekleştirildiği, sonuçların nasıl yorumlandığı, nasıl raporlandığı ve elde edilen sonuçların nasıl finansal denetim amaçlarına girdi teşkil ettiği ve bu kapsamdaki maddi doğruluk testlerinin kapsamını nasıl belirlediğine yer verilecektir.

Bu kapsamda araştırmanın önemi, bağımsız finansal denetim faaliyetlerinde özellikle bankacılık sektörü gibi bilgi sistemlerinin yoğun kullanıldığı sektörlerde bilgi sistemleri denetiminin önemini vurgulamak ve denetim amaçlarının sağlıklı olarak karşılanması için bilgi sistemleri denetim faaliyetlerinden ve bilgisayar destekli denetim araçlarından yararlanmanın kaçınılmaz olduğunu ortaya koymaktadır.

2. BİLGİ SİSTEMLERİNİN YÖNETİMİ VE TEMEL KONTROL KAVRAMLARI

Bilgi sistemleri ("BS") denetiminin doğru yapılabilmesi için bilgi teknolojileri ("BT") denetçisinin öncelikle bilgi teknolojileri yönetimi kavramını ve bilgi teknolojileri içerisinde yer alan kontrol kavramlarını yeterli düzeyde anlaması gerekmektedir. Bu nedenle çalışmaya öncelikle bilgi sistemleri yönetimi ve temel kontrol kavramları açıklanarak başlanmaktadır.

2.1. Bilgi Sistemlerinin Temel Fonksiyonları

Bilgi sistemi yönetimine ve bilgi sistemi tanımlarına geçmeden önce günümüzde vazgeçilmez bir yeri olan bilgisayar kavramını tanımlamak gerekmektedir. Temel olarak bilgisayar, belli bir sonuç üretmek amacıyla verilen girdilerle çeşitli işlemleri gerçekleştirmek üzere tasarlanmış çeşitli elektronik manyetik ve mekanik donanımın oluşturduğu bir sistemdir. Diğer bir ifadeyle çok temel olarak tanımlamak gerekirse, bilgisayar önceden tanımlanmış biçimde veriler kabul eden, sonrasında bu verileri işleyen ve işlem sonuçlarını da yine belirlenen amaçta ve şekilde kullanıcılara sunan veya diğer sistemlere aktaran yazılım ve donanım birimlerinden oluşan bir makinedir[1].

Teknolojide yaşanan hızlı gelişime paralel olarak, organizasyonlarda kullanılan bilgisayar sistemleri de her geçen gün daha karmaşık bir hal almaktadırlar. Yaşanan bu hızlı gelişim ile açık sistemler, mobil sistemler, yapay sinir ağları, uzman sistemler, bilgi güvenliği, kurumsal kaynak yönetimi sistemleri gibi birçok yeni kavram hayatımıza girmiştir. Bu kadar hızlı gelişen bir sektör içinde en zor görevlerden biri de bilgi sistemleri denetçilerini beklemektedir. Söz konusu organizasyonda bilgi sistemleri denetimini gerçekleştirebilmek için öncelikle organizasyonun bilgi sistemlerini anlayabilmek, iş süreçlerini tanımlayabilmek ve bu bilgilere hangi yollar ile ulaşabileceğini bilmesi gerekmektedir. Bu nedenle bilgi sistemleri denetçisi öncelikle temel bilgisayar kavramlarına hakim olmakla birlikte gelişmelere uygun olarak bilgilerini de güncel olarak tutmak zorundadır.

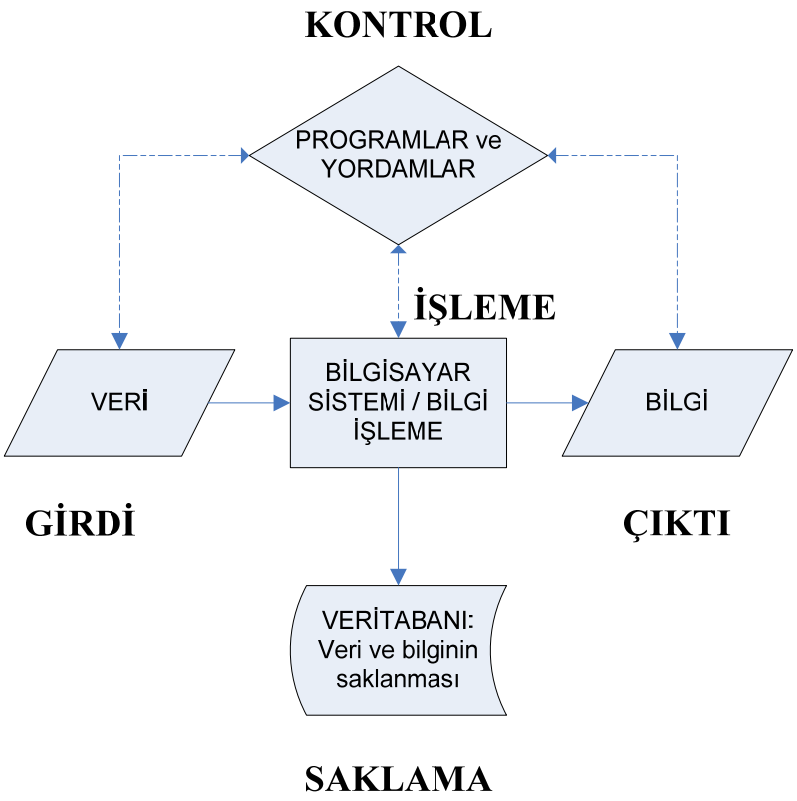
Bilgisayarın tanımına paralel olarak bilgi sistemi kavramını tanımlamak gerekirse, ulaşılması istenen ortak amaca uygun olarak, girdileri kabul ederek çıktılar üreten ve birbirleriyle ilişkili

[1] Melih Erdoğan, **Denetim Kavramsal ve Teknolojik Yapı**, 3. baskı (Ankara: Maliye ve Hukuk Yayınları, 2006), 133

bileşenlerden oluşan bir süreçtir. Daha yalın anlatımla bilgi sistemi verileri girdi olarak kabul ederek işleyen, kontrol eden, saklayan ve bilgi çıktısı olarak veren bir sistemdir.

Bilgi sistemleri yönetimi temel olarak tanımlamak gerekirse, organizasyonun amaçlarına paralel olarak bilgi sistemleri kaynaklarının etkin kullanılması ile birlikte verimli olarak yürütülmesidir[2]. Bu noktada hem organizasyonun amaçlarına destek olunması hem de organizasyona değer katılması amaçlanmaktadır. Bu yönetim sürecinin doğal bir parçası da bilgi sistemlerinin denetimi ve kontrol altında tutulmasıdır. Bilgi sistemlerinin denetim ilkelerine ve yöntemlerine diğer bölümlerde yer vermeden önce, temel bilgi sistemleri kavramlarını değinmekte yarar vardır.

Bilgi sistemi ve işleyişi temel olarak aşağıdaki şekil yardımıyla tanımlanabilmektedir:



Şekil 1: Bilgi Sisteminin İşleyişi

[2] Shelly Cashman Rosenblatt, **System Analysis and Design**, 5. Edition (USA: Thomson Learning, 2002), 16

Yukarıdaki şekilden de anlaşılacağı üzere, bilgi sistemleri donanım, yazılım ve insan faktörleri temelinde veri giriş, veri işleme ve çıktı süreçlerinden oluşmaktadır[3].

2.1.1. Veri Giriş Süreci

Veri girişi süreci, işlemlerin kayıt altına alınması ile birlikle başlangıç aşamasını temsil etmekte ve bilgi sistemi sürecinin en önemli kısmını oluşturmaktadır. Zira sisteme başından yanlış olarak girilen bir verinin doğru bir sonucu vermesi de imkansız hale gelmektedir.

Günümüz teknolojisinde bir sistemin çıktısının başka bir sistemin girdisi haline geldiği bütünleşik sistemlerden oluşmaktadır. Örneğin ana bankacılık sisteminde oluşturulan toplu EFT ("Elektronik Fon Transferi") işlemlerinin çıktı olduğu gibi aynı zamanda girdi olarak TCMB ("Türkiye Cumhuriyeti Merkez Bankası") EFT sistemine işlemlerin gerçekleşmesi için iletilmesinden bahsedilebilmektedir.

Verilerin sisteme girişi temel olarak üç aşamada ele alınabilmektedir:

1. Kaynak belgelerin içeriğinin incelenerek bilgi işlem süreci için gerekli olan bilgi türleri belirlenmektedir.
2. Verilerin sisteme girişinin yapılmasına uygun hale getirilmesi veya düzenlenmesidir.
3. Verilerin sisteme doğru bir şekilde aktarıldığından emin olmak için giriş işlemleri kontrol edilmesidir.

Verilerin kaynağından bilgi sistemlerine ya da uygulamaya ait programlara aktarılmasındaki temel amaç değişmese de günümüzde veri girişi ile ilgili olarak birçok yöntem ve araç geliştirilmiştir. Başlıca veri giriş tekniklerden aşağıda örnekler verilerek bahsedilmiştir[4]:

1. Bar Kod Sistemi: Bilginin makineler tarafından okunabilir şekilde görsel olarak bir yüzey üzerinde sunulması, optik okuyucular ve özel veri tanıma programları aracılığıyla bu verilerin otomatik olarak bilgisayara aktarılmasını sağlayan sistemlerdir.
2. Elektronik Veri Değişimi: Genel olarak bir sistemdeki bilginin diğer bir sisteme entegre olması sağlanmaktadır. Daha geniş bir tanımla, organizasyonlar arası bilgi paylaşma ve değişim yeteneğine sahip olan bir iletişim paketi kullanılarak, bir bilgisayar ve diğeri

[3] Erdoğan, **age**, 133
[4] Tamer Saka, **Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi**, Yayın:224 (İstanbul: Türkiye Bankalar Birliği, 2001), 8

arasında elektronik olarak bilgi değişiminin yapıldığı bir sistemdir. Bu noktada bankalar ile TCMB arasındaki EFT uygulamaları güzel bir örnek teşkil etmektedir.

3. Terminaller: Ana bilgisayar sistemine bağlı olarak çalışan, üstünde veri ve uygulama bulundurmayıp kullanıcının genellikle sisteme sadece veri giriş amacıyla ve ana bilgisayar sisteminden çıktı olarak gönderilen bilgileri görüntülemek amacıyla kullanılan bilgisayarlardır.
4. Görüntü Tarama ve İşleme Birimleri: Kağıt üzerindeki görüntülerin belirli formatta optik okuyucular vasıtasıyla taranması ve bilgisayara girdi olarak aktarılmasıdır. Bankalarda, kredi kartı başvuru formlarının optik okuyucular ile okunarak sisteme aktarılması bu veri girişi tekniğine güzel bir örnek oluşturmaktadır.
5. Ses Tanıma Sistemleri: Konuşmaların otomatik olarak bilgisayar sistemine girdi olarak aktarılması tekniğidir. Günümüzde gelişme aşamasında olan bir tekniktir. Özellikle bankaların dağıtım kanallarından biri olan telefon bankacılığında gelişim göstermektedir.

Yukarıda da görüldüğü gibi veri girişleri ile ilgili olarak birçok farklı ortam, süreç ve kontrol söz konusudur. Özellikle kontrol açısından bakıldığında, verinin hangi kaynaktan girdiğinin, en az verinin sisteme nasıl girdiğinin bilinmesi kadar önemli olduğu unutulmamalıdır. Bilgi sistemindeki tüm süreçlere yönelik işlemler girilen bilgiler esas alınarak işleneceğinden, verilerin eksiksiz, güncel olması, verilerin doğruluğu ve bütünlüğü büyük önem taşımaktadır.

Sonuç olarak bilgi sistemleri denetçisinin en yoğun biçimde önem vermesinin gerektiği alanlardan biri girdi kontrolleridir. Daha sonraki bölümlerde açıklanacak olsa da genel olarak girdi kontrolleri; kaynak belge kontrolleri, veri kodlama kontrolleri, yığın işlem kontrolleri, girdi geçerlilik kontrolleri ve yetki kontrolleri gibi bölümlerde sınıflandırılabilmektedir.

2.1.2. Veri İşleme Süreci

Veri işleme süreci, veri girişinin tamamlanmasından sonra istenen formatta çıktı elde edilmesi amacıyla bilgisayar tarafından gerçekleştirilen tüm faaliyetleri kapsamaktadır. Gerçekleştirilen bu faaliyetleri, düzenleme, hesaplama, özetleme, sınıflandırma, güncelleştirme ve kaydetme olarak sınıflara bölebiliriz. Sırasıyla bu faaliyetleri açıklamak gerekirse[5];

[5] Saka, **age**, 10

1. Düzenleme: Girilen verinin geçerliliğinin, doğruluğunun ve istenen formatta uygunluğunun kontrolü amacıyla sisteme girişi yapılan verilerin önceden tanımlı kriterlere uygunluğunun kontrol edilme işlemidir. Örneğin sisteme toplu olarak aktarılan verinin uygun veri formatında ve deseninde sisteme iletildiğinin kontrol edilmesidir.
2. Hesaplama: Bilgi sistemlerinin veri işleme süreci içinde temel olarak gerçekleştirdiği faaliyettir. Veri girişi yapılan bilgiler üzerinde aritmetik hesaplamaların yapılarak istene sonuca ulaşılması faaliyeti olarak tanımlanabilir. Örneğin vadeli hesap açılışı bilgilerinden ana bankacılık sistemi üzerindeki programlar vasıtasıyla birikmiş faiz tutarının hesaplanmasıdır.
3. Özetleme: Genel olarak tanımlamak gerekirse, düzenleme ve hesaplama faaliyetlerinden sonra verinin istemem biçimde özetlenmesi ve toplamların alınmasıdır. Örneğin, müşteri bazında hesaplanan birikmiş faiz tutarlarından, aylık olarak bankanın faiz borcu rakamına ulaşması için alınan genel toplamlardır.
4. Sınıflandırma: Çeşitli dosyalarda hesaplanmış verilerin istenen çıktı formatında sınıflandırılması faaliyetidir. Yukarıdaki örneklerin devamı olarak birikmiş faiz borcunun şubeler bazında ara toplamlarının alınması ve sınıflandırılması örnek olarak verilebilir.
5. Güncelleştirme: Sistem içinde mevcut olan bilgiler üzerinde yapılan ekleme, değiştirme veya silme faaliyetleriyle söz konusu bilgilerin içeriklerinde veya biçimlerinde gerçekleştirilen düzenleme faaliyetlerini ifade etmektedir. Örneğin, vadesi dolan vadeli hesap bilgilerinin ana bankacılık sistem üzerinde otomatik olarak güncellenerek ilgili hesabın kapatılması veya temdit edilmesidir.
6. Kaydetme: Herhangi bir işlemin gerçekleştirilmesinden sonra nihai sonucun elde edilmesine kadar sistem üzerinde kayıt altına alınması işlemidir. Bilgi sistemlerinin işlemleri gerçekleştirirken temel olarak tümünde gerçekleştirdiği faaliyetlerden biridir.

En az veri girişi süreci kadar, verinin doğru olarak işlenmesi de doğru ve geçerli bilgiye ulaşmak için önemlidir. Bilgi sistemleri denetçisi veri girişi kontrollerini incelediği gibi verinin doğruluğu, güvenliği ve bütünlüğü açısından aynı şekilde veri işleme sürecine yönelik kontrolleri de incelemek zorundadır. Daha sonraki bölümlerde açıklanacak olsa da genel olarak veri işleme kontrolleri; geçiş kontrolleri, işletmen kontrolleri ve denetim izi kontrolleri gibi genel sınıflara ayrılabilmektedir.

2.1.3. Veri Çıkış Süreci

Bilgi sistemi süreçlerinin son aşamasını olan veri çıkış süreciyle girilen verilerin işlenmesi sonucunda çıkan bilgiler çıktı olarak adlandırılmaktadır. Çıktılar;

- Güncellenmiş veri dosyaları
- Bilgisayar ekranındaki görüntüler
- Basılı halde olan rapor veya dokümanlar olabilmektedirler.

Çıktılar temel olarak bilgi sisteminin amacına uygun olarak işletmenin faaliyetlerini yürütmesi ve bu faaliyetleri analiz etmesi için gerekli bilgileri içeren ürünlerdir.

Çıktılar bilgi sistemlerinde kullanılan çıkış birimleri vasıtasıyla kullanılabilir hale getirilmektedir. Genel olarak bilgisayar ekranları, yazıcılar, çiziciler, ses çıktı birimleri, taşınabilir bellek ve diskler gibi kayıt ortamları çıktı birimi olarak sayılabilir[6].

Bilgi sistemleri denetçisi olarak, çıktıların amaca uygun olarak dağıtılması, çıktı verilerinin kullanılabilirliği ve çıktılar üzerinde güvenlik sağlayıcı yöntemlerin incelenmesi temel olarak önem verilmesi gereken başlıklardır. Bu aşamada genel olarak denetçi, bilgi sistemini tanıyabilmek için öncelikle girdilerin kaynağını, yapısını ve hangi çıktıların hangi süreçler sonunda elde edildiğini en iyi şekilde anlamak zorundadır.

Her şeyden önce anlaşılmadır ki, çıktıların doğruluğu ve güvenilirliği yüksek oranda veri girişi ve veri işleme süreçlerindeki kontrollerin etkinliğine bağlıdır. Ancak kesin doğruluğu ve güvenilirliği sağlamak amacıyla çıktıların bilgisayardan alınma aşamasında da kontroller oluşturmak gerekmektedir. Çıktıların kontrolü açısından üzerinde durulması gereken üç temel nokta çıktıların doğrulanması, çıktıların dağıtımı ve özel bilgilerin veya raporların yönetimidir.

2.2. Bilgi Teknolojileri Yönetimi

Bilgi sistemleri yönetimi, organizasyon içindeki bilgi sistemlerinin organizasyonun hedef ve amaçlarına destek olacak şekilde idare edilmesini ve bununla birlikte organizasyona amaçları doğrultusunda değer katmaya yönlendirilmesini ifade etmektedir. Bilgi sistemlerinin yönetimine yönelik faaliyetler genel olarak dört alana ayrılarak açıklanabilmektedir[7]:

---

[6] Saka, **age**, s. 11
[7] Everett C. Johnson, Robert D. Johnson, **CISA Review Manual 2007** (USA: ISACA, 2007), 1-2

1. Sistem ve Alt Yapı Yönetimi
2. Bilgi Sistemleri Servis Sunumu ve Destek
3. Bilgi Varlıklarının Korunması
4. İş Sürekliliği ve Felaketten Kurtarma Süreci

2.2.1. Sistem ve Alt Yapı Yönetimi

Organizasyon içindeki bilgi sistemlerinin iyi bir şekilde yönetilmesi için sistem ve uygulamaların geliştirilmesi, edinilmesi veya yenileme projelerinin yürütülmesi gibi süreçlerin kontrol altında tutularak iyi yönetilmesi gerekmektedir.

Öncelikle bilgi sistemleri yönetiminin bir parçası olarak program ve proje yönetimi anlayışının bilgi teknolojileri yönetimi içinde oluşturulması gerekmektedir. Bu noktada program ve proje kavramlarını birbirinden ayırarak tanımlamak gerekmektedir. Program, bir grup birbirine bağlı ve ilişkili olan projeden oluşan, genel amaçları ve bütçesi olan, bununla birlikte belirli bir zamanlamaya bağlı olarak genel bir stratejiye bağlı olarak sistem ve alt yapı yönetimi için oluşturulmuş bir plandır. Diğer taraftan, proje ise bir proje yöneticisine bağlı olarak bir alt amacı gerçekleştirmek için yönetilen sistem geliştirme veya alt yapı planının bir parçasıdır[8].

Genel olarak bilgi sistemlerinin yönetiminde yukarıdaki faaliyetlerin takibi ve belirlenen kalite kriterleri doğrultusunda proje ve programların yönetilmesi için proje yönetimi ofisleri kurulmaktadır. Kuruluşundaki esas amaç proje ve program yönetimindeki kalitenin iyileştirilmesi ve projelerin önceden belirlenen aktiviteler kapsamında başarılı olarak tamamlanmasını sağlamaktadır.

Proje yönetiminde temel olarak üç ana organizasyon yapısı kullanılmaktadır[9]:

1. Etkileme Yollu Proje Organizasyonu: Bu organizasyonda proje yöneticisi proje ekibi içinde yer alıp mutlak otoriteye sahip olmak yerine proje ekibine aktiviteleri hakkında yol gösterici tavsiyeler bulunarak projeyi yönetmektedir.
2. Temel Proje Yönetimi Organizasyonu: Genelde uygulanan bu tip proje organizasyonunda proje yöneticisi tüm proje aktivitelerinde sorumlu olup tüm ekip üzerinde mutlak otoriteye sahiptir.

[8] Johnson, **age**, 125
[9] **age**, 128

3. Matris Proje Organizasyonu: Bu tip proje yönetimi organizasyonunda ise otorite proje yöneticisi ile çalışanın bağlı olduğu bölüm müdürünün arasında paylaşılmaktadır.

Proje organizasyonu türlerine ek olarak proje yönetiminin temel aşamalarından da bahsedilmesi gerekmektedir[10]:

1. Proje Başlangıcı: Proje yöneticisinin veya sponsorunun gerekli bilgiyi toplamasından sonra iş sahiplerinin proje başlatılmasına dair onayından sonra başlatılmalıdır. Genellikle proje talep dokümanının onaylanması ile projeye başlanmaktadır.

2. Proje Planlaması: Talep edilen sistem geliştirmesi, iyileştirmesi veya alt yapı projesini gerçekleştirmek için gerekli proje adımlarının öncelikle proje yöneticisi tarafından ekip ile birlikte görüşerek belirlemesi gerekmektedir. Sonrasında bu proje adımlarının önceliğinin belirlenmesi, zamanlama planlaması, her birinin bütçe ve maliyet analizinin yapılması, sağlanması gereken bilgi teknolojileri kaynakları vb. gibi konularda proje yöneticisi tarafında planlama yapılması ve dokümante edilmelidir. Bu aşamada proje yöneticisine proje planı yapmasında ve proje aşamalarının ilerleyişini izlemede çeşitli teknikler yardımcı olabilmektedir. GANNT şeması, fonksiyonel nokta analizi, kritik yol metodolojisi, yazılım maliyeti ve bütçe analizi gibi teknikler kullanılabilmektedir[11].

3. Projenin Kontrol Edilmesi: Projenin kontrol edilmesinde, belirlenen kapsamda ilerlenip ilerlenmediği, kaynak kullanımının öngörülen miktarda olup olmadığı ve projenin risk değerlendirmesinin yapılması adımlarını kapsamaktadır.

4. Projenin Kapatılması: Son adım olarak gerekli testlerden sonra proje sponsorunun ve ilgili iş sahiplerinin projeden memnun olması durumunda proje teslim edilerek kapatılmaktadır. Tabi diğer yandan projenin yanlış planlamasından ve yönetilmesinden ötürü proje maliyetlerinin artması ve istenen amaca ulaşılamayacağının anlaşılması durumunda da başarısız olarak ilgili proje durdurulup kapatılabilmektedir.

Şimdiye kadar yukarıda anlatılan kısımda proje ve programların yönetilmesini ve proje organizasyonlarının detaylarını vermiş bulunmaktayız. Tüm alt yapı / sistem geliştirme ve iyileştirme çalışmaları bir proje kapsamında ele alınarak organizasyonun amaçları doğrultusunda

[10] Shankar Swaroop, "Managing Multiple Medium and Small Scale Projects in Large IT Organization", **Information Systems Control Journal**, volume 4 (2007), 24
[11] Ian Sommerville, **Software Engineering**, 6. Edition (England: Pearson Educated Limited, 2001), 82

yönetilmelidir. Bunun yanında yazılım geliştirme veya iyileştirme (değişiklik yönetimi) sürecinin ek olarak belirli aşamalar vasıtasıyla yönetilmesi gerekmekte ve bu aşamalara bağlı olarak proje yönetimi sağlanmalıdır.

Bilgisayar uygulama sistemlerinin geliştirilmesi ve/veya iyileştirilmesi birçok faaliyeti kapsamakta olup belirli ve yazılı olan standartlara göre yönetilmelidir. Bu standartlardan en çok kullananı ve genel olanı ise şelale yönetimidir. Bu standarda göre bir yazılım geliştirme süreci minimum olarak aşağıdaki fazları sırasıyla tanımlamalı ve yönetmelidir[12]:

1. Uygulanabilirlik Tespiti: Bu faz içinde yeni uygulamanın stratejik avantajları, sağladığı faydaları ve katlanılan maliyetleri geri ödeme zamanı analiz edilir. Sağladığı faydalar, gelecek yıllardaki maliyet azalması, üretimdeki artış imkanları gibi somut faydalar olabileceği gibi, iş süreçlerinin geliştirilmesi, kullanıcıların hazır olmaları gibi soyut faydalar da göz önünde bulundurularak genel olarak projenin uygulanabilirliği analiz edilmektedir.

2. Gereksinimlerin Belirlenmesi: Yeni bilgi sistemi geliştirme veya iyileştirme çalışmasının uygulanabilirliği onaylandıktan sonra iş gereksinimlerinin detaylı olarak belirlenmesi bu fazda yapılmaktadır. Ayrıntılı olarak iş ihtiyaçlarının tespiti projeyi bu aşamada üçüncü taraftan yeni uygulama alıp kullanmaya, alınan uygulamanın ihtiyaca uygun olarak uyarlanmasına veya sıfırdan bir uygulama geliştirmeye götürebilmektedir.

3. Tasarımın Belirlenmesi: İş gereksinimleri belirlendikten sonra bu gereksinimlere uygun olarak geliştirilecek uygulamanın teknik gereksinimleri ve tasarımı oluşturulur. Uygulamanın sistem ve alt sistemler olarak tanımlamaları, önyüzleri, üzerinde çalışacağı donanımlar, programların tasarımı, veritabanı tanımlamaları ve güvenlik ihtiyaçları gibi yazılım geliştirme aşamasını besleyecek tüm detaylar bu aşamada belirlenmektedir.

4. Yöntem Tespiti (Geliştirme veya Satın Alma): Bu safha içinde seçilen yöntem sıfırdan yazılım geliştirme ise, yazılım teknik tasarım detaylarına göre proje ekibi tarafından geliştirilir ve yine proje ekibi içindeki test işlemlerinden görevli kişiler tarafından birim ve sistem testleri gerçekleştirilir. Diğer taraftan seçilen yöntem satın alınan bir uygulamanın uyarlanması ise satın alınan uygulama iş ihtiyaçlarına ve teknik tasarım dokümanına göre üçüncü taraf firma tarafından uyarlanmakta ve test edilmektedir.

[12] Johnson, **age**, 140

5. Yazılımın Test Edilmesi ve Uygulanması: Bu aşamada yazılımın geliştirmesi veya uyarlaması tamamlanmış olup teknik taraftaki testler de gerçekleştirilmiştir. Son kullanıcı testleri ve iş tarafının onayı alındıktan sonra uygulamanın test ortamından üretim ortamına geçişi bu safha içinde tamamlanmaktadır.

6. Sonradan Gözden Geçirme: Uygulamanın üretim ortamına geçişinden ve organizasyon içinde kullanılmaya başlanmasından itibaren geçen ve genelde üç ay olarak belirlenen izleme evresidir. Uygulamanın üzerinde olası hataların tespit edilip düzeltilmesi ve olası iyileştirme ihtiyaçlarının tespiti için gerçekleştirilen izleme evresidir.

Bu aşamalardan en kritik olanı yeni bir uygulama ya da fonksiyon gereksinimi için alımdan ya da geliştirmeden önce iş ihtiyaçlarının etkin ve verimli bir yaklaşımla karşılandığı bir analiz gerçekleştirilmesidir. Süreç ihtiyaçların tanımlanmasını, alternatif kaynakların göz önüne alınmasını, teknolojik ve ekonomik yapılabilirliklerin gözden geçirilmesini, risk analizi ve maliyet-kazanç analizinin uygulanmasını ve 'geliştirme' ya da 'alma' son kararının neticesini içermektedir. Bütün bu adımlar, organizasyonların hedeflerini başarmaya yönelik ortamı sağlarken çözüm alma ve uygulama maliyetini düşürmesini sağlamaktadır. Yukarıdaki açıklanan şelale metodolojisinde ilk iki faz bu işlevi yerine getirmektedir.

2.2.2. Bilgi Teknolojileri Servis Sunumu ve Destek

Bilgi sistemleri operasyonun günlük olarak yönetimi ve bilgi sistemleri kapsamında organizasyonun ihtiyaçlarına göre desteklenmesi bilgi sistemleri yönetiminin servis sunumu ve destek başlıklı bölümünü oluşturmaktadır. Bilgi sistemleri operasyonunun yönetimi ve servis sunumu ile ilgili olarak gerçekleştirilen başlıca faaliyetler şu şekilde açıklanabilmektedir[13]:

1. Bilgi Teknolojileri Servis Yönetimi: Dış tedarikçiler tarafından sağlanan servislerin iş taleplerine uygun olduğundan emin olabilmek için dış tedarikçi yönetim sürecine gereksinim bulunmaktadır. Bu süreç, dış tedarikçi anlaşmalarında rol, sorumluluk ve beklentilerin açıkça tanımlanmış olması gerektiği kadar anlaşmaların yararlılığının ve uygunluğunun gözden geçirilmesi ve izlenmesiyle de başarılmaktadır. Örneğin bankaların ATM ("Automatic Teller Machine") alımı yaptığı firmalar ile ilişkileri ihtiyaca uygun olarak belirlemesi ve takibini yapması bu kapsama girmektedir. Bunun yanında organizasyon içindeki iç müşterilere sunulan hizmetlerin tanımlanması, her servisin belirli

[13] Johnson, **age**, 256

servis seviyesi anlaşmasına bağlanması, takibinin yapılması ve raporlamasının yapılması ikinci bu faaliyetlerin diğer kısmını oluşturmaktadır. Bu alanda da örnek vermek gerekirse bilgi teknolojileri bölümünün banka içindeki bölümlere ve/veya holding içindeki diğer iştiraklere sağladığı servisleri tanımlı olan servis seviyesi anlaşmalarına göre yönetmesidir.

2. Alt Yapısal Bilgi Sistemleri Operasyonları: Genel olarak bilgi sistemleri için önceden tanımlı olan ve belirli bir zamanda çalışması gereken işlerin tam, etkin ve zamanında çalışmasını sağlanmasıdır. İlgili işlerin çalıştırılması, olası hatalara karşı bu işlerin takibinin yapılması, oluşabilecek sistem durmalarına karşı sistemin tekrar ayağa kaldırılması, sistem yedeklerinin zamanında ve belirlenen sıklıkta alınması ve sistem kaynaklarının verimli kullanılmasının, performansın, kapasitenin ve erişilebilirliğin izlenmesi gibi bilgi sistemleri operasyonları gerçekleştirilmektedir. Genel olarak organizasyon içindeki mevcut bilgi sisteminin çalışır durumda tutulması ve organizasyon içindeki desteğinin kesintiye uğramaması için bu kapsamda hizmet sunumu gerçekleştirilmektedir.

3. Vaka ve Problem Yönetimi: Bu faaliyet kapsamını açıklamadan önce vaka ve problem kavramlarını tanımlamak gerekmektedir. Vaka, bilgi sistemleri üzerinde meydana gelen ve olağan olmayan her türlü durum tespitidir. Örneğin banka şubesinin ağ üzerideki bağlantısının kısa süreli olarak kesilmesi veya sistemdeki boş kapasitenin eşik değerinin üzerine çıkması gibi. Problem ise tespit edilen vakaların kendini tekrar etmesi ile kendini açıkça belli eden ve ilerleyen safhalarda kronik duruma gelen olağan dışı durumlardır. Aynı örneğimize devam edecek olursak, belirli bir şubenin ağ bağlantısı her gün kopuyorsa mevcut kronik bir problemin tespiti yapılmalıdır. Bu kapsamda öncelikle mevcut bilgi sistemlerin olası vakalara karşı izlenmesi ve bu sürecin de yine etkin bir problem ve değişiklik yönetimi ile desteklenmesi gerekmektedir. Etkin problem yönetimi problemlerin belirlenerek sınıflandırılmasını, sebep-sonuç analizini ve problemlerin çözümünü gerektirir. Problem yönetim süreci aynı zamanda iyileştirme çalışmaları için gelen önerilerin kaydedilmesi, problem kayıtlarının saklanması ve kayıt üzerine yapılan düzeltici hareketlerin statülerinin gözden geçirilmesini içerir. Etkin problem yönetim

süreci bilgi sistemlerinin hizmet kalitesini artırır, maliyetleri azaltır ve kullanıcıların memnuniyetini artırır[14].

4. Değişiklik Yönetimi: Son kullanıcılardan gelen taleplere veya tespit edilen bir probleme göre mevcut sistemlerde bazı yazılımsal veya donanımsal değişikliklere gidilebilmektedir. Mevcut sistemler üzerinde gerçekleştirilen yazılım veya alt yapı değişiklikleri de belirli bir yönteme uygun olarak tasarlanmış değişiklik yönetimine bağlı olarak gerçekleştirilmelidir. Üretim ortamı içinde altyapı ve uygulamalarla ilgili tüm değişiklikler, acil bakım ve yamalar da dahil olmak üzere, resmi olarak kontrollü bir şekilde yönetilmelidir. Değişiklikler (prosedürler, prosesler, sistem ve hizmet parametreleri dahil olmak üzere) uygulamadan önce kayıt altına alınmalı, değerlendirilmeli, yetkilendirilmeli ve uygulamayı müteakip planlanmış sonuçlara göre incelenmelidir. Bu kapsamda gerçekleştirilen hizmetler ise değişiklik yönetimi faaliyetleri adı altında yer almaktadır.

5. Kütüphane Yönetimi ve Kalite Kontrol: Bilgi sistemlerinin kaynak kodlarının bütünlüğünün ve güvenliğinin sağlanması açısından aktarımın, saklamasının ve güncellenmesinin yönetilmesidir. Genel olarak kütüphane yönetim uygulamaları yardımıyla test ve üretim ortamı kütüphaneleri ayrılarak kaynak kodların güvenliği sağlanmakta ve yetkili onaylardan sonra kütüphanelerdeki kaynak kodlar güncellenmektedir. Bunun dışında sistem üzerindeki değişikliklerin onaylanması, test edilmesi ve kontrollü bir şekilde üretim ortamında uygulaması gibi konularda kalite kontrolün yapılması ve gözlenmesi de hizmet sunumu faaliyetleri kapsamında gerçekleştirilmektedir.

2.2.3. Bilgi Varlıklarının Korunması

Bilgi varlıklarının korunması bilgi sistemleri yönetimin en kapsamlı ve en önemli faaliyetlerinden biridir. Varlıklara sistem odalarındaki fiziksel erişimlerimden başlayarak son kullanıcının bilgi güvenliği konusunda bilinçlendirilmesi ve mantıksal erişim kontrollerine kadar çok geniş bir kapsamı içine almaktadır. Genel olarak sekiz faaliyet alanına bölünerek bilgi varlıklarının korunması kapsamında bilgi teknolojileri bölümünün gerçekleştirdiği görevler aşağıda açıklanmaktadır.

[14] ISACA**, IT Assurance Guide** (USA: 2007), 205

1. Bilgi Güvenliği Yönetimi: Bilgi bütünlüğünün sağlanılması ve bilgi teknolojileri varlıklarının korunması için öncelikle bir güvenlik yönetim süreci bulundurulmaktadır. Bu süreç, bilgi teknolojileri güvenlik rollerinin oluşturulması ve rollerin düzenli gözden geçirilmesi ve bakımını içermektedir. Ayrıca ilgili politikaların, standartların ve prosedürlerin oluşturulması gerekmektedir. Güvenlik yönetimi bunların dışında, güvenlik izlemesini, periyodik güvenlik testlerinin yapılmasını ve belirlenmiş güvenlik açıklarının kapatılması uygulamalarını da kapsamaktadır. Etkin olarak işleyen bir bilgi teknolojileri güvenlik yönetimi güvenlik açıklarından doğabilecek olumsuz etkileri en düşük seviyede tutmalı ve bilgi varlıklarını etkin bir şekilde korumalıdır[15].

2. Bilgi Teknolojileri Güvenlik Planı: Bilgi teknolojileri güvenliğinin en yüksek organizasyon seviyesinde yönetilmesi gerekmekte birlikte, organizasyon içinde yürürlükte bulunan bir bilgi teknolojileri güvenlik planı oluşturulur. Bu plan kurumsal bilgi işlem kullanımı, bilgi teknolojileri yapılanışı, bilgi risk ve hareket planları ile bilgi güvenlik kültürünü içermektedir. Bilgi teknolojileri güvenlik planı, organizasyonun güvenlik politika ve prosedürlerinde uygulanır; şirket hizmet, personel, yazılım ve donanıma gerekli yatırımı yaparken bu plan göz önüne alınır.

3. Kimlik Yönetimi: Bilgi teknolojileri güvenlik planı ve prosedürlerinin yanı sıra, bilgi sistemleri üzerinde tüm kullanıcıların aktiviteleri (iş uygulamaları, sistem operasyon, geliştirme ve bakım) tek başlarına tanımlanabilir hale getirilir. Kullanıcıların sistemlere ve veriye erişim hakları; tanımlanmış ve dokümante edilmiş iş ihtiyaçları ve görev gereksinimleri ile uyumlu olarak tasarlanmaktadır. Kullanıcı erişim hakları; kullanıcının yöneticisi tarafından talep edilmeli ve sistem sahibi tarafından onaylanmalıdır[16].

4. Kullanıcı Hesaplarının Yönetimi: Kullanıcı hesaplarının ve ilgili kullanıcı haklarının talep edilmesi, oluşturulması, kullanıcılara atanması, askıya alınması ve kapatılması işlemlerinin ne şekilde gerçekleştirileceği kullanıcı hesapları yönetimi sürecinde belirlenmiştir. Veri veya sistem sahiplerinin onayıyla talep edilen erişim haklarının kullanıcılara verilmesi süreci kullanıcı hesapları yönetimi dâhilindedir. Kurumsal sistemler ve bilgi kaynaklarına erişim ile ilgili haklar ve yükümlülükler her tip kullanıcı

[15] ISACA, **COBIT: Control Objectives for Information and related Technology 4.1** (USA, 2007), 118
[16] ISACA, **COBIT**, 118

için sözleşmeye dayalı olarak düzenlenir. Ek olarak tüm hesaplar ve ilgili erişim hakları düzenli olarak yönetim tarafından gözden geçirilir.

5. Güvenlik Testleri: BT güvenlik uygulamaları test edilmeli ve aktif olarak gözlemlenmelidir. BT güvenliğinin; onaylanmış güvenlik seviyesinin sürdürülmesini sağlamak için düzenli aralıklarla kalitesi arttırılır. Arşivleme ve fonksiyon gözlemlenmesi; tespit edilmeye gerek duyabilecek seyrek veya olağandışı aktiviteleri erken tanısını bu faaliyetler yardımıyla mümkün kılınmaktadır. Arşiv verisine erişim; erişim hakları ve alıkoyma gereksinimleri açısından, iş gereksinimleri ile uyumlu olmalıdır.
6. Güvenlik Vakalarının Yönetimi: Potansiyel güvenlik vakalarının karakteristikleri açık şekilde tanımlanır ve bildirilir; bu şekilde güvenlik vakaları, vaka ve problem yönetimi süreci vasıtasıyla uygun şekilde düzeltilir. Karakteristikler, neyin güvenlik vakası olarak tanımlanacağını ve etki seviyesini içerir. Kısıtlı sayıdaki etki seviyeleri açıklanır ve ihtiyaç duyulan her belirli aksiyon ve bildirime ihtiyaç duyulan kişiler için tanımlanır.
7. Zararlı Yazılımların Önlenmesi: Organizasyon bünyesinde bilgi teknolojileri sistemlerini, virüs, solucan, casus yazılım ve iç veya dış kullanıcılar tarafından geliştirilmiş diğer zararlı yazılımlardan koruyacak, önleyici, tespit edici ve düzeltici sistemlerin mevcut olması sağlanmaktadır.
8. Ağ Güvenliği: Güvenlik tekniklerinin ve ilgili yönetim prosedürlerinin (örneğin firewall, güvenlik cihazları, ağların bölümlenmesi ve istenmeyen girişlerin tespiti) girişleri onaylamak ve ağ içinde akan bilginin kontrol edilmesi için kullanılması sağlanmaktadır[17].

Yukarıdaki faaliyet alanlarından da anlaşılacağı gibi bilgi güvenliği ve varlıkların korunması ayrı alanlarda ancak aynı amaca paralel olarak sürdürülmesi geren bir bilgi sistemleri yönetim faaliyetlerinden birisidir.

2.2.4. İş Sürekliliği ve Felaketten Kurtarma Süreci

Organizasyon için iş sürekliliğinin sağlanması diğer bir deyişle faaliyetlerinin sürdürebilmesi, belirlediği hedeflerin gerçekleştirilebilmesi için hayati önem taşımaktadır. Günümüz teknolojisinde mevcut operasyonel faaliyetlerin bilgi teknolojileri servislerine oldukça bağımlı

[17] ISACA, **COBIT**, 118

olduğu düşünülürse bilgi teknoloji servislerinin devamlılığını sağlamak da hayati önem taşımaktadır. Örneğin ana bankacılık sistemi çalışmayan bir bankanın tüm şubelerindeki müşteriye sunulan hizmetlerinde aksama olacak hatta mevduat bankalarının temel işlevi olan mevduat toplama ve kredi verme işlemleri duraksayacaktır.

Bu sebepledir ki, bilgi teknolojileri ("BT") hizmetlerinin sürekliliğini sağlamak amacıyla BT süreklilik planı geliştirilmeli ve bu plan belli aralıklarla gözden geçirilmelidir. Ayrıca bu plan test edilmeli ve ilgili kişilere süreklilik planı ile ilgili eğitimler verilmelidir[18].

Ek olarak alınan sistem ve veri yedekleri ofis dışında saklanmalıdır. Etkin olarak işleyen sürekli hizmet süreci, temel iş fonksiyonları ve süreçleri üzerindeki BT hizmetinin kesilmesinden doğan negatif etkiyi azaltmaktadır.

İşletmenin yönetim desteğinin devamlılığının için tutarlı bir süreçle bilgi sistemleri sürekliliği için yapı geliştirilmelidir. Yapının amacı; karar verilmiş altyapı gereksinimlerine yardımcı olmak, felaket kurtarma ve bilgi sistemleri olasılık planlarını yürütmektir. Yapı; yönetim devamlılığı için organizasyon yapısını, rolleri, görevleri ve iç ve dış tedarikçileri, onların yönetimini ve müşterilerini, kuralları, doküman hazırlanışı, felaket kurtarma ve bilgi sistemleri olasılık planlarının test edilip uygulanmasını da kapsamalıdır. Bu plan aynı zamanda kritik kaynakların tanımı, erişilebilir kritik kaynakların izlenmesi ve raporlanması, alternatif süreçler, kurtarma ve yedekleme kuralları gibi konular hakkında bilgi vermelidir[19].

Bilgi sistemleri devamlılık planları geliştirilirken anahtar iş fonksiyonlarındaki ana bozulmaların etkisini azaltacak şekilde tasarlanmalıdır. Esneklikle oluşturulmuş bilgi sistemleri devamlılık planında en kritik olarak belirtilen konulara dikkat edilmelidir ve felaket durumlarında öncelikler belirlenmelidir. Planlar; esneklik, alternatif işleyiş, tüm kritik bilgi sistemleri hizmetleri için kurtarma kapasitesi için gereksinimleri kapsamalıdır[20]. Ayrıca, kullanım kılavuzları, görevler ve sorumluluklar, prosedürler, iletişim süreçleri ve test yaklaşımı hakkında bilgi de içermelidir.

Bilgi sistemleri devamlılık planı içinde masraflar kabul edilebilir bir seviyede tutulurken, sözleşmeler ile yasal gereksinimlere uyulurken; daha az kritik olan noktaların kurtarılmasından kaynaklanan dikkat dağınıklığından kaçınılmalı, tepkilerin ve kurtarmanın öncelikli iş

[18] TUBİTAK UEKAE, **Yedekleme ve İş Sürekliliği Kontrol Listesi**, 1
[19] ISACA, **COBIT**, 114
[20] Edward S. Devlin, Cole H. Emerson ve diğerleri, "**Business Resumption Planning**" (USA: AUERBACH, 2000), II-2

gereksinimleriyle aynı doğrultuda olması sağlanmalıdır. Dört saatte bir, 24 saatte dört kez, 24 saatten daha fazla ve kritik işlerin operasyon süreleri gibi farklı diziler için esneklik, tepki ve kurtarma gereksinimleri plan içinde hesaba katılmalıdır.

Bilgi sistemleri süreklilik planı oluşturduktan sonra işletmenin görevi sona ermemektedir. Plan her daim güncel tutulması için ve devamlı olarak gerçek iş gereksinimlerine yanıt verdiğinden emin olmak amacıyla, değişiklik kontrolü prosedürlerinin tanımlanması ve uygulanması gerekmektedir. Prosedürdeki değişikliklerin ve sorumlulukların açık bir şekilde ve zamanında tartışılması önemlidir. Bu noktada bilgi sistemleri süreklilik planının; bilgi sistemlerinin etkili olarak kurtarıldığından, noksanlıkların belirlendiği ve planın hala uygun olduğundan emin olmak amacıyla periyodik olarak test edilmelidir. Bu test; dikkatli hazırlığı, belgelemeyi, test sonuçların raporlanmasını ve sonuçlara göre eylem planı hazırlanmasını gerektirmektedir. Tek uygulamaların kurtarılmasının testinden, tüm test aşamalarını baştan sona kapsayan test senaryolarına ve tedarikçi testine kadar olan kapsam değerlendirilmelidir[21].

Bunun yanında ilgili tüm birimlerin; prosedürler, sahip oldukları roller ve kaza ya da felaket anında yerine getirecekleri sorumluluklar hakkında düzenli eğitim almaları temin edilmelidir. Planların uygun ve güvenli bir şekilde dağıtıldığından ve ihtiyaç duyulan yerde ve zamanda yetki verilmiş ilgili birimlerin uygun bir şekilde erişebildiğinden emin olmak adına tanımlanmış ve gözetilmiş bir dağıtım stratejisi bulunmalıdır. Tüm felaket senaryoları durumunda planların erişilebilir olmasına dikkat edilmelidir[22].

İş sürekliliğinin sağlanması ve BT kaynaklarının, bir ciddi sorun veya felaket durumunda tekrar çalışır hale gelmesi için, bütün kritik yedekleme üniteleri, ilgili dokümantasyon ve kritik BT kaynakları ofis dışında saklanmalıdır. Alınacak yedekler ve içerikleri iş süreç sahipleri ve BT personeli işbirliği ile kararlaştırılmalıdır. Ofis dışındaki yedekleme ünitesi, kurumun veri sınıflandırma politikasına ve genel veri depolama uygulamalarına uygun olmalıdır. BT Yönetimi ofis dışı düzenlemelerinin periyodik olarak, en azından yıllık olarak; içerik, genel güvelik ve fiziksel güvenlik açısından kontrol edildiğinden emin olmalıdır. Arşivlenmiş verinin geri döndürülebilmesi için kullanılan donanım ve yazılımın kurumun temel sistemlerine uyumluluğu kontrol edilmeli ve periyodik veri geri döndürme testleri yapılmalıdır.

[21] ISACA, **IT Continuity Planning Audit/Assurance Program**, www.isaca.org [01.03.2009], 33
[22] ISACA, **IT Continuity Planning Audit/Assurance Program**, www.isaca.org [01.03.2009], 35

Bilgi sistemleri yönetiminin; felaket sonrasında, bilgi sistemlerinin işlevini başarılı şekilde devam ettirilmesinde, planın yeterliliği ve düzenli olarak güncellendiğini değerlendirmek için prosedürler oluşturup oluşturmadığına karar verilmelidir.

Sonuç olarak yukarıda bahsettiğimiz faaliyetleri, bilgi teknolojileri birimi ile yönetim eş güdümlü olarak çalışması sonucu iş sürekliliği servisi sunulmaktadır. Bu noktada bilgi teknolojileri bölümünün görevi iş tarafından gelen iş sürekliliği ihtiyaçlarına göre bilgi sistemlerini ayağa kaldırmak ve devamlılığını sağlayabilmektedir.

2.3. Bilgi Teknolojileri Kontrollerinin Kapsamlarına Göre Sınıflandırılması

Bilgi sistemleri denetçisi organizasyonun bilgi sistemleri faaliyetlerini değerlendirirken, kapsamlarına göre inceleyeceği bağlıca iki tip kontrol alanı vardır. Bunlardan ilki bilgi teknolojileri genel kontrol ortamına yönelik genel kontroller, diğeri ise spesifik bir uygulamaya yönelik uygulama kontrolleridir.

Her iki kapsamda da denetçi önleyici veya belirleyici kontrolleri tespit edip değerlendirmesini yapacaktır. Önleyici kontrol isminden de anlaşılacağı gibi problem çıkmadan önce problemi önleyen kontrollerdir. Örneğin güvenlik önlemi olarak şifrelerin belirli sayıda hatalı giriş denemesinden sonra hesabın kilitlenmesidir. Diğer kontrol tipi ise belirleyici kontrol olup olası meydana gelen bir hatanın tespitini sağlamaktadır. Buna örnek olarak sistem üzerinde gerçekleşen veri aktarımlarına yönelik girdi ve çıktı alanları arasında otomatik mutabakat kontrollerinin yapılması verilebilir.

Kapsamlarına göre bilgi teknolojileri kontrolleri ikiye ayrılarak sonraki bölümlerde ayrıntılı olarak açıklanmaya çalışılacaktır.

2.3.1. Bilgi Teknolojileri Genel Kontrol Ortamı

İşletme içerisinde kullanılan tüm sistemlerde meydana gelebilecek hataları veya yoksulsuzlukları önlemeyi ve/veya belirlemeyi hedefleyen politikalara, prosedürlere veya uygulamalara bilgi teknolojileri genel kontrolleri adı verilmektedir. Genel kontrollerin amacı organizasyon genelinde mevcut bilgi sistemleri faaliyetleri üzerinde etkin bir kontrol sistemi tesis ederek iç kontrol ortamı ile ilgili belirlenmiş amaçlara ulaşılmasına yardımcı olmaktır. Genel olarak bağımsız finansal denetim kapsamından da bilindiği üzere iç kontrol ortamının etkinliği sonradan yapılacak olan maddi doğruluk testlerinin kapsamını ve harcanacak zamanı etkilemektedir. Benzer olarak

bilgi sistemleri genel kontrol ortamının etkinliği de uygulama kontrollerinin kapsamını ve güvenilirliğini de aynı şekilde etkilemektedir. Şekil ile daha açık anlatılması gerekirse[23];

Şekil 2: Zayıf BT Genel Kontrol Ortamı

*KPMG, **KPMG IT Audit Methodology Presentation**, www.kworld.com, [05.03.2009]*

BT genel kontrol ortamı zayıf olan bir ortamda uygulama kontrollerinin etkinliği de zayıf olacaktır. Bunun asıl sebebi tasarlanan uygulama kontrollerinin mevcut BT genel kontrol ortamının üstüne tesis edilmesidir.

Şekil 3: Güçlü BT Genel Kontrol Ortamı

*KPMG, **KPMG IT Audit Methodology Presentation**, www.kworld.com, [05.03.2009]*

[23] KPMG, **KPMG IT Audit Methodology (KAM)**, www.kworld.com [23.03.2009]

Bir önceki şeklin aksine BT genel kontrol ortamı sağlam olan bir organizasyon içinde uygulama kontrollerinin etkinliği ve güvenilirliği de aynı derecede artacaktır.

Genel kontrol ortamı kontrolleri sınıflandırarak anlatılmadan önce özet olarak organizasyon genelindeki bilgi sistemleri kontrol ortamının şekil yardımıyla açıklanması yerinde olacaktır[24].

Şekil 4: BT Kontrol Ortamları

Şekilden de anlaşılacağı gibi örgütsel BT kontrol ortamı üzerine BT genel kontrol ortamı onunda üzerine BT uygulama kontrolleri organizasyon içinde tesis edilmektedir. Aynı bir binanın temelinin sağlam olmasının gerekliliğine benzer bir şekilde bir alt bölüm üsttekinin etkinliğini ve güvenilirliği destek olmaktadır.

Literatür içinde bilgi teknolojileri çok çeşitli sınıflandırmalar yardımıyla anlatılabilmektedir. Örneğin çeşitlerine göre yönetsel ve sistem geliştirme kontrolleri olarak ikiye ayrılabileceği gibi kapsamlarına göre dört bölüme ayrılarak aşağıdaki gibi de anlatılabilmektedir. Kapsamlarına göre açıklamak, kontrollerin daha sağlıklı olarak ayrılmasını sağlayacağından bu sınıflandırma yöntemine göre kontroller aşağıda açıklanacaktır.

[24] KPMG, **KPMG IT Audit Methodology (KAM)**, www.kworld.com [23.03.2009]

1. Veriye ve Programlara Erişim: Bu kapsamda BT genel kontrol ortamı içinde bilgi sistemlerine ve veriye erişim kapsamında tesis edilen kontroller incelenmektedir. Uluslararası Muhasebeciler Federasyonu'nun Uluslararası Denetim Uygulamaları Komitesine göre yapılan sınıflandırmada yapısal ve faaliyetsel kontroller ile erişim kontrolleri kapsamına giren kontroller bu kapsamda incelenmektedir.

Genel başlıklar ile bu kapsamda incelenen kontroller maddeler halinde yazılabilmektedir:

- *Bilgi teknolojilerine yönelik güvenlik politika ve süreçlerinin tesisi ve sürekli uygunluk kontrolleri*: Güvenliğin personelden başlaması üzerine kullanıcıların bilgi güvenliği konusunda bilinçlendirilmesi ve kurumsal anlamda uyması gereken politika ve süreçlerin belirlenmesi kapsamındaki kontroller bu alanda incelenmektedir.
- *Programlara ve verilere yönelik mantıksal erişim kontrolleri*: Bu kapsamdaki kontroller ile veri girişi ve programlar üzerinde etkili bir güvenliğin sağlanması amaçlanmaktadır. Bunun sebeple öncelikle sisteme girilecek işlemler üzerinde yetkilendirme yapısının kurulması ile veri ve programlara erişimin yetkilendirilmiş kişilerle sınırlandırılması kapsamında kontroller incelenmektedir.
- *Sistem odalarına ve kritik donanımlara yönelik fiziksel erişim kontrolleri*: Mantıksal erişim sınırlandırmalarının yanında fiziksel erişim kapsamında kritik donanımlara erişimin de yetkili kişilerce sınırlandırıldığı ve periyodik olarak kontrol edilmesi bu kapsamda incelenmektedir.
- *Görevler ayrılığının bilgi teknolojileri bölümünde tesis edilmesi ve kritik görevlerin birbirinden ayrılarak tek kişi üzerine verilmesinin önlenmesi*: Genel olarak BT ortamına uygun olarak üç temel görevler ayrılığı ilkesinin varlığı bu alanda sorgulanmalıdır. Öncelikle veri işleme faaliyetlerinin veri girişi yapan kullanıcılardan ayrılmalıdır. Sonrasında veri işleme süreci ile ilgili birimlerin işlemlerin yaratılması ve/veya yetkilendirilmesi faaliyetlerinden ayrılması gerekmektedir. Son olarak veri işleme süreci içerisindeki faaliyetlerin (programlama, işlemler, dosyaların korunması, veri kabulü ve dağıtımı) birbirinden ayrılması gerekmektedir.
- *Programlara ve veriye erişime yönelik hakların dönemsel olarak incelenmesi*: Bu kapsamda ise bilgi sistemlerine ve veriye yetkili erişimin sağlanması amacıyla verilen

sistemsel hakların tasarlandığı şekilde muhafaza edilmesine yönelik periyodik incelemelerin yapılıp yapılmadığı kontrol edilmelidir.

2. Bilgi Sistemlerindeki Program Değişiklikleri: Bu kapsamdaki kontroller sistemlerin organizasyon tarafından belirlenmiş standartlara, politikalara ve süreçlere uygun olarak değiştirilmesini ve/veya iyileştirilmesini hedeflenmiştir.

Genel başlıklar ile bu kapsamda incelenen kontroller maddeler halinde yazılabilmektedir:

- *Değişiklik yönetim süreçlerinin tesis edilmesi*: Sistem yazılım değişikliklerinin yetkilendirilmesi, onaylanması, test edilmesi, üretim ortamına alınması diğer bir ifadeyle uygulanması ve son olarak bu sürecin belgelendirilmesi kapsamında değişiklik yönetimi sürecinin organizasyonun ihtiyaçlarına ve gereksinimlerine uygun olarak tesis edilmesi bu kontrol hedefinin kapsamı alanındadır.
- *Değişikliklerin uygulama alınmadan önce test edilmesi*: Gerçekleştirilecek olan yazılım değişikliklerinin uygulamaya alınmadan önce gerekli olan test adımlarından geçirilmesi ve test sonuçlarının kayıt altına alınıp onaylanması bu kontrol hedefinin kapsamı alanındadır.
- *Sistem değişikliklerinin ihtiyaçlara uygun olarak yazılı hale getirilmesi*: Yazılım değişikliklerine yönelik işlemlerin iş ihtiyaçlarının uygun olarak belirlenip yazılı hale getirilmesinden sonra ilgili değişikliğin teknik tasarımının belirlenmesi ve son olarak bu dokümanların onaylanması bu kontrol hedefinin kapsamı alanındadır.
- *Sistemlerin canlı ortamlarına erişimin sınırlandırılması*: Sistem ile ilgili belgelere ve sistem dosyalarına erişimin yetkili kişiler tarafından yapıldığından emin olunması bu kontrol hedefinin kapsamı alanındadır.
- *Acil değişiklik yönetim süreçlerinin tesis edilmesi*: Normal değişiklik sürecinin yanında sistemlere acil müdahale durumunda nasıl bir yol izleneceğine ve yapılan acil değişikliklerin sonradan nasıl kontrol edilmesine yönelik sürecin tesis bu kontrol hedefinin kapsamı alanındadır.
- *Bilgi sistemleri üzerinde uyarlamalara yönelik sürecin tesis edilmesi*: Son olarak mevcut bilgi sistemleri üzerinde yapılacak uyarlamaların yetkilendirilmesi, onaylanması, test edilmesi, uygulanması ve belgelendirilmesi bu kontrol hedefinin kapsamı alanındadır.

Uyarlamalar bilgi sisteminin teknik alt yapısı ile ilgili olabileceği gibi uygulamanın son kullanımındaki akışını etkileyecek parametre değişiklikleri de olabilecektir. Örneğin bilgi sistemine ait veri tabanında bir üst sürüme güncelleme yapılması teknik bir uyarlamayken, bankacılık ile ilgili bir bilgi sistemi üzerinde ek faiz oranının onaya tabi olup olmaması ile ilgili parametre değişikliği uygulama üzerindeki uyarlamalardır.

3. Bilgi Sistemleri Geliştirmeleri ve Alımlar: Bu kapsamdaki kontroller sistemlerin organizasyon tarafından belirlenmiş standartlara, politikalara ve süreçlere uygun olarak geliştirilmesini veya üçüncü taraf firmalardan edinilip uyarlanmasını hedeflenmiştir.

Genel başlıklar ile bu kapsamda incelenen kontroller maddeler halinde yazılabilmektedir:

- *Yazılım geliştirme sürecinin tesis edilmesi*: Yeni oluşturulan veya gözden geçirilen sistemlerin test edilmesi, değiştirilmesi, uygulanması ve belgelenmesine yönelik faaliyetler bu kontrol hedefinin kapsamı alanındadır. Önceki bölümlerde açıklanmış olan şelale metodolojisine benzer bir yazılım geliştirme süreci organizasyonun ihtiyacına yönelik olarak tesis edilmelidir.
- *Yazılım geliştirme taleplerinin uygun taraflarca onaylanması*: Yazılım geliştirme taleplerinin uygulanabilirliğin değerlendirilmesi, ihtiyaçların belirlenmesi ve satın lama veya sıfırdan geliştirme gibi izlenecek yönteme karar verilmesi açısından bilgi teknolojileri bölümü ve yönetim tarafından eş güdümlü olarak proje üzerinde karar verilmelidir.
- *Yazılım geliştirme projelerinin test edilmesi*: Yazılım geliştirme süreci içinde geliştirmenin tamamlanma aşamasında (yazılımcının gerçekleştirdiği birim testleri gibi) ve sonrasında (son kullanıcının fonksiyonel onay testleri gibi) ihtiyaç duyulan testlerin yapılmasına yönelik süreçlerin tesisi bu kontrol hedefinin kapsamı alanındadır.
- *Veri ve sistem dönüşüm sürecinin tesis edilmesi*: Mevcut sistemdeki verinin dönüştürülmesinde veya mevcut sistem dosyalarının dönüştürülmesinde gerekli yedeklerin alınması, testlerin gerçekleştirilmesi, onayların alınması ve geriye dönüş planlarının hazırlanmasına yönelik sürecin tesisi bu kontrol hedefinin kapsamı alanındadır.

4. Bilgi Sistemlerinin Operasyonel Yönetimi: Bilgisayar temelli sistemlerin işleyişini kontrol altında tutmak, bu kapsamda iş tarafına sunulan servis sürekliliğini sağlamak ve bu tarz

faaliyetler için kabul edilebilir bir güvenlik düzeyi sağlamak amacıyla oluşturulan kontrol hedefleri bu kapsama girmektedir.

Genel başlıklar ile bu kapsamda incelenen kontroller maddeler halinde yazılabilmektedir:

- *Bilgi sistemleri işleyişinin izlenmesi ve kontrolü*: Bu kontrol hedefinin kapsamında sistemler sadece yetkilendirilmiş ve onaylanmış amaçlar doğrultusunda kullanılmalıdır. Sistem dahilinde sadece onaylanmış programlar ve yazılımlar kullanılmalıdır. Zamanlı çalışan işlerin yönetilmesi ve olası işlemsel hataların etkili bir şekilde ortaya çıkarılması ve düzeltilmesi yine bu kontrol hedefinin kapsamı alanındadır.

- *Yedekleme ve yedekten geri dönme süreçlerinin tesis edilmesi*: Bilgi sistemlerinin kaynak kodlarının ve sistem ait verilerin yedeklenmesine ve periyodik olarak test edilmesine yönelik sürecin tesis edilmesi gerekmektedir. Bilgi işlem merkezinin bulunduğu yapı dışında konumlandırılan bir yerde verilerin ve programların yedeklemesi ve her türlü kasti ya da kasti olmayan aksaklıklar sonrası başvurulacak sistem kurtarma süreçleri belirlenmelidir. Yukarıdaki kapsamda belirtilen tüm kontroller bu kontrol hedefinin kapsamı alanındadır.

- *Vaka ve problem yönetimi sürecinin tesis edilmesi*: Son olarak bilgi sistemlerinin izlenmesi, olası aksaklıkların tespiti ve vakaların tespit edilmesi, sonrasında bunların kayıt altına alınıp çözülmesi bu kontrol hedefinin kapsamı alanındadır. Ek olarak son kullanıcıların yaşadığı problemlerin çözümüne yönelik sürecin tesis edilmesi de yine bu kontrol hedefinin kapsamı alanındadır.

2.3.2. Bilgi Teknolojileri Uygulama Kontrolleri

Bilgi teknolojileri uygulama kontrollerinin temel amacı sayısal nitelikte uygulamalar üzerindeki tüm işlemlerin eksiksiz ve tam olarak kayıtlara geçirildiği, doğru zamanda tümünün işleme tabi tutulduğu ve yine tüm işlemlerin uygun bir şekilde yetkilendirildiği konusunda kabul edilebilir güvence sağlayacak kontrollerin tesis edilmesidir. Ancak bununla birlikte uygulama kontrollerinin etkin olarak çalışabilmesi için yine güvenilir ve etkin bir bilgi teknolojileri genel kontrol ortamı sunulmalı ve uygulama kontrollerinin bu genel kontrol ortamı ile uyumlu olarak çalışması sağlanmalıdır.

Genel olarak uygulama kontrollerini sınıflandırarak açıklamadan önce tanımını yapmak yerinde olacaktır. Uygulama kontrolleri, satışlar, satın almalar, ödemeler, tahsilatlar, stoklar gibi

işletmenin bilgisayar ortamında yürüttüğü birçok işlem döngülerine yönelik uygulama yazılımlarına yerleştirilen kontrollerdir. Genel olarak bilgi sistemi sürecine paralel olarak, veri girişinden kaynaklananlar, veri işleme sürecinden kaynaklananlar ve bilgi çıkışından kaynaklananlar olmak üzere üç kısımda incelenebilirler.

1. Veri Girişinden Kaynaklanan Kontroller: Veri girişi ile ilgili olarak etkin bir kontrol ortamının tesis edilmesi için işlemlerin uygun bir şekilde yetkilendirilmesi, gerçekleşen işlemlerin doğru biçime dönüştürülüp veri dosyalarında kayıt altına alınabilmesi gerekmektedir. Bununla birlikte işlemlerin eksiksiz, ekleme yapılmadan ve üzerinde uygunsuz değişiklikler yapılmaksızın bir kez işleme tabi tutulduklarının da güvence altına alınması gerekmektedir. Bu noktada sistemlerin hatalı işlemleri tanımlaması, bu tür işlemleri reddetmesi ve tekrar doğrulatması gibi yetkinliklere de sahip olması beklenmelidir. Veri girişinden kaynaklanan kontroller sınıflandırarak maddeler halinde aşağıda açıklanmaya çalışılmıştır[25].

- *Verilerin Bütünlüğünün Sağlanmasına Yönelik Kontroller*: Bütünlük kontrolleri verinin içeriğine bakmaksızın sadece kayıtların kendisi ile ilgilidir. Bütünlük kontrollerinde önemli olan tüm işlemlerin kayıtlara geçirilmiş olduğunun ve işleme tabi tutulduğunun saptanmasıdır. Veri kodlama kontrolleri, yığın işlem kontrolleri ve mutabakat yoluyla hata raporlamasına yönelik kontroller bu kapsamdaki kontroller arasında sayılabilmektedir. Veri kodlama kontrollerinde veri girişi yapılan işlemin içindeki bilgiler belirlenen program algoritmasının uygulanması ile elde edilen sayının veri girişi yapılan sağlama sayısı ile karşılaştırılması sonucu yapılan kontrollerdir. Örneğin hesap kodu girişi yapıldığında bilginin eksiksiz olup olmadığının kontrolü için yine girişmiş olan bir sağlama sayısı ile girilen bilgilerden elde edilen rakamın karşılaştırılması ile kontrol edilebilmektedir. Yığın işlem kontrollerinde ise sıra numarasına bağlı kontroller, girişi yapılan verilerin daha önce işleme tabi olmamış işlemlerle karşılaştırılmasının yapılması veya yığını tanıtan ek bir değere bağlı olarak toplam veya kayıt sayısı kontrolleri ile tüm veri girişinin bütünlüğü kontrol edilebilmektedir. Son olarak, veri girişi için girilen işlemler sırasında olası hataların tespit edilip raporlanmasına yönelik kontroller de bütünlüğün korunması için tesis edilmektedir. Diğer bir ifadeyle veri girişi yapılan bilgiler ile verinin işlenmesi sırasında tespit edilen hatalar kayıt altına alınıp raporlanabilmektedir.

[25] Erdoğan, **age**, 162

Bu tespitin yapılması için giriş i yapılan bilgileri ile kayıt altına alınan bilgiler arasında otomatik mutabakat yapılmaktadır. Örneğin 100 adet 1000 YTL tutarında para transfer işlemi girildiği biliniyorsa, bu işlemlerin bilgisayara aktarılmasından sonra kayıt sayısının 100 ve toplam tutarın da 100.000 YTL olup olmadığı karşılaştırılıp hatalı aktarılan kayıtlar tespit edilmektedir.

- *Verilerin Doğruluğunun Sağlanmasına Yönelik Kontroller*: Doğruluk kontrolleri verinin içeriği içindeki dosyalar ve bilgileri ile ilgilidir. Doğruluk kontrollerinde önemli olan kayıtların içeriklerinin incelenmesi ve önceden belirlenmiş olan ölçütlere uygun olup olmadıklarının saptanmasıdır. Sadece doğruluk kontrolleri ile işlemlerin gerçeği tam olarak yansıttığı konusunda güvence verilemese de, sistem içerisinde belirlenmiş olan parametreler ve standartlara uygun olarak işlem yapılması sağlanabilmektedir. Kaynak belge kontrolü ve girdi geçerlilik kontrolleri bu kapsamdaki kontroller arasında sayılabilmektedir. Kaynak belgeler üzerinde yapılacak herhangi bir hata veya hile eğer bu sırada yakalanmaz ise, bu tür girdilerin sonraki aşamalarda yakalanması oldukça zor olacaktır. Bu nedenle, kaynak belge kontrolleri ile kaynak belgeler sırasal olarak numaralandırılmakta ve ilgili işlem kayıtları ile bu sıra numaraları arasında ilişki kurularak kontrol sağlanmaktadır. Girdir geçerlilik kontrolleri ise, işlem verisinin işlenmeden önce kontrol ederek hataları ortaya çıkaran program kontrollerinden oluşmaktadır. Örneğin girilen kodun, karakter sayısının veya alan boyutunun veri girişi sırasında kontrol edilmesi bu tip kontrollerdendir. Daha somut bir örnek vermek gerekirse, fatura tutarının girildiği alana rakam yerine karakter girişi denendiğinde sistemin verdiği hata mesajı vermesinde bahsedebiliriz. Bunun dışında veri girişini genelleştirerek doğrulama kontrolleri de yapılabilmektedir. Örneğin, bir satın alma siparişine ve ona ait fatura kaydına ait tutar bilgisinin tek noktadan girişinin sağlanarak her iki kayıt için de uyumlu olmasının sağlanması ile işlemlerin veri girişi aşamasında doğruluğu saplayacaktır.

2. Veri İşleme Süreci Üzerindeki Kontroller: Kaynak belgelerdeki verilerin bilgisayarın okuyabileceği ortama geçirilmesinden sonra verilerin bilgisayarda işlenerek bilgi yaratma aşamasına geçilmektedir. Bu aşamada, sistem tarafından yaratılmış işlemler dahil olmak üzere tüm işlemler sistem tarafından uygun olarak işleme tabi tutulmalıdır. Tüm işlemler eksiksiz,

ekleme yapılmadan, üzerinde yetkisiz işlem yapılmadan ve bir kez işleme tabi tutulmalıdır. Son olarak işlemler sırasında olası hataların zamanında tanımlanması ve çözülmesi gerekmektedir[26].

- *Mutabakat*: Veri girişi yapılan bilginin, işlenmesi öngörülen tasarımda manüel olarak hesaplanarak çıkan sonuç ile karşılaştırılabilmektedir. Bu yöntem genellikle işleyen organizasyonlar yerine dış denetçiler tarafında kullanılan bir kontrol yöntemidir. Manüel mutabakata ek olarak, işlenecek dosyadaki verinin belirlenen kriterdeki toplam değerine bakılarak veri işleme öncesi ve sonrasındaki değerlerin otomatik olarak karşılaştırılması ile de yapılabilmektedir. Bu tarz kontroller yardımıyla da otomatik olarak mutabakatlar yapılabilmektedir.
- *Geçiş Kontrolleri*: Diğer bir kontrol tipi ise geçiş kontrolleridir. Sistem içerisinde veri işleme sırasında her bir geçiş arasında kontrol sayıları yeniden hesaplanmakta ve veri girdi geçişinden gelen kontrol toplamları ile karşılaştırılarak ilerlenmektedir. Verinin birden fazla okunması ya da aritmetik işlemlerin tekrarlanması yoluyla elde edilen sonuçların karşılaştırılması gibi mutabakat kontrolleri de veri işleme süreci içinde tasarlanabilmektedir.
- *Programlanmış Kontroller ve Geçiş Kontrolleri*: Bunun dışında programlanmış kontroller ve kontrol değeri yardımıyla da veri işleme süreci kontrol edilebilmektedir. Verinin işlenmeden önceki değerleri ile işlendikten sonra elde edilen sonuç, kontrol değeri ve veri işleme sırasında çalıştırılan bir program vasıtasıyla yapılabilmektedir. Böylelikle hatalı olarak işlenen kayıtlar istisna olarak raporlanabilmekte ve düzeltilebilmektedir.
- *Mantıksal Değer ve Limit Kontrolleri*: Veri işleme sırasında mantıksal ve limit kontrolleri yardımıyla da elde edilen bilginin doğruluğu ve bütünlüğü kontrol edilebilmektedir. Örneğin limit kontrolünde, belirli bir sınırın konulmasına sebebiyle yanlış veri işleme gerçekleşse de bu sınırın üstünde işlem başarıyla gerçekleşmeyecektir. Örneğin mantıksal kontrollerde işlem sonucunda mantıksız rakamlara ulaşan işlemlerin raporlanması sağlanabilmekte ve işlem tamamlanmadan incelemeye alınabilmektedir.

3. Bilgi Çıkışından Kaynaklanan Kontroller: Bilgi işlem süreci sonunda elde edilen sonuçların sistem tarafında raporlanması ile oluşan çıktılar üzerinde temel olarak iki başlıkta kontrol noktaları tesis edilmelidir. İlkinde işlem sonuçlarının doğru ve tam olması sağlanmalı, ikincisinde

[26] Erdoğan, **age**, 167

ise çıktılara erişimin yetkilendirilmiş kişilerle sınırlandırılması ve bu kişilere uygun zamanda ulaştırılması gerekmektedir[27].

- *Çıktıların Doğrulanması*: Girdi teşkil eden veriler, işlenen veri sonrası elde edilen çıktı ve kontrol toplamları arasında mutabakat yapılarak çıktıların doğruluğu kontrol edilmelidir. Veri işleme sırasında denetim izlerinin tutulması sayesinde veri işleme süreci içindeki ara çıktıların ve mutabakat verisinin incelenmesi de sağlanabilmektedir. Buna ek olarak programlanmış kontroller yardımıyla hata tespit edilen çıktıların raporlamasına yönelik kontroller de tesis edilebilmektedir.
- *Çıktıların Dağıtımı ve Yetkilendirilmesi*: Bu kapsamdaki kontroller de ise çıktıların yetkili kişiler tarafından erişilmesinin sağlanması amaç edinilmiştir. Rapor sonuçlarına erişim için sistem üzerinde mantıksal erişim kontrollerinin tesisi veya çıktı basılacaksa bilgiye erişmesi gereken kişinin yazıcısında raporun basılması gibi kontroller uyarlanabilmektedir. Örneğin kişilerin maaş ödeme bilgilerine erişebilmek için sistem üzerinde yetkilendirme yapılarak sadece insan kaynakları müdürüne yetki verilebilmektedir. Ancak bu noktada bilgi teknolojileri genel kontrol ortamı ile de bu tarz uygulama kontrolleri desteklenmelidir. Örneğin sistem üzerindeki yetkilendirme sürecinin onaylara bağlı olması, tek kişinin yetkilendirme yapamaması ve veritabanı üzerinde gizli bilgilere direkt erişimin kısıtlanması gibi genel kontrol ortamına yönelik kontroller ile de örneğini verdiğimiz uygulama kontrolü desteklenmelidir. Son olarak hassas bilgilerin çıktı olarak iletilmesine yönelik elektronik imza ile onay ve/veya şifreleme yöntemleri ile iletilmesi gibi yöntemler de kullanılabilmektedir.

2.4. Uygulama Sistemleri ve Üzerindeki Kontrollere Yönelik Denetim Teknikleri

Bilgi sistemleri denetçisinin uygulama kontrollerini test etmeden önce aşağıdaki görevleri yerine getirmesi gerekmektedir.

- Uygulama kontrollerinin test edileceği uygulama sistemine yönelik olarak ilgili teknik dokümantasyonun incelenmesi ve yetkili kişiler ile görüşerek bilgi alınması yollarıyla uygulamanın önemli modüllerinin belirlenmesi ve bu modüller üzerinde işlemlerin akış mantığını anlaşılması gerekmektedir.

[27] Erdoğan, **age**, 169

- Sistem üzerindeki uygulama kontrollerinin gücü belirlenmeli ve olası kontrol zayıflıkları değerlendirilerek her bir uygulama kontrolü için test stratejisi oluşturulmalıdır.
- Uygulama sistemini ve işlevlerini daha iyi anlamak için aşağıda belirtilen dokümanların uygulama kontrollerinin testinden önce incelenmesi gerekmektedir[28].
    - Uygulama sisteminin geliştirilme metodolojisine ait dokümanlar
    - Fonksiyonel tasarım dokümanları
    - Uygulama üstüne yapılan program değişikliklerinin listesi ve önemli olanlarının dokümanları
    - Kullanıcı el kitabı
    - Sistem yönetimine ait olarak hazırlanan teknik dokümantasyon

Uygulama sistemine ait dokümantasyon incelemesi ve ilgili kişiler ile görüşmeler yapıldıktan sonra sistem üzerinde işlemlerin akışını anlatan bir akış diyagramı hazırlanması veya önceden hazırlanmış olan diyagramının üzerinden gidilmesi gerekmektedir. Bu aşamanın asıl amacı sistem üzerindeki veri girişinden, verinin işlenip çıktı haline dönüşmesine kadarki süreçler içinde olası kontrol zayıflıklarını veya eksikliklerini önceden belirlemek ve test stratejisini bu yönde belirlenmesidir.

Bir sonraki aşama olarak ise uygulama sistemine yönelik risk değerlendirmesinin yapılması ve tasarlanan uygulama kontrollerinin bu yönde analiz edilmesidir. Tasarlanan iç kontrollerin etkinliği, son denetim döneminden itibaren geçen dönem, işlemlerin karmaşıklığı, işlemlerin yoğunluğu, işlemlerin hassaslığı ve önceki denetim sonuçları gibi birçok faktörün değerlendirilmesi ile risk değerlendirmesi yapılmakta ve tasarlanan uygulama kontrolleri değerlendirilmektedir.

Uygulama kontrollerinin test edilmesinden önce bilgi teknolojileri genel kontrol ortamı ve kullanıcılara bağlı olarak gerçekleşen bazı kritik prosedürler izlenmeli ve test edilmelidir. Bu kritik işlemlerden bazıları şunlardır[29]:

[28] Johnson, **age**, 203
[29] **age**, 204

1. *Görevler Ayrılığı Prensibinin Uygulanması*: Uygulana üzerinde bir işlemi başından sonuna kadar hiç kimsenin tek başına tamamlayamadığı kontrol edilmeli ve kritik yerlerdeki görev ayrılığına yönelik kurallar incelenmelidir.
2. *Veri Girişine Yönelik Yetkilendirme*: Sistem üzerinde her kullanıcı kendi yetkili olduğu işlemlerin girişini yapabilmelidir. Örneğin muhasebe fişi girişini sadece muhasebe çalışanları yapabilmeli diğer bölümlerden kimsenin sistem üzerinde erişiminin olmaması gerekmektedir.
3. *Mutabakat ve Geçiş Kontrolleri*: Sistem üzerinde gerçekleşen veri işleme sürecine yönelik tasarlanan mutabakat ve geçiş kontrollerinin tasarlandığı gibi zamanında çalıştığına emin olunmalıdır.
4. *Hata Kontrolü ve Düzeltme*: Sistem üzerinde olası tespit edilen hatalar raporlar yardımıyla periyodik olarak tespit edilmeli ve gerekli düzeltme işlemleri tamamlanmalıdır. Bu sürecin uygun tasarlanıp tasarlanmadığı değerlendirilmelidir.
5. *Raporların Dağıtımı*: Genel olarak sistem ile ilgili kritik rapor veya çıktıların güvenli bir alanda tutulması ve kontrollü bir şekilde dağıtılmasına yönelik sürecin tesis edilip edilmediği değerlendirilmelidir.

Yukarıda bahsettiğimiz genel incelemeler ve değerlendirmeler sonucunda uygulama kontrollerinin değerlendirilmesine ve uygun test tekniği ile test edilmesine geçilebilmektedir. Uygulama kontrollerinin etkin olarak test edilebilmesi için uygun denetim tekniğinin belirlenmesi hayati önem taşımaktadır. Uygulama sistemlerinin ve üzerindeki kontrollerin testine yönelik olarak kullanılabilen bazı denetim tekniklerini aşağıda sıralayarak kısa açıklamalarını vermek yerinde olacaktır:

1. Anlık Görüntü Analizi: Belirlenen bazı işlemlerin incelenen program akışındaki kayıtlarının anlık durumlarını inceleme yöntemidir. Programın çalışma mantığının anlaşılmasında yardımcı olmaktadır.
2. Akış Haritasını Çıkarmak: Uygulama üzerinde incelenecek programı belirleyerek çalışması sırasındaki akışı çıkararak analiz etme yöntemidir.

3. İzleme ve Etiketleme: Uygulama üzerinde belirlenmiş örnek işlemler girdi olarak verilerek ve bu girdilerle belirlenen kontrolün çalışması izlenerek istenen sonuca ulaşılıp ulaşılmadığının incelenmesine izleme ve etiket yoluyla denetim tekniği adı verilmektedir.
4. Test Verisini Kullanma: Test edilmesi planlanan gerçek programlar üzerinde test verisi ile simülasyon yaparak test etme yöntemidir.
5. Paralel Operasyon: Genellikle önceden test edilmiş ve doğru veri işleme yapan bir program veya sistemin yerine başka bir sistem tasarlandığında kullanılabilecek bir yöntemdir. Aynı gerçek girdiler ile eski ve yeni sistemlerin çıktıları alınarak birbiri ile karşılaştırma yoluyla test edilme yöntemidir.
6. Entegre Test İmkanı: Sistem üzerinde gerçek veri ile birlikte gerçek olmayan fakat ayrıştırıla bilen sahte verinin de aynı anda işlenmesini sağlayarak test edilmesi yöntemidir.
7. Paralel Simülasyon: Sistemin verdiği çıktılar ve aldığı girdiler örnek olarak alınarak test edilecek programın mantığının denetim için kullanılan başka bir uygulamada benzer şartları oluşturarak incelenmesi yöntemidir.
8. Bütünleşik Denetim Yöntemi: Bazı uygulama sistemleri kendi içlerinde denetime ve kontrole yönelik olarak yazılımlar bulundurmaktadırlar. Örneklem yöntemi ile uygulama üzerinde mevcut yazılım fonksiyonu kullanılarak inceleme yapılabilmekte ve üretim ortamındaki istatistikler görülebilmektedir[30].

Yukarıda sayılan yöntemlerin dışında uygulama sistemi üzerinde test edilmesi planlanan kontrollere yönelik farklı denetim teknikleri de geliştirilebilmektedir. Yukarıda bahsi geçen teknikleri çoğu bilgisayar sisteminin bir bütün olarak incelenmesini ve bir yazılım yardımıyla bilgisayar destekli denetim tekniklerinin uygulanması kapsamında gerçekleştirilen faaliyetlerdir. Bunun yanında sisteme yapılan girişler ile çıktıların değerlendirilmesine göre uygulama kontrollerin test edilme yönetimi de izlenebilmektedir. Bu yönteme kara kutu yaklaşımı adı verilmektedir. Bilgisayar sistemi içinde işlemlerin nasıl yürüdüğünden ziyade işlemlerin sonucunun değerlendirilmesine odaklanmış bir test yöntemidir.

[30] Johnson, **age**, 206-207

Son olarak bilgi sistemleri denetiminde günümüzde oldukça fayda sağlayan bilgisayar destekli denetim teknikleri ve buna yönelik uygulamalar ile aşağıdaki faaliyetler gerçekleştirilebilmektedir:

- Genel bilgi teknolojileri kontrollerinin uygunluk testleri
- Uygulama kontrollerinin uygunluk testleri
- Analitik inceleme
- İşlemlerin ve bakiyelerin ayrıntılı testleri

3. BİLGİ SİSTEMLERİ DENETİM SÜRECİ VE ESASLARI

Bilgi sistemlerinin yönetimi ve temel kavramlarını bir önceki bölümde açıkladıktan sonra bu bilgilere paralel olarak bilgi sistemleri denetimi kavramını ve esaslarını açıklamak konumuzun devamı için yerinde olacaktır. Çalışmamızın bu bölümünde, denetimin tanımı, türleri, denetim sürecinin sınıflandırılması, bilgi sistemleri denetiminin amaçları, organizasyon içindeki yeri, finansal denetim ve iç kontrol ortamı üzerindeki etkileri, risk odaklı bilgi sistemleri denetimi ve bilgi sistemleri denetim süreci konuları temel noktalar esas alınarak açıklanacaktır.

3.1. Denetimin Tanımı ve Amacı

Bilgi sistemleri denetimine geçmeden önce denetim kavramını ve amacını kısaca değinmek yerinde olacaktır. "*Denetim*", iktisadi faaliyet ve olaylarla ilgili iddiaların daha önceden saptanmış ölçütlere uygunluk derecesini araştırmak ve sonuçları ilgi duyanlara bildirmek amacıyla tarafsızca kanıt toplayan ve bu kanıtları değerleyen sistematik bir süreçtir[31].

Genel olarak yukarıda tanımlanmış olan denetim kavramının temel unsurları ve özellikleri sırasıyla şu şekilde açıklanabilmektedir[32]:

1. *Denetim iktisadi faaliyet ve olaylar ile ilgili iddiaların incelenmesini amaç edinmiştir*: İktisadi faaliyet ve olaylarla ilgili iddialar ifadesi ile muhasebenin iktisadi bilgileri teşhis etme, ölçme ve raporlama işlevleri belirtilmek istenmektedir. Denetim sürecinin özü bu ifade içinde aranmalıdır. Uzman denetçi bir denetim faaliyetine başlarken denetlediği işletmenin finansal tabloları ve iktisadi faaliyetleri hakkındaki raporlar kendisine sunulur. Bu raporlar o işletme yönetiminin belirli bir döneme ait iktisadi faaliyetler hakkındaki bildirim ve iddialarını yansıtır. Uzman denetçi gerekli incelemelerini yaparak işletme yönetiminin kendisine sunduğu bu raporlardaki iddiaların doğruluğunu ve güvenirliliğini araştırır ve onaylar. Bu finansal denetim süreci içinde de bilgi sistemleri denetimi ile günümüz gelişen teknolojisi içinde yönetim iddialarının doğruluğuna makul bir güvence verilmesi için destek olunmaktadır.
2. *Denetim faaliyeti önceden belirlenmiş ölçütlere göre gerçekleştirilmektedir:* Genel olarak denetçinin yönetim iddialarını ve edindiği bilgileri değerlendireceği standartlardır. Doğal olarak kullanılan ölçütler denetimin amacına ve sınıfına göre farklılıklar gösterecektir.

[31] Celal Kepekçi, **Bağımsız Denetim**, 5. baskı (İstanbul: AVCIOL Basım Yayın, 2007), 1
[32] Nejat Bozkurt, **Muhasebe Denetimi**, 3. baskı, (İstanbul: Alfa Basım Yayım, 2000), 23

Örneğin denetimin amacı mali tabloların doğruluğuna ilişkin görüş bildirmek ise, karşılaştırma ölçütü olarak genel kabul görmüş muhasebe ilkeleri kullanılacaktır. Diğer yandan ise Türkiye'deki bankalarda gerçekleştirilecek olan bilgi sistemleri denetimi amaç edinilmiş ise yasal mevzuat gereği olan ilkeler tebliği ve bilgi teknolojileri yönetimindeki kontrol hedefleri ("COBIT") çerçevesindeki ilkeler benimsenecektir.

3. *Denetim süreci belirlenen ölçütlere uygunluk seviyesinin belirlenmesini amaç edinmiştir*: Uygunluk derecesi yönetim tarafından ileri sürülen iddia ve bildirimlerin saptanmış ölçütlerle ne derecede uyum içinde bulunduğunu belirleyen bir ölçüdür. Bu uygunluk ya da uyumsuzluk nicel olarak veya nitel olarak saptanıp belirlenebilir.
4. *Denetim sonuçları ilgi duyan taraflara bildirilmelidir*: İlgi duyanlar ilgili çıkar gruplarını ve genel anlamda kamuyu ifade etmektedir. Denetçinin bulgularını ve yargısını kullanan her birey ilgili taraf olmaktadır. Örneğin Türkiye'deki bankalarda gerçekleştirilen bilgi sistemleri denetiminin öncelikli ilgi duyan tarafları banka üst yönetimi, Bankacılık Düzenleme ve Denetleme Kurumu ("BDDK") ve Türkiye Cumhuriyeti Merkez Bankası ("TCMB")'dır.
5. *Denetim süreci içinde kanıtlar tarafsızca toplanır ve değerlendirilir*: Denetimin amaçlarına ulaşılması için, denetimde elde edilen her türlü bilgi ve veri kanıt olarak kullanılabilir. Bu aşamada denetçinin bir ön yargıya dayanmadan bağımsız bir uzman kişi olarak, yapılmış bildirimleri özenle incelemesi ve sonuçların titizlikle değerlemesi gerekmektedir.
6. *Denetim süreci sonunda sonuçlar raporlanmalıdır*: Denetçinin elde ettiği bulguların bilgi kullanıcılarına iletilmesini ifade etmektedir. Sonuç bildirme temelde bir onaylama işlemidir. Denetçi işletme yönetimince ileri sürülen iddia ve bildirimlerin geçerliliğini ve güvenirliliğini inceleyerek bunları onaylar ya da reddeder. İnceleme ile ilgili bulguların ve denetçi görüş ve yargısının açıklanması yazılı bir raporla olur. Kısaca denetim sonuçları; işletme yönetimi tarafından açıklanan bilgilerin, önceden belirlenmiş kriterlere denetimle saptanmış olan uygunluk derecesi demektedir.
7. *Denetim faaliyetleri sistematik bir süreçtir*: Denetim ile ilgili tüm tanımlamalarda denetimin bir süreç olduğu belirtilmektedir. Bu yolla denetimin dinamik bir faaliyet olduğu ortaya konmaktadır. Bu süreç denetim faaliyetleri için gerekli olan bilgi ve kanıtların sağlanması, bunların işlenmesi ve değerlendirilmesi, değerlendirme

sonuçlarına göre bir denetim görüşüne ulaşılması ve bu görüşün denetim raporu ile ilgili yerlere iletilmesi evrelerini içerir. Bu açıdan denetim süreci bir bilgi üretme ve karar verme süreci olarak düşünülmelidir[33].

3.2. Denetimin Türleri

Denetim faaliyetleri denetimin konusuna veya denetçinin statüsüne göre genel olarak türlere ayrıştırılabilmektedir. Bu bölümde her iki yönteme göre denetim türleri açıklanacak olup bilgi sistemleri denetiminin açıklanan türlerin hangilerinde nasıl dahil olduğuna da yer verilecektir.

3.2.1. Konusuna Göre Denetim Türleri

Denetimin konusuna göre denetim, finansal denetim (mali tabloların denetimi), uyguluk denetimi ve faaliyet denetimi olarak üçe ayrılmaktadır[34]:

1. *Finansal Denetim*: Finansal denetim, bir işletmenin mali tablolarının önceden belirlenmiş ölçütlere uygun olarak düzenlenip düzenlenmediğini konusunda bir görüşe ulaşmak amacıyla mali tabloların incelenmesini kapsayan bir denetim türüdür. Bu ölçütler genel kabul görmüş muhasebe ilkeleri veya vergi mevzuatından oluşmaktadır. Bu denetim türü genel olarak bağımsız denetçiler ve kamu denetçileri tarafından yürütülmektedir. Bilgi sistemleri denetimi ise bu denetim faaliyeti içinde destek sağlayan bir denetim sınıfıdır. İşletmelerdeki işlemlerin yoğunluğu ve günümüz teknolojik gelişmelere paralel olarak bu verilerin otomatik işlenmesinden dolayı finansal denetçilerin bilgi sistemlerinden aldıkları raporların doğruluğuna, eksiksizliğine ve bütünlüğüne yönelik olarak bilgi sistemleri denetçilerinden aldıkları desteğe ve bu amaçla ortaya çıkan denetim türüne bilgi sistemleri denetimi adı verilmektedir.
2. *Uyguluk Denetimi*: Uygunluk denetimi, işletme faaliyetlerinin bir üst makam tarafından konulan standart ve/veya ölçütlere göre ne ölçüde uygun olduğunun incelenmesine yönelik olarak yapılan denetim faaliyetidir. Bu üst makam işletme içindeki üst yönetim olup iç kontrol prosedürleri olabileceği gibi işletme dışı yetkili bir merci olup zorunlu kıldığı bir mevzuat da olabilmektedir. Tanımdan da anlaşılacağı gibi çok geniş kapsamı olan bir faaliyet türüdür. Örneğin, Bankacılık Düzenleme ve Denetleme Kurumu

[33] Kepekçi, **age**, 2
[34] Ömer Duman, **SM, SMMM, ve YMM Sınavları için Muhasebe Denetimi ve Raporlama**, 2. baskı (Ankara: Siyasal Kitabevi, 2008), 13-14

("BDDK")'nun Türkiye'deki bankalar için belirlediği mevzuata göre zorunlu kıldığı bilgi sistemleri denetimi, bu denetim türünün içine girmektedir.

3. *Faaliyet Denetimi*: İşletmenin amacına ulaşmasında önemli olan faaliyetlerin etkinliğinin ve verimliliğinin incelenmesi amacıyla gerçekleştirilen denetim faaliyetidir. Faaliyet denetiminde, faaliyet sonuçları verimlilik standartları ile karşılaştırılır ve işletmenin önceden belirlenmiş amaç ve hedeflere ulaşıp ulaşmadığı ölçülmektedir. Faaliyet denetiminde, finansal ya da finansal olmayan bilgileri değerlendirmek amacıyla ölçütleri belirlemede son derece öznel olduğundan faaliyet denetim bir yönüyle yönetim danışmanlığına da benzemektedir. Faaliyet denetimi konusunda göre bilgi sistemleri denetimini de içinde barındırabilmektedir. Örneğin birçok firmaya verilerin yedeklenmesi amacıyla ağ bağlantısı, veri aktarımı ve boş kayıt alanı hizmeti sağlayan bir işletmenin performans ve verimlilik denetimi bilgi sistemleri faaliyet denetimi olacaktır. Verdiğimiz örnek işletmenin kendi sistemleri üzerinde iş sürekliliğini düşünerek yedekleme süreçlerinin incelenmesini de kapsayabilmektedir.

Sonuç olarak yukarıdaki açıklamalarımızdan da görüleceği gibi bilgi sistemleri denetimi, denetimin konusuna göre her üç denetim türüne de destek olan bir denetim sınıfı olduğu açıkça görülmektedir.

3.2.2. Denetçinin Durumuna Göre Denetim Türleri

Denetçinin durumuna göre denetim, iç denetim, kamu denetimi ve bağımsız denetim olarak üçe ayrılmaktadır[35]:

1. İç Denetim: İç denetçi işletmede devamlı olarak çalışan ve devamlılık arz eden denetim faaliyetlerini yönetimin belirlediği ilke ver prensiplere göre yerine getiren personeldir. Kapsamlı olarak iç denetim kavramını tanımlayacak olursak, bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyeti olup, kurumun risk yönetim, kontrol ve yönetişim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmada yardımcı olan bir denetim faaliyetidir. İç denetçiler bir önceki bölümde bahsedilen üç denetim türünü de işletme içinde yerine getirmektedirler. Doğal olarak bilgi sistemleri denetiminin iç denetçiler tarafından

[35] Duman, **age**, 15–16

gerçekleştirilmesi ile bilgi sistemleri denetimini de kapsamına almaktadır. Bankalarda teftiş birimleri altında kurulan bilgi sistemleri denetim ekipleri bu kapsamdaki denetim türü içinde yer almaktadır.

2. Kamu Denetimi: Kamu denetimi, yasal yürütme organına bağlı çeşitli birimler tarafından yasal yetkileri çerçevesinde yapılan denetim olup kamu denetçileri ise yasal yürütme organına bağlı olarak çalışan ve kamu adına denetim yapmakta görevli ve yetkili kişilerdir. Bankacılık Düzenleme ve Denetleme Kurumu ("BDDK") bünyesinde oluşturulan bilgi sistemleri denetim ekibi vasıtasıyla bağımsız bilgi sistemleri denetim raporlarının incelenmesi ve bankalardaki bilgi teknoloji faaliyetlerinin yasal mevzuata göre yasal murakıplarca incelenmesi bilgi sistemleri denetiminin bu denetim türü içindeki yerine bir örnek olarak verilebilmektedir.

3. Bağımsız Denetim: Son olarak bağımsız denetim serbest meslek sahibi olarak kendi adına çalışan veya bir denetim şirketinin ortağı ya da yetkili denetçisi olan kişiler tarafından işletmelerinin mali tablolarının Türk Ticaret Kanunu, Sermaye Piyasası Kanunu ve Vergi Kanunları ile genel kabul görmüş muhasebe ilkelerine uygunluk derecesini belirlemek amacıyla yapılan denetim çalışmalarıdır[36]. Bu kapsamda bağımsız denetçiler tarafından Türkiye'deki bankalarda düzenleyici kurum tarafından zorunlu kılınan yasal mevzuat gereğince bilgi teknolojileri yönetiminin uygunluğuna yönelik yapılan denetim faaliyetleri de bağımsız denetim türünün kapsamına girmektedir.

3.3. Denetim Sürecinin Sınıflandırılması

Bir önceki bölümde denetim türlerini ve bu türlerin içinde bilgi teknolojiler denetiminin yerini inceledikten sonra, denetim sürecini amaçları doğrultusunda ayrıntılı olarak sınıflandırıp tanımlamak yerinde olacaktır.

3.3.1. Finansal Denetim

Finansal denetimin esas amacı önceki bölümlerde de bahsettiğimiz üzere kurumun finansal tablolarının belirlenen ölçütlere göre doğruluğunu değerlendiren bir denetim alanıdır. Genel

[36] Duman, **age**, 17

olarak detay maddi doğruluk testlerini içerse de kontrol temelli denetimi ve bilgi sistemleri denetimini de destek alacak şekilde ilerleyebilmektedir[37].

3.3.2. Operasyonel Denetim

Önceden belirlenen bir amaç doğrultusunda kurumun iç kontrol yapısını değerlendirmek için tasarlanan denetim faaliyetleridir. Önceden belirlenen uygulama kontrollerine yönelik bilgi sistemleri denetimi veya sistemlerin mantıksal erişimine yönelik bilgi sistemleri denetimi bu kapsamdaki denetim alanına örnek olarak verilebilir[38].

3.3.3. Bilgi Sistemleri Denetimi

Bilgi sistemleri denetim süreci gerekli kanıtları toplayıp değerlendirerek, bilgi sistemlerinin ve ilgili kaynakların yeterli derecede korunduğunun, veri ve sistem bütünlüğünün korunduğunun, organizasyon amaçları doğrultusunda güvenilir ve doğru bilgi sağlandığının, kaynakların verimli kullanıldığının ve iç kontrol ortamının etkinliğine katkıda bulunduğunun incelendiği denetim alanıdır.

3.3.4. Entegre Denetim

Entegre denetim genel itibariyle finansal denetim ile operasyonel denetim adımlarının bir araya getirildiği bir denetim alanıdır. Entegre denetim iç ve dış deneticiler tarafından gerçekleştirileceği gibi finansal bilgilerin doğruluğu, kurum kaynaklarının korunması, etkinlik ve uygunluk açısından değerlendirme gibi geniş bir kapsamı içine alarak gerçekleştirilen ve bilgi sistemleri denetiminden de destek olan bir denetim alanıdır[39].

3.3.5. Yönetsel Denetim

Yönetime danışmanlık veya yön gösterme amacıyla kaynakların verimli kullanılmasının ve operasyonel etkinliğin değerlendirildiği bir denetim alanıdır.

3.3.6. Adli denetim

Enron, Worldcom, Adelphia, Xerox gibi başlıca işletmelerde gerçekleşen skandalları muhasebe denetiminin önemini ve denetçi sorumluluğunu artırmıştır. Yapılan muhasebe hileleri yalnızca şirket sahiplerini ve yatırımcıları değil, çalışanlar, kredi kurumları, devlet ve denetim firmaları

[37] Johnson, **age**, 23
[38] **age**, 23
[39] **age**, 23

gibi pek çok kesiminde zarar görmesine neden olmaktadır. Bilânço çıkarma, muhasebe defterleri, faturalar vb. konularda uzman olan bazı kötü niyetli kişiler hileyle rakamları değiştirebilmekte ve bir anda binler milyonlara, karlar zarara, zararlar kayba dönüştürülebilmektedir.

Bu kapsamda görünen değerleri kabul etmeyip arka planına bakarak, dokümanlar hakkında şüphe duyarak, gerçek niyeti araştıran, bilirkişi raporu hazırlayan, özellikle birilerinin yalan söyleme ihtimalinin olduğu durumlarda ortaya çıkan, bireylerle çok detaylı mülakatlar yaparak gerçeği ayrıntılarıyla ortaya koymaya çalışıp olası hile ve dolandırıcılık durumlarını ortaya çıkarmayı amaçlayan denetim alanına adli denetim adı verilmektedir.

Ek olarak kurum içindeki varlıkların korunması kapsamında da adli denetim faaliyetleri yapılmaktadır. Örneğin banklardaki teftiş kurumunun başlıca olarak şubelerdeki gerçekleştirdiği denetim ve soruşturmalar şirket varlıkları üzerinde gerçekleştirilen yolsuzluk ve hilelerin tespit edilmesine yöneliktir.

3.3.7. Özel Amaçlı Denetim

Yukarıdaki denetim alanlarının dışında özel olarak amaçlarının belirlenip gerçekleştirildiği denetim çalışmaları da bulunmaktadır. Bu kapsamda gerçekleştirilen denetim faaliyetlerine özel amaçlı denetim adı verilmektedir. Örneğin bilgi sistemleri denetim kategorisi altında değerlendirilecek olursak, üçüncü taraf firmalardan alınan destek hizmetlerine yönelik denetim faaliyetleri veya bilgi sistemleri adli denetim faaliyetlerinden bahsedilebilir.

Örneğin AICPA ("Uluslararası Muhasebe Uzmanları Federasyonu"), SAS70 standartları ile bilgi sistemlerine yönelik servis sağlayan organizasyonların iç kontrollerinin değerlendirilmesine yönelik profesyonel olarak incelemeye alınacak denetim standartlarını belirleniş bulunmaktadır. Bu kapsamda yapılan bir denetim çalışması bilgi sistemleri denetim faaliyeti alanında yapılan özel amaçlı bir denetim alanı olarak adlandırılmaktadır[40].

3.4. Bilgi Sistemleri Denetiminin Amaçları

Bilgi sistemleri denetimini kısaca kurumların sahip oldukları bilgi sistemlerini ve bilgi teknolojileri kaynaklarını değerlendirmesi olarak tanımlayabiliriz. Yaşadığımız bilgi çağının gereği olarak bireysel ya da kurumsal ekonomik her türlü gelişme internet ve bilgi teknolojileri sistemlerine daha da fazla bağlı hale gelmektedir. Bunun en doğal sonucu olarak da bilgi

[40] Johnson, **age**, 24

sistemleri üzerindeki riskler daha fazla fark edilmekte ve önemli olarak görülmektedir. Bilgi sistemleri üzerindeki güvenlik açıkları ya da hatalar ciddi iş krizlerine ve itibar kayıplarına yol açabilmektedir. Bu sebeple bilgi teknoloji sistemlerinin ve kaynaklarının karşı karşıya olduğu riskler belirlenerek bu risklere karşı gerekli kontrol süreçleri geliştirilmelidir. Bu aşamada diyebiliriz ki, bilgi sistemleri denetiminin temel amacı, bilgi sistemleri ve kaynaklarına yönelik mevcut kontrol standartlarını, politikalarını ve süreçlerini incelemek ve bu kapsamda bilgi teknolojileri risklerini azaltabilecek ek kontrolleri tanımlamaktır.

Risk odaklı bilgi sistemleri denetimin gerçekleştirilmesi, tespit edilen risklere karşı tasarlanan kontrollerin eksik taraflarının tespiti, bu kontrol eksikliklerinin ortaya çıkma koşulları ve nedenleri ile bu eksikliklerin kurumun operasyonel faaliyetlerine etkilerinin bir arada değerlendirildiği bir denetim sürecinin gerçekleştirilmesi bilgi sistemleri denetiminin esas amacını oluşturmaktadır.

3.5. Bilgi Sistemleri Denetiminin Organizasyon İçindeki Yeri ve Önemi

Yaşadığımız bilgi çağının ve küreselleşmenin bir sonucu olarak artan rekabet, bilginin önemini de artırmıştır. İşletmeler bu rekabet ortamında ayakta kalabilmek ve koşullara olabildiğince çabuk tepki verebilmek için detaylı bilgi ve raporlama sistemlerine ihtiyaç duymaktadırlar. Bilgi sistemi; planlama, kontrol, koordinasyon, analiz ve karar verme için bilgi toplama, saklama ve yayma amacıyla birlikte çalışan ve birbiriyle ilişkili unsurlar topluluğudur. Tümleşik bilgi sistemi olan yönetim bilgi sistemleri ise, bir işletmenin muhasebeden insan kaynaklarına kadar tüm fonksiyonlarını birbirleriyle ilişkilendiren ve fonksiyonlar arasında bilgi alış-verişini sağlayan sistemlerdir. Bu noktada kurumun amaçlarına göre hareket edip stratejik ve operasyonel hedeflerini mevcut rekabet ortamında gerçekleştirebilmesi için etkini ve verimli çalışıp güvenilir bilgi sunan bir bilgi sistemlerinin önemi büyüktür.

Bu noktada temel işlevi yöneticilerin karar almalarına yardımcı olacak bilgileri sağlamak olan muhasebe, yönetim bilgi sistemlerinin odağı konumundadır. Gelişen bilgi teknolojileri ve yönetim bilgi sistemleri muhasebe sistemlerinde de değişiklikler meydana getirmektedir. Önceleri bilgisayar yazılımları sadece muhasebede defter tutma ile devlet birimlerine verilecek beyanname ve bildirgeleri düzenleme amacıyla kullanılırken, daha sonra stok kontrolü, müşteri takibi, çek-senet, bordro, banka hesaplarının takibi işlevlerine de sahip bütünleşik uygulamalar diğer bir ifadeyle sistemler kullanılmaya başlanmıştır. B noktada işletmelerin bütün bölüm ve

fonksiyonlarını bir bilgisayar sisteminde tümleşik hale getiren "SAP", "Oracle e-Business Suite" gibi Kurumsal Kaynak Planlaması uygulamaları geliştirilmiştir. Bu noktada bankacılık faaliyetleri göz önüne alındığında bankaların da kendi içlerinde ana bankacılık sistemleri geliştirerek kurumsal kaynaklarını yönettiği gözlemlenmektedir. Bu sistemler sayesinde işletmeler bütün fonksiyonlarını bütünleşik ve eş zamanlı hale getirebilmekte ve hedeflerine uygun olarak işletme faaliyetlerini yönlendirebilmektedirler.

Bilgi sistemlerinin ve kaynaklarının işletme açısından stratejik önemi yukarıdaki açıklamalar üzerinde anlaşıldıktan sonra bu süreç üzerindeki risklerin yönetilmesinin de işletme için ne kadar önemli olduğu da bir o kadar açıklanmış olmaktadır.

Bilgi her işletme için kritiktir ve çoğunluğu bilgi teknolojileri ve uygulamaları vasıtasıyla oluşturulur, işlenir, iletilir ve saklanır. Örneğin, işletme içindeki verimlilik artışı ve büyümenin sonucu olarak mevcut bilgi teknolojileri sistemi talebi karşılayamayacak duruma gelebilir. Bunun doğal sonucu olarak da işletme rekabet üstünlüğünü bilgi sistemlerinin performans yetersizliği nedeniyle kaybedebilir. Bu örnekte de görüldüğü gibi bilgi teknolojilerinin karşı karşıya olduğu riskler ile iş riskleri birbiriyle örtüşür hale gelmektedir.

Bu sebepledir ki, bilgi teknolojileri riskleri kurumdaki tüm risklerin bir parçası olarak belirlenmeli, ölçülmeli ve yönetilmelidir. Bu kapsamda bilgi risklerini yönetmek ve dengelemek için uygulanan yaklaşıma bilgi teknolojileri risk yönetimi adı verilmektedir ve bilgi sistemleri denetiminin ön fazlarından birini oluşturmaktadır. Risk odaklı bilgi sistemleri denetimi, mevcut risklerin değerlendirilmesi ile birlikte bilgi sistemlerindeki olası kontrol eksikliklerinin belirlenip önlem alınması açısından kurum içinde hayati bir öneme ve yere sahiptir.

3.6. Bilgi Sistemleri Denetiminin Finansal Denetim Üzerindeki Etkileri

Günümüzde bilgi teknolojilerinin kullanımının artması faaliyetlerin yürütülme şeklini ve üzerindeki kontrol noktalarını etkilediği gibi denetim sürecini etkilemiş bulunmaktadır. Denetim süreç ve yöntemlerinde ihtiyaca yönelik olarak değişiklikler olsa da, denetimin nihai amacı ve kapsamında bir değişiklik olmamıştır. Buna göre dış denetim açısından denetçilerin amacı finansal tabloların gerçeği, doğru ve dürüst bir şekilde genel kabul görmüş muhasebe ilkelerine ve diğer düzenlemelere uygun bir şekilde yansıtıp yansıtmadığı konusunda bir görüş bildirmektedir. Bu noktada bilgi teknolojiler denetimi ile finansal dış denetim açısından temel

denetim amaçları açısından bir fark bulunmamakta sadece denetim sürecindeki yeni ihtiyaçlara yönelik eklemeler bulunmaktadır.

Bu noktada öncelikle temel denetim ihtiyaçlarını açıklayarak finansal denetim ve bilgi sistemleri denetimi arasındaki ilişki ifade edilmeye çalışılacaktır[41].

1. *Meydana Gelme*: Yönetimin öne sürdüğü iddialara uygun olarak bilançoda varlıkların, yükümlülüklerin ve öz kaynakların bilanço tarihinde gerçekten var olup olmadıkları ve gelir tablosunda yer alan gelir ve giderlerin de aynı şekilde ilgili muhasebe dönemine ait olarak var olup olmadıklarının tespit edilmesidir.

2. *Bütünlük*: Finansal tablolarda gösterilmesi gereken tüm işlemlerin ve hesapların, eksiksiz ve tam bir şekilde temel finansal tablolarda yer alıp almadığının tespit edilmesidir. Örneğin gerçekleşen fakat gelir tablosundaki satışlar bölümünde gösterilmeyen tutarlar bütünlük amacının ihlalini doğuracaktır.

3. *Değerleme veya Dağıtım*: Finansal tablolarda yer alan varlıkların, yükümlülüklerin, öz sermayenin, gelirlerin ve giderlerin finansal tablolarda uygun ve doğru tutarlarda gösterilip gösterilmediğinin tespit edilmesidir. Örneğin yıpranma payı giderlerinin doğru hesaplanıp ayrıldığının kontrolü bu amaca hizmet etmektedir.

4. *Hak ve Yükümlülükler*: Finansal tabloların hazırlanma tarihi itibariyle yönetim tarafından finansal tablolarda gösterilen varlıkların işletmenin hakları olup olmadığının ve finansal tablolarda gösterilen borçların da yine aynı işletmenin yükümlülükleri içerisinde olup olmadığının belirlenmesidir.

5. *Sunum ve Açıklık*: Finansal tablo unsurlarının genel kabul görmüş muhasebe standartlarına ve ilkelerine uygun olarak sınıflandırıldığının, tanımlandığının ve açıklandığının tespit edilmesidir. Örneğin kısa dönem olan bir borcun uzun dönem borçlar altında bilançoda gösterilesi bu denetim amacındaki kural ihlaline bir örnektir.

Genel olarak denetim süreci içerisinde finansal tabloların doğruluğu ile ilgili olarak meydana gelme, bütünlük, yetki, değerleme, dönemsellik, uygunluk ve etkinlik kapsamındaki kontrol noktaları üzerinde incelemeler yapılmaktadır. Finansal denetimde, günümüz teknolojisinin bir

[41] Brenda Porter, Jon Simon, David, Hatherly, "**Principles of External Auditing**" (USA: John Wiley & Sons, 1996), 298

ihtiyacı olarak destek olan bilgi sistemleri denetiminin de temel amacı bağımsız denetim açısından budur.

Bağımsız denetçiler işletme içinde finansal tabloları oluşturan sürecin bilgi sistemlerine bağlı olmasına veya manüel olmasına bakılmaksızın yukarıdaki temel amaçlara uymak için aşağıdaki denetim süreci adımlarına uymak zorundadırlar[42]:

1. *Müşteri seçimi, işin alınması ve sözleşme yapılması*: Müşteri firmanın faaliyetlerinin ve içerisinde bulunan endüstri dalının özellikleri anlaşılmalıdır. Analitik incelemeler sonucunda denetim risk alanlarının ve denetim riskinin derecesinin belirlenmesi gerekmektedir. Bu noktada firmanın bilgi teknolojilerini yoğun kullanıldığı düşünüldüğünde bilgi teknolojileri riskleri de temel amaçlar kapsamında değerlendirilmelidir. Sonrasında firmanın iç kontrol sisteminin ve buna bağlı muhasebe sisteminin etkinliği değerlendirilmelidir. Son olarak denetim kaynaklarının yeterliliği işin kalitesi açısından değerlendirilmeli ve denetimin sınırları ve kapsamı belirlenmelidir. Tüm bu faaliyetler gerçekleştirildiğinde müşteri ile gerekli şartları içeren bir sözleşme denetim çalışması öncesinde imzalanmalıdır.
2. *Planlama ve içerindeki programların hazırlanması*: Müşteri hakkında elde edilen bilgiler, analitik inceleme sonucunda ulaşılan sonuçlar ve iç kontrol sisteminin özellikleri baz alınarak bir denetim planı oluşturulmalıdır. Bu aşamada planlama yaparken aşağıdaki aşamaları sırasıyla gerçekleştirmek gerekmektedir:
    a. Müşteri işletmeyi tanıma ve hakkında bilgi toplanması: İşletme hakkında genel ve tarihi bilgiler, muhasebe ve iç kontrol sistemine ait bilgiler ve işletmenin çevresi ile ilişkilerine yönelik bilgiler toplanıp incelenmektedir.
    b. Denetim çalışmalarının bölümlere ayırma: Belirli bir yaklaşıma göre denetim çalışmaları bölümlere ayrılmalıdır. Örneğin faaliyetler ön plana alınarak hasılat işlemleri, harcama işlemleri, sabit varlıklar işlemleri, stok ve üretim işlemleri ve finansman işlemleri şeklinde bölümler oluşturulabilir.

[42] Kepekçi, **age**, 31

c. Denetim amaçlarını tespit etme: Önceki bölümlerde açıkladığımız temel denetim amaçları ile yönetimin iddiaları arasındaki ilişkiler kurularak denetime yönelik kontrol hedeflerinin belirlenmesi yapılmaktadır.

d. İç kontrol sistemini inceleme ve değerlendirme: Etkin bir iç kontrol ortamı ile denetimin kapsamı ters orantılı olacağından değerlendirilmesi büyük bir önem taşımaktadır. Etkin bir iç kontrol ortamının değerlendirilmesi sonucu denetim sırasında kritik kontrol testlerine ağırlık verilerek zaman alıcı maddi doğruluk testleri de bir o kadar azalarak denetim süresi kısaltılabilecektir.

e. Denetim riskini tespit etme: Denetim riski içinde olumsuz yanlışlıklar ve düzensizlikler olduğu halde ilgili finansal tablolar hakkında olumlu görüş verme olasılığına verilen isimdir. Bu aşamada yapısal risk, kontrol riski ve bulgu riski değerlendirilerek denetim riski belirlenmektedir. Yapısal risk, iç kontrol sisteminin olmadığı varsayıldığında, hazırlanan finansal tabloların ve bu finansal tablo kalemlerinin kendi özelliğinden veya şirketin yapısal özelliğinden dolayı kendiliğinden yanlış olma olasılığıdır. Kontrol riski ise, iç kontrol sisteminin etkinliğine bağlı olarak finansal tabloların hatalı olma olasılığına verilen isimdir. Son olarak bulgu riski ise, bağımsız denetim firmasının finansal tablolardaki var olan önemli hata ve düzensizlikleri belirlenen kapsamda ortaya çıkaramama olasılığıdır.

f. Önemlilik sınırının tespit edilmesi: Önemlilik muhasebe bilgilerinde bulunan herhangi bir hatanın veya düzensizliğin, mali tablo kullanıcılarına verebileceği kararları etkileme derecesidir. Bu noktada önemlilik sınırının diğer bir ifadeyle kabul edilebilir hata düzeyinin belirlenmesi olası tespitlerin değerlendirilmesi için hayati öneme sahiptir.

g. Denetim programlarının taslağının hazırlanması: Denetim sahasında yapılacak işleri ve uygulanacak prosedürleri gösteren ve açıklayan dokümanlara iş programları adı verilmektedir. Denetim süreci içerisinde test aşamasına gelmeden önce bu programların düzenli olarak hazırlanması gerekmektedir.

h. İş gücü planlaması: Denetim çalışmasının kaliteli olarak yapılmasını sağlayacak iş gücü planlaması yapılması ve denetim sözleşmesi içinde yer verilmelidir.

i. Zaman planlaması: Son olarak, denetim süreci içerisinde testlerin etkin ve zamanında gerçekleştirilmesi için uygun zaman planın da yapılması ve denetim sözleşmesi içinde yer verilmesi gerekmektedir.

3. *Test etme sürecinin gerçekleştirilmesi*: İç kontrol süreçlerinin test edilmesi ve muhasebe verilerinin geçerliliği, bütünlüğü ve doğruluğunu güvence altına alıp almadıkları test edilerek incelenmelidir. Bu noktada bilgi teknolojilerine dayanan kontroller de tespit edilip bilgi teknolojileri denetçileri tarafından test edilmelidir. Kontrol testlerinin sonrasında hesap bakiyelerinin ve işlemlerin maddi doğruluk testlerinin gerçekleştirilmesi gerekmektedir. Son olarak test çalışmalarının tamamlanması ve gözden geçirilmesi gerekmektedir.

4. *Denetimin tamamlanması ve raporlanması*: Son olarak sonuçların değerlendirilmesi, müşterinin bilgilendirilmesi ve raporlanarak ilgili mercilere dağıtımı için tespitlerin raporlanması ve bağımsız görüşün belirlenmesi gerekmektedir.

Günümüzde bilgi sistemleri yoğun olarak kullanılan işletmelerde doğal olarak yukarıda belirtilen denetim adımlarının nasıl yürütüleceğini etkilenmekte ve bunun doğal bir sonucu olarak denetim süreci kapsamının içine bilgi sistemleri denetimi de dahil olmaktadır. Yukarıda belirtilen denetim adımlarının temel olarak içeriğinde ve amaçlarında bir değişiklik olmamakta birlikte, bilgisayar teknolojisinin yaygınlaşması ve buna bağlı olarak denetim süreçlerinde bilgisayar teknolojisinin bir araç olarak kullanılması denetim sürecinin etkin yürütülmesinde bir ihtiyaç olarak doğmakla birlikte, zaman ve iş gücü planlaması açısından da faydası dokunmuştur.

Sonuç olarak, günümüzde bilgi çağında ve küreselleşmenin getirdiği rekabet ortamında bilgi teknolojileri işletmelerin faaliyetlerinin ayrılmaz bir parçası olduysa aynı şekilde ihtiyaca paralel olarak bilgi sistemleri denetimi de finansal denetimin ayrılması bir parçası haline dönüşmüştür.

3.7. Bilgi Sistemleri Denetim Standartları ve Prensipleri

Bilgi sistemleri denetimi ile ilgili olan faaliyetleri düzenleyen standart ve prensipleri temel olarak üç grupta inceleyebiliriz. Bu noktada bilgi teknolojileri denetçisi kaliteli bir denetim faaliyeti yürütebilmek için işlemlerinde öncelikle;

1. Genel kabul görmüş denetim ilkeleri ve denetim standartlarına uyması,

2. ayrıntılı denetim çalışmaları için uzmanlarca hazırlanmış denetim standartları ve işlemlerine uyması,
3. son olarak ise bilgi teknolojisi süreçlerinin zorunlu kıldığı denetim tekniklerini kullanması gerekmektedir.

Genel kabul görmüş denetim ilkeleri ve denetim standartları, her bir denetim faaliyeti için denetçilere ayrıntılı olarak yol gösteren ve onlara denetim sırasında neler yapmaları, hangi denetim işlemlerine başvurmaları gerektiği gibi hususlarda ayrıntılı bilgi veren standartlar olmasa da, tüm denetim çalışmalarında olduğu gibi genel belirleyici özelliğe sahip bu standartlara uyulması gerekmektedir. Genel kabul görmüş denetim ilkeleri ve denetim standartları, denetim çalışmasının yürütülmesi, bulguların elde edilmesi ile ilgili genel kabul görmüş standartlardan oluşmaktadır. Buna göre üç ana grupta bu standartlar toplanabilmektedir[43]:

1. *Genel standartlar*: Bu standartlar denetçi ile onun çalışmasın kalitesi ile ilgili standartlardan oluşmaktadır. Mesleki eğitim ve yetkinlik standardı, bağımsız davranabilme standardı ve mesleğin gerektirdiği özenin gösterilmesi standardından oluşmaktadır.
2. *Çalışma sahası standartları*: Çalışma sahası standartları ise dış denetçi tarafından denetim çalışmalarında izlenecek yöntemleri gösterir. Denetimin ne şekilde, hangi önceliklerde ve hangi yöntemlerle yapılacağı çalışma sahası standartları ile belirlenir. Bu standartlar planlama ve gözetim, iç kontrol sisteminin incelenmesi ve kanıt toplamaya ilişkin standartlardan oluşur.
3. *Raporlama standartları*: Raporlama standartları denetim sonucunda varılan görüşün açıklandığı raporların kapsam ve düzenlemeleriyle ilgili standartlardır. Genel kabul görmüş denetim on denetim standardından dördü denetim raporunun konusunu içermektedir. Bunlar, genel kabul görmüş muhasebe ilkelerine uygunluk standardı, genel kabul görmüş muhasebe ilkelerine değişmezlik standardı, mali tablolardaki açıklamaların yeterliliği standardı ve görüş bildirime standardıdır. Görüldüğü gibi görüşün alınması gerektiği konuların raporda yer alması ve görüşün nasıl belirtileceği ile ilgili tüm maddeler raporlama standartlarına göre belirlenmiş durumdadır.

[43] Duman, **age**, 44

Bilgi teknolojileri ile ilgili denetim standartları söz konusu olduğunda AICPA ("Uluslararası Muhasebe Uzmanları Federasyonu"), IIA ("İç Denetim Derneği") ve ISACA ("Bilgi Sistemleri Denetimi ve Kontrolü Derneği") adlı üç kuruluşun çalışmaları göze çarpmaktadır.

Amerika Birleşik Devletleri sınırlarında resmi bir meslek kuruluşu olarak yaptırım gücüne sahip olan AICPA, denetim faaliyetlerinin yürütülmesinde belirleyici rol oynamaktadır. Kuruluş oluşturduğu denetim standartları, denetim yorumları ve denetim el kitapları ile denetim mesleğinin icrasında rehberlik teme görevini üstlenmiştir. Bilgi sistemlerinin denetimi ve ilgili faaliyetleri kapsamında AICPA bünyesinde "*Bilgisayar Denetimi Alt Komitesi*" kurulmuştur[44]. Planlama ve denetim stratejilerinin belirlenmesi, denetimin yürütülmesi ve tamamlanması ve denetim sonuçlarının ve raporların iletimi ile ilgili olarak bilgi sistemleri denetimine dolaylı veya dolaysız yoldan yol gösterecek standartlar oluşturulmuştur.

AICPA gibi resmi kurumların yanında İç Denetim Derneği gibi bir sivil toplum kuruluşu bilgi teknolojileri faaliyetlerini de kapsamına alacak standartlar geliştirmiştir. Bu kapsamda oluşturulan denetim standartlarının bazıları şöyledir[45]:

1. *310 Bilginin Güvenilirliği ve Bütünlüğü*
2. *320 Politikalar, Planlar, Kanunlar ve Düzenlemelere Uyumluluk*
3. *330 Varlıkların Korunması*
4. *340 Kaynakların Ekonomik ve Etkin Kullanılması*
5. *Faaliyet veya Programlar için Belirlenmiş Amaç ve Hedeflerin Gerçekleştirilmesi*

Son olarak sivil toplum kuruluşlarından biri olan Bilgi Sistemleri Denetimi ve Kontrolü Derneği ("ISACA") de bilgi sistemleri denetiminin standartlarına yönelik çalışmalar oluşturmuş ve birçok araştırma gerçekleştirmiştir. Bu kapsamda bilgi sistemleri denetimine yönelik olarak 16 standart ve 40 adet bilgi sistemleri denetim prensipleri belirlemiştir. Belirlenen bilgi sistemleri standartları, şu şekilde sıralanıp açıklanabilmektedir[46]:

1. *Denetim Tüzüğü*: Bilgi sistemleri denetim fonksiyonunun amacını, sorumluluğunu, otoritesini ve yerini tanımlayan standarttır.

[44] Saka, **age**, 78
[45] AICPA, **Audit Standards**, www.aicpa.org [03.03.2009]
[46] ISACA, **IT Audit Standards**, http://www.isaca.org/Template.cfm?Section=Standards&CONTENTID=47286&TEMPLATE=/ContentManagement/ContentDisplay.cfm [03.03.2009]

2. *Bağımsızlık*: Bilgi sistemleri denetçilerinin profesyonel anlamda ve organizasyon içindeki bağımsızlıklarını tanımlayan standarttır.
3. *Profesyonel Etik ve Standartlar*: Bilgi sistemleri denetçisinin görevlerini yerine getirirken uymaları gereken profesyonel etik kuralları belirleyen standarttır.
4. *Profesyonel Yeterlilik*: Bilgi teknolojileri denetçisinin profesyonel anlamada görevlerini yerine getirmek için sahip olması ve sürdürmesi gereken yetkinliği açıklayan standarttır.
5. *Planlama*: Risk odaklı bilgi sistemleri denetiminin nasıl planlanması ve yürütülmesi gerektiğini açıklayan standarttır.
6. *Denetim Çalışmasının Gerçekleştirilmesi*: Bilgi sistemleri denetiminin yürütülmesi, kanıt toplanması ve çalışma kağıtlarının hazırlanması ile ilgili açıklayan standarttır.
7. *Raporlama*: Bilgi sistemleri denetim sonuçlarının raporlanması ile ilgili açıklamayı yapan standarttır.
8. *Takip Çalışmaları*: Bilgi sistemleri denetim sonucunun raporlanması sonrası bulguların ve tavsiyelerin gerekli aksiyon planlarına göre takibinin yapılmasını açıklayan standarttır.
9. *Uyumsuzluklar ve Yasal Olmayan Durumlar*: Denetim riski kapsamında bilgi sistemleri denetiminde olası uyumsuzlukların ve yasal olmayan durumların değerlendirilmesi ile ilgili olan standarttır.
10. *Bilgi Teknolojileri Yönetişimi:* Organizasyon hedefleri ile uyumlu bir bilgi teknolojileri yönetiminin tesisi ile ilgili açıklamada bulunan standarttır.
11. *Denetim Planında Risk Değerlendirmesinin Kullanımı*: Bilgi sistemleri denetim faaliyetlerinin planlanması öncesinde risk değerlendirmesinin kapsamını açıklayan standarttır.
12. *Denetimde Önemlilik*: Bilgi sistemleri denetiminde önemlilik kavramının değerlendirilmesi ve denetim riskinin belirlenmesi ile ilgili açıklamaları yapan standarttır.
13. *Başkalarının Denetim Çalışmalarını Kullanma*: Bilgi sistemleri denetimi sırasında başkalarının (örneğin iç denetim çalışmaları) çalışmalarının değerlendirilmesi ve kullanılması ile ilgili açıklama yapan standarttır.

14. *Denetim Kanıtları*: Bilgi sistemleri denetimi sonucunun güvenilir olarak verilmesi için yeterli ve güvenilir kanıt toplama ile ilgili açıklamaların yapıldığı standarttır.
15. *Bilgi Teknolojileri Kontrolleri*: İç kontrol sisteminin bir parçası olarak bilgi teknolojileri kontrollerinin incelenmesi ve değerlendirilmesi ile ilgili açıklamaları yapan denetim standardıdır.
16. *Elektronik Ticaret*: Son olarak elektronik ticaret ile ilgili olarak uygun kontrollerin belirlenmesi ve incelenmesi ile ilgili açıklama yapan denetim standardıdır.

Son olarak ise bilgi teknolojisi süreçlerinin zorunlu kıldığı denetim tekniklerini kullanması gerekmektedir. Bu noktada yukarıda bahsetmiş olduğumuz denetim standartlarının yanında incelenen bilgi sistemlerine göre özel olarak hazırlanmış denetim tekniklerinin bulunduğu denetim programları mevcuttur. Örneğin SAP kurumsal kaynak planlaması sistemi inceleniyorsa, bilgi teknolojileri genel kontrol ortamının denetimi için hazırlanmış özel denetim programları da kullanılabilmektedir.

3.8. Bilgi Sistemleri Denetiminde Risk Analizi

Bilgi sistemleri denetiminde risk analizini açıklamadan önce risk kavramını tanımlamak yerinde olacaktır. Risk genel anlamıyla zarar verici bir aktiviteye açık olma potansiyeli olarak tanımlanabilmektedir. Tehditler, zayıflıklar, etkiler ve olabilirlik riskin bileşenleri olup risk analizi sırasında incelenmesi gereken unsurlardır.

Bilgi sistemleri riski ise, iş süreçlerini olumsuz yönde etkileyecek şekilde bilgi sistemi uygulamalarının, ağ veya diğer kritik bilgi teknolojileri kaynaklarının kaybedilmesi olasılığıdır.

Bilgi teknolojileri riskleri genel olarak iş organizasyonu ile ilişkili diğer iş risklerinin içinde yer almakta ve bir bütünlük arz etmektedir. Örneğin, bir işletmenin değişen iş şartlarının zorunlu kıldığı ve bilgi sistemlerinin altyapısında gerekli görülen değişiklikler, sistemin beklenmedik ve geri getirilemeyecek bir şekilde çökmesi riski ile sonuçlanabilir. Bu da işletmenin faaliyetlerinin aksaması eve dolayısıyla gelir kaybı ile sonuçlanabilmektedir. Özellikle günümüz işletmelerinin veri ve bilgi teknolojileri altyapılarına artan bağımlılıkları sebebiyle, bilgi teknolojileri risklerinin iş riskleri yönetim stratejileri içerisinde ele alınması yaygın olarak benimsenmektedir. Bu sebepledir ki, bilgi teknolojileri riskleri kurumdaki tüm risklerin bir parçası olarak belirlenmeli,

ölçülmeli ve yönetilmelidir. Bu kapsamda, bilgi risklerini yönetmek ve dengelemek için uygulanan yaklaşıma ise bilgi teknolojileri risk yönetimi adı verilmektedir.

Çeşitli kuruluşlarca bilgi teknolojileri risk yönetimi alanında birçok uluslararası standart ve yaklaşıp hazırlanmış olup organizasyonlarda uygulanabilmesi için sunulmuştur. Bunlardan bazılar COBIT, ITIL, ISO 27001 olup temelde bilgi teknolojilerinin risklerinin belirlenip yönetilmesi ile ilgili aynı hedefleri öngörmektedirler.

Bilgi teknolojileri risk yönetimi kısaca, riskin belirlemesi, değerlendirmesi ve belirlenen risklerin kabul edilebilir bir seviyeye indirmesi için aksiyon alması süreçlerinden oluşmaktadır. Bilgi sistemleri risk yönetimini, her biri farklı öneme sahip ancak birbirini etkileyen ve destekleyen altı temel fonksiyonla yerine getirilmesi mümkündür[47]:

1. *Risk Yönetim Çerçevesinin Oluşturulması ve İş Riskleri ile Bilgi Teknolojileri Risk Yönetimi Arasındaki Uyumun Sağlanması*: Bilgi teknolojilerinin yönetimi, risk yönetimi ve kontrol yapısının; organizasyonun iş risklerini yönettiği yapı ile bütünleşik bir çerçevede incelenmesi gerekmektedir. Kritik bilgi sistemleri değerlerini belirlemek için bilgi teknolojileri, ilgili iş süreçleri yöneticileri, denetçiler bir araya gelerek ortak bir çalışma yapması gerekmektedir. Bilgi sistemleri zayıflıklarının belirlenmesi, ilgili risklerin önceliklendirilmesi ve uygun risk karşılama stratejisi geliştirmek ve gerçekleştirmek iş ve bilgi teknolojileri taraflarında uyumlu bir çalışmaya ihtiyaç vardır. Kurum genelinde bu yapının tasarlanıp uygulanması bilgi teknolojileri risk yönetiminde atılan ilk adım olacaktır.
2. *Bilgi Teknolojileri Risklerinin Belirlenmesi*: Organizasyonun işle ilgili, düzenleyici, hukuksal, teknolojik, ticari ortaklık, insan kaynakları ve operasyonel alanlardaki hedeflerinde ya da operasyonlarında potansiyel olarak olumsuz etki yaratabilecek olayların ve risklerin belirlenmesi bu adım altında yapılmaktadır. Bilgi teknolojileri risk alanları çok çeşitli olup her biri organizasyonun yapısına göre belirli olaylara göre değerlendirilip maruz kalınan riskler belirlenmelidir. Bu risk alanlarından bazılarını açıklarsak;

[47] Barış Bağcı, **Bilgi Teknolojileri Risk Yönetimine Genel Bakış**, (İstanbul: Deloitte Touche Tohmatsu, 2007), 4-5

a. Bilgi teknolojileri yönetim ve strateji riski: Bilgi teknolojileri stratejilerinin iş stratejileri ile uyumlu olmaması ve paylaşılmaması sonucu bilgi teknolojilerinin iş tarafı ile uyumlu bir birim olarak çalışamaması riski

b. Bilgi teknolojileri beceri ve teknolojik gelişme riski: Bilgi teknolojilerinin işletmeyi sektörün önde gelenleri arasında tutacak ve iş yeteneklerini geliştirecek yenilikleri gerçekleştirmek konusunda başarısız kalması riski

c. Bilgi teknolojileri mimari riski: Bilgi teknolojilerinin iş birimlerinin ihtiyaçlarının verimli, maliyet-etkin ve iyi kontrol edilebilir şekilde olmasını destekleyecek etkin, standart ve sürdürülebilir alt yapısının olmaması riski

d. İş sürekliliği riski: Bilgi teknolojilerinin iş tarafına destek olan kritik operasyon ve süreçleri devam ettirememesi riski

e. Uyumluluk riski: Bilgi teknolojilerinin yasal düzenleyicilerin gerekliliklerini yerine getirecek desteği iş tarafına verememesi riski

f. Bilgi teknolojilerine yönelik kaynak riski: Bilgi teknolojilerine ait olan insan ve finansal kaynaklarını gerekli planlamayıp yapamayıp verimli olarak yönetememesi riski

g. Tedarikçi yönetim riski: Bilgi teknolojileri ile ilgili olarak organizasyonların tedarik, dış kaynak alım ve servis sağlayıcılar ile uygun ilişki kuramaması ve bu ilişkileri yönetememesi riski

h. Proje geliştirme riski: Bilgi teknolojilerinin olumsuz proje planlaması ve yönetimi sonucu iş tarafında oluşan riskler

i. Bilgi teknolojilerine yönelik itibar ve müşteri memnuniyeti riski: Bilgi teknolojileri bölümünün, iş isteklerini, hizmet seviyesi anlaşmalarını ve desteğini uygun şekilde karşılayamaması riski

j. Bilgi riski: Hassas ve önemli iş bilgilerinin uygun şekilde yönetilememesi ve saklanamaması riski

k. Bilgi teknolojileri güvenlik riski: Bilgi teknolojileri alt yapısı ve kaynaklarının güvenlik tehditlerine karşı korunamaması ve bilginin gizli bilgilerin açığa çıkması veya değiştirilmesi riski

3. *Bilgi Teknolojileri Risk Analizinin Yapılması*: Her risk, bilgi sistemleri değerinin gizliliği, bütünlüğü veya erişilebilirliğini olumsuz yönde etkileyen belirli bir tehditle ilişkilidir. Tehdit ise, zarar oluşması olasılığı olarak değerlendirilebilir. Bu aşamada tehdide olan açıklık ise, bilgi sistemi kaynakları ve/veya süreçleri için tehdidin gerçekleşmesine sebep olabilecek bir zayıflıktır. Bu kavramların yanında etki ve olabilirliğin de değerlendirilmesi ile bilgi teknolojileri risk analizi yapılabilmektedir. Etki, tehdidin zayıflıktan yararlanarak oluşturduğu olaya ilişkin maliyet olarak adlandırılmaktadır. Olasılık ise tehdidin gerçekleşmesi olasılığıdır ve sistem mimarisi, sistem ortamı, bilgi sistemlerine erişim kontrolleri, motivasyon, tehdidin gücü, açıkların varlığı ve mevcut kontrollerin etkinliği gibi pek çok faktöre bağlıdır. Tehdit, tehdide açıklık, etki ve olasılıklar kapsamında, çeşitli nitel ve nicel yöntemler kullanarak, belirlenen tüm risklerin etkisi ve bu risklerin tekrar etme olasılıkları değerlendirilmektedir. Olayı doğası gereği mevcut riskler ile önlem sonrası öngörülen ya da geriye kalan riskler ile ilişkilendirilerek tüm risklerin oluşma olasılıkları ve etkileri değerlendirilmeli, analizi yapılmalıdır.

4. *Bilgi Teknolojileri Risk Değerlendirmesinin Yapılması*: İş süreçlerinin etkilendiği bilgi sistemleri üzerindeki tüm riskler, nasıl kontrol edilecekleri ve yönetilecekleri belirlenmek üzere analiz edilir. Uygulanan risk değerlendirme yapısının doğru sonuçlar vermeyi garanti ettiği bir kapsamın kurulması gereklidir. Bu kontrol, risk değerlendirmesinin hem iç hem dış kapsamının belirlenmesi, değerlendirmenin amacının belirlenmesi, risklerinin değerlendirildiği ölçütlerin belirlenmesini içermelidir. Kurumlar bilgi sistemleri risk değerlendirmelerinin yanı sıra risk yönetiminin izlenmesi faaliyetlerini de iç ve/veya dış denetçilere yaptırmaktadırlar. Yapılan değerlendirmeler sonucu riskler belirlenmekte ve tespit edilen bulguların düzeltilmesi aktiviteleri ile reaktif bir yaklaşım izlenmektedir[48].

5. *Bilgi Teknolojileri Risklerine Karşı Müdahale Planının Oluşturulması*: Risklerin analiz edilip değerlendirilmesinden sonra risk sahibinin ve etkilenen sürecin sahiplerinin de katılarak belirleyeceği bir risk müdahale planı oluşturulmalıdır. Risklere karşı tasarlanan

[48] John P. Pironti, "**Key Elements of an Information Risk Management Program**", Information Systems Control Journal, volume 2 (2008), 43

kontrollerin maliyeti ve risklerin yaratacağı zarar arasında optimum bir çözüm sağlayan bir risk müdahale planı hazırlanmalıdır. Risk müdahale planı içindeki risk tepkileri kaçınma, azaltma, paylaşma ya da kabul edilme gibi risk stratejilerini belirleyebilmektedir. Bu tepki geliştirilirken, kar ve zararlar göz önünde tutulmalı; artan riskleri, belirlenen risk toleransı seviyesinde sınırlayan bir tepki seçilmelidir. Riske müdahale yöntemleri aşağıdaki gibi sınıflandırılabilir:

a. *Azaltma*: Riske karşı ek kontroller tesis ederek riskin gerçekleşmesi sonrası etkisinin azaltılması amaçlanmaktadır. Örneğin iş sürekliliği riskine yönelik olarak ayrı bir merkezde hazır olarak bekleyen ikinci bir sistem hazırlaması ile çalışma merkezinde gelecek bir afette diğer merkeze bağlanıp işlerin devam ettirilebilmesi sağlanacaktır. Bu noktada riskin etkisi sadece merkezde meydana gelen zarar ve diğer merkezdeki sistemin ayağa kaldırılması sırasında geçen zaman olacaktır.

b. *Transfer*: Belirlenen riske karşı kontrol tesis ederek bu riskin başka taraflara devrinin amaçlamaktadır. Örneğin sistem odasındaki kritik cihazlar sigortalanarak olası bir maddi zararda tazmini sağlanabilmektedir. Bu örnekte risk sigorta şirketine devredilmiştir.

c. *Sakınma*: Belirlenen riske maruz kalmamak için riskin gerçekleşme olasılığının azaltılması veya yok edilmesi yolunu izleyen yöntemdir.

d. *Kabul Etme*: Son olarak belirlenen risk, riskten kaçınılması için gereken maliyetleri ve riski yaratan işin aynı zamandaki getirisi de göz önüne alındığında işletme tarafından olduğu gibi de kabul edilebilmektedir[49].

6. *Bilgi Teknolojileri Risk Yönetim Sürecinin İzlenmesi*: Her seviyedeki kontrol aktivitesinin, gerekli olduğunda tanımlanan risk tepkilerini gerçekleştirmek için (zararların, karların, uygulama sorumluluğunun tanımlanması gibi), planlanıp, öncelik sırasına konulması gerekmektedir. Önerilen eylemler için onay ve geri kalan riskler için kabul aranması ve ortaya konan eylemlerin etkilenen sürecin sahibine ait olduğunun garanti altına alınması gerekmektedir. Risk yönetiminde uygulanan bilgi teknolojileri müdahale planında herhangi bir sapma durumunda yürütülen plan ve raporların üst yönetime iletilmesi ve üst yönetimin bu noktadaki desteğinin de alınması çok önemlidir.

[49] ISACA COBIT, **age**, 64

Bankacılık Düzenleme ve Denetleme Kurumu ("BDDK") tarafından yayınlanan "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" uyarınca bankalara COBIT ("Control Objectives For Information and related Technology") çerçevesinde yer alan usul ve esaslar yasal mevzuat gereği uygulanmak zorundadır. Bu kapsamda COBIT'in önemli konu başlıklarından biri de "*Bilgi Sistemleri Riskinin Değerlendirilmesi ve Yönetimi*" kontrol hedefinin Türkiye'deki bankalarda uygulanmasıdır. COBIT çerçevesinde oluşturulan bilgi teknolojileri risk yönetimi genel olarak yukarıda da açıklandığı gibi risk yönetim çerçevesinin oluşturulması, risk kapsamının kurulması, olay belirleme, risk değerlendirme, risk yanıtlama ve risk aksiyon planlarının yürütülmesi ve izlenmesi faaliyetlerinden oluşmaktadır.

COBIT'in yanında BDDK tarafından yayınlanan "*Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ Taslağı*"nın 5. maddesinde yer aldığı üzere "bankalar, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri tanımlamalı, analiz etmeli, izlemeli ve yönetmek üzere gerekli önlemleri almalıdır" şeklinde bilgi teknolojileri risklerinin yönetiminin zorunluluğuna yer veren ifadeler de bulunmaktadır[50].

Bankaların, risk yönetimlerini ve politikalarını, bilgi teknolojilerinin kullanımına bağlı olarak gözden geçirmesi ve bilgi sistemleri kullanımından kaynaklanan risklerin yönetimini içerecek şekilde yenilemesi gerekmektedir. Bilgi teknolojilerinin yönetimi ve izlenmesine yönelik çalışmalardan edinilen veriler bankanın risk yönetim çerçevesinin bir parçası haline gelmeli ve bilgi teknolojilerinden kaynaklanan riskleri de içeren bütünleşik bir risk yönetim yaklaşımı uygulanmalıdır. Bankaların, kendi risk durumuna, kurumun operasyonel yapısına, yönetim kültürüne ve ilgili diğer yasal yükümlülüklerle belirtilen çerçeveye uygun olarak risk yönetimini oluşturulması ve bilgi teknolojileri risklerini de bu kapsamda değerlendirmeye alması gereklidir. Belirlenecek sıklıkta veya bilgi sistemlerindeki önemli değişikliklerden önce risk analizlerini tekrarlamalı ve analizlere ilişkin yazılı politikalar belirlemelidir.

Sonuç olarak, başarılı bir risk yönetim programı üst yönetimin sorumluluk almasına, bilgi teknolojileri ekibinin tam desteğine ve katılımına, risk değerlendirme ekibinin yetkinliğine, organizasyon üyelerinin farkındalığına ve işbirliğine bağlıdır. Risk değerlendirme ekibi belirlenen sistemler üzerinde risk değerlendirme yöntemlerini uygulayabilmeli, kritik riskleri

[50] BDDK, "**Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ**", (Madde 5, Sayı 26643; Tarih 14 Eylül 2007), 2

belirlemeli, organizasyona uygun ve ihtiyacı karşılayan maliyet-etkin uygulamalar önerebilmelidir.

3.9. İç Kontrol Sistemi

Genel olarak işletmenin amaçlarına sağlıklı bir biçimde ulaşmasının sağlayacak politikalara, prosedürlere ve usullere işletme için kontroller adı verilmektedir. İşletme içinde bu kontrollerin oluşturduğu yapıya ise genel anlamıyla iç kontrol yapısı adı verilmektedir.

3.9.1. İç Kontrol Sisteminin Tanımı ve Bankacılık Sektöründeki Yeri

İç kontrol, bir işletmenin yönetim kurulu üyeleri, yönetim ve diğer personeli tarafından etkilenen ve faaliyetlerin etkinliği ve verimliliği, finansal raporların güvenilirliği, uygulanabilir yasa ve düzenlere uygunluk amaçlarına ulaşmada dikkate alınacak yeterli güveni sağlamak üzere tasarlanmış bir süreçtir.

Uluslararası muhasebe uzmanları federasyonuna göre bir başka ifadeyle iç kontrol sistemini tanımlarsak; iç kontrol sistemi

- İşletmenin varlıklarının korunması
- Yanlışlıkları ve yolsuzlukların önlenmesi
- Muhasebe bilgilerinin doğruluk ve güvenilirliğinin sağlanması
- Muhasebe bilgilerinin zamanında hazırlanmasının sağlanması
- İşletme faaliyetlerinin yönetim politikalarına uygunluğunun sağlanması

amaçlarına ulaşmak için, işletme faaliyetlerinin düzenli ve etkin bir şekilde yürütülmesini sağlamada yardımcı olan, işletme yönetimi tarafından kabul edilmiş politika ve prosedürlerdir[51].

İşletmenin belirlenen amaçlarına ulaşması için, işletme yöneticilerinin almış olduğu önlemlere ve uyguladığı yöntemlere kontrol adı verilmektedir. İşletme faaliyetlerine yönelik olarak tesis edilen iç kontrol sistemi bünyesinde bulunan kontroller genel olarak üç türe ayrılabilir:

1. *Önleyici Kontroller*: İşletme faaliyetlerinde istenen amaca uygun olarak işlemlerin gerçekleştirilmesini, hataya veya eksikliğe sebep olabilecek aksi bir durumun gerçekleşmeden önlenmesini sağlayan kontrol türüdür. Örneğin, sistemde tanımlanan

[51] Duman, **age**, 68

mevduat faiz oranının üstünde şubeler tarafından faiz verilmesine sistemin izin vermesi gibi.

2. *Belirleyici Kontroller*: İşletme faaliyetleri ile ilgili olarak işlemlerin gerçekleşmesi sonrası olası hataları veya eksikleri sonradan tespitini sağlayan kontrol türleridir. Örneğin gün sonu kasa mutabakatı yaparak kasa açıklarının veya fazlalıklarının tespit edilmesi gibi.
3. *Düzeltici Kontroller*: İşletme faaliyetleri ile ilgili olarak işlemlerin gerçekleşmesi sonrası olası hataları veya eksikleri sonradan tespitini sağlamakla birlikte bu hata veya eksiklikleri düzelten kontrol türleridir.

İç kontrol sisteminin tanımını ve kontrol türlerini inceledikten sonra Türkiye Bankacılık sektörü içerisinde iç kontrol sisteminin yeri, amaçları ve iç denetim ile arasındaki ayrımı açıklık getirmek yerinde olacaktır.

Bankalarda iç kontrol sisteminin amaçları;

1. Bankanın varlıklarının korunmasını,
2. Faaliyetlerin etkin ve verimli bir şekilde Bankacılık Kanuna ve ilgili diğer mevzuata, banka içi politika ve kurallara ve bankacılık teamüllerine uygun olarak yürütülmesini,
3. Muhasebe ve finansal raporlama sisteminin güvenilirliğini, bütünlüğünü ve bilgilerin zamanında elde edilebilirliğini, sağlamaktır.

İç kontrol sistemi faaliyetleri; bankanın günlük tüm faaliyetlerinin bir parçasını oluşturur ve faaliyetlerin icrasına yönelik işlemlerin kontrolü, iletişim kanalları ile bilgi sistemlerinin ve finansal raporlama sisteminin kontrolü ve uyum kontrollerini kapsamaktadır.

İç kontrol biriminde bir yönetici ile bankanın ölçeği, faaliyetlerinin niteliği ve karmaşıklığına göre yeterli sayıda ve mesleki uzmanlığa sahip iç kontrol personeli görev yapar. Bununla birlikte iç kontrol personeli, iç kontrol faaliyetleri dışında bir faaliyette bulunamazlar.

İç kontrol sisteminin yanında banka içinde iç denetim işlevini gören bir bölüm de oluşturulmaktadır. Bankalarda iç denetim görevi, iç denetim birimi tarafından yürütülür. İç denetim biriminde; bankanın büyüklüğüne, faaliyetlerinin karmaşıklığına, yoğunluğuna, kapsamına ve risklilik düzeyine bağlı olarak, Bankacılık Kanunu ve ilgili mevzuat ile banka içi

düzenlemelerde öngörülen denetim hizmetlerinin aksatılmadan ve bu hizmetlerin gerektirdiği seviyede yerine getirilmesi amacıyla, yeterli sayıda müfettiş ve iç denetim elemanı çalıştırılır.

İç denetim işlevi sayesinde iç kontrol sistemi içinde tesis edilen kontrollerin etkinliği test edilmekte, kontrollerin işlerlikleri veya olası kontrol eksikliklerine yönelik inceleme yapılabilmektedir. Bunun yanında iç denetim ekibi içindeki müfettişler bilgi sistemleri denetim faaliyetlerini de yerine getirmektedir. Ancak müfettişlerden, bankanın bilgi sistemlerinin denetimini icra edeceklerin bilgi teknolojileri ile bilgi teknolojilerine dayalı denetim teknikleri konularında öğrenim alanları itibariyle veya aldıkları eğitim sertifikalarıyla kanıtlanabilir asgari bilgi ve beceriye sahip olmaları zorunludur.

İç denetim faaliyetleri,

1. Bankaların dönemsel ve riske dayalı iç denetim faaliyetleri,
2. İç denetim planının hazırlanması, yürürlüğe konulması, çalışma programları aracılığıyla icrası,
3. Sonuçların iç denetim birimi yönetimine, ilgili birim yönetimine ve ilgili iç sistem sorumlusuna, denetim komitesine, denetim komitesi aracılığıyla yönetim kuruluna raporlanması
4. Denetim raporları çerçevesinde ilgili birim yönetimlerince alınan önlemlerin izlenmesi faaliyetlerini kapsar.

3.9.2. İç Kontrol Sisteminin Amaçları

Bir işletmede iç kontrol sistemi kurulmasının amaçları şu şekilde sınıflandırılabilmektedir[52]:

1. *İç kontrol sisteminin esas amaçları*: İç kontrol sisteminin esas amaçları işletmenin varlıklarının korunması, muhasebe bilgilerinin doğruluk ve güvenilirliğinin sağlanması, faaliyetlerin verimliliği ve politikalara uygunluğun sağlanması ve kaynakların ekonomik ve verimli kullanımının sağlanmasından oluşmaktadır.
    a. İşletmenin varlıklarını korumak: Varlıkların yönetilmesinde, işlemlerin yürütülmesinde ve kaydında yapılan hata ve yoksulsuzluklardan doğacak zararlara

[52] Kepekçi, **age**, 74-75

karşı işletmenin varlıklarının korunması amacıyla yönetim tarafından uygulanan usul ve yöntemler varlıkların korunma amacı olarak anlaşılmaktadır.

b. Muhasebe bilgilerinin doğruluk ve güvenilirliğinin sağlanması: Muhasebe bilgilerinin doğruluğu, finansal nitelikteki işlemlerin kaydedilmesinde, sınıflandırılmasında, özetlenmesinde ve raporlanmasında genel kabul görmüş muhasebe ilkelerinin ve ilgili yasaların uygulandığını ifade etmektedir. Diğer yandan muhasebe bilgilerinin güvenilirliği ise, belge ve kayıtların işletmenin gerçek işlemlerini yansıtmasını, kayıt dışı bırakılmış işlemlerin olmadığını ifade etmektedir.

c. Faaliyetlerin verimliliği ve politikalara uygunluğun sağlanması: İşletme yönetimi, faaliyetlerdeki verimliliğin ölçümlenmesi için veya işletme amaçlarını gerçekleştirmek için çeşitli bütçeler, kurallar ve ilkeler saptamaktadır. İç kontrol sistemi, faaliyetlerin benimsenen bütçe ve yönetim politikalarına uygunluğunu ve verimliliği sağlamaya yardımcı olmaktadır.

d. Kaynakların ekonomik ve verimli kullanımının sağlanması: Belirlenmiş amaçlara ve hedeflere ulaşma derecesi etkinlik olarak tanımlanmaktadır. Bu noktada iş programlarında planlanmış sonuçlar ile gerçekleşen sonuçlar karşılaştırılarak faaliyet etkinliğinin değerlendirilmesi iç kontrol sistemi tarafından yapılmaktadır.

2. *İç kontrol sisteminin genel amaçları*: Genel kontrol amaçları, bir işletmenin belirli işlem gruplarını yürütmek için gerekli kontrol usul ve yöntemlerine sahip olup olmadığının göz önünde bulundurulmasında genel bir çerçeve oluşturmaktadır. Bu noktada muhasebe iç kontrol sistemine yönelik olarak genel kontrol amaçları şu şekilde sınıflandırılabilir:

   a. İşlemler yönetimin devrettiği genel ve özel yetkilere uygun olarak yürütülmelidir.

   b. İşlemler, genel kabul görmüş muhasebe ilkelerine uygun olarak ve hesap verme yükümlülüğünü yerine getirecek şekilde kaydedilmelidir.

   c. Varlıklara ve belgelere erişim yetkili personelle sınırlandırılmalıdır.

   d. Mevcut varlıklar belirli sorumluluk kayıtlarıyla karşılaştırılmalı ve herhangi bir fark belirlendiğinde, farkın özelliğine göre gerekli soruşturma yapılamalıdır.

3. *İç kontrol sisteminin özel amaçları*: Bir işletmenin belirli işlem gruplarını yürütmek için genel kontrol amaçlarına ek olarak özel kontrol amaçlarının da belirlenmesi gerekmektedir. Bu işlem hasılat işlemleri veya ödeme işlemleri gibi işletme faaliyetlerinle herhangi biri olabilir. İlgili işleme yönelik özel kontrol amaçları yetki, meydana gelme, bütünlük, değerleme, kayıtsal doğruluk, sınıflandırma, zamanlılık, özetleme, mutabakat ve varlıkları koruma gibi muhasebe denetim amaçları atında oluşturulmalıdır. Örneğin kredi satış işlemleri ve zamanlılık muhasebe denetim amacıyla ilgili olarak "kredili satış işlemleri, işlemin gerçekleştiği dönemin kayıtlarında gösterilmelidir" şeklinde iç kontrol sistemine yönelik bir özel amaç belirlenebilir.

Yukarıdaki bahsi geçen iç kontrol sistemine ait amaçlara yönelik bilgi teknolojileri sistemlerinden destek alınarak da kontroller tesis edilebilmektedir. İç kontrol sisteminin etkinliğinin değerlendirilmesinde bilgi teknolojileri ile ilgili kontrol noktalarında ise iç denetim kapsamı altında bilgi sistemleri denetimi faaliyete geçmektedir. Buna benzer bilgi teknolojilerinin iç kontrol sistemi üzerindeki etkileri bir sonraki bölümde detaylı olarak açıklanacaktır.

3.9.3. Bilgi Teknolojilerinin İç Kontrol Sistemi Üzerindeki Etkileri

Önceki bölümlerimizde de bahsettiğimiz gibi bilgi teknolojilerinin gelişiminde yaşanan hızlı gelişim ve büyüme süreci denetim mesleğini de ciddi olarak etkilemiştir. İşletmelerin birbirinden farklı yapılarda ve büyüklüklerde bilgi teknolojileri sistemlerine sahip olduklarını ve bu sistemlerde teknolojinin gerektirdiği şekilde hızlı bir değişim ve gelişme süreci yaşandığını görmekteyiz. Bu faktörler göz önüne alındığında verilerin güvenilirliği, bütünlüğü ve eksiksizliği gibi faktörler göz önüne alınarak finansal tablolar üzerine görüş bildiren denetim mesleğinin ve denetçilerin karşı karşıya oldukları zorluklar daha net olarak anlaşılacaktır.

Yeni nesil terminallerde, bilgisayar ağ yapısında ve sunucularda yaşanan teknik gelişmeler paralel olarak uygulamaların veri işleme kapasitelerinde, karmaşıklığında ve hızında önemli gelişmeleri de beraberinde getirmiştir. İşletmelere destek amaçlı kurulan bilgi sistemlerinde bu gelişmeler beraberinde yazılım, donanım gibi bilgi teknolojileri alanında ihtiyaçları doğurmuştur. Bu aşamada, işletmelerde yaşanan ihtiyaçlara paralel olarak bilgi teknolojileri alanında hizmet sağlayan üçüncü taraf firmaların sayısı artmış ve birçok bilgi işlem faaliyetinin yönetilmesi için dışarıdan destek alınması, daha düşük maliyetlerden dolayı tercih edilmiştir. Günümüzde de dış desteğe yönelik yan servislerin üçüncü taraf firmalardan sağlanması ve işletmelerin rekabet için

sadece uzmanlaştıkları alandaki işlere yönelmeleri gelişmelerin süreceğini tahmin edebiliriz. Örneğin bir firmanın iş sürekliliği adına merkezden ayrı bir yerde yedek sistemler kurması yerine iş sürekliliği kapsamında hizmet sağlayan bir firmadan bu hizmeti satın alması daha az maliyetli duruma gelmektedir. Bu hizmeti sağlayan firma birçok işletme ile anlaşarak hem alanında uzmanlaşmakta hem de ölçek ekonomisinden dolayı maliyetlerini düşürebilmektedir. Bu tarz gelişmelerin sonucu olarak bilgisayar ağları, veritabanı sistemlerinin oluşturulması ve yönetimi ve sistemlere erişimin kontrol altına alınması gibi konular bilgi işlemlerin yönetimi alanında işletmelerin öncelikleri arasında yer bulmuştur.

Bilgi sistemlerinde yaşanan hızlı gelişme sonucunda muhasebe verileri besleyen faaliyetler otomatik olarak sistemler aracılığıyla beslenmekte ve finansal raporlara yansımaktadır. Örneğin kurumsal kaynak planlaması sistemlerinde satın alma sürecine yönelik işletme içinde farklı iş kollarına ait olan satın alma talebi, onayı, irsaliye ve faturalama ve ödeme süreçleri tek bir sistem üzerinde yürütülebilmekte ve muhasebeleştirilmektedir. Verinin bu hızda aktığı bir bilgi sistemi ile finansal raporlar bu bilgiler ile beslenmekte ve doğal olarak da iç kontrol sistemlerine yönelik kontroller, yine bu sistemler üzerinde programlanmakta ya da yaratılmaktadır. Örneğin;

- Sistem üzerinde bilgilere ve programlara erişimin mantıksal erişim kontrollerine dayalı güvenlik yazılımları ile sınırlandırılması
- Periyodik olarak yevmiye defteri kayıtları ile büyük defter kayıtları arasında otomatik mutabakatın yapılması
- Sistem içinde uygun olarak tamamlanmayan işlemlerin önlenmesi ve kabul edilmeyen iş emirlerinin periyodik olarak raporlanması

gibi iç kontrol sistemine yönelik otomatik kontroller bilgi sistemleri ile iş süreçlerinin iç içe geçmesi ve bilgi teknolojilerinin gelişimine paralel olarak ortaya çıkmaktadır. Bu aşamada, finansal denetim alanında faaliyet gösteren denetçilere destek amaçlı olarak bilgi sistemleri denetim faaliyetlerinin gerçekleştirilmesi zorunluluk kazanmaktadır. Otomatik kontroller ile tesis edilen iç kontrol ortamının etkin işleyip işlemediğinin test edilmesi ve değerlendirilmesi bilgi sistemleri denetimi ile gerçekleşmekte, bu da finansal denetim faaliyeti gösteren denetçilere maddi doğruluk testlerinde vereceği zamanı planlaması açısından makul bir güvence verecektir.

Sonuç olarak hızla gelişen bilgi sistemlerinin işletmenin iş süreçleri ile entegre ve kompleks hale gelmesinden dolayı tasarlanan iç kontrol sisteminin de otomatik kontroller içermesi kaçınılmaz

olmuştur. Bu nedenle iç kontrol sisteminin değerlendirilmesi sürecinde finansal ve bilgi sistemleri denetimlerinin de eş güdümlü olarak yürütülmesi bir zorunluluk haline dönüşmüştür.

3.10. Bilgi Sistemleri Denetim Süreci

Daha önce de bahsettiğimiz gibi, denetim iktisadi faaliyet ve olaylarla ilgili yönetim iddialarının daha önceden saptanmış ölçütlere uygunluk derecesini araştırmak ve sonuçları ilgi duyanlara bildirmek amacıyla tarafsızca kanıt toplayan ve bu kanıtları değerleyen ve yetkin ve bağımsız kişiler tarafında gerçekleştirilen sistematik bir süreçtir. Bilgi sistemleri denetimi ise, bilgi sistemlerinin üzerindeki otomatik kontrolleri, bilgi sistemleri ile ilişkili olan diğer önyüz ve otomatik olmayan kontrolleri kapsamına alan, inceleyen ve değerlendiren bir denetim alanı olarak tanımlanabilir.

Bilgi sistemleri denetim sürecini gerçekleştirmek için birkaç temel adımın tamamlanması gerekmektedir[53]:

1. *Planlama*: İlk adım olarak bilgi sistemleri denetimini etkin olarak gerçekleştirmek için yeterli ölçüde planlamanın yapılması gerekmektedir. Bilgi sistemleri denetim hedefleri, genel bilgi teknolojileri kontrol ortamı ve incelenecek bilgi sistemleri ("uygulamaları") üzerindeki riskler değerlendirilerek belirlenmeli ve uygun denetim metodolojisi üzerine karar verilmelidir.
2. *Denetim Programlarının Hazırlaması*: Temel denetim hedeflerini karşılayacak kontrol hedefleri oluşturulmalı ve bu kontrol hedeflerinin testine yönelik uygun denetim programları hazırlanmalıdır.
3. *Testlerin Gerçekleştirilmesi ve Kanıt Toplanması*: Test edilecek kontrollerin kuvvetli ve zayıf yönlerini tespit edip inceleyen taraflara gösterecek seviyede yeterli ve objektif kanıt toplanıp değerlendirilmelidir. Kontrollerin testine ek olarak, denetim hedeflerine yönelik kontrol eksiklikleri de belirlenmeli ve ispat edecek yeterli kanıt oluşturulmalıdır.
4. *Denetim Raporunun Hazırlanması*: Gerçekleştirilen testler sonucunda tespit edilen bulguların veya eksikliklerin üst yönetime tarafsız olarak sunulması amacıyla rapor oluşturma faaliyetidir.

[53] Johnson, **age**, 25

Bilgi sistemleri denetimi sürecine başlanmadan önce etkin ve verimli bir denetim süreci için kaynak ihtiyacının (zaman, ekip vs.) analizi yapılmalıdır. Yine denetim öncesinde denetim kapsamı, hedefleri ve kriterleri tespit edilmelidir. Sonrasında kapsama ve hedeflere uygun olarak denetim prosedürleri oluşturularak test gerçekleştirilecek, kanıt toplanacak ve bir görüş altında tespitler üst yönetim ile birlikte ilgili taraflara raporlanacaktır.

Bilgi sistemleri denetiminin genel adımlarından yukarıda bahsettikten sonra denetim süreci içindeki her bir önemli adımdan ayrıntılı olarak sonraki bölümlerde bahsetmek faydalı olacaktır.

3.10.1. Bilgi Sistemleri Denetim Hedefleri

Denetim hedefleri denetim süreci içerisindeki temel amaçlara işaret ederken, kontrol hedefleri ise tasarlanan iç kontrollerin nasıl işlemesi gerektiğine işaret etmektedir. Denetim hedefleri iş risklerini minimize edecek seviyede iç kontrollerinin tesis edildiğinden ve bu kontrollerin işlediğinden emin olunmasına yönelik değerlendirmelere odaklanmıştır. Dolayısıyla denetim hedefleri bilgi sistemleri denetimin temel amaçları olan yasal düzenlemelere ve mevzuata uyuma ve bilgi ile birlikte bilgi sistemleri kaynaklarının bütünlüğüne, güvenilirliğine, erişilebilirliğine ve gizliliğine odaklanan hedefleri barındırmaktadır.

Bilgi sistemleri planlamasındaki en can alıcı nokta da temel denetim hedeflerine yönelik olarak uygun bilgi sistemleri denetim hedeflerinin belirlenmesidir. Örnek vermek gerekirse, finansal denetimin iç kontrol sistemini değerlendirdiği bir denetim hedefi olarak, bilgi sistemleri üzerinde gerçekleşen tüm yevmiye kayıtların işlem türlerine bağlı olarak büyük deftere eksiksiz olarak aktarıldığından emin olunmak istenmektedir. Buna uygun olarak bilgi sistemleri denetiminde yukarıdaki denetim hedefi genişletilebilmektedir. İşlemlerin aktarımı sırasında veri akışını kontrol eden ve muhtemel hataları tespit eden programlanmış kontrollerin etkin çalıştığından ve güvenliğinin sağlandığından emin olunması olarak uygun bilgi sistemleri denetim hedefine dönüştürülebilmektedir. Bilgi sistemleri denetçisinin planlama aşamasında temel denetim hedeflerini ve incelenecek bilgi sistemlerini anlaması, uygun bilgi sistemleri kontrol hedeflerini oluşturması için hayati önem sahiptir. Belirlenen bilgi sistemleri kontrol hedeflerine göre denetim sürecinin detay planlaması yapılabilecek ve denetim süresi belirlenebilecektir.

Genel anlamda bahsetmek gerekirse bilgi teknolojileri denetçisi bilgi sistemleri üzerindeki anahtar kontrolleri tespit etmelidir. Sonrasında bu anahtar kontrolleri denetim hedefleri açısından test edip etmeyeceğine karar vermelidir. Bu sebeple iş süreçlerini destekleyen servisleri ve bilgi

sistemleri bilgi teknolojileri denetçisi tarafından incelenip anlaşılmalı ve çalışma kağıtlarına dökülmelidir. Bu sayede genel kontrol ortamı ve uygulamalar üzerinde anahtar kontroller daha net olarak belirlenebilecek ve denetim hedeflerine hizmet eden kritik bilgi sistemleri kontrolleri test edilebilecektir. Bilgi sistemleri denetçisinin süreçleri anlaması ve kontrolleri tespiti için gerçekleştirdiği bu ön çalışmaya gözlemleme ("walkthrough") adı verilmektedir.

Bilgi teknolojileri kontrol hedeflerinin tespitine yönelik olarak temel denetim faaliyetlerine (iç denetim veya finansal denetim) verilen desteğin yanında finansal denetçiler tarafında gerçekleştirilen maddi doğruluk testlerine de destek verilebilmektedir. Günümüz teknolojisinde işlemlerin yoğunluğu ve karmaşıklığı bu verilerin analizi için bilgisayar destekli yazılımların kullanımını da beraberinde getirmiştir. Bu aşamada bilgi teknolojileri denetçisi, maddi doğruluk testinin amacına yönelik olarak uygun veriyi işletmenin bilgi sistemlerinden temin edilmesi ve analiz edilmesi alanında da destek hizmet sağlayabilmektedir.

3.10.2. Bilgi Sistemleri Denetim Metodolojisi

Bilgi sistemleri denetim metodolojisi, planlanan denetim hedeflerine ulaşmak için hazırlanan denetim programlarının bir bütününden, diğer bir ifadeyle setinden oluşmaktadır. Denetim metodolojisi, denetim sürecinin kapsamını, denetim hedeflerini ve çalışma programlarını ortaya koyan bir denetim anlayışı oluşturmaktadır. Bu anlayış denetim yaklaşımına tutarlılık getirmesi ve istenen temel hedeflere ulaşılması için bir yol gösterici olmaktadır. Bu sebepledir ki, denetim metodolojisi denetim amaçlarına ulaşmayı sağlayacak tutarlılıkla ve yetkinlikte oluşturulmalı, denetim komitesi tarafından onaylanmalı ve belirtilen denetim metodolojisine uygun olarak denetim faaliyetlerinin kurum tarafında yürütülmesi sağlanmalıdır.

Kurum içinde bilgi sistemleri denetim faaliyetleri aşağıda sıralamış olduğumuz denetim fazlarını detay olarak açıklayacak bir denetim metodolojisine göre yürütülmelidir[54]:

1. <u>*Denetim Konusu*</u>: Öncelikle denetim faaliyetlerinin gerçekleştirileceği alana yönelik tespitin yapılması uygun kriterlerde yapılması gerekmektedir.
2. <u>*Denetim Hedefleri*</u>: Bilgi sistemleri denetim hedefleri, denetim konusuna uygun olarak belirlenmelidir. Örneğin, program kaynak kodları değişikliklerinin tanımlı ve kontrollü bir ortamda gerçekleştirildiğinin tespit edilmesi denetim hedefi olarak belirlenebilir.

[54] Johnson, **age**, 25

3. *Denetim Kapsamı*: Bilgi sistemleri denetim kapsamı içine alınacak olan sistemlerin, işlemlerin ve organizasyon içindeki bölümlerin belirlenmesine yönelik yöntemlere yer verilir ve denetim kapsamı belirlenir. Bir önceki örneğimiz ile bağlantı kurmamız gerekirse, belirli bir uygulamanın belirli bir faaliyet dönemi içindeki program konu değişiklikleri denetim kapsamına alınabilir.

4. *Ön Denetim Planlaması*: Bilgi sistemleri denetim faaliyetinin kapsamına ve hedeflerine uygun olarak gerekli yetkinlikler ve kaynakların belirlendiği, test ve inceleme süreci için gerekli bilgi kaynaklarını ve denetim alanlarının belirlendiği bir süreç adımı oluşturulmalıdır.

5. *Denetim Prosedürlerinin Hazırlaması ve Veri Toplama*: Belirlenen kontrolleri test etme yöntemlerinin belirlenip seçileceği sonrasında kimler ile görüşmeler yapılacağına dair süreç adımının tesis edilmesi gerekmektedir. Bununla birlikte kontrollerin testine yönelik olarak bilgisayar destekli denetim uygulamalarının kullanım alanları ve veri toplama yöntemleri de denetim metodolojisi içinde bu adım altında belirlenmelidir.

6. *Testlerin Gerçekleştirilmesi ve Değerlendirilmesi*: Organizasyon ihtiyacına yönelik olarak uygun testlerin gerçekleştirilme ve değerlendirme yöntemleri belirlenmelidir. Örneğin tespitlerin nasıl sınıflandırılacağı ve risk analizinin yapılacağı bu alanda metodolojiye entegre edilmelidir.

7. *Üst Yönetim ile İletişime Yönelik Prosedürler*: Yine organizasyonun ihtiyaçlarına uygun olarak bilgi sistemleri denetimi sonucundaki değerlendirmelerin ve tespitlerin üst yönetimine sunulma biçimine ve yöntemlerine denetim metodolojisi içinde yer verilmelidir.

8. *Denetim Raporunun Hazırlanması*: Bilgi sistemleri denetimi sonucundaki tespitlerin ve değerlendirmelerin belirlenen rapor formatında yazılı hale getirilme yöntemleri, tespitlerin düzeltilmesine yönelik takip prosedürlerin oluşturulması ve belirlenen hedef zaman diliminde aksiyon planlarının ilerleme durumunun takip edilmesi gibi süreç adımları denetim metodolojisi içinde açıklanmalıdır.

Tüm denetim planları, programları, aktiviteleri, testleri ve bulgular denetim metodolojisinde belirtilen şekliyle yazılı hale getirilmelidir. Tüm dokümanların ve çalışma kağıtlarının yazılı hale getirilmesindeki şekil ve seçilen medya (basılı doküman veya elektronik doküman) ihtiyaca

yönelik olarak seçilebilecektir. Önemli olan hepsinin izlenebilir, açık ve anlaşılır biçimde sunulur hale getirilmeleridir. Tüm çalışma kağıtlarının ve yukarıdaki bahsi geçen dokümanların takip edilebilir şekilde sunulmasının yanında kanıt dokümanlarına da bağlanması ve kanıtların uygun şekilde muhafaza edilmesi gerekmektedir.

Bilgi sistemleri denetim faaliyetleri sürecinde çalışma kağıtlarının ve bunlara bağlı kanıtların denetim hedefleri ile denetim raporu arasında bir köprü görevi göreceği unutulmamalıdır. Bu sebeple belirlenen denetim metodolojisine uygun olarak denetim faaliyetlerinin yürütülmesi ve çalışma kağıtlarının oluşturulması beraberinde denetim hedeflerine uygun olarak hazırlanmış bir denetim raporunu getirecektir.

Son olarak bilgi sistemleri denetiminin, denetçilerin zamanı ve bilgi birikimi düşünüldüğünde pahalı ve nadir kaynakları yönettiği düşünmelidir. Bu sebepledir ki, denetim metodolojisi oluşturulurken, test ve analizlerin sonucunda otomatik olarak çalışma kağıtlarını oluşturan bilgisayar destekli uygulamaların kullanımı da desteklenmelidir.

3.10.3. Bilgi Sistemleri Denetim Programları

Bilgi sistemleri denetim programları oluşturulurken denetimin kapsamı ve finansal veya iç denetim amaçlarına paralel olarak oluşturulmuş bilgi sistemleri denetim hedefleri temel olarak alınmalıdır. Bilgi sistemleri denetçileri genellikle bilgi sistemleri fonksiyonlarını ve sistemleri farklı perspektiflerden değerlendirebilmektedir. Bunlar, güvenlik (gizlilik, bütünlük ve erişilebilirlik), kalite (etkinlik ve etkililik), güvenilirlilik, servis yönetimi veya kapasite açısından olabilmektedir. Bu noktada önemli olan denetim programının denetim stratejisini ve planını ortaya koymasıdır.

Denetim programı, kapsam ve denetim hedeflerinin direktifleri altında yeterli denetim kanıtlarını içeren denetim prosedürleri oluşturup denetim görüşünü ve sonucu etkileyecek yeterli bilgiyi elde etmeye odaklanmalıdır. Denetim prosedürleri ise denetimin gerçekleştirilmesi için gerekli adımları tanımlayan dokümanlardır. Buna göre, genellikle denetim prosedürleri şu adımları içermektedir:

1. Bilgi sistemleri denetim konusu içindeki ortamın ve uygulamaların anlaşılması ve çalışma kağıtlarında kaydedilmesi.
2. Risk değerlendirmesinin yapılması ve buna uygun olarak denetim planının oluşturulması.

3. Denetim konusu içindeki ortamın ve uygulamaların anlaşılmasına yönelik olarak ön denetim ve gözlem çalışmasının yapılması
4. Denetim konusu içindeki bilgi teknolojileri genel kontrol ortamı ve uygulamaları üzerindeki tasarlanan kontrollerin belirlenmesi ve değerlendirilmesi.
5. Tasarlanan kontrollerin amaca uygun olarak uygulandıklarına ve etkin olarak çalıştıklarına yönelik testler gerçekleştirilmesi.
6. Test sonuçlarının takip edilebilir ve açık bir şekilde üst yönetime raporlanması.
7. Rapor içinde yer alan tespitlere yönelik aksiyon planlarının ve düzeltme tarihlerinin kayıt altına alınarak takibinin yapılması[55].

Bilgi sistemleri denetçisi, tasarlanan bilgi sistemleri kontrollerinin test edilmesi ve değerlendirilmesine yönelik olarak denetim program ve prosedürlerini en iyi şekilde anlamak zorundadır. Bilgi sistemleri denetçisi, yukarıdaki adımlar altında akış diyagramı oluşturma teknikleri, bilgi sistemlerinin otomatik denetim raporlarını kullanma, bilgisayar destekli denetim uygulamalarını kullanma ve gözlemleme gibi detay prosedürlere de hakim olmak zorundadır.

3.10.4. Bilgi Sistemleri Denetim Riski ve Önemlilik Derecesi

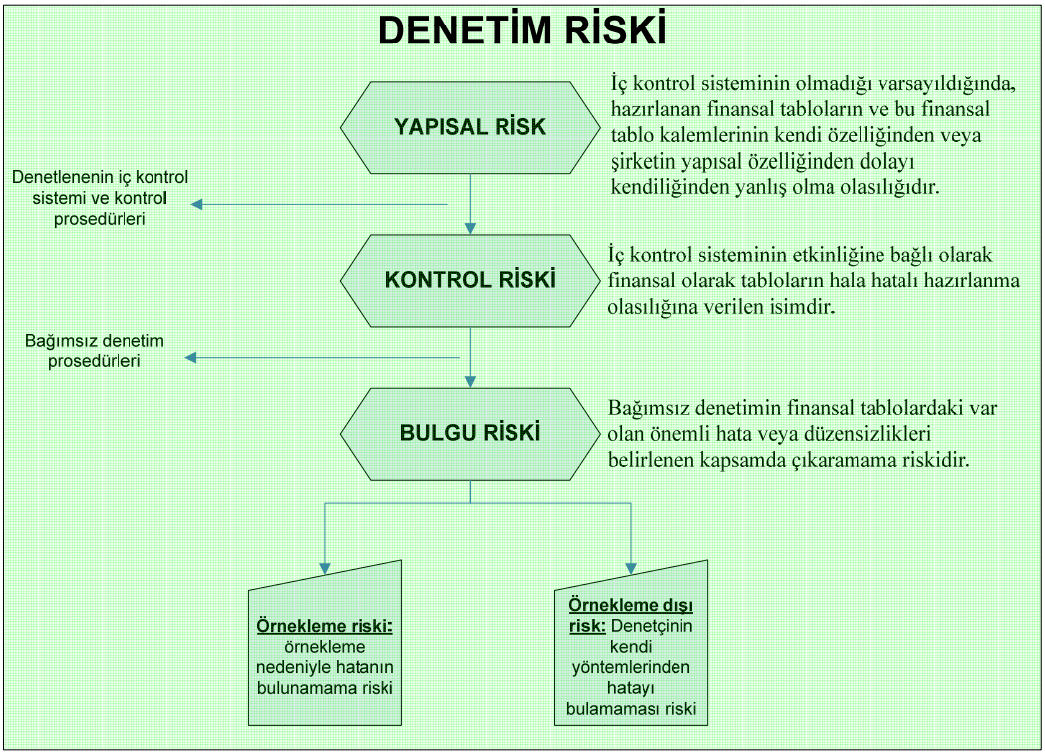
Günümüzde risk odaklı denetim yaklaşımı, sürekli denetim sürecinin geliştirilmesinde ve iyileştirilmesinde kullanılmaktadır. Bu yaklaşım ile bilgi sistemleri denetçisi risk analizi yaparak kontrol testlerine yönelik çalışmalara veya detay maddi doğruluk testlerine vereceği desteği belirleyen bir yaklaşım benimsemektedir. Kurum genelinde risk odaklı denetim yaklaşımıyla da iş süreçlerine paralel olarak sürekli denetim anlayışının yaygınlaşması ve operasyonel faaliyetlere entegre edilmesi sağlanmaktadır. Buna ek olarak risk odaklı denetim yaklaşımı bilgi sistemleri denetçisine gerçekleştireceği testlerin kapsamının ve detayının belirlenmesi için yol da göstermektedir.

Denetim riski genel olarak denetim işleminin mahiyetinden kaynaklanan risk olup, mali tablolarda önemli yanlışlıklar olduğu halde, denetçinin mali tabloların doğru olarak sunulduğu sonucuna varması ve mali tablolar hakkında olumlu görüş bildirmesi olasılığıdır. Bunun yanında işletme riski ise, mali tabloların denetimi ile ilişkili olarak, denetçinin veya denetim şirketinin bir

[55] Johnson, **age**, 24

davadan veya söylentiden dolayı mesleki uygulamasına zarar gelmesi veya kayba uğraması riskidir[56].

Denetim riski aşağıdaki risk kategorilerinin bir arada yorumlanması ile birlikte değerlendirilebilmektedir. Diğer bir ifadeyle kontrol hedefine yönelik olarak aşağıdaki her bir risk kategorisinin değerlendirilmesi genel denetim riskini ortaya çıkaracaktır:

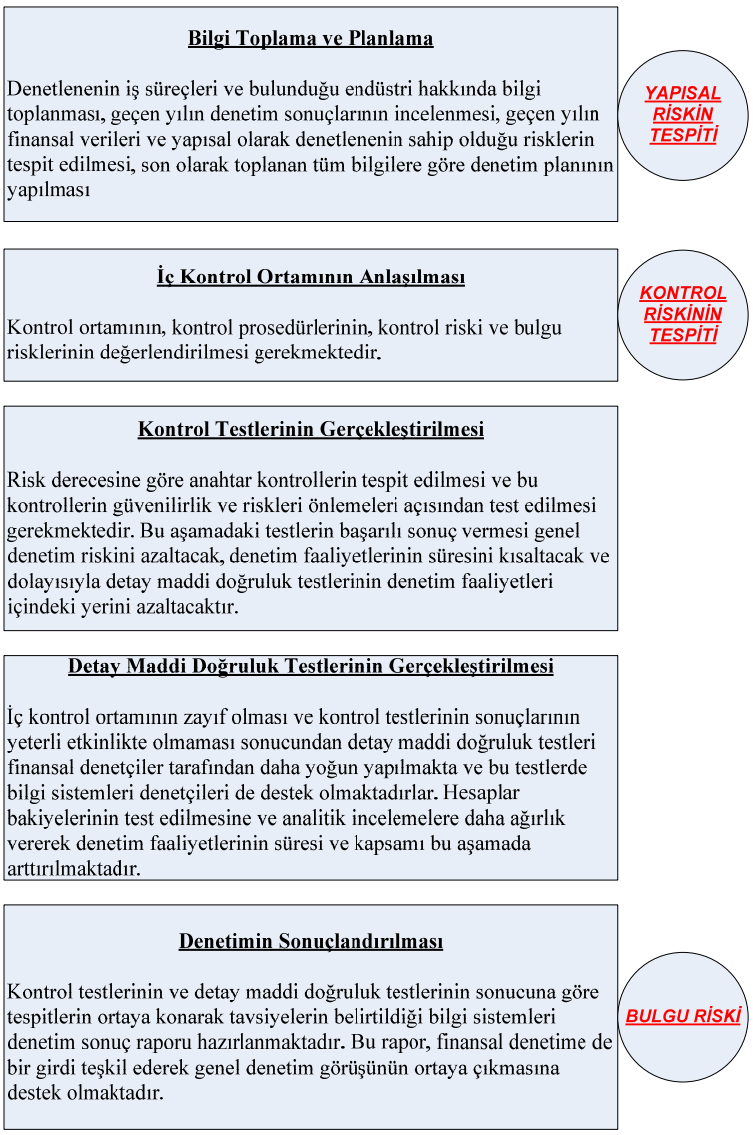


Şekil 5: Denetim Riski

Bilgi sistemleri denetçisi, denetim faaliyetlerini planlamada denetim riskini yukarıda bahsedilen kategorilerde değerlendirmenin yanında denetlenenin operasyonel kontrollerini ve bilgi sistemleri yönetiminde genel bilgi seviyesini de değerlendirmelidir. Bu kapsamda yapılacak bir değerlendirme maliyet fayda analizi ve risk arasında bir karşılaştırma yapılmasını sağlayarak karar verilmesini sağlayacaktır. Bu karara göre de bilgi sistemleri denetim faaliyetleri planlanıp yürütülecektir.

[56] Johnson, **age**, 27

Denetlenen işletmenin yapısı incelenerek, bilgi sistemleri denetçisi mevcut riskleri belirleyip sınıflandırabilmekte ve risk modelini oluşturabilmektedir. Risk modelinin oluşturulmasının basit bir şekilde anlatılması gerekirse, tehditler ve onları doğuran riskler, risklerin olasılıkları, iş süreçleri üzerindeki etkileri ve ağırlıkları tasarlanan bir denklem üzerinde değerlendirilerek önemli risklerin tespiti yapılmaktadır. Yukarıda açıkladığımız bilgiler ışığında risk odaklı denetim yaklaşımını şekil yardımıyla da gösterebiliriz. Denetçinin bu yaklaşımdaki ana amacı, hedeflenen risk seviyesine göre denetim sürecini yönetmesi ve denetim sonucuna ulaşmasıdır:



Şekil 6: Denetim Faaliyetleri ile İlgili Risk Noktalarının Yerleri

Önemlilik ise, muhasebe bilgilerinde bulunan herhangi bir hata veya düzensizliğin, mali tablo kullanıcılarının verecekleri kararları etkileme derecesidir. Kısacası önemlilik sınırı denetim çalışmaları gerçekleştirilirken kabul edilebilir hata olarak belirlenen bir sınırdır. Önemlilik sınırının tespiti, profesyonel bir değerlendirme ve olası hata ve risklerin organizasyon genelinde neden olacağı etkilerin değerlendirilmesine göre belirlenmektedir. Örneğin iç kontrol ortamının zayıf olduğu bir işletme risklere karşı daha savunmasız olacağından finansal kayıp, müşteri güveninin kaybı veya iş kesintileri gibi iş risklerinin gerçekleşme olasılıklarının artması ile birlikte finansal tablolarda olası hataları ve hilelerin meydana gelme ihtimali de artacaktır. Bu aşamada işletmenin önemlilik sınırı belirlenirken iç kontrol ortamının bir parçası olan bilgi teknolojileri destekli kontrol ortamının değerlendirilmesi için bilgi sistemleri denetçisi de sürece katkıda bulunmalıdır.

Sonuç olarak denetim riskinin tespiti, önemlilik sınırının belirlenmesi ve risk odaklı denetim anlayışının uygulanarak denetim faaliyetlerinin planlanması ve uygulanması bilgi sistemleri denetçisinin bilmesi gereken başlıca konulardandır.

3.10.5. Bilgi Sistemleri Risk Değerlendirme Teknikleri

Bilgi sistemleri denetimi sürecinde denetim konusu olarak belirlenecek fonksiyonel alanın belirlenmesi sırasında, bilgi teknolojileri denetçisi çeşitli denetim konularıyla ve doğal olarak denetim riskini oluşturan çeşitli riskler ile karşılaşacaktır. Bu sırada yüksek risk seviyesinin tespit edildiği alanların belirlenmesi ve bu alanlarda denetim faaliyetlerinin yoğunlaştırılması önemlilik arz etmektedir. Bu sebepledir ki, çeşitli risk değerlendirme teknikleri denetim testlerine geçilmeden önce bilgi teknolojileri denetçisi tarafından gerçekleştirilmelidir.

Çok çeşitli risk değerlendirme teknikleri bilgi sistemleri denetçisi tarafından kullanılabilmektedir. Bunlarda çok basit olarak bilgi teknolojileri denetçisinin bilgi birikimine ve tecrübesine dayanarak yüksek, orta ve düşük risk kategorilerinde sınıflandırma yapmasından başlayıp bilimsel olarak oluşturulan ve modellere dayanan yöntemlere kadar çeşitlenmektedir. Bu aşamada genel bilgi olması açısından üç temel risk değerlendirme tekniğinden kısaca bahsedilmesi yerinde olacaktır[57]:

1. *Puanlamaya Dayalı Risk Değerlendirme Tekniği*: Çeşitli değişkenler ağırlıkları ile birlikte belirlenerek her denetim konusu verilen puanlar yönünden karşılaştırılır ve denetim planı

[57] Johnson, **age**, 29

ve faaliyetlerinde risk puanı yüksek çıkan konulara ağırlık verilir. Bilgi sistemleri denetimi açısından teknik karmaşıklık, kontrol prosedürlerinin etkinliği ve finansal kayıp olasılığı ve seviyesi gibi faktörler değişken olarak kabul edilerek her birine verilen ağırlıklar ile ilgili denetim alanının (herhangi bir bilgi sistemi veya alt bir süreci) risk seviyesi puanlanır. Sonrasında her bir denetim alanı risk puanlarına göre karşılaştırılır ve denetim planı oluşturulur.

2. *Yargısal Risk Değerlendirme Tekniği*: İsminden de anlaşılacağı gibi denetim alanlarına yönelik risk değerlendirmesi ve bunların önceliklendirilmesi denetçinin değerlendireceği bazı bilgilere göre profesyonel yargısına bağlı olarak yapılmaktadır. İş süreci hakkında bilgilere, üst yönetimin direktiflerine, tarihsel bilgilere, iş hedeflerine ve çevresel faktörlere göre her bir denetim alanı üzerinde bağımsız bir karar oluşturulmaktadır.
3. *Karma Risk Değerlendirme Tekniği*: Son risk değerlendirme tekniği ise yukarıdaki her iki değerlendirme yöntemini de bir arada kullanarak denetim alanlarının risk durumunu değerlendiren yöntemdir.

Sonuç olarak risk değerlendirmesi yapılarak denetim alanlarının tespit edilmesi şu faydaları sağlayacaktır:

1. Yönetimin sınırlı denetim kaynaklarını etkin olarak paylaştırması ve yönetmesi
2. Denetim aktivitelerinin iş süreçlerinin riskli olduğu noktalara yönetilmesi ve şirkete değer katma fırsatının ortaya çıkarılması
3. Denetim faaliyetlerinin etkin olarak yönetilmesinde temel oluşturması
4. Tek bir denetim konusunun organizasyon seviyesindeki genel etkisinin yorumlanmasında özet bilgi teşkil etmesi[58]

3.10.6. Bilgi Sistemleri Denetimine Yönelik Testler

Bilgi sistemleri denetimi, geniş kapsamda değerlendirildiğinde uygulama kontrollerinin ve genel kontrol alanlarının denetiminden oluşmaktadır. Bunun dışında bilgi sistemleri denetim, denetlenen tarafta kapsama göre sadece uygulama kontrollerinin denetimi veya sadece genel kontrol alanlarının denetimi şeklinde de uygulanabilmektedir. Bu noktada finansal denetim ile

[58] Johnson, **age**, 29

birlikte entegre olarak çalışmak, destek gereken noktalarda risk odaklı denetim anlayışına uygun olarak bilgi sistemleri denetiminin kapsamını belirlenmek önem taşımaktadır.

Bu bölümde bilgi sistemleri denetiminin kapsamına giren uygulama kontrollerinin denetimi ve genel kontrol alanlarının denetimi kapsamında yapılan testler hakkında kısaca bilgi verilmesi amaçlanmıştır.

1. *Genel Bilgi Ortamına Yönelik Testler*: Bilgi teknolojileri yönetimi ile ilgili olarak tesis edilen süreçlerin üzerindeki kontrollere genel bilgi teknolojileri kontrolleri adı verilmektedir. Bu kapsamda veriye ve programlara erişim, program değişikliklerinin yönetilmesi, yeni program geliştirmelerinin yapılması ve bilgi sistemleri operasyonunun yönetimi gibi alanlardaki kontroller belirlenmekte ve test edilmektedir. Bu aşamada genel kontrol alanlarının güvenilir olması üzerinde tesis edilen uygulama kontrollerinin de bir o kadar güvenilir olmasına zemin hazırlamaktadır. Genel bilgi sistemleri süreçleri kapsamında, değişim yönetimi, kapasite yönetimi, donanım yönetimi, veritabanı yönetimi, fiziksel güvenlik, felaketten kurtarma süreci gibi birçok süreç üzerinde testler gerçekleştirilmekte ve genel bilgi sistemleri kontrol ortamı hakkında bir görüş oluşturulmaktadır. Bu aşamada yapılan testler ile finansal denetim amaçlarını birebir eşleştirilemese de finansal denetim amaçları ile ilişkili olan uygulama kontrollerinin güvenilir bir ortamda tesis edilmesini gözlemlemek için genel kontrol alanlarının denetimi gerçekleştirilmelidir. Test sonuçlarına göre hangi uygulama kontrollerine güvenilebileceği veya hangisine güvenilmeyeceği ortaya çıkarılabilmektedir. Örneğin, internet bankacılığı uygulaması üzerindeki uygulama kontrollerinin doğru ve güvenilir olarak çalıştığı tespit edilse de, arka taraftaki veritabanı yönetiminin düzgün yapılmaması ve çok sayıda gereksiz kişinin veritabanına erişimi tespit edilmişse, genel kontrol ortamının zayıf olduğu anlaşılacaktır. Dolayısıyla bu ortam üzerinde tesis edilen uygulama kontrollerine de genel kontrol ortamının zayıflığına bağlı olarak güvenilemeyecektir.
2. *Uygulama Kontrollerine Yönelik Testler*: Uygulama kontrolleri, bilgi sistemlerinin iş süreçlerini desteklediği noktalarda kontrol amaçlı tesis edilen kontrollerdir. Daha geniş bir ifadeyle, bilgi sistemleri içerisinde yer alan ve iş sürecine yönelik faaliyetlerin yürütülmesi veya desteklenmesi için finansal verilerin tanımlanması, üretilmesi, kullanılması, bütünlük ve güvenilirliğinin sağlanması, verilere erişimin yetkilendirilmesi

gibi tüm iş süreçlerinde kullanılması gereken iç kontrollerin etkinliğinin ve yeterliliğinin denetlenmesini ve değerlendirilmesini kapsayan kontrollerdir. Uygulama kontrolleri, bilgi sistemlerindeki verinin işlem akışına göre veri girişinden kaynaklanan, veri işleme süreci üzerindeki ve veri çıkışından kaynaklanan kontroller olarak sınıflandırılabilmektedir. Uygulama kontrollerinin denetimini sürecinde özelikle bilgi sistemleri üzerindeki eksiksiz olma, veri bütünlüğü, doğru yetkilendirme, kayıtsal doğruluk, kayıtsal hesaplama ve görevler ayrılığı gibi çeşitli denetim hedefleri doğrultusunda testlerin gerçekleştirilmesi gerekmektedir. Bu aşamada uygulama kontrollerinin denetim amaçları ile finansal denetim amaçları arasında ilişki kurmak test sonuçlarının değerlendirilmesinin ve olası tespitlerin önemlilik seviyesi üzerindeki etkisinin yorumlanmasında büyük önem taşımaktadır. Uygulama kontrollerinin testi sırasında özellikle bilgisayar destekli denetim tekniklerinin ve araçlarının yoğun kullanılması gerekebilmektedir. Son olarak örnek vermek gerekirse, alternatif dağıtım kanalları içerisinde internet bankacılığı uygulamasının üzerindeki kontrollerin test edilmesi uygulama kontrollerinin denetimi kapsamına girmektedir. Para transferi işlemlerindeki doğrulama kontrolleri veya güvenlik kontrolleri üzerindeki testler bu kapsamda yapılan testlerden sadece bazılarıdır.

3.10.7. Örneklem Belirleme ve Kanıt Toplama

Bilgi sistemleri denetim faaliyetleri gerçekleştirilirken işlemlerin yoğunluğu ve denetim zaman ve maliyetinin kısıtlı olmasından dolayı işlemlerin tümü incelenememektedir. Bu sebepledir ki, ve tüm işlemleri temsil eden evrenin içinden onu yansıtan ve hata olma olasılığının yüksek olabileceğinin öngörüldüğü seviyede örneklem oluşturulması ve testin bu örneklem üzerinden gerçekleştirilmesi zorunludur. Özellikle iç kontrol ortamında bilgi teknolojileri ile ilgili kontrollerin testine yönelik olarak kontrolün uygulanma sıklığı ve önlediği risk göz önünde bulunarak örneklem tespiti yapılması gerekmekte ve test bu örneklem üzerinde gerçekleştirilmelidir. Örneğin günlük otomatik mutabakat kontrolü yapılıyorsa, kontrolün teknik detayı incelenmek ile birlikte mutabakat sonuçlarına yönelik olarak aksiyon alınıp alınmadığı seçilen örneklem kapsamında değerlendirilmelidir. Bu nedenle bilgi sistemleri denetçisinin örneklem belirleme teknikleri konusunda da bilgi sahibi olması gerekmektedir.

Genel olarak örnekleme yöntemleri istatistiksel ve yargısal örnekleme yaklaşımları olarak ikiye ayrılmaktadır[59].

1. *İstatistiksel Örnekleme Yaklaşımı*: Örneklem boyutunu ve seçim kriterlerini objektif olarak belirleyen bir yaklaşımdır. Genel itibariyle matematiksel olasılık hesaplamaları uygulanarak örneklem boyutu hesaplanır, örnekler belirlenir ve seçilen örnekler değerlendirilerek sonuca ulaşılır. Bilgi sistemleri denetçisi istatistiksel örneklem yaklaşımında örneklemin evreni hangi oranda temsil edebileceği önceden belirleyebilmektedir.
2. *Yargısal Örnekleme Yaklaşımı*: Bu yöntem ile bilgi sistemleri denetçisi, örnek boyutuna evrenin büyüklüğünü kendi bilgi birikimi ve tecrübesi ile değerlendirerek karar vermektedir. Bunun yanında yine yargısal olarak riskli gördüğü alanlara yoğunlaşarak örneklem seçimlerini yapmaktadır. Bu yöntemin başarısı direkt olarak bilgi sistemleri denetçisinin tecrübesine, bilgi birikimine ve yargılarına bağlıdır.

İster istatistiksel yaklaşım isterse yargısal yaklaşıma göre örneklem belirlenmiş olsun, bilgi sistemleri denetçisi örneklemini oluşturmalı, örnekleme yönelik denetim prosedürlerini ve testlerini gerçekleştirmeli ve test sonucu oluşturacak yeterli, güvenilir, konu ile alakalı kanıt toplamalıdır. Yukarıdaki bölümlerde de açıkladığımız gibi bilgi sistemleri denetçisinin buradaki bulgu riski oluşturduğu örneklemden dolayı veya örneklemden bağımsız olarak denetim prosedürlerinde izlediği yöntemden dolayı kaynaklanabilir.

Yukarıda bahsettiğimiz örnekleme yaklaşımlarının yanında bilgi sistemleri denetçisi başlıca niteliksel veya değişken örnekleme yöntemlerini kullanmaktadır. Niteliksel örneklem yöntemi genel olarak kontrol testlerinde kullanılmakta ve bir niteliğin veya durumun meydana gelme veya gelmeme durumuna göre oluşturulmaktadır. Örneğin, yazılım geliştirme isteklerinin bir talep formu üzerinde onaylanması ile ilgili bir kontrol için mevcut yazılım geliştirme işleri arasında örneklem belirlenerek ilgili formların onayları ile birlikte oluşturulup oluşturulmadığı test edilmektedir. Örneklem belirlenirken evrenin büyüklüğü, denetçinin kontrolün etkin çalıştığına karşı görüşünün oluşması ana faktörleri oluşturmaktadır.

Diğer taraftan detay maddi doğruluk testlerini bilgi sistemleri denetimi kapsamında gerçekleştirirken, değişken örneklem yöntemi kullanılmaktadır. İstatistiksel örneklem yaklaşımı

[59] Johnson, **age**, 33

uygulanarak evreni temsil edebilen optimum örneklem boyutu oluşturulmakta ve maddi doğruluk testlerinde kullanılmaktadır.

Genel olarak test sırasında örneklem oluşturulması ve örnek seçimi ile ilgili ana noktalar şu şekilde sıralanabilmektedir:

1. Test kapsamında olan denetim hedefinin belirlenmesi
2. Örneklem oluşturulacak evrenin belirlenmesi
3. Örneklem yöntemi ve yaklaşımının belirlenmesi
4. Örneklem boyutunun hesaplanması
5. Örneklem seçiminin gerçekleştirilmesi
6. Örneklemin test kapsamında değerlendirilerek sonucun oluşturulması

Örneklem oluşturmadan sonra bilgi sistemleri denetimi açısından kanıtları tanımlamak ve kanıt toplama sürecinden bahsetmek yerinde olacaktır. Bilgi sistemleri denetim faaliyeti sırasında denetim amaçlarına uygun olarak toplanan her bilgi kanıt teşkil etmektedir. Denetim raporunun oluşturulması, desteklenmesi ve dolayısıyla denetim görüşünün oluşması açısından yeterli, konuyla ilgili ve güvenilir kanıt toplamak her denetçide olduğu gibi bilgi sistemleri denetçisi için de bir gerekliliktir.

Kanıtlar bilgi sistemleri denetçisinin gözlemleri, görüşmeler sırasında aldığı notlar, sistemsel kanıtlar, denetlenenin kendi prosedürleri veya dokümanları ve denetim prosedürleri sonucunda elde edilen test sonuçlarından oluşabilmektedir. Amaçlarına göre tüm kanıtlar üç ana kategoride sınıflandırılabilmektedir[60]:

1. *Sistem Kanıtları*: İşletmede işleyen muhasebe sistemi ve iç kontrol sisteminin işletimi sırasında alınan her türlü belgeye sistem kanıtları adı verilir. Örneğin bilgi teknolojileri bölümündeki pozisyonların görev tanımları gibi.
2. *Genel Kanıtlar*: İşletmenin genel durumu ve tarihi bilgileri hakkında bilgi veren kanıtlara genel kanıtlar adı verilmektedir. Örneğin bilgi teknolojileri alanında yaptığı yatırımlara veya planlara yönelik firmadan alınan bilgiler gibi.

[60] Duman, **age**, 92

3. *Temel Kanıtlar*: Cari yılda bulunan muhasebe bilgilerine ve kayıtlara yönelik olarak toplanan kanıtlara temel kanıtlar adı verilir. Örneğin bilgi sistemlerindeki reeskont hesaplamasına yönelik gerçekleştirilen test sonuçları gibi.

Kanıt sayısını etkileyen başlıca faktörler ise şunlardır[61]:

1. *Önemlilik*: Kanıt toplanacak alanın önemlilik derecesi yüksek ise aynı oranda toplanacak olan kanıt sayısı da yüksek olacaktır.
2. *Risklilik*: Kanıt toplanacak alanın risklilik derecesi yüksek ise aynı oranda toplanacak olan kanıt sayısı da yüksek olacaktır.
3. *Maliyet*: Her iki kanıt sayısının aynı güvence verdiği anlaşıldığında, maliyet açısından uygun olan kanıt sayısı tercih edilmelidir.
4. *Kanıtların Niteliği*: Kanıtların güvenilirliği ne kadar fazla ise, kanıt sayısı da o derece düşük olabilecektir.
5. *Ana Kütlenin Yapısı ve Büyüklüğü*: Ana kütlenin büyük ve çeşitli olması toplanacak kanıt sayısını arttıracaktır.

Son olarak toplanan kanıtların güvenilirliğini etkileyen faktörlerden de bahsedilerek kanıt toplama ile ilgili verilecek bilgilerin tamamlanması istenmektedir:

1. *Kanıtların İlgili Olması*: Toplanan kanıt denetçinin test etmekte olduğu denetim amacıyla ne kadar ilgiliyse o oranda güvenilirdir. Diğer bir ifadeyle denetçinin görüşünü etkiyen her bir kanıt geçerli olarak nitelendirilebilir.
2. *Kanıtların Kaynağı ve Elde Ediliş Şekli*: İşletme dışı bağımsız kaynaklardan sağlanan kanıtlar işletme içinden elde edilenlere göre daha güvenilirdir. İyi çalışan ve güvenilir bir iç kontrol sistemi ortamında yetkin kişilerce hazırlanan kanıtlar iç kontrol ortamı iyi çalışmayan bir yerden alınan kanıtlara göre daha güvenilirdir. Son olarak doğrudan doğruya bilgi sistemleri denetçisinin çeşitli yollarla incelemesi ile alınan kanıtlar dolaylı yoldan alınan kanıtlara göre daha güvenilirdir. Görüldüğü gibi kanıtların kaynağı ve elde ediliş şekilleri kanıtların güvenilirliği direkt olarak etkilemektedir.

[61] Duman, **age**, 96-103

3. *Nesnellik*: Bir kanıtın nesnelliği bir denetim kanıtı karşısında aynı derecede bilgi seviyesine sahip farklı denetçilerin aynı sonucu çıkarabilmesine bağlıdır. Bir kanıt ne kadar nesnel olursa, o derece güvenilir olacaktır.
4. *Zamanlılık*: Son olarak kanıtın ilgili olduğu dönem ile denetlenen dönem arasında bir uyum söz konusu olmalıdır. Bu aşamada denetim anına en uygun ve en yakın tarihli kanıtların denetim süresine yaygın olarak alınması kanıtların güvenilirliğini arttıracaktır.

Son olarak belirtilmesi gereklidir ki, kanıtların güvenilirliğini etkileyen faktörler aynı zamanda kanıt sayısını belirleyen "nitelik" unsurunu etkileyen başlıca faktörlerdir.

3.10.8. Bilgisayar Destekli Denetim Teknikleri

Denetim prosedürlerinin uygulanması esnasında, bilgi sistemleri denetçisinin denetim amaçlarına ulaşması için yeterli, konuyla ilgili ve güvenilir kanıt toplaması ve denetim sonuçlarını bu kanıtlara dayandırması gerekmektedir. Denetim sonucundaki tespitlerin, denetçinin görüşünün, kısacası denetim raporunun, elde edilen kanıtların doğru bir şekilde analiz edilmesi ve yorumlanması ile oluşmaktadır. Günümüz teknoloji çağında bilgi teknolojileri denetçisinin en önemli hedefi sistemler üzerindeki veriyi denetim amaçlarına ulaşmak için en doğru şekilde analiz edebilmek ve yorumlayabilmektir. Bu noktada bilgisayar destekli denetim teknikleri vasıtasıyla denetim amacına uygun olarak verinin toplanması ve analiz edilmesi sağlanmaktadır. Örneğin finansal verilerin yoğun olarak sistemler üzerindeki veriye dayandığı bankacılık sektöründe finansal denetimin kapsamındaki denetim amaçlarına ulaşmak için bilgi sistemleri denetiminin ve dolayısıyla bilgisayar destekli denetim teknikleri kullanımının gerekliliği çok büyük öneme haizdir. Bankacılık sektöründeki bilgi sistemleri denetimi, bilgisayar destekli denetim tekniklerinin uygulanışı ve entegre denetim faaliyetlerinin öneminin ortaya konması araştırma konumuzun uygulama kısmında detaylı olarak yer verilecektir. Bu nedenle bu bölümde sadece bilgisayar destekli denetim teknikleri hakkında genel bilgi verilmesi amaç edinilmiştir.

Bilgisayar sistemlerinin farklı donanım ve yazılım ortamına sahip olması, farklı veri kayıt ve işleme yapılarına sahip olması sebebiyle bilgi sistemleri denetçisinin kanıt toplama ve değerlendirme sürecini bir yazılım aracı kullanmadan gerçekleşmemesi hemen hemen günümüz teknoloji ortamında imkansızdır. Bu bakımdan bilgisayar destekli denetim araçları ve teknikleri bilgi sistemleri denetçisine veriyi bağımsız bir şekilde elde etmesinde ve analiz etmesinde destek sağlamaktadır.

Genel olarak yukarıda verilen bilgiler sonucunda bilgisayar destekli denetim tekniklerini şu şekilde tanımlanabilir: *Denetim planına uygun olarak belirlenen denetim amaçları için veriye erişilmesi, erişilen verinin analiz edilmesi ve buna bağlı olarak kayıtların ve sistemin güvenilirliği temel alınarak bulguların raporlanması kapsamında araçların kullanılmasına bilgisayar destekli denetim teknikleri adı verilmektedir*[62]. Bilgisayar destekli denetim tekniklerinin uygulamasında sonuçların güvenilirliğini etkileyen en büyük etken verilerin alındığı kaynak sistemdeki verilerin güvenilirliğidir. Bu sebeple genel bilgi sistemleri kontrol ortamının etkinliği bu aşamada büyük önem taşımaktadır.

Bilgisayar destekli denetim teknikleri kapsamında çok çeşitli yazılım araçları kullanılmaktadır. Bu araçlar genel olarak aşağıdaki denetim prosedürlerinin uygulanmasında kullanılmaktadır:

1. Sistem üzerindeki işlem kayıtlarına ait detayların ve bakiyelerin test edilmesi
2. Sistemden alınan veri üzerinde analitik analizlerin yapılması
3. Bilgi sistemleri genel kontrol ortamına ait kontrollerin uygunluğunun test edilmesi
4. Bilgi sistemleri uygulama kontrollerin uygunluğunun test edilmesi
5. Bilgi sistemleri üzerindeki potansiyel zayıflıkların değerlendirilmesine yönelik testler (Örneğin bilgi sistemleri güvenliğinin sağlanması açısından ağ üzerinde çeşitli araçlar ile saldırı testlerinin yapılması ve zayıf noktaların tespit edilmesi gibi.)

Bilgi sistemleri denetçisi bilgisayar destekli denetim tekniklerini yukarıdaki denetim prosedürleri kapsamında ne zaman, nerede, nasıl ve hangi aracı kullanarak uygulayacağına doğru olarak karar vermek ve uygulamakla yükümlüdür.

Bilgi sistemlerinin günümüzde yoğun kullanılmasının bir gereği olarak bilgi sistemleri denetim tekniklerinin denetim prosedürleri içinde uygulanması zorunluluk haline gelmektedir. Bunun dışında tasarlanan denetim programının uygulanması ve otomatik olarak yapılan test kapsamında dokümantasyonun yine kullanılan araç tarafından oluşturulması ile denetim faaliyetlerinde etkin olarak zamanın kullanılması sağlanılmaktadır. Bu kapsamda bilgisayar destekli denetim tekniklerinin ve kullanılan araçların faydalarını kısaca şu şekilde özetleyebiliriz:

1. Verinin tümünün işlenmesi ve analiz edilebilmesi ile denetim riskinin azaltılması

[62] Johnson, **age**, 36-37

2. Denetçinin analizine ve yorumlamasına göre daha bağımsız denetim sonuçlarının elde edilmesi
3. Veriye daha kolay ulaşılabilirlik
4. Zamanın etkin kullanılabilmesi ile daha geniş ve tutarlı denetim kapsamının oluşturulması
5. İç kontrol ortamındaki zayıflıkların daha etkin olarak ortaya çıkarılabilmesi
6. Zamanın etkin kullanımı ile maliyetin azaltılması

Bilgi sistemleri denetçisi bilgisayar destekli denetim tekniklerinin ve araçlarının uygulanmasında fayda-maliyet analizini göz önünde bulundurmalıdır. Buna göre mevcut denetim elemanlarının denetim araçlarını kullanım kolaylığı, eğitim ihtiyacı, kullanılacak yazılım aracının kodlanması ve bakımı, yazılım üzerinde sağlanan esnek kullanım imkanları, kaynak verinin yazılım aracını beslemesinin sağlanmasına yönelik çaba gibi maliyet faktörleri ve sağlanacak faydalar bir arada değerlendirilerek testlerin gerçekleştirilmesi sırasında bilgisayar destekli denetim tekniklerinin kullanılıp kullanılmayacağına karar verilmesi gerekmektedir. Bu nedenle bilgi sistemleri denetçisi, finansal denetim ekipleri ile entegre olarak çalışarak fayda-maliyet analizini denetim sürecinin planlaması aşamasında belirlenen denetim amaçları doğrultusunda uygun olarak yapmalıdır.

3.10.9. Bilgi Sistemleri Denetim Sonuçlarının Raporlanması

Test çalışmaları tamamlandığında ve çalışma kağıtlarına göre bilgi sistemleri denetimine yönelik tespitler ortaya çıktığında denetim sonuçlarının yönetim ile paylaşılması ve tartışılması için kapanış toplantısı yapılmalıdır. Denetim amaçlarından ve denetimin kapsamından bahsetmekle birlikte bilgi sistemleri denetim sürecinin nasıl ilerlediği konusunda kısa bilgi vermek yerinde olacaktır. Ayrıca bilgi sistemleri denetçisinin aşağıdaki adımları da kapanış toplantısında gerçekleştirmesi beklenmektedir:

1. Bilgi sistemleri denetim raporunda sunulan tespitler üzerinde yönetim ile mutabık kalınması
2. Bilgi sistemleri denetim raporunda sunulan tespitlerin düzeltilmesi için yönetimden aksiyon planı ve zamanı konusunda bilgi alarak düzeltme talebinin iletilmesi

Denetim komitesine ve yönetime denetim sonuçlarının sunulmasının yanında denetim sürecinin nihai ürünü olarak denetim raporu hazırlanarak denetlenen taraf ile birlikte varsa ulaştırılması gereken resmi mercilere raporun iletilmesi gerekmektedir. Bilgi sistemleri denetim raporu genel olarak bilgi sistemleri denetçisinin tespitlerini, bu tespitlere yönelik oluşan riskleri ve düzeltme tavsiyelerini yazılı olarak iletmesinden oluşmaktadır. Rapor, gerçekleştirilen testler, çalışma kağıtları ve denetim kanıtları ile desteklenmelidir.

Bilgi sistemleri denetim raporunun özel bir formatı olmasa da çeşitli yasal düzenlemelere uygun olarak geliştirilen rapor formatları da mevcuttur. Örneğin Türk Bankacılık Sektöründe gerçekleştirilen bilgi sistemleri denetimine yönelik olarak rapor formatı Bankacılık Denetleme ve Düzenleme Kurulu ("BDDK") tarafından yayınlanan yönetmeliklere uygun olarak hazırlanmak zorundadır. Bu konuyla ilgili araştırma konumuza paralel olarak detay bilgi 3. bölüm altında verilecek olup bu bölümde genel olarak bilgi sistemleri denetim raporunun genel kabul görmüş yapı olarak hangi bölümlerinin olması gerektiği konusunda bilgi verilecektir[63]:

1. Giriş Bölümü: Bilgi sistemleri denetim raporunun ilk kısmını olup denetimin amacı, kapsamı, denetimin periyodu ve denetim prosedürlerinin test esası yöntemine göre uygulanmakla birlikte iç kontrol ortamının doğası gereği olası hata riskinin de kaçınılmaz olduğu belirtilmektedir.
2. Genel Olarak Denetim Sonucu ve Denetçinin Görüşü: Bilgi sistemleri kontrol ortamının yeterliliği ve test edilen kontrollerin etkinliği hususunda değerlendirmelerin, bu sonuçların finansal denetim ve iç kontrol ortamı üzerindeki etkilerinin de değerlendirildiği genel sonuca, denetçinin genel görüşü ile birlikte yer verilmektedir.
3. Detaylı Denetim Tespitleri ve Tavsiyeler: Bilgi sistemleri denetim süreci sonucunda yapılan tespitlerin önemliliğine göre ve raporun muhatabı kişilerin kimliğine göre bu bölümde gerekli bulgulara, bulguların yarattığı risklere ve bulguların düzeltilmesi öngörülen tavsiyelere yer verilmektedir. Örneğin denetim komitesine sunulan bir bilgi sistemleri denetim raporunda önemlilik seviyesi yüksek olan bulgulara yer verilirken yönetime tüm bulguların sunulması gibi bir yol izlenebilmektedir.
4. Denetim Sırasındaki Sınırlamalar: Denetim çalışması sırasında denetlenen tarafından ve/veya başka nedenlerde sınırlandırmalar mevcut ise bu olaylardan ve etkilerinden

[63] Johnson, **age**, 39

raporda bahsetmek gerekmektedir. Örneğin analiz yapılacak bir veri kümesinin denetlenen tarafından verilmemesi önemlilik seviyesi de göz önüne alınarak denetim çalışmasına bir sınırlama getirmektedir.

5. Genel Açıklama: Bilgi sistemleri denetim süreci sırasında genel olarak izlenen standartlara ve kılavuzlara atıfta bulunularak denetim çalışmasının gerçekleştirildiğinden bahsedilmelidir. Örneğin, Türk Bankacılık Sektöründe gerçekleştirilen bilgi sistemleri denetim çalışmalarında BDDK tarafından kabul edilen "CobiT 4.1" standart olarak kullanılmakta ve denetim faaliyetleri "CobiT 4.1" üzerinde belirtilen detay kontrol hedefleri kapsamında gerçekleştirilmektedir.

Mevzuat gereği oluşturulmuş bir format mevcut değilse genel olarak bilgi sistemleri denetim raporunun içeriğine ve hangi kısımlardan oluşacağına nihai olarak bilgi sistemleri baş denetçisi karar vermektedir. Rapor içerisinde sadece negatif yönlerin ve bulguların belirtilmesinin yanında olumlu tarafların da öne çıkarılarak bu kapsamdaki kontrollerin etkinliğinin arttırılmasına ve iyileştirilmesine yönelik yorumların eklenmesine özen gösterilebilir. Böylelikle rapor daha dengeli bir içerik içinde denetlenene sunulabilmektedir.

Denetim raporunun sunulması ile birlikte yönetim tarafından bulguların düzeltilmesine yönelik öngördüğü aksiyon planları ve yönetimin cevapları alınmalıdır. Özellikle uygulanması planlanan aksiyon planları için bir son tarih belirlenmesine ve rapordaki bulgulara göre sonraki bilgi sistemleri denetim dönemlerinde düzeltilmenin yapılıp yapılmadığının takip edilmesine özen gösterilmelidir.

Sonraki denetim dönemlerinde bulguların durumunun takip edilmesinde bulguların kritiklik derecesine ve aksiyonların belirtilen tarihte tamamlanmasına göre ek testler gerçekleştirilmeli ve bulgunun son durumu hakkında nihai karar bilgi sistemleri denetçisi tarafından oluşturulmalıdır. Bu denetim dönemi içerisindeki denetim sonuçlarının raporlanmasının yanında bir önceki dönemden gelen bulguların son durumlarının değerlendirilmesine yönelik bölüme de bilgi sistemleri denetim raporu içerisinde yer verilmelidir.

Bilgi sistemleri denetim sürecinin nihai ürünü denetim raporu olsa da bu denetim raporunun oluşmasında destek sağlayan çalışma kağıtlarının ve dokümantasyonun da bilgi sistemleri denetçisi tarafından hazırlanması beklenmektedir. Çalışma kağıtlarının ve kanıtların bulunduğu

dosyaların mülkiyeti denetlenene ait olup bu dokümanların mevzuatın gerektirdiği süre içerisinde güvenli olarak muhafaza edilmesinden bizzat bilgi sistemleri denetçisi sorumludur.

Bilgi sistemleri denetçisinin denetim süreci aşamasında oluşturması beklenen dokümanlar genel olarak şunlardır:

1. Bilgi sistemleri denetim planı, kapsamı ve denetim amaçları
2. Denetlenenin bilgi sistemleri ortamının açıklanması ve grafiksel çizimleri (ağ, sistem mimarisi vs.)
3. Bilgi sistemleri yönetimine yönelik bazı süreçler bazında yapılan yerinde gözlem çalışmalarının dokümantasyonu (Örneğin, kullanıcı hesaplarının yönetimine yönelik sürecin izlenmesi)
4. Bilgi sistemleri denetim programları
5. Gerçekleştirilen denetim prosedürlerinin sonucundaki toplantı tutanakları, listeler, analiz sonuçları gibi toplanan kanıtlar ve açıklamaları
6. Diğer denetçilerin veya uzmanların çalışmalarının kullanılmasına yönelik dokümanlar
7. Denetim sonucundaki bulguların listesi ve sınıflandırılması

Yukarıda bahsi geçen dokümanların kaliteli oluşturulma derecesi, bu dokümanlardan desteklenen ve beslenen bilgi sistemleri denetim raporunun kalitesini de aynı derece arttıracak ve raporun içeriğini destekleyecektir. Bu nedenle bilgi sistemleri denetim süreci sonucunda oluşan tüm dokümanların gözden geçirilmesi ve olası eksikliklerin tamamlanması hem dokümantasyonun ve raporun hem de denetim faaliyetlerinin kalitesini arttıracaktır.

4. TÜRK BANKACILIK SEKTÖRÜNDE BİLGİ SİSTEMLERİ DENETİMİ VE YASAL MEVZUAT

Türk bankacılık sektöründe Bankacılık Düzenleme ve Denetleme Kurumu ("BDDK") tarafından 31 Aralık 2007 tarihi itibarıyla 16 Mayıs 2006 tarih 26170 sayılı Resmi Gazete'de yayımlanan Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik kapsamında bilgi sistemi denetime dair zorunlu esaslar belirlenmiştir. Buna göre bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemlerin üzerindeki uygulama kontrollerine ve genel kontrol alanlarına dair bağımsız denetim faaliyetleri Türkiye'de faaliyet gösteren tüm bankalar için zorunlu hale getirilmiştir.

Ayrıca bankalar tarafından bilgi sistemlerine yönelik olarak genel kontrollerin ve uygulama kontrollerinin 14 Eylül 2007 tarih ve 26643 sayılı Resmi Gazete'de yayımlanan Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ'de belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesi zorunlu hale getirilmiştir.

Bilgi teknolojilerinin yoğun olarak kullanıldığı Türk Bankacılık sektöründe bu kapsamdaki mevzuat değişiklikleri ile bankaların daha güvenilir ve kontrollü bilgi sistemleri yönetiminin oluşması, dolayısıyla da Türkiye'de bilgi sistemleri denetiminin yaygınlaşmasına katkıda bulunulmuştur. Bu bölümde genel olarak Türk Bankacılık sektöründe bilgi sistemleri denetiminin esasları ve getirilen yasal düzenlemeler üzerine açıklamada bulunulacaktır.

4.1. Bankalarda Bilgi Sistemleri Denetiminin Amacı ve Kapsamı

26170 sayılı "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik", bankaların bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemlerinin, yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesiyle ilgili usul ve esasları düzenleme amacını taşımaktadır[64].

Yönetmelik gereği bankalarda gerçekleştirilecek bilgi sistemleri denetimi, uygulama kontrolleri denetimi ile genel kontrol alanları denetimini kapsamaktadır. Her sene uygulama kontrolleri

[64] BDDK, "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**" (Madde 1, Sayı 26170; Tarih: 16 Mayıs 2006), 1

denetiminin bağımsız denetim kuruluşlarında gerçekleştirilmesi gerekirken, yönetmelik gereği genel kontrol alanlarına yönelik denetim iki sene de bir gerçekleştirilmesi zorunlu tutulmuştur.

Bağımsız denetim çalışmaları genel olarak denetlenen bankayı ve bu bankanın finansal tablolarında önemli etkileri bulunan iştirakleri ve/veya bağlı ortaklıkları kapsamaktadır.

Bilgi sistemleri denetim kapsamına girmesi öngörülen uygulama kontrollerine ait süreçlerin önemlilik kavramı göz önüne alınarak belirlenmesi gerekmektedir. Genel olarak önemlilik kavramının değerlendirilmesi mesleki tecrübeye dayalı bir yargı konusu olup kontrol zayıflıkları sonucu ortaya çıkan hataların, ihmallerin, prosedürlere aykırılıkların ve yasa dışı fiillerin, bankaların finansal verilerini raporlamalarına, güvenli ve kesintisiz hizmet sağlamalarına olan etkisinin değerlendirilmesidir. Ayrıca uygulama süreçleri üzerindeki finansal verilerin bütünlüğü, tutarlılığı, güvenilirliği, gereken durumlarda gizliliği ve süreklilik ihtiyacı önemlilik seviyesinin değerlendirilmesinde dikkate alınmaktadır. Uygulama kontrolleri denetimi çerçevesinde denetlenen bankadaki süreçlerin önemlilik seviyeleri değerlendirilerek denetim kapsamı belirlenmek ve süreç üzerindeki kontroller test edilmektedir. Aşağıda uygulama kontrolleri denetimi kapsamına girebilecek süreçlerden bazıları görülebilmektedir:

1. Menkul Kıymetler ve Hazine Süreci
2. EFT ve SWIFT Varlık Transfer ve Mutabakat Süreci
3. Alternatif Dağıtım Kanalları Süreci
4. Krediler Süreci
5. Mevduat Süreci v.b.

Uygulama kontrolleri denetiminin kapsamının belirlenmesinin yanında genel kontrol alanlarına yönelik denetim kapsamı da bağımsız denetim kuruluşu tarafından belirlenmelidir. Ancak uygulama kontrolleri denetimindeki önemlilik seviyesine göre kapsam belirlenmesinden farklı olarak yasal mevzuat genel kontrol alanları denetiminin kapsamını belirlemiş bulunmaktadır. Buna göre 31 Aralık 2007 tarihi itibarıyla 16 Mayıs 2006 tarih 26170 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" kapsamındaki 14, 15, 16 ve 17. maddelerinde genel kontrol alanlarının denetlenmesi ile ilgili kapsam belirlenmiş bulunmaktadır. Yönetmelik genel kontrol alanlarının denetiminde ISACA isimli uluslararası bir kuruluşun oluşturduğu BT yönetişim

standardı olan "Bilgi Teknolojilerine Yönelik Kontrol Hedefleri" ("CobiT") dokümanını kapsam olarak zorunlu kılmıştır.

Buna göre bilgi sistemleri genel kontrol alanları denetimi kapsamında aşağıdaki süreçler bazıda denetim faaliyetlerinin bağımsız denetim kuruluşu tarafından yürütülmesi zorunlu kılınmıştır.

1. **PO** (Plan and Organize) - Planlama ve Organizasyon
2. **AI** (Acquire and Implement) - Tedarik ve Uygulama
3. **DS** (Delivery and Support)- Hizmet Sunumu ve Destek
4. **ME** (Monitor and Evaluate)- İzleme ve Değerlendirme[65]

Yukarıdaki kapsama ek olarak 14 Eylül 2007 tarihli ve 26643 sayılı "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler Tebliği" 1 Ocak 2008 tarihinde yürürlüğe girmiş bulunmaktadır. "Genel Kontrol Alanları" ve "Uygulama Kontrolleri" denetim çalışmaları kapsamında, bu tebliğin gereklerinin de denetlenen bankalar tarafından yerine getirilip getirilmediğinin belirlenmesi bağımsız denetim kuruluşlarının çalışmalarının kapsamına girmektedir.

4.2. Bankalarda Bilgi Sistemleri Denetiminde Yetkili Kuruluşlar ve Aranan Şartlar

Bankalarda bilgi sistemi denetimi yapmak isteyen yetkili bağımız denetim kuruluşlarının öncelikle iki şartı sağlamaları gerekmektedir:

1. "Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ"e (Seri: X, No:22) göre 3. ve 4. maddelerdeki kuruluş, yönetici ve bağımsız denetçi şartlarını yerine getirerek bankalarda bağımsız denetim yapma yetkisine sahip olunması gerekmektedir.
2. 26170 sayılı "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" gereği bilgi sistemleri denetim faaliyetlerini yürütecek yeterli sayı ve nitelikte denetçi istihdam edilmesidir.

İlk şartın detaylarını açıklamak gerekirse, bağımsız denetim yetkisini alacak kuruluşun öncelikle aşağıdaki kuruluş şartlarını yerine getirmesi gerekmektedir[66]:

[65] ISACA COBIT, **age**, 12–13
[66] SPK, "**Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ**" (2. Kısım, Madde 3 ve 4, Seri: X, No: 22), 5-6

1. Anonim şirket şeklinde kurulmuş olması ve hisse senetlerinin nama yazılı olması,
2. Ticaret unvanlarında "bağımsız denetim" ibaresinin bulunması,
3. Şirket ortaklarının ve yöneticilerinin SPK'nın Seri X / No: 22 bağımsız denetim tebliğinin 4. maddesindeki şartları yerine getirmesi, (Müflis olmamaları ve yüz kızartıcı bir suçtan mahkum bulunmamaları, Türkiye'de yerleşik olmaları gibi şartlar belirtilmektedir.)
4. Esas sermayenin en az %51'inin sorumlu ortak baş denetçilere ait olması,
5. Sadece bağımsız denetim ve mesleki alanda faaliyet göstermeleri,
6. Organizasyon, mekan, teknik donanım, belge ve kayıt düzeninin bağımsız denetim işini yürütecek düzeyde bulunması
7. Hazine Müsteşarlığı ve Hazine Müsteşarlığının bağlı olduğu Bakanlık tarafından belirlenen usul ve esaslar çerçevesinde mesleki sorumluluk sigortası yaptırmaları gerekmektedir.

İkinci şartı detay olarak açıklamak gerekirse, bilgi sistemleri denetimi faaliyetinde bulunmak isteyen bağımsız denetim kuruluşu tarafından BDDK'ya verilecek başvuru dilekçesine yeterli ve uygun vasıfta denetçi istihdam ettiğini belgeleri ile birlikte göstermek zorundadır. Buna göre[67]:

1. İstihdam edilen denetçilerin varsa Bilgi Sistemleri Denetçisi Sertifikalarını ("CISA"), ve bilgi sistemleri denetimi kapsamında aldığı veya verdiği eğitimlere ilişkin belgelerin noterce tasdik edilmiş kopyaları,
2. İstihdam edilen denetçilerin mesleki tecrübelerini içeren ayrıntılı özgeçmişleri,
3. İstihdam edilen denetçilerinin adli sicil belgeleri,
4. İstihdam edilen denetçilerinin birden fazla bağımsız denetim kuruluşunda ortaklığının bulunmadığına ve denetlenenlerde veya 2499 sayılı Sermaye Piyasası Kanununa tabi şirketlerde denetim yapma yetkisi iptal edilmiş olan bağımsız denetim kuruluşlarında ortak veya yetki iptaline neden olan denetim faaliyetinde bağımsız denetçi veya denetçi sıfatı ile yer almadığına dair beyanları,

[67] BDDK, "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**" (Madde 6, Sayı 26170; Tarih: 16 Mayıs 2006), 2

5. Son olarak istihdam edilen denetçilerinin mesleki faaliyetler dışında çalışmadıklarına dair beyanları BDDK bildirilmek zorundadır.

BDDK'ya sunulan bilgi ve belgeler çerçevesinde kurul tarafından mesleki ve teknik açıdan değerlendirme yapılmaktadır. Hatta yeterliliklerin tespitine yönelik yerinde inceleme de yapılarak talepte bulunan kuruluşlara kurul kararıyla uygun bulunduğu takdirde bankalarda bilgi sistemi denetimi yapma yetkisi verilmektedir.

Kurul kararıyla bankalarda bağımsız denetim yapma yetkisi 01.03.2009 tarihi itibarıyla aşağıdaki kuruluşlara verilmiştir[68]:

1. Güney Bağımsız Denetim ve Serbest Muhasebeci Mali Müşavirlik A.Ş.
2. Rehber Bağımsız Denetim ve Yeminli Mali Müşavirlik A.Ş.
3. Başaran Nas SMMM A.Ş.
4. Denetim Serbest Mali Müşavirlik A.Ş.
5. Akis Serbest Muhasebeci Mali Müşavirlik A.Ş.

4.3. Bilgi Sistemleri Denetimindeki Yükümlülükler

26170 sayılı "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik" hem denetlenen bankalara hem de bilgi sistemleri denetimini gerçekleştirecek kuruluşlara bazı yükümlülükler getirmektedir.

4.3.1. Denetlenen Bankaların Yükümlülükleri

Bankaların bilgi sistemleri ve bunlara ait dokümantasyon; finansal veri üretim süreçlerine ait dokümantasyon ile her türlü kayıt, bilgi, belge, yapı ve uygulama; bilgi sistemleri kapsamındaki her türlü genel kontrollerin ve uygulama kontrollerinin oluşturulması, etkin olarak işletilmesi ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması denetlenen bankaların sorumluluğu altındadır[69].

Denetlenen bankalar, denetçi bağımsız kuruluşun bilgi sistemleri denetimine yönelik talep ettiği her türlü bilgi ve belgeyi vermekle yükümlü tutulmaktadır. Buna ek olarak denetlenen bankalar,

[68] BDDK, "**Bilgi Sistemleri Denetim Yetkisi Verilen Kuruluşlar**", www.bddk.org.tr [28.03.2009]
[69] BDDK, "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**" (Madde 10, Sayı 26170; Tarih: 16 Mayıs 2006), 4

faaliyetlerinde kullandıkları tüm sistem ve uygulamaları ve kullanım amaçlarını kapsayan uygulama listesini bildirmekle yükümlüdür. Örneğin, hazine ve menkul kıymet sistemleri, krediler, mevduat gibi temel bankacılık sistemleri gibi bankacılık fonksiyonlarının yerine getirildiği tüm sistemleri kullanım alanlarına göre denetçiye bildirmekle yükümlüdür.

Finansal veri üretim süreçlerini ve içerdikleri verileri oluşturan, destekleyen, kullanan ve saklayan tüm kritik sistemler ve uygulamalar için üzerlerindeki uygulama kontrolleri denetlenen tarafından belirlenmek, değerlendirilmek ve raporlanmak zorundadır. Uygulama kontrollerinin değerlendirilmesi aşamasında aşağıdaki kriterleri göz önünde bulundurması gerekmektedir:

1. Sistemlerin yazılı dokümantasyonlara uyumu
2. Yazılı kontrollerin yeterliliği ve uygulanması
3. Sistemlerin içerdikleri verilerin güvenliği, bütünlüğü ve sürekliliği

Uygulama kontrolleri ile ilgili denetlenen bankalara verilen bu sorumlulukların yanında genel kontrol alanlarının denetimine yönelik sorumluluklar da verilmiştir. Buna göre, CobiT kapsamında yönetmeliğin 14. maddesinden 17. maddesine kadar belirlenen genel kontrol konusu olan her bir sürece ilişkin olarak aşağıda sayılan hususlara uygun bir ortamın tesis edilmesinden sorumludur[70].

1. ***Süreç Sahibi***: Her genel kontrol konusu süreç için sorumluluğu açıkça tanımlanmış bir süreç sahibi atanır.
2. ***Tekrarlanabilirlik***: Genel kontrol konusu süreçler tekrarlanabilir biçimde tanımlanır.
3. ***Hedefler ve Amaçlar***: Etkin bir biçimde çalışmalarını sağlamak amacıyla her genel kontrol konusu süreç için açıkça tanımlanmış hedefler ve amaçlar oluşturulur.
4. ***Roller ve Sorumluluklar***: Etkin bir biçimde çalışmalarını sağlamak amacıyla her genel kontrol konusu süreç için açık bir şekilde roller, faaliyetler ve sorumluluklar tanımlanır.
5. ***Süreç Performansı***: Belirlenen hedeflere göre her genel kontrol sürecinin performansı ölçülür.

[70] BDDK, "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**" (Madde 10, Sayı 26170; Tarih: 16 Mayıs 2006), 4

6. ***Politikalar, Planlar ve Prosedürler***: Her bir genel kontrol süreciyle ilgili politikalar, planlar ve prosedürler yazılı hale getirilir, belli aralıklarla gözden geçirilir, güncellenir, onaylanır ve tüm ilgili birimlere duyurulur[71].

4.3.2. Denetleyen Yetkili Denetim Kuruluşlarının Yükümlülükleri

En genel şekilde bağımsız denetim yapan kuruluşların üzerlerine düşen sorumluluk, yapılan denetim çalışmasına istinaden görüş bildirmektir. Detay olarak bu sorumluluğu açıklamaya çalışırsak; bağımsız denetimi gerçekleştiren kuruluşların üzerine düşen sorumluluk, denetlenen bankaların bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve 1 Kasım 2006 tarih ve 26333 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Gerçekleştirecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik" ile 16 Mayıs 2006 tarih ve 26170 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik"te belirtilen usul ve esaslara uygun bir denetim çalışması gerçekleştirmektir.

Bağımsız denetim kuruluşları, denetim faaliyetleri çerçevesinde bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemler üzerindeki kontrollerin tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyulan ölçüde benzeri diğer denetim tekniklerinin uygulanmasını gerçekleştirmekle yükümlüdür.

Gerçekleştirilen denetim faaliyetleri sonucunda tespit edilen bulgular mevzuatta yer verilen kıstaslara göre sınıflandırılarak, değerlendirilerek bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemleri üzerinde görüş bildirilmesi ve rapora bağlanmasından bağımsız denetim kuruluşları sorumlu tutulmaktadır.

Yukarıda bahsi geçen temel yükümlülüklerin haricinde aşağıdaki ek sorumluluklar da denetçi bağımsız denetim kuruluşlarına yönetmelik gereği yüklenmiş bulunmaktadır[72]:

1. Ortaya çıkan hata ve suiistimaller hakkında denetlenen bankaların ilgili yöneticilerine her aşamada bilgi verilmesi zorunludur.

---

[71] BDDK, "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**" (Madde 10, Sayı 26170; Tarih: 16 Mayıs 2006), 4-5

[72] BDDK, "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**" (Madde 11, Sayı 26170; Tarih: 16 Mayıs 2006), 5

2. Bağımsız denetim kuruluşunun ana sözleşme, yönetim ve organizasyon yapılarındaki değişiklikler ile bilgi sistemleri denetim kadrosunda meydana gelen her türlü değişikliğin gerekçeleri ile bildirilmesi zorunludur.
3. Yetkili denetçi kuruluşlar, istihdam ettikleri bilgi sistemleri denetçilerinin süreklilik arz edecek şekilde eğitim programlarına katılmalarını sağlamakla yükümlüdür.
4. Yetkili denetçi kuruluş, sözleşme süresi içinde bilgi sistemleri denetiminden çekilmesi ya da denetim sözleşmesinin feshedilmesi hallerinde, durumu gerekçesiyle birlikte beş iş günü içerisinde BDDK'ya bildirmek zorundadır.
5. Bilgi sistemleri denetçisi; mesleğin zorunlu kıldığı mesleki ilkelere ve yasal mevzuata uymak zorundadır.
6. Bilgi sistemleri içerisinde yer alabilecek riskleri ve zayıflıkları dikkate alarak ve mesleki şüphecilik çerçevesinde bir bilgi sistemleri denetimi planı hazırlamak, denetlenene sunmak ve uygulamak, yöneticilerin açıklamalarını yeterli denetim kanıtı olarak kabul etmemek ve bilgi sistemlerine ve finansal veri üretim süreçlerine ilişkin bilgi sistemleri denetimi raporunu oluşturmak ile yükümlüdür
7. Bilgi sistemleri denetimi faaliyeti sırasında uygunsuz işlemlerin, suiistimal veya hataların tespiti durumunda, denetlenen bunları gidermiş olsa dahi bu hususun bilgi sistemleri denetçisi tarafından ivedilikle BDDK'ya ve banka yöneticilere bildirilmesi ve bilgi sistemleri denetimi raporunun bu çerçevede hazırlanması zorunludur.
8. Denetçiler, bilgi sistemleri denetimi çerçevesinde ilgililerce kendilerine tevdi edilen dokümantasyon ve belgeleri işlerinin gerektirdiği süre içinde iyi niyetle ve değiştirmeden muhafaza etmekle ve işin bitiminde iadesiyle yükümlüdürler. Bunun yanında denetim kanıtı oluşturan dokümanların kopyaları yetkili denetçi kuruluş tarafından saklanabilmektedir.
9. Yetkili kuruluşlar ve denetçiler, bilgi sistemleri denetimi faaliyetleri dolayısıyla öğrendikleri ve ilgili düzenleme hükümlerine göre sır kapsamında bulunan bilgileri kanunen açıkça yetkili kılınanlardan başkasına açıklayamaz ve doğrudan veya dolaylı şekilde kendi yararlarına kullanamazlar.

10. Yetkili bağımsız denetçi kuruluşlar, bilgi sistemleri denetiminin gerçekleştirileceği dönemde, denetlenenin bağımsız denetim faaliyetini de yürütüyor olmak zorundadırlar.

Yönetmelikle getirilen son maddedeki zorunluluktan yetkili yasal merciinin finansal bağımsız denetim faaliyeti ile bilgi sistemleri denetiminin bir arada aynı yetki kuruluş tarafından yapılmasını zorunlu kılmakta ve bu vasıtayla daha etkin bir denetim olan entegre denetimin gerçekleşmesini desteklemektedir.

4.4. Bilgi Teknolojilerine İlişkin Kontrol Hedefleri (CobiT)

1 Kasım 2006 tarih ve 26333 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Gerçekleştirecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik" genel kontrol alanlarının denetimi kapsamında uluslararası bir kuruluş olan Bilgi Teknolojileri Yönetimi Enstitüsü tarafından yayınlanan "CobiT" dokümanını standart olarak kabul etmiştir.

CobiT ("*Control Objectives for Information and related Technology*") genel olarak kurumların BT yönetişim alanında gelişme kaydetmesindeki amaçları ve yolları gösteren, kurumların BT yönetişim alanında kendilerini değerlendirmeyi sağlayan yol gösterici bir dokümandır. Bu nedenle CobiT'in detay açıklamalarına girmeden önce, ulaşmayı hedeflediği etkin BT yönetişimin tanımını yapmak yerinde olacaktır[73].

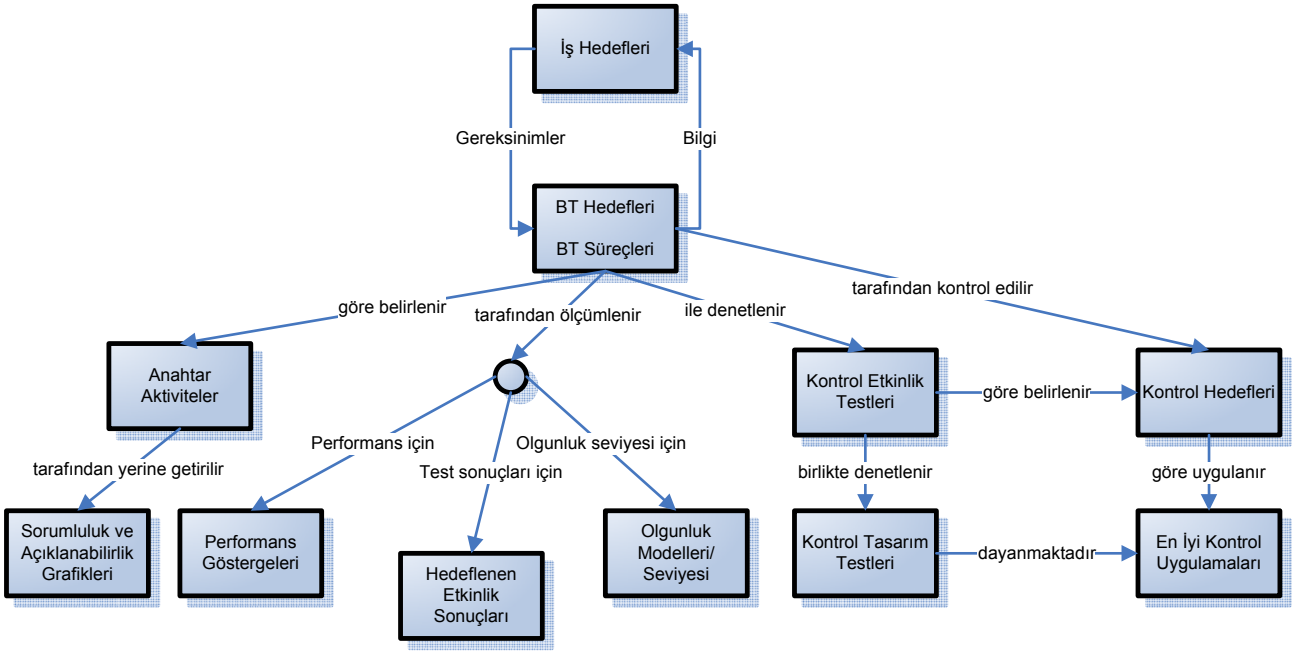
BT Yönetişim ("IT Governance"), üst yönetimin sorumluluğunda olup liderlik, organizasyonel yapı, kurumun stratejilerinin ve hedeflerinin genişletilmesinde ve desteklenmesinde BT fonksiyonundan stratejik olarak faydalanılmasını sağlayan yönetim biçimi ya da anlayışıdır. CobiT bu kapsamda konusunda uzman kişilerin fikir birliğine vardığı ve BT yönetişimin etkin olarak sağlanmasında destek olacak en iyi örnekleri, yönetilebilir ve mantıksal bir çerçevede sunmayı hedefleyen bir dokümandır[74].

BT'nin iş amaçlarına uygun olarak servis sağlaması için yönetim BT'ye yönelik iç kontrol ortamını veya çerçevesini tesis etmek zorundadır. Bu kapsamda CobiT bu ihtiyaca yönelik olarak aşağıdaki faaliyetlerde yardımcı olarak katkıda bulunmayı hedeflemektedir[75].

1. İş gereksinimleri ile BT faaliyetleri arasında ilişkiyi tesis etmek ve korumak

[73] Robert Lawton, "**Transitioning IT From a Compliance to a Value-driven Enterprise Using CobiT**", Information Systems Control Journal, volume 6 (2007), 43
[74] ISACA COBIT, **age**, 5
[75] ISACA COBIT, **age**, 6

2. BT aktivitelerinin genel kabul görmüş standartlara göre yönetmek, organize etmek.
3. BT kaynaklarını belirlemek ve etkin olarak yönetmek
4. BT faaliyetleri alanında yönetimin kontrol hedeflerini belirlemek



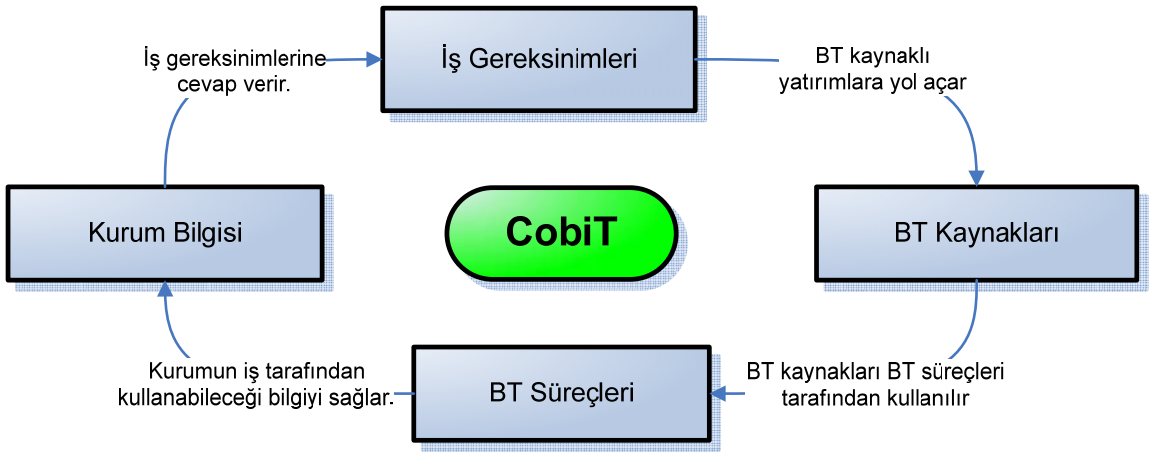
Şekil 7: CobiT Model Bileşenleri Arasındaki İlişkiler

ISACA, "**Control Objectives for Information and related Technology**" (USA: ISACA, 2007), 8

Yukarıdaki şekil üzerinde CobiT ile getirilen BT yönetişim anlayışı ve kavramlar arasındaki ilişkiler ifade edilmektedir. Yukarıdaki şekilden de anlaşılacağı gibi CobiT kontrol ortamının gereksinimleri, teknik sorunlar, iş riskleri ve kontrol seviyesinin hak sahipleri ile paylaşımı gibi konularda uyumluluğun sağlanmasında yöneticilere araç sağlayan bir çerçeveyi oluşturmaktadır. Bu kapsamda öncelikle iş hedefleri ile BT hedefleri ve süreçleri arasındaki uyumluluğu sağlamayı hedeflemektedir. Sonrasında uyumluluğun sağlanması için anahtar BT aktivitelerin nasıl belirleneceğini ve bu aktivitelere kimlerin sorumlu olarak atanacağını dair yol göstermektedir. Diğer taraftan CobiT'in önerdiği kontrol hedefleri ile belirlenen BT aktivitelerinin nasıl denetlenip değerlendirileceği ve BT aktivitelerine yönelik faaliyetlerin nasıl ölçümleneceğine dair yöneticilere yol göstermektedir.

CobiT'in yukarıda bahsi geçen çerçevede uygulanmasıyla BT yönetişim kapsamında aşağıdaki faydaların kuruma sağlanması hedeflenmektedir[76]:

1. İş odaklı ve iş hedeflerine uyumlu BT stratejisi ve yönetimi
2. BT fonksiyonunun yönetim tarafından daha anlaşılır olması
3. Süreçlerin belirginleşmesi, dolayısıyla da açık olarak süreç sahipliklerinin ve sorumluluklarının belirlenmesi
4. Üçüncü taraf yasal düzenleyiciler ve kurumlar tarafından genel kabul görmüşlük
5. Hak sahipleri arasında ortak bir anlayışın BT yönetişimi kapsamında oluşturulması
6. İç kontrol ortamının BT faaliyetleri açısından güçlendirilmesi



Şekil 8: CobiT Temel Prensipleri

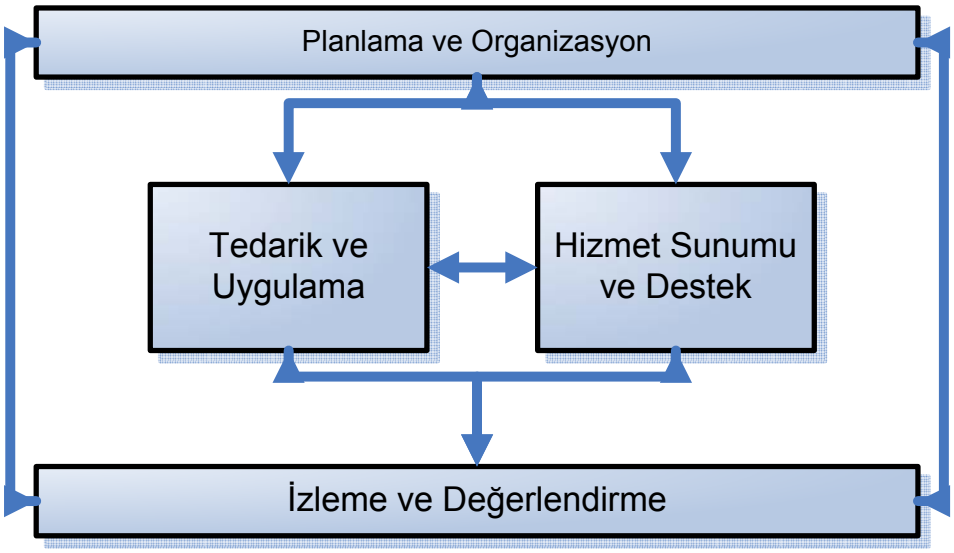
ISACA, "**Control Objectives for Information and related Technology**" (USA: ISACA, 2007), 8

CobiT yukarıdaki şekil ile de ifade edildiği gibi iş gereksinimlerine göre BT kaynaklarının oluşturulması, etkin BT süreçleri ile bu kaynakların yönetimi ve iş gereksinimlerine cevap veren kurum bilgisinin oluşturulmasını temel prensip olarak belirlemiştir.

[76] ISACA COBIT, **age**, 8

Bu kapsamda planlama, organize etme, yürütme ve izleme/kontrol fonksiyonlarına benzer olarak CobiT 34 adet kontrol hedefinin belirtildiği BT süreci dört ana genel kontrol alanı altında toplamıştır[77]:

1. ***Planlama ve Organizasyon***: BT faaliyetleri kapsamında uygulama geliştirilmesi ve tedarik edilmesi ile BT hizmetlerinin sunulması, iş tarafına destek faaliyetlerinin sunulması kapsamında yön gösterici olan 10 adet kontrol hedefini tanımlamaktadır.
2. ***Tedarik ve Uygulama***: İş gereksinimleri kapsamında uygulama çözümlerinin oluşturulması ve servislere dönüştürülmesine ait 7 adet kontrol hedefini tanımlamaktadır.
3. ***Hizmet Sunumu ve Destek***: Uygulama çözümlerine ait servislerin belirlenmesi ve bunların iş tarafı için yönetilmesine ve idame ettirilmesine yönelik 13 adet kontrol hedefini tanımlamaktadır.
4. ***İzleme ve Değerlendirme***: Son olarak belirlenen BT süreçlerinin ve faaliyetlerinin istenen seviyede yönetilip yönetilmediği konusunda izleme ve değerlendirme yapılmasına ait 4 adet kontrol hedefini tanımlamaktadır.



Şekil 9: CobiT Kontrol Başlıkları Arası İlişkiler

ISACA, "**Control Objectives for Information and related Technology**" (USA: ISACA, 2007), 12

[77] ISACA COBIT, **age**, 12

Dört ana genel kontrol alanının yukarıdaki açıklamalar kapsamında birbirleri ile olan ilişkileri yukarıdaki şekil üzerinden de görülebilmektedir.

1 Kasım 2006 tarih ve 26333 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Gerçekleştirecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik" ile BDDK Türk bankacılık sektöründeki bankalarda yapılacak bilgi sistemleri denetiminin genel kontrol alanı kapsamındaki denetiminde yukarıda ifade edilen CobiT'in dört ana kontrol alanını temel almıştır. Buna göre yönetmeliğin 14. ve 17. maddeleri arasında genel kontrol alanı denetimini CobiT'de olduğu gibi dört temel kısma bölmüştür:

1. *Planlama ve organizasyon faaliyetlerinin denetimi*
2. *Tedarik ve uygulama faaliyetlerinin denetimi*
3. *Hizmet sunumu ve destek faaliyetlerinin denetimi*
4. *İzleme ve değerlendirme faaliyetlerinin denetimi*

Bu kapsamdaki detay bilgi yönetmeliği ve CobiT'e uyumlu olarak "4.7 Genel Kontrol Alanlarının Denetimi" bölümünde verilmiştir.

4.5. Bilgi Teknolojileri Yönetimine İlişkin İlkeler ve Denetim Kapsamı

14 Eylül 2007 tarihli ve 26643 sayılı "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler Tebliği" 1 Ocak 2008 tarihinde yürürlüğe girmiş bulunmaktadır. Yayınlanan ilkeler tebliği kapsamında yasal kurum (BDDK) "Genel Kontrol Alanları" ve "Uygulama Kontrolleri" denetim çalışmaları kapsamında, denetlenen bankalar tarafından yerine getirmesi gerekli olan şartları, diğer bir ifadeyle bilgi sistemlerinin yönetiminde esas alınacak asgari usul ve esasları belirlenmiş bulunmaktadır. BDDK tebliğin yayınlanma tarihinden itibaren bankalara tebliğdeki usul ve esaslara uymaları için azami iki yıl, diğer bir ifadeyle 2010 yılına kadar, süre tanımıştır.

Yayınlanan tebliği genel olarak üç temel bölümden oluşmaktadır. Bunlar:

1. *Bilgi Sistemlerine Yönelik Risk Yönetimi*
2. *Bilgi Sistemlerine Yönelik İç Kontrollerin Tesisi ve Takibi*
3. *İnternet Bankacılığı ve ATM gibi Önemlilik Arz Eden Bazı Konular Hakkında Hükümler*

Tebliğin ilk bölümü olan "*Bilgi Sistemlerine Yönelik Risk Yönetimi*" kapsamında aşağıdaki konu başlıkları altında bankaların yerine getirmekle zorunlu olduğu hükümler ifade edilmiştir. Aşağıdaki konu başlıklarının çoğu CobiT çerçevesine uyum ile birlikte sağlanabilen konular olmakla birlikte yayınlanan tebliğ sayesinde bu konular denetlenen bankalar için da belirgin hale getirilmek istenmiştir. Bunlar;

- *Bilgi Sistemleri Risk Yönetimi:* Denetlenen bankaların, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor olmasından kaynaklanan riskleri ölçmesi, izlemesi, kontrol etmesi ve raporlaması için tebliğde belirtilen esaslar ölçüsünde asgari önlemleri alması gerektiği belirtilmektedir[78].
- *Yönetim Gözetimi:* Bilgi sistemleri kullanımından kaynaklanan risklerin yönetilmesi için denetlenen bankaların üst yönetiminin etkin bir gözetim sürecini tesis etmesi gerektiği belirtir. Bu amaç kapsamında bankaların üst yönetimi tarafından değerlendirilmiş ve uygunluğu onaylanmış kapsamlı bir süreç hazırlanmalı ve bilgi sistemlerinin kullanımından kaynaklanan riskler bu sayede yönetilmelidir.
- *Güvenlik Kontrol Sürecinin Tesis Edilmesi ve Yönetimi:* Bilgi sistemlerinin ve üzerinde islenmek, iletilmek, depolanmak ve yedek olarak saklanmak üzere bulunan verilerin gizlilik, bütünlük ve ulaşılabilirliklerini sağlayacak önlemlere ilişkin kontrol altyapısının geliştirilmesi ve düzenli olarak güncellenmesi, denetlenen bankaların üst yönetimi gözetiminde tebliğ esaslarına uygun olarak sağlanmak zorundadır.
- *Bilgi Sistemlerine İlişkin Destek Hizmeti Alım Sürecinin Yönetimi:* Bankaların bilgi sistemleri kapsamında aldıkları destek hizmetlerine ilişkin olarak, söz konusu hizmetin destek hizmeti alımı yoluyla gerçekleştirilmesinin banka açısından doğuracağı risklerin yeterli düzeyde değerlendirilmesi, yönetilmesi ve destek hizmeti kurulusu ile ilişkilerin etkin bir şekilde yürütülmesi için asgari olarak tebliğ esasları çerçevesinde etkin bir gözetim mekanizması denetlenen bankaların üst yönetimi tarafından tesis edilmek zorundadır.
- *Kimlik Doğrulama:* Bankaların bilgi sistemleri üzerinde gerçeklesen işlemler için uygun bir kimlik doğrulama mekanizması tesis etmesi gerekmektedir. Bilgi sistemleri veya

[78] BDDK, "**Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ**" (Madde 5, Sayı 26643; Tarih 14 Eylül 2007), 2

uygulamalar üzerinde kullanıcıların oturum açılışından kapanışına kadar tüm süreci içinde barındıracak bir mekanizmanın getirilmesi gerekmektedir.

- *İnkar Edilmezlik ve Sorumluluk Atama:* Bilgi sistemleri dâhilinde gerçeklesen ve kapsamını bankaların belirleyeceği kritik işlemler için, inkâr edilemezlik ve sorumluluk atama imkânlarını içeren tekniklerin kullanılması zorunludur[79].

- *Görevler Ayrılığı Prensibi:* Bilgi sistemlerinin yönetimine yönelik faaliyetler (uygulamaların geliştirilmesinde, veritabanı yönetimi vb.) görevler ve sorumluluklar ayrılığı prensibine göre çalışanlara atanmak zorundadır. Bu prensibe göre başında sonuna hiçbir kritik faaliyeti tek bir kişinin tamamlamamasını sağlamak gerekmektedir. Ek olarak bankaların belirledikleri görevler ve sorumluluklar görevler ayrılığı kurallarına göre periyodik olarak atanan sorumlulukları gözden geçirmek zorundadır.

- *Yetkilendirme:* Bilgi sistemlerine ilişkin veritabanlarına, uygulamalara ve sistemlere erişim için denetlenen bankaların uygun bir yetkilendirme ve erişim kontrollerini tebliğdeki esaslara uygun olarak oluşturmaları gerekmektedir. Bilgi sistemlerindeki yetkilendirme düzeyinin ve erişim haklarının atanmasında kullanıcıların görev ve sorumlulukları göz önünde bulundurularak, gerekli olacak en düşük yetkinin atanması ve en kısıtlı erişim hakkının verilmesi yetkilendirme sürecinde temel yaklaşım olarak kabul edilmek zorundadır.

- *İşlemlerin, Kayıtların ve Verilerin Bütünlüğü:* Bilgi sistemleri üzerinden gerçeklesen işlemlerin, kayıtların ve verilerin bütünlüğünün sağlanmasına yönelik gerekli tedbirlerin denetlenen bankalar tarafından tebliğdeki gerekli esaslar çerçevesinde alınması zorunlu olup, bunların doğruluğunun, tamlığının ve güvenilirliğinin de temin edilmesi gerekmektedir.

- *Denetim İzlerinin Oluşturulması:* Bilgi sistemleri üzerindeki riskler, sistemlerin boyutu ve faaliyetlerin karmaşıklığı göz önünde bulundurularak bilgi sistemlerinin kullanımına ilişkin etkin bir denetim izi kayıt mekanizması denetlenen bankaların bilgi sistemleri için oluşturulmak zorundadır. Bu sayede bilgi sistemleri dâhilinde gerçeklesen ve bankacılık

[79] BDDK, "**Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ**" (Madde 6-10, Sayı 26643; Tarih 14 Eylül 2007), 3-5

faaliyetlerine ait kayıtlarda değişikliğe sebep olan işlemlere ilişkin yeterli detayda ve açıklıkta bilgi edinilmesinin, tutulan denetim izleri ile sağlanması hedeflenmektedir.

- *Veri Gizliliği:* Denetlenen bankalar, bilgi sistemleri faaliyetleri kapsamında gerçekleştirdikleri işlemlerin ve bu işlemler kapsamında iletilen, işlenen ve saklanan verilerin gizliliğini sağlayacak kontrol ortamını tebliğde belirtilen mevzuat hükümlerine uygun olarak sağlamak zorundadır[80].
- *Müşterilerin Bilgilendirilmesi:* Denetlenen bankalar tarafından sunulan alternatif dağıtım kanalları (internet, telefon, televizyon, WAP/GPRS, ATM vb.) hizmetlerinden yararlanacak müşteriler; hizmetlere ilişkin şartlar, riskler ve istisnaî durumlarla ilgili olarak açık bir şekilde bilgilendirilmek zorundadır. Buna ek olarak bilgi sistemlerinden ve bunlara dayalı olarak verilen hizmetlerden dolayı müşterilerin yasayabileceği sorunların takip edilebileceği ve müşterilerin şikâyetlerini ulaştırmalarına imkân tanıyacak mekanizmaların da denetlenen bankalar tarafından oluşturulması zorunlu tutulmaktadır.
- *Müşteri Bilgilerinin Mahremiyeti:* Denetlenen bankalar, faaliyetlerinin ifası sırasında bilgi sistemleri aracılığıyla edindiği veya sakladığı müşteri bilgilerinin mahremiyetini sağlamaya yönelik prosedürleri ve süreçleri oluşturmak zorundadır.
- *Bilgi Sistemlerine İlişkin İş Sürekliliği ve Kurtarma Planı*: Denetlenen bankalar, kullandıkları bilgi sistemlerinde yaşanabilecek problemler nedeniyle faaliyetlerinin kesintiye uğramasını önlemek üzere bilgi sistemlerine ilişkin bir iş süreklilik ve kurtarma planı hazırlamak zorunda ve plan için gerekli olan yedekleme altyapısını tesis etmek zorundadır. Örneğin tebliğin getirdiği bu zorunluluk, BDDK'nın kabul ettiği CobiT çerçevesi altındaki "Hizmet Sunumu ve Destek" kontrol alanı altındaki iş sürekliliğinin sağlanması detay kontrol hedefi ile de bankaları için zorunlu hale getirilmiş bulunmaktadır. Bu madde gibi diğer maddelerin çoğu CobiT çerçevesine uyumun sağlanması ile birlikte yerine getirilecek maddelerden oluşmaktadır[81].

Tebliğin ikinci bölümü ise "*Bilgi Sistemlerine Yönelik İç Kontrollerin Tesisi ve Takibi*" kapsamında denetlenen bankaları, bilgi sistemleri kontrol ortamına yönelik olarak gerekli olan

[80] BDDK, "**Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ**" (Madde 11-15, Sayı 26643; Tarih 14 Eylül 2007), 5-7
[81] BDDK, "**Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ**" (Madde 16-19, Sayı 26643; Tarih 14 Eylül 2007), 7-8

uygulama kontrollerini ve genel kontrolleri tesis etmek ile sorumlu tutmaktadır. Uygulama kontrolleri, bankanın is süreçlerinin kontrolünü ifade eden iş döngüsü kontrolleri içerisinde yer alan, bilgisayar destekli ve manüel yordamlarla gerçekleştirilen özelleşmiş kontrollerdir. Diğer taraftan bilgi sistemleri genel kontrolleri ise, banka bilgi sistemlerinin tamamına veya büyük bir bölümüne tatbik edilen, bilgi sistemlerinin kendilerinden beklenen fonksiyonları doğru bir şekilde yerine getirmesi, istenmeyen olayların engellenmesi, belirlenmesi ve düzeltilmesi ile ilgili olarak yeterli derecede güvence oluşturulması ile uygulama kontrollerinin işlevselliği için güvenilir bir ortamın oluşturulmasını hedefleyen politika ve prosedürlerden oluşur. Genel kontroller, bankanın bilgi sistemlerinin bir bütün olarak kendisinden beklenen fonksiyonları doğru, zamanında ve güvenilir bir şekilde gerçekleştirilmesine yönelik ortamın tesisinde temel unsurları oluştururlar.

Tebliğin bu bölümüne göre denetlenen bankaların bilgi sistemleri genel kontrollerini tesis etmek üzere kullanacağı standart, çerçeve veya metodolojinin CobiT'te ele alınan kontrol hedeflerini gerçekleyebilmesi, eğer bu konuda eksiklikleri varsa da buna ilişkin kontrollerin ayrıca ele alınarak tesis edilmesi gerekmektedir.

Uygulama kontrollerin ve genel kontrollerin tesis ile birlikte özetle, denetlenen bankaların bilgi sistemlerinin yönetimini kurumsal yönetim uygulamalarının bir parçası olarak ele alması gerekmektedir. Bu kapsamda bankalara yol gösterecek önemli çerçeve olarak da yasal kuruluş tarafından CobiT işaret edilmektedir. Böylelikle bankaların operasyonlarını istikrarlı, rekabetçi ve gelişen bir çizgide sürdürebilmesi için bilgi sistemlerine ilişkin stratejinin is hedefleri ile uyumlu olması sağlanmalı, bilgi sistemleri yönetimine ilişkin unsurlar yönetsel hiyerarşi içerisinde uygun yere yerleştirilmeli ve bilgi sistemlerinin doğru yönetimi için gerekli finansman ve insan kaynağı tahsis edilmelidir.

Son olarak tebliğin üçüncü bölümü ise "*İnternet Bankacılığı ve ATM gibi Önemlilik Arz Eden Bazı Konular Hakkında Hükümler*" kapsamında internet bankacılığı kullanımında, ATM güvenliğinde ve kablosuz haberleşme kullanımında zorunlu hükümler getirmektedir.

Tebliğin diğer bölümlerinde yer alan hükümler internet bankacılığı kapsamında yapılan çalışmalar için geçerli olsa da uyulması gereken ek yükümlülükler bu bölümde internet bankacılığına özel olarak getirilmiştir. Bunlar;[82]

- İnternet bankacılığına yönelik olarak güvenlik kontrol sürecinin tesis edilmesi, yönetilmesi ve yılda en az bir kez sızma testlerinin yaptırılması
- İnternet bankacılığına özel olarak birbirinden bağımsız en az iki bileşenden oluşan kimlik doğrulama metotlarının uygulanması ve diğer özel kimlik doğrulama şartları
- İnkar edilemezlik ve sorumluluk atama fonksiyonu altında internet bankacılığı üzerindeki işlemlere yönelik denetim izlerinin tutulması ve güvenli olarak saklanmasına yönelik sürecin tesis edilmesi
- Müşterilerin internet bankacılığı hizmetine ilişkin mevcut politika ve prosedürler hakkında bilgilendirilmesi
- İnternet bankacılığına yönelik olarak bankaların müşterilerine taahhüt ettiği servis sürekliliğini sağlaması

İnternet bankacılığının yanında ATM güvenliğine yönelik olarak ek hükümler de yine bu bölüm altında getirilmiştir. Bunlardan bazıları şunlardır[83]:

- ATM cihazları üzerinde gerçekleştirilen işlemler için kullanılan iletişi ağı, veri güvenliğini, gizliliğini ve bütünlüğünü sağlamalıdır.
- ATM cihazlarının servis sürekliliği sağlanmalı ve uzaktan yönetim ve takip sistemleri ile kontrol edilmelidir.
- ATM yönetimine ait mutabakatlar yeterli sıklıkla görevler ayrılığına uygun olarak iki kişi tarafından gerçekleştirilmelidir.
- ATM operatörleri ve teknisyenleri, ATM cihazlarına ilişkin güncel bütün sahtekârlık yöntemleri konusunda eğitilmeli ve bu gibi personelin ATM cihazlarını düzenli olarak kontrol etmeleri sağlanmalıdır.

[82] BDDK, "**Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ**" (Madde 24-31, Sayı 26643; Tarih 14 Eylül 2007), 10-12
[83] BDDK, "**Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ**" (Madde 32, Sayı 26643; Tarih 14 Eylül 2007), 12-13

Yukarıdaki maddelere benzer ATM güvenliği ile ilgili olarak ek hükümler tebliğ ile birlikte bankalar için zorunlu hale gelmiştir.

Son olarak tebliğin bu bölümünde bilgi sistemleri alt yapısında, temel bankacılık faaliyetlerinin ifasında ve alternatif dağıtım kanallarının tesisinde kullanılan kablosuz haberleşme teknolojilerine ilişkin riskleri yönetmek üzere gerekli önlemleri alması konusunda denetlenen bankalara zorunluluk getirilmiştir.

Böylelikle bankalardaki bilgi sistemleri denetiminin kapsamı, CobiT ve İlkeler Tebliği'ne bağlı olarak uygulama kontrollerinin, genel kontrollerin ve tebliğin getirdiği özel hükümlerin incelenmesinden ve rapora görüş bildirilerek bağlanmasından oluşmaktadır.

4.6. Uygulama Süreçlerinin Denetimi

Uygulama kontrolleri, bilgi sistemleri içerisinde yer alan ve bankacılık faaliyetlerini yürütmek veya desteklemek için kullanılan finansal verilerin tanımlanması, üretilmesi, kullanılması, bütünlük ve güvenilirliğinin sağlanması, verilere erişimin yetkilendirilmesi gibi tüm iş süreçlerinde kullanılması gereken iç kontrollerin etkinliğinin ve yeterliliğinin denetlenmesini ve değerlendirilmesini kapsar. Bilgi sistemleri denetimi içerisinde denetlenen bankaların kritik bankacılık sistemleri üzerindeki uygulama kontrollerinin yeterliliğinin ve etkinliğinin test edilerek değerlendirilmesine uygulama kontrollerinin denetimi adı verilmektedir. Bu kontroller genel olarak denetlenen bankların sistemlerine ve iş sürecine bağlı olarak uygun kontrol ortamının tesis edilmek istenmesi üzerine oluşturulmuş bilgisayar destekli ve/veya manüel yordamlarla gerçekleştirilen kontrollerdir.

1 Kasım 2006 tarih ve 26333 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Gerçekleştirecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik" genel olarak denetlenecek uygulama kontrollerini sınıflandırmış ve denetimi gerçekleştiren bağımsız denetim firmasının da bu sınıflandırmaya uygun olarak kontrolleri yasal kuruma ("BDDK") raporlamasını istemektedir. Uygulama kontrollerinin sınıflandırılmasında yasal kurum CobiT çerçevesinin öngördüğü yaklaşımdan yararlanmıştır.

Bunun yanında yasal kurum, bankaların asgari olarak denetlenmesi gereken iş süreçlerini de yine aynı yönetmelik içerisinde belirtmiştir.

4.6.1. Uygulama Kontrollerinin Türleri

Denetlenen bankalarda tespit edilen ve test edilerek değerlendirilen uygulama kontrolleri aşağıdaki şekilde sınıflandırılmak zorundadır[84]:

1. ***Veri oluşturma/yetkilendirme kontrolleri:*** Genel olarak kaynak verilerin, belgelerin oluşturulması ve sistem üzerindeki yetkilendirme gerçekleştirilmesi ile ilgili olan beş ayrı kategoriye bölünen kontrol tiplerinden oluşmaktadır. Bunlar;[85]
    a. *Veri hazırlama prosedürleri*
    b. *Kaynak belge yetkilendirme prosedürleri*
    c. *Kaynak belge verilerinin toplanması*
    d. *Kaynak belgelerdeki hataların ele alınması*
    e. *Kaynak belgelerin muhafazası*
2. ***Girdi kontrolleri***: Bilgi sistemleri veri işleme sürecinin başlangıcı olan girdi alt sürecine yönelik belirlenmiş olan üç ayrı kategorideki kontrollerdir. Bunlar;[86]
    a. *Girdi yetkilendirme prosedürleri*
    b. *Doğruluk, bütünlük ve yetkilendirme kontrolleri*
    c. *Veri girdilerindeki hataların ele alınması*
3. ***Veri işleme kontrolleri***: Bilgi sistemleri içerisinde veri işleme süreci ile ilgili sınıflandırılan üç ayrı kategorideki kontrollerdir. Bunlar;[87]
    a. *Veri işlemede bütünlük*
    b. *Veri işlemede onaylama ve değiştirme*
    c. *Veri işlemedeki hataların ele alınması*

---

[84] BDDK, "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**" (Madde 18, Sayı 26170; Tarih: 16 Mayıs 2006), 8-9
[85] ISACA, **Control Objectives for Information and related Technology 4.0** (USA, 2005), 17
[86] ISACA, **Control Objectives for Information and related Technology 4.0** (USA, 2005), 17
[87] ISACA, **Control Objectives for Information and related Technology 4.0** (USA, 2005), 17-18

4. ***Çıktı kontrolleri***: Bilgi sistemlerinde veri girişinin ve veri işlenmesinin tamamlanmasından sonra çıkan veri üzerinde tesis edilen kontrollerdir. Bu aşamada ise beş ayrı kontrol tipi sınıflandırılmıştır. Bunlar;[88]

    a. *Çıktıların ele alınması ve muhafazası*

    b. *Çıktıların dağıtımı*

    c. *Çıktı uyumluluğu ve mutabakatı*

    d. *Çıktıların gözden geçirilmesi ve hataların ele alınması*

    e. *Çıktı raporlarının güvenliğinin sağlanması*

5. ***Sınır kontrolleri***: Organizasyon dışından elde edilen verinin uygunluğunun ve bütünlüğünün sağlamasına ve hassas bilginin güvenli olarak iletilmesine ve korunmasına yönelik iki kategoride sınıflandırılan kontrollerdir. Bunlar; [89]

    a. *Aslına uygunluk ve bütünlük kontrolleri*

    b. *Hassas bilginin iletim ve nakil esnasında korunması*

Yönetmeliğin yasal kurum tarafından yayınlandığı sırada CobiT 4.0 versiyonundan yararlanılarak yukarıdaki şekilde uygulama kontrolleri sınıflandırılmıştır. Ancak sonrasında ISACA tarafından CobiT 4.1 yayınlandıktan sonra uygulama kontrollerinin daha sade olarak altı kategori altında sınıflandırıldığını görmekteyiz. Yeni sınıflandırma yaklaşımı ile uygulama kontrollerinin daha rahat sınıflandırılması ve takip edilmesi sağlanmıştır. Yeni sınıflandırma yaklaşımına göre kontrol sınıfları şu şekildedir[90]:

1. ***Kaynak Veri Hazırlama ve Yetkilendirme:*** Kaynak dokümanların yetkili ve yetkin kişiler tarafından tanımlı prosedürlerin kullanılmasıyla hazırlanmasını sağlanan kontrollerdir. Süreç içindeki görevler ayrılığı prensibinin de göz önünde bulundurulması ile veri hazırlama ve onaylama süreçlerinin de birbirinden ayrılması beklenmektedir. Bu kontroller ile kaynak verilerin doğru olarak hazırlaması ve olası hataların raporlanmasını sağlayan bir kontrol ortamı oluşturulmaya çalışılmaktadır.

[88] ISACA, **Control Objectives for Information and related Technology 4.0** (USA, 2005), 18
[89] ISACA, **Control Objectives for Information and related Technology 4.0** (USA, 2005), 18
[90] ISACA COBIT, **age**, 16

2. ***Kaynak Veri Toplama ve Girişi:*** Sistemlere veri girişinin yetkin ve yetkili kişiler tarafından yapılmasını amaçlayan kontrollerdir. Örneğin bankacılık uygulamasında mevduat faizlerinin iki ayrı kişi tarafından sisteme doğru girilmesi ile sistemde kullanılabilir hale gelmesi gibi.

3. ***Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri:*** Sistem üzerindeki verilerin doğru, tam ve geçerli olmasını sağlayan kontrollerdir. Veri girişi sırasında geçerlilik kontrolü yapılması veya sistem üzerinde uygun yetkilendirmenin yapılması gibi kontroller bu kategori altına girmektedir. Örneğin müşteri bilgilerinin girişi esnasında adres bilgisinin sisteme girilirken il seçimine göre uygun ilçelerin seçilmesinin sistem tarafından zorlanması gibi.

4. ***Veri İşlemede Bütünlük ve Geçerlilik:*** Veri işleme esnasında işlenen verinin bütünlüğünün ve geçerliliğinin sağlanmasına yönelik kontrollerdir. Örneğin, sistemler üzerinde çalışan programların hatalı işlem girişlerini belirlemesi ve veri işleme süreci tamamladığından ayrı olarak raporlaması gibi kontrollerdir.

5. ***Çıktıların Gözden geçirilmesi, Mutabakat ve Hataların Ele Alınması:*** Çıktı raporlarının doğruluğunun, çıktıları sağlayan kişiler ve uygun kullanıcılar tarafından gözden geçirilmesini ve mutabakatını temin eden kontrollerden oluşmaktadır. Ayrıca, çıktılarda bulunan hataların tanımlanması ve ele alınması ile ilgili de kontrollerde bu kategori altına dahil edilmelidir. Örneğin EFT işlemlerinin gün sonu mutabakatlarının bankalar tarafından yapılması bu kontrol sınıfı bir örnek oluşturmaktadır.

6. ***İşlemlerin Yetkilendirilmesi ve Bütünlük***: İşlemlerin ve dolayısıyla verinin sistemlere ait ara yüzler ve fonksiyonlar arasından iletilirken bütünlüğünün sağlanmasına ve işlemlerin belirlenen yetkiler çerçevesinde gerçekleşmesine yardımcı olan kontrollerdir. Örneğin, internet bankacılığı ön yüzünden gerçekleştirilen işlemin arka taraftaki ana bankacılık sisteminde bütünlüğü bozan bir işlem olması sebebiyle sistem tarafından gerçekleştirilmesine izin verilmemesi gibi.

Bağımsız denetçi kuruluş, bilgi sistemleri denetimi kapsamında uygulama kontrollerinin denetlenmesinde aşağıdaki asgari kurallara uymak zorundadır:

- Önemli uygulama bileşenlerinin ve hareketlerin sistem üzerinden akışının tanımlanması, mevcut dokümantasyonun gözden geçirilmesi ve uygun personelle görüşülmesi suretiyle uygulamanın detaylarının anlaşılması,
- Uygulama kontrollerinin güçlü yanlarının tanımlanması ve toplanan bilgiler incelenerek kontrol zaaflarının test stratejisine etkisinin değerlendirilmesi,
- Uygun denetim prosedürleri kullanılarak kontrollerin fonksiyonellik ve etkinliklerinin test edilmesi,
- Test sonuçlarının ve diğer denetim bulgularının incelenmesi ile kontrol ortamının değerlendirilmesi adımlarını gerçekleştirilmelidir.

4.6.2. Bankacılık Sektöründe Asgari Olarak Denetlenen Süreçler

1 Kasım 2006 tarih ve 26333 sayılı Resmi Gazete'de yayımlanan "Bankalarda Bağımsız Denetim Gerçekleştirecek Kuruluşların Yetkilendirilmesi ve Faaliyetleri Hakkında Yönetmelik" gereği denetlenen bankalarda gerçekleştirilen uygulama kontrollerinin denetimi ve değerlendirilmesi asgari olarak aşağıdaki süreçleri kapsamalıdır[91]:

- Mükerrer bilgi sistemleri ve çift kayıt sisteminin varlığının ve bunların önlenmesine ilişkin kontrollerin incelenmesi,
- Faiz ve gelir tahakkuk ve reeskont hesaplamaları, gider reeskontları ve amortisman hesaplamaları, takip hesaplarına aktarım süreci ve karşılık hesaplamaları, yaşlandırma raporlarının hazırlanması,
- Muhasebe fişi kesilmesine ilişkin yetkili personelin belirlenmesi ve yetkilendirilmesi süreçleri ile mizanın oluşumu, geriye dönük muhasebe fişi kesilmesi işlemleriyle ilgili yetkilendirmelerin varlığı ve ilgili kayıtların bütünlüğü ve izlenebilirliği, işlem numaralarının ardışıklığının korunmasını sağlamak gibi genel muhasebe kontrolleri, işlem limitlerinin ve yetkilerinin kontrolü,
- Elektronik Fon Transferi, Elektronik Menkul Kıymet Transferi ve Takasbank işlemleri, SWIFT işlemleri ve bunlarla ilgili güvenlik kayıtları gibi ödeme sistemi kontrolleri,

[91] BDDK, "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**" (Madde 18/5, Sayı 26170; Tarih: 16 Mayıs 2006), 9-10

- Nostro, vostro ve loro bakiyelere ilişkin mutabakatlar ve muhabir kayıtları, şube ve genel müdürlük kayıtları arasındaki mutabakatlar, yasal ve yardımcı defterler arası mutabakatlar, banka ile kart merkezi mutabakatları gibi mutabakat kontrolleri,
- Banka ve kredi kartına limit tahsisi, banka kartlarının kullanımı ve hediye puanı gibi uygulamalara ilişkin kontrolleri,
- Kredi başvuruları ve onayları, kredi limitleri ile kredi geri ödeme tabloları ve hesaplamalarına ilişkin kontroller, mevduat işlemleri ve mevduatın sınıflandırılması gibi hesaplama ve kontrolleri,
- Banka kayıtlarının ve bilgi kaynaklarının finansal raporlamalarda kullanım sürecinin kontrolü,
- Menkul kıymet ve fon yönetimi iş süreçlerinin kontrolü,
- Vade ve valör tarihlerine ilişkin kayıtların güvenilirliği ve bütünlüğünün kontrolü,
- Elektronik bankacılık/alternatif dağıtım kanalları (internet, telefon, televizyon, WAP/GPRS, Kiosk, ATM, vb) ile ilgili muhasebe ve süreç kontrolleri.

Bilgi sistemleri denetçileri yukarıda belirtilen süreçlerdeki uygulama kontrollerini değerlendirmenin yanında, bankaların finansal raporlama sistemi ile ilgili iç kontrollerinin yeterliliğini, yöneticilerin bu iç kontrollerin yeterliğini ve etkinliğini ölçmedeki performansını da değerlendirmek zorundadır. Finansal raporlama ile ilgili iç kontrollerin değerlendirilmesinde aşağıdaki hususlar asgari olarak kapsama alınmak zorundadır[92]:

- Kontrol ortamı,
- Risk değerlendirme süreci,
- Kontrol faaliyetleri,
- Bilgi ve iletişim kanalları, yetkilendirme, kayıtların saklanması süreçleri,
- Oluşturulan kontrollerin denetlenen tarafından izlenmesi.

Türk bankacılık sektöründe gerçekleştirilen bilgi sistemleri denetiminin kapsamına giren uygulama kontrollerinin ve iç kontrol ortamının denetimini kısaca bu bölüme kadar açıklamış

[92] SPK, "**Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ**" (10. Kısım, Madde 11, Seri: X, No: 22), 50

bulunmaktadır. Bir sonraki bölümde bilgi sistemleri denetimin son kapsam alanı olan genel kontrol alanlarının denetimi ile ilgili açıklamalarda bulunulacaktır.

4.7. Genel Kontrol Alanlarının Denetimi

Denetlenen bankalarda bağımsız denetim kuruluşları tarafından gerçekleştirilen bilgi sistemleri denetiminin kapsamına uygulama kontrollerinin denetiminin yanında genel kontrol alanlarının denetimi de girmektedir. Önceki bölümlerde de bahsedildiği gibi uygulama kontrollerinin etkinliği ve güvenilirliği, genel bilgi sistemleri kontrol ortamının güvenilir olma derecesine de bağlıdır. Bu sebeple bilgi sistemleri genel kontrol alanının etkin olarak tesis edilmesi bankalar ve bu kapsamda görüş veren bağımsız denetim kuruluşları için önem taşımaktadır. CobiT çerçevesine uygun olarak dört ana bölümde genel kontrol alanı denetiminin gerçekleştirilmesi BDDK tarafından zorunlu kılınmıştır. Bunlar;[93]

1. *Planlama ve organizasyon faaliyetlerinin denetimi:* Planlama ve organizasyon faaliyetleri, iş hedeflerinin yerine getirilmesi amacıyla bilgi teknolojileri desteğinin en uygun verilme şeklinin belirlenmesine yönelik strateji ve yöntemleri içerir. Farklı bakış açılarını içerecek şekilde planlanan stratejiler, organizasyon içerisindeki ilgili birim ve kişilere iletilir. Teknolojik alt yapının, sağlıklı bir örgütsel yapı içerisinde verimli ve etkin çalışabileceği hususu bilgi sistemleri denetimi sürecinde dikkate alınır.
2. *Tedarik ve uygulama faaliyetlerinin denetimi:* Tedarik ve uygulama faaliyetleri, bilgi teknolojisi stratejilerinin gerçekleştirilmesiyle ilgili bilgi teknolojisi çözümlerinin tanımlanması, geliştirilmesi veya harici destek sağlayıcılardan temin edilmesi, uygulanması ve iş süreçleriyle bütünleştirilmesini kapsar. Sistemlerdeki bakımlar ve değişiklikler de bu kontrol alanında değerlendirilir.
3. *Hizmet sunumu ve destek faaliyetlerinin denetimi:* Hizmet sunumu ve destek faaliyetleri, gerekli eğitimin verilmesi de dahil olmak üzere ihtiyaç duyulan hizmetlerin güvenli ve sürekli bir şekilde sunulmasını ifade eder.
4. *İzleme ve değerlendirme faaliyetlerinin denetimi:* İzleme faaliyetleri, bilgi teknolojilerine ilişkin tesis edilen kontrollerin uygunluk ve kalitesinin, denetlenen tarafından düzenli aralıklarla değerlendirilmesini kapsar.

[93] ISACA COBIT, **age**, 13

Yukarıda açıklanan sırada her bir faaliyet adımı bir sonrakine girdi teşkil ederek bir döngü oluşturmakta ve uygun kontrol ortamının tesisiyle birlikte bilgi sistemleri yönetimi etkin olarak sağlanmaktadır. Her bir faaliyet adımının altında hangi kontrol hedeflerinin bulunduğu ve denetim sürecinde hangi konu başlıklarına dikkat edilmesi gerektiği aşağıdaki bölümlerde sırasıyla açıklanmıştır.

4.7.1. Planlama ve Organizasyon Faaliyetlerinin Denetimi

1. *Stratejik bilgi teknolojileri planının tanımlanması:* [94] İş tarafı ile birlikte çalışılarak kurumsal bilgi teknolojileri ("BT") odaklı yatırımlar portföyünün gerçek iş projelerine dayanan programları içermesi sağlanmalıdır. Belirli stratejik iş hedeflerine ulaşabilmek için programlar belirlenmeli, tanımlanmalı, değerlendirilmeli, önceliklendirilmeli, seçilmeli, başlatılmalı, yönetilmeli ve kontrol edilmeli, iş tarafı ile birlikte BT odaklı yatırım programları yönetilmelidir. Yöneticilerin, mevcut teknoloji kapasitesi ve gelecek hedefler, BT'nin sunduğu fırsatlar ve bu fırsatlardan faydalanmak için organizasyonun ne yapması gerektiği konusunda eğitilmeleri gerekmektedir. BT ile uyumlu iş stratejilerinin organizasyon tarafından anlaşılması sağlanmalıdır. BT'nin organizasyonun stratejik hedefleri ve ilgili gider ve risklerine nasıl bir katkıda bulunacağının anlatıldığı bir stratejik plan ilgili paydaşlar ile işbirliği içinde hazırlanmalıdır. Sonrasında, BT stratejik planından türetilmiş bir BT taktik planı portföyü yaratılmalıdır[95]. BT taktik planları işin nedeni olan BT gereksinimini, kaynak gereksinimini, kaynak kullanımının nasıl olacağını ve beklenen faydanın yönetilebilir ve görüntülenebilir olmasının nasıl sağlanacağını tanımlamalıdır.
2. *Bilgi mimarisinin tanımlanması:*[96] Uygulama geliştirme ve karar destek çalışmalarının BT planları ile uyumlu olmasını sağlamak için "Kurumsal Bilgi Modeli" kurulmalı ve sürekliliği sağlanmalıdır. Organizasyonun veri sentaks kurallarını içeren Kurumsal Veri Sözlüğü oluşturulmalıdır. Bu veri sözlüğü veri unsurlarının uygulamalar ve sistemler arasında paylaşımını, BT ve iş tarafı kullanıcılarının veriyi ortak bir dilde anlamalarını ve uygun olmayan veri unsurlarının yaratılmasını engelleme gibi konuları içermelidir.

[94] ISACA COBIT, **age**, 29
[95] Alex Bakman, "**If Compliance is so critical , Why are we still failing audits**?", Information Systems Control Journal, volume 5 (2007), 37
[96] ISACA COBIT, **age**, 33

Ayrıca, kurumsal seviyede uygulanan ve kurumsal verinin kritiklik ve hassasiyet (örn; genel, gizli, çok gizli) düzeyine dayanan bir sınıflandırma şeması oluşturulmalıdır.

3. *Teknolojik yönün belirlenmesi:*[97] Hali hazırdaki ve gelişen teknolojiler analiz edilmeli ve hangi teknolojik yönelim, BT stratejine ve iş yönetim mimarisine daha uygun olduğu planlanmalıdır. Bu kapsamdaki teknolojik yön planı sistem mimarisini, teknolojik yönelimi, dönüşüm stratejilerini ve altyapı bileşenlerinin acil durum hallerini içermelidir. Teknolojik yöne planına, bilgi teknolojileri stratejik ve taktik planlarına uygun bir teknoloji altyapı planı da bu yine bu faaliyet adımı altında oluşturulmalıdır.

4. *Bilgi teknolojisi süreçlerinin, organizasyonunun ve ilişkilerinin tanımlanması:*[98] BT stratejik planının uygulanması için BT süreci tanımlanmalıdır. BT süreci, yapı ve ilişkileri sahiplik, olgunluk, performans ölçümü, ilerleme, uygunluk, kalite hedefleri ve planları içermelidir. BT süreç sistemi, BT portföy yönetimi, iş ve değişim süreçlerine özgü süreçleri birleştirmeli, kalite yönetim sistemi ve iç kontrol taslağına entegre edilmesi gerekmektedir. BT strateji komitesinin oluşturulması, BT yönlendirme komitesinin oluşturulması, BT işlevinin organizasyonel yerleşiminin sağlanması, rol ve sorumlulukların belirlenmesi, görevler ayrılığı prensibinin organizasyon içerisinde tesisi ve BT personel yönetiminin sağlanması gibi detay kontrol hedefleri kapsamında BT sürecinin hedefine uygun olarak oluşturulması bu faaliyet adımında amaçlanmaktadır.

5. *Bilgi teknolojisi yatırımlarının yönetimi:*[99] Bilgi sistemleri yatırımları, iş durumları ve bilgi sistemleri bütçesini, bilgi sistemleri varlık hizmetlerinin masraflarını içeren portföyün yönetilmesini sağlayacak şekilde finansal bir çerçeve hazırlanmalı ve korunmalıdır. Bu kapsamda, bilgi sistemleri bütçesinin oluşturulması ve bütçe hedeflerinin önceliklendirilmesi sağlanmalıdır. Ek olarak yapılan masrafların bütçeye uygunluğunu ölçen masraf yönetimi uygulanmalıdır. Bilgi sistemleri yatırım programlarının bir parçası veya operasyonel desteğin bir parçası olarak da bilgi sistemlerinin iş süreçlerine katkısı belirlenmeli ve dokümante edilmeli, bu katkı üzerinde ortak karara varılmalı, gözlemlenmeli ve raporlanmalıdır.

[97] ISACA COBIT, **age**, 37
[98] **age**, 41
[99] **age**, 47

6. *Yönetimin amaçlarının ve talimatlarının iletilmesi:*[100] Kurumun yönetim felsefesi ve operasyonel stiline uyumlu olarak bilgi teknolojileri kontrol ortamına ilişkin elementler tanımlanmalıdır. Bu elementler, bilgi teknolojileri yatırımlarından değer sağlanması, risk isteği, uyum, etik değerler, personelin yeterliliği, açıklanabilirlilik ve sorumluluk gibi gereksinimleri/beklentileri içermelidir. Kontrol ortamı, önemli riskleri yöneterek değer sağlayan, bölümler arası koordinasyonu ve takım çalışmasını destekleyen, uyumu ve sürekli süreç iyileştirmeyi teşvik eden ve süreçten sapmaları (başarısızlık da dâhil) idare edebilen bir kültüre dayandırılmalıdır. Bilgi teknolojileri kaynak ve sistemlerini korumakla birlikte, değer yaratacak ve kurumun genel olarak risk ve iç kontrol yaklaşımı oluşturarak bir yapı tesis edilmeli ve sürdürülmelidir. Ayrıca bu kapsamda BT stratejisini destekleyen politikalar geliştirilmeli ve güncel tutulmalıdır.

7. *İnsan kaynakları yönetimi:*[101] BT personelinin işe alım süreci tüm organizasyonun personel politikası ve prosedürleri ile uyum içinde olmalıdır. Yönetim, organizasyon hedeflerine ulaşabilmek için gerekli yetenekleri olan BT personeli işe aldığından emin olmak için bu süreçleri uygulamalıdır. Personelin organizasyon içerisinde üstlenmiş olduğu rollerine uygun olarak gerekli yetenek ve yeterliliğe sahip olup olmadığı, eğitim durumu ve/veya tecrübe bazlı olarak düzenli olarak kontrol edilmelidir. BT yetenek ve yeterlilik kriterleri tanımlanmalı, uygun eğitim ve sertifikasyon programları ile sürekliliği sağlanmalıdır. Bilginin muhafaza edilmesi (dokümantasyon), bilgi paylaşımı, birbirini izleyen işlerin planlanması ve BT personelinin yedeğinin sağlanması gibi yöntemler vasıtasıyla kilit bilgi teknolojileri personeline bağımlılık asgari seviyeye indirilmelidir. Son olarak, BT personeline ait performansın etkin olarak değerlendirilmesi sağlanmalıdır.

8. *Kalite yönetimi:*[102] Kalite yönetimiyle iş gereksinimlerini örtüştüren, standart, resmi ve daimi bir yaklaşım sunan bir "Kalite Yönetimi Sistemi" ("KYS") oluşturulmalıdır. KYS, rolleri, görevleri ve sorumlulukları kapsayan kalite yönetimi organizasyonel yapısını tanımlamalıdır. Tüm anahtar alanları, kriterleri, politika ve kayıtlı kalite verilerini baz alan kalite planları oluşturmalıdır. Projelerin yönetimi ve servislerin beklendiği kalitede iş tarafına sunulması için kalite yönetim sistemi anlayışını tesis edilmesi bu faaliyet alanı

[100] ISACA COBIT, **age**, 51
[101] **age**, 55
[102] **age**, 59

kapsamında ele alınmalıdır. Sürekli iyileşme, kalite ölçümlemesi ve raporlama KYS'nin hedefleri içerisinde kabul edilmelidir.

9. *Bilgi sistemleri riskinin değerlendirilmesi ve yönetimi:*[103] Bilgi teknolojileri yönetimi, risk yönetimi ve kontrol yapısının; organizasyonun risk yönetimi yapısıyla entegrasyonu sağlanmalıdır. Bu kapsamda BT risk yönetimi anlayışının kurum içinde tesis edilmesi gerekmektedir. Öncelikle uygulanan risk değerlendirme yapısının doğru sonuçlar vermeyi garanti ettiği bir kapsamın kurulması gerekmektedir. Sonrasında BT risk değerlendirilmesi kapsamında nitel ve nicel yöntemler kullanarak, belirlenen tüm risklerin etkisi ve bu risklerin tekrar etme olasılıkları değerlendirilmelidir. Bir sonraki adım olarak, risk sahibi ve etkilenen sürecin sahibinin belirlenip, fiyat olarak uygun kontrollerin ve güvenlik ölçütlerinin, risklere karşı korunmasızlığı devamlı bir şekilde azaltmayı garanti ettiği bir risk tepkisinin geliştirilmesi ve sürdürülmesi gerekmektedir. Diğer bir adıyla belirlenen risklere karşı bir risk eylem planı oluşturulmalıdır. Son adım olarak da risk eylem planının güncellenmesi ve izlenmesi sağlanmalıdır.

10. *Proje yönetimi:*[104] BT tarafından geçerli kılınmış yatırım programları ile ilgili projeler için, projelerin tanımlandığı, değerlendirildiği, öncelendirildiği, seçildiği, başlatıldığı, yönetildiği ve kontrol edildiği bir proje programı oluşturulmalıdır. Projelerin, bu programın hedeflerini desteklediği güvence altına alınmalıdır. Çoklu projelerin aktiviteleri ve birbirinden bağımsızlıkları koordine edilmeli, programda yer alan tüm projelerin beklenen çıktılara olan katkıları, kaynak gereksinimleri ve çatışmaları yönetilmelidir. Bunun yanında yürütülen her bir proje için, proje yönetiminin sınırlanın ve kapsamının ve her bir projeye uygulanan ve uyarlanan yöntemlerin tanımlandığı bir proje yönetim çerçevesi belirlenmelidir. Proje yönetimi çerçevesi kapsamında proje yönetim yaklaşımı, hak sahiplerinin destek şekli, proje kapsamının belirlenmesi, proje fazlarının yönetimi, proje kaynaklarının yönetimi, proje planlaması, proje risk planlaması, proje kalite planlaması ve proje performans izleme ve raporlaması gibi konular bu faaliyet adımı altında gerçekleştirilmelidir.

[103] ISACA COBIT, **age**, 63
[104] **age**, 67

4.7.2. Tedarik ve Uygulama Faaliyetlerinin Denetimi

1. *Otomasyon çözümlerinin belirlenmesi:*[105] BT odaklı yatırım programının beklenen sonuçlarına ulaşabilmek için gerekli olan işlevsel ve teknik gereksinimler tanımlanmalı, önceliklendirilmeli ve açıklanmalıdır. Bu gereksinimlerin kabul edilebilmesi için gerekli kriterler belirlenmelidir. Organizasyonun gereksinimlerini geliştirme sürecinin bir parçası olarak, iş süreçleri ile ilgili olan riskler belirlenmeli, analiz edilmeli ve dokümante edilmelidir. Sonrasında gereksinimlerin uygulanma olasılığını inceleyen bir uygulanabilirlik çalışması yapılmalıdır. Bu çalışma tespit edilmiş işlevsel ve teknik gereksinimleri karşılamaya yönelik yazılım, donanım, hizmet ve yetkinliklerden oluşan alternatif yöntemler içermeli ve her planın BT odaklı yatırım programı dahilinde teknolojik ve ekonomik yapılabilirliği (olası masraf ve kar analizleri) hesaplanmalıdır. Son olarak iş sahibi birim işlevsel ve teknik gereksinimler ve yapılabilirlik çalışması raporlarını daha önceden belirlenmiş kilit aşamalarda onaylamalı, uygulama geliştirme veya satın alma sürecine girdi sağlamalıdır.
2. *Uygulama yazılımının geliştirilmesi ve bakımı:*[106] Organizasyonun teknolojik rotası ve bilgi yapısı göz önünde bulundurularak, iş istekleri yazılım geliştirme için yüksek düzey tasarım şartnamesine dönüştürmeli ve bu şartnameye uygun olarak detaylı tasarım ve teknik uygulama gereksinimleri hazırlanmalıdır. Uygulama geliştirme sürecinde iş kontrollerinin yanlışsız, tam, zamanında, yetkilendirilmiş ve denetlenebilir bir şekilde uygulama kontrollerine yansıtıldığından emin olunmalıdır. Uygulama geliştirme sürecinde olacağı gibi satın alınan uygulama yazılımlarında da kurulum, kabul ve test prosedürleri uygulanmalıdır. Ek olarak yazılım geliştirme sürecinde, otomatik fonksiyonelitenin tasarım özellikleri, geliştirme ve dokümantasyon standartları ve kalite gereksinimleri ile uyumlu olarak geliştirilmenin yapıldığından emin olunmalıdır. Son olarak geliştirilen yazılımların kalite güvencesinin sağlanması, uygulama yazılımlarının bakımı ve yayınlanması için bir strateji ve plan geliştirilmesi bu faaliyet adımı altında gerçekleştirilmelidir.

[105] ISACA COBIT, **age**, 73
[106] **age**, 77

3. *Teknoloji alt yapısının oluşturulması ve bakımı:*[107] Organizasyonun teknolojik hedefleriyle uyumlu olan, fonksiyonel ve teknolojik gereksinimleri kapsayacak şekilde teknolojik altyapı alımı, kurulması ve bakımı için plan yapılmalıdır. Kaynakların korunması, bütünlük ve kullanıma hazır olmalarının sağlanması amacıyla iç kontrol, konfigürasyon süresince denetim ve güvenlik ölçümleri, yazılım ve donanımların birleştirilmesi ve bakımı gerçekleştirilmelidir. Altyapı ekipmanlarının bakımı için bir strateji ve plan hazırlanmalıdır. Hazırlanan planlar iş gereksinimlerini, yama yönetimini, altyapı yükseltme stratejileri ile risk ve savunma değerlendirme ve güvenlik gereksinimleri içeren dönemsel gözden geçirmeleri kapsamalıdır. Son olarak bu faaliyet adımında altyapı değişikliklerinin uygulanabilir test ortamında denenmesinden sonra canlı ortamda uygulanmalıdır.

4. *Operasyon ve kullanımın sağlanması:*[108] Bu kontrol hedefi kapsamında geliştirilen uygulamalar ile ilgili olarak teknik, operasyonel ve kullanım yönlerinin belirlenmesi, kimin nasıl kullanacağı ve sorumlulukların yerine getirilmesi için çözümlerin sağlanması ve bunların nasıl dokümante edileceğini içeren bir plan hazırlanmalıdır. Böylece operasyonel çözümlerin planlanması gerçekleştirilmektedir. Sonrasında oluşturulan dokümantasyon ve eğitim aktiviteleri ile bilginin iş yönetimine, son kullanıcılara ve operasyondan sorumlu personele transfer edilmesi sağlanmaktadır.

5. *Bilgi sistemleri kaynaklarının karşılanması:*[109] Tedarik ve uygulama kapsamında yapılan iş için gerekli olan bilgi sistemleri altyapı, tesis, yazılım, donanım ve hizmetler için alım stratejisinin oluşturulması gerekmektedir. Ayrıca bu stratejinin organizasyonun alım süreciyle de uyumlu olan prosedürler ve standartlar ile yönetilmesi sağlanmalıdır. Bu kapsamda tüm tedarikçi kontratlarının oluşturulması, değiştirilmesi ve sona erdirilmesi sağlanmalı, tedarikçi seçimi tanımlı kriterlere göre gerçekleştirilmeli ve organizasyonun satın alma kapsamında hakları korunmalıdır.

6. *Değişiklik yönetimi:*[110] Tüm değişiklik taleplerinin standartlaşmış bir şekilde yönetmek amacıyla, uygulamalar, prosedürler, işlemler, sistem ve servis parametreleri ve bunların

[107] ISACA COBIT, **age**, 81
[108] **age**, 85
[109] **age**, 89
[110] **age**, 93

temelini oluşturan platformlar için resmi bir değişiklik yönetimi prosedürü oluşturulmalıdır. Değişiklik yönetimi kapsamında bütün değişiklik taleplerinin operasyonel sistem ve sistemin işlevselliği üzerindeki etkilerinin değerlendirildiğinden emin olunmalıdır. Ayrıca değişikliklerin statülerinin takibinin ve raporlanmasının sağlanması ve değişikliğe bağlı olan kullanıcı dokümantasyonu ve prosedürleri güncellenmelidir. Son olarak mevcut değişiklik yönetimi prosedürü dışında gerçekleşen acil değişikliklerin de tanımlanmasını, değerlendirilmesini ve onaylanmasını içeren bir acil değişiklik prosedürü bu kontrol hedefi kapsamında oluşturulmalıdır.

7. *Sistem çözümlerinin ve değişikliklerin uygulanması ve akredite edilmesi:*[111] Bilgi sitemlerinin veya uygulamalarının gelişimi, uyarlaması veya değiştirilmesi projesinin parçası olarak, etkilenen kullanıcı bölümleri ve BT fonksiyonlarının operasyon grupları belirlenmiş eğitim ve uyarlama planına göre eğitilmelidir. Ayrıca geliştirilen uygulamalar için test planı oluşturulmalı ve testler ayrı bir test ortamında plana uygun olara gerçekleştirilmelidir. Gerçekleştirilen testlerin kapsamında son kullanıcı kabul testleri ve kalite güvence testleri de dahil edilmelidir. Ayrıca değişiklikler, operasyonel ortama taşınmadan önce, tanımlanmış kabul planına uygun olarak, ayrı bir test ortamında, programcılardan bağımsız bir test grubu tarafından, performans ölçümlemeyi de kapsayan etki ve kaynak değerlendirmesini içeren şekilde test edilmelidirler. Bilgi sistemlerinin geliştirilmesi sürecinde gerçekleştirme planı oluşturulmalıdır. Bu plan; versiyon tasarımını, versiyon paketlerinin oluşturulmasını, yeni oluşturulmuş prosedürleri/yüklenmesini, vakaların tespit edilmesini, dağıtım kontrolünü de içermelidir. Son olarak canlı ortama alınan bilgi sistemleri veya uygulamalar için gözden geçirme yapılmalı ve olası eksik noktalar iyileştirilmelidir.

4.7.3. Hizmet Sunumu ve Destek Faaliyetlerinin Denetimi

1. *Hizmet seviyelerinin tanımlanması ve yönetimi:*[112] Müşteri olan iş tarafı ile servis sağlayıcısı bilgi teknolojileri fonksiyonu arasında düzenlenmiş hizmet düzeyi yönetim sürecini sağlayan bir çerçeve oluşturulmalıdır. Çerçeve, müşteri ve hizmet sağlayıcılar arasında sürekli iş gereksinimleri ile uyumu ve öncelikleri kapsamalı ve müşterek bir uzlaşımı kolaylaştırmalıdır. Çerçeve, hizmet gereksinimlerinin oluşturulması için servis

[111] ISACA COBIT, **age**, 97
[112] **age**, 101

tanımları, hizmet düzey anlaşmalarını, operasyon düzey anlaşmalarını ve yatırım kaynakları süreçlerini içermelidir. Bu özellikler, bir hizmet kataloğunda düzenlenmiş olmalıdır. Ayrıca tanımlanmış hizmet düzey performans ölçütleri sürekli olarak izlenmelidir. Hizmet düzeyindeki başarılar üst düzey yönetimin anlayacağı formatta raporlanmalıdır. Son olarak hizmet düzey anlaşmaları düzenli olarak gözden geçirilmelidir. Böylece iş tarafı ve BT fonksiyonu arasındaki servislerin yönetimi hedefine uygun olarak yürütülebilecektir.

2. *Üçüncü kişilerden alınan hizmetlerin yönetimi:*[113] Bilgi teknolojileri servislerinin sağlanması kapsamında BT bölümünün hizmet sağlayıcı üçüncü taraf firmalar (tedarikçiler) ile ilişkilerini yönetmesi ve servisleri hizmet seviyesi anlaşmalarına uygun olarak alması gerekmektedir. Bu sebeple, tüm tedarik hizmetlerinin tanımlanması ve tedarik türü, önemi ve kritikliğine göre kategorilendirilmesi gereklidir. Tedarikçilerin rollerininin, sorumluluklarının, hedeflerinin, beklenen servislerinin ve referans bilgilerinin belirtildiği teknik ve organizasyonel ilişkilerin resmi dokümantasyonu sağlanmalıdır. Ayrıca, tedarikçinin hali hazırdaki iş gereksinimlerini karşıladığından, sözleşme maddeleri ve servis seviyesi anlaşması ile örtüştüğünden, performansının diğer tedarikçiler ve piyasa şartları ile rekabet edebildiğinden emin olmak için bir süreç de tesis edilmelidir. Örneğin denetlenen bankaların ATM makineleri kapsamında edindiği donanım hizmeti bu kapsamda yönetilecek servislerden sadece biridir.

3. *Performans ve kapasite yönetimi:*[114] Bilgi teknolojileri kaynaklarının kapasite ve performanslarının gözden geçirildiği bir planlama süreci bu kontrol hedefi kapsamında kurulmalıdır. Kapasite ve performans planları, BT kaynaklarının hem mevcut ve hem de öngörülen performans, kapasite ve girdileri için model oluşturabilecek uygun modelleme tekniklerini içermelidir. Mevcut performans ve kapasite seviyeleri ile gelecekte ulaşılması öngörülen performans ve kapasite BT yönetimi içerisinde karşılaştırılmalı olarak izlenmeli ve gerekli aksiyonlar alınmalıdır. Diğer bir ifadeyle bilgi teknolojileri kaynaklarının performans ve kapasitesi sürekli olarak takip edilmelidir. Örneğin denetlenen bankalardaki mevcut kullanılan bilgi sisteminin, tüm müşterilere kesintisiz olarak hedeflenen performans seviyesinde hizmet sunacağından emin olunmalıdır.

[113] ISACA COBIT, **age**, 105
[114] **age**, 109

4. *Hizmet sürekliliğinin sağlanması:*[115] Organizasyonun yönetim faaliyetlerinin devamlılığı için bilgi sistemleri sürekliliği yapısı geliştirilmelidir. Yapının amaç, karar verilmiş altyapı gereksinimlerine yardımcı olmak, felaket kurtarma ve bilgi sistemleri olasılık planlarını yürütmektir. Bu kapsamda anahtar iş fonksiyonlarında ve süreçlerinde önemli aksaklıkların veya bozulmaların etkisini azaltacak şekilde tasarlanmış bir yapıyı temel alan, bilgi sistemleri devamlılık planları geliştirilmelidir. Bilgi sistemleri süreklilik planının güncel olduğundan ve devamlı olarak gerçek iş gereksinimlerine yanıt verdiğinden emin olmak amacıyla, değişiklik kontrolü prosedürlerinin tanımlanması ve uygulanması için bilgi sistemleri yönetimi yönlendirilmelidir. Ayrıca, bilgi sistemleri süreklilik planı; bilgi sistemlerinin etkili olarak kurtarıldığından, noksanlıkların belirlendiği ve planın hala uygun olduğundan emin olmak amacıyla periyodik olarak test edilmelidir. Son olarak plandaki ilgili tüm birimlerin; prosedürler, sahip oldukları roller ve kaza ya da felaket anında yerine getirecekleri sorumluluklar hakkında düzenli eğitim almaları temin edilmeli ve plan yetkili kişilere dağıtılmalıdır. İş sürekliliği planlarının tesisinin yanında olağanüstü durum merkezinin kurulması ve felaket kurtarma planlarının da bilgi sistemleri yönetimi tarafından oluşturulması gerekmektedir.

5. *Sistem güvenliğinin sağlanması:*[116] Bilgi sistemlerinin güvenliği organizasyonun en üst seviyesinde yönetilmelidir ve güvenlik aksiyonlarının yönetimi ile iş gereksinimleri arasında uyum sağlanmalıdır. Kurumsal bilgi işlem kullanımı, bilgi teknolojileri yapılanışı, bilgi risk ve hareket planları ile bilgi güvenlik kültürünü içeren bilgi teknolojileri güvenlik planı oluşturulmalıdır. Plan, organizasyonun (denetlenen bankaların) güvenlik politika ve prosedürlerinde uygulanmalı; kurum hizmet, personel, yazılım ve donanıma gerekli yatırımı yaparken de göz önüne alınmalıdır. Bunun dışında bilgi sistemleri üzerindeki tüm kullanıcıların faaliyetlerinin izlenebildiği kimlik yönetim mekanizması ile kullanıcı hesaplarının ve ilgili kullanıcı haklarının talep edilmesi, oluşturulması, kullanıcılara atanması, askıya alınması ve kapatılması işlemlerinin ne şekilde gerçekleştirileceği kullanıcı hesapları yönetimi sürecinin de belirlenmiş olması beklenmektedir. Bunun dışında, güvenlik testlerinin gözetimi ve izlenmesi, güvenlik vakasının tanımlanması, güvenlik teknolojilerinin korunması, kriptoğrafik anahtar

[115] ISACA COBIT, **age**, 113
[116] **age**, 117

yönetimi, zararlı yazılımların önlenmesi, belirlenmesi ve düzeltilmesi, ağ güvenliği ve hassas verilerin alışverişi konularında da kontrol noktalarının tanımlanması bu başlık altında beklenmektedir.

6. *Maliyetlerin belirlenmesi ve dağıtılması:*[117] Tüm bilgi teknolojileri ("BT") harcamalarının belirlenmesi ve bunların şeffaf bir maliyet modelini desteklemek için BT hizmetlerine tahsis edilmesi gerekmektedir. Bu kapsamda BT birimi tarafından sağlanan her servisin geri ücretlendirme oranlarının hesaplanmasını desteklemek için hizmet tanımlamalarına dayalı bir BT maliyetlendirme modelinin oluşturulması gerekmektedir. Sonrasında tahmini ve gerçekleşen maliyetler arasındaki farklılıklar, kurumun finansal ölçüm sistemleriyle uyumlu bir şekilde analiz edilmeli, raporlanmalı ve maliyet modelinin sürekliliği sağlanmalıdır.

7. *Kullanıcıların eğitimi:*[118] Bilgi teknolojileri personelinin eğitim ihtiyaçlarının tespit edilmesi ve personelin yetkinliklerinin organizasyonun ihtiyaçları çerçevesinde geliştirilmesi için bir strateji belirlenmelidir. Belirlenen eğitim ihtiyaçları doğrultusunda hedef gruplar ve üyeleri, etkin eğitim yöntemleri ve eğitmenler tanımlanmalıdır. Son olarak eğitimin tamamlanmasının ardından eğitim ve eğitmen; uygunluk, kalite, verimlilik, bilginin tekrarı, maliyet ve değer açısından değerlendirilmelidir. Bu değerlendirmenin sonuçları gelecekte hazırlanacak eğitim planları ve eğitim yöntemleri hakkında fikir edinmek için kullanılmalıdır.

8. *Hizmet sunumu yönetimi ve olay yönetimi:*[119] Bu kontrol hedefi kapsamında hizmet masası ve vaka yönetimi fonksiyonu bilgi teknolojileri ("BT") birimi tarafından iş tarafına sağlanması amaçlanmıştır. BT ile kullanıcı ara yüzlü, kaydetme, iletişim, tüm çağrıları analiz edip gönderen bir hizmet Masası fonksiyonu kurulmalı, olaylar, hizmet ve bilgi talepleri raporlanmalıdır. Çağrıların, vakaların, hizmet taleplerinin ve ihtiyaç duyulan bilgilerin kaydedilmesine ve takip edilmesine izin veren bir yapı ve sistemin kurulması gerekmektedir. Kurulan sistem, olay yönetimi, problem yönetimi, değişiklik yönetimi, kapasite yönetimi, uygunluk yönetimi gibi süreçlerle uyumlu olarak çalışmalıdır. Sorun

[117] ISACA COBIT, **age**, 121
[118] **age**, 125
[119] **age**, 129

çözüldüğü zaman, çözüm adımlarının yardım masasında kaydı sağlanmalı ve atılan adımlar müşteri tarafından onaylanmış olduğu doğrulanmalıdır.

9. *Konfigürasyon yönetimi:*[120] Konfigürasyon öğeleri ile ilgili tüm bilgileri içeren destekleyici bir araç ve merkezi arşiv oluşturulmalıdır. Tüm varlıklar ve varlıklardaki değişimler izlenmeli ve kayıt tutulmalıdır. Her sistem ve servis için konfigürasyon öğelerinden dayanak oluşturulmalı ve bu temel konfigürasyon bilgileri değişiklikler sonrasında geri dönüşüm kontrol noktaları olarak kullanılmalıdır. Ek olarak konfigürasyon arşivindeki tüm değişikliklerin kaydının tutulması ve yönetimini destekleyici, konfigürasyon prosedürü hazırlanmak zorundadır. Son olarak geçmiş ve güncel konfigürasyonların bütünlüğünü doğrulamak için konfigürasyon verileri belirli periyotlarla gözden geçirilmeli ve mutabakatı sağlanmalıdır.

10. *Problem yönetimi:*[121] Problem yönetiminde, vaka yönetimi kapsamında değerlendirilen sorunların raporlanması ve sınıflandırılması için ilgili süreçler uygulanıyor olmalıdır. Vaka yönetimine entegre olarak gerektiğinde vakaların problem seviyesinde problem yönetimi sürecine yükseltilmesi beklenmektedir. Problemlerin kategori, etki, aciliyet ve önceliklerinin belirlenerek sınıflandırılması gerekmektedir. Bu kontrol hedefi kapsamında tesis edilecek problem yönetim sistemi; problem izleme, analiz etme, raporlanan bütün problemlerin ana sebeplerinin belirlenmesi ve yeterli işlem geçmişi raporlaması gibi olanakları sağlıyor olmalıdır. Problem kayıtlarının, bildirilen hatanın başarılı bir şekilde çözüldüğünün onayından sonra veya alternatif olarak problemin nasıl üstesinden gelineceğinin problemi açan iş tarafıyla mutabık kalınmasından sonra kapatılacağı ile ilgili bir prosedür oluşturulmalıdır. Genel olarak problem ve vakaların etkin yönetiminden emin olunması için değişiklik, konfigürasyon ve problem yönetimleri ile ilgili süreçlerin birbirine entegre olması gerekmektedir.

11. *Veri yönetimi:*[122] Verinin erişilebilir ve kullanılabilir olması için, veri depolama ve arşivleme süreçlerin tanımlanması ve uygulanması gereklidir. Bu süreçler geri yükleme gereksinimlerini, maliyet uygunluğunu ve güvenlik gereksinimlerini de göz önünde bulundurmalıdır. Yedekleme araçlarının (disk, kartuş) envanterinin tutulduğu ve

[120] ISACA COBIT, **age**, 133
[121] **age**, 137
[122] **age**, 141

kullanılabilirliklerinin izlendiği bir kütüphane yönetim sistemi oluşturulmalıdır. Sistemlerin/verinin yedeklenmesi ve bunların geri çağrılması ile ilgili dokümantasyonun iş ihtiyaçlarına ve süreklilik planına uygun olarak hazırlanması v uygulamaya konması beklenmektedir. Ek olarak hassas veri ve mesajların alınması, işlenmesi, fiziksel depolaması ve çıktılarına yönelik güvenlik gereksinimlerinin belirlenip uygulanması gerekmektedir.

12. *Fiziksel çevre yönetimi:*[123] Bilgi teknolojileri sistemlerinin bulunacağı fiziki bir yerin seçimi ve düzenlenmesi esnasında, sağlık ve güvenlikle ilgili yasal mevzuatın, doğal ve/veya insan kaynaklı felaket ve hatalardan doğabilecek risklerin göz önünde bulundurulması gerekmektedir. İş ihtiyaçlarına uygun olarak fiziksel güvenlik önlemlerinin belirlenmesi ve uygulamaya konulması gerçekleştirilmelidir. Özellikle, kritik bilgi sistemleri operasyonlarının fiziksel güvenliği sağlanırken dikkat çekilmemelidir. Bunun yanında iş gereksinimleri doğrultusunda ve acil durumlarda, kritik alanlara (sistem odası, elektrik odası gibi) erişimi onaylayan, kısıtlayan ve kaldıran prosedürler uygulanmalıdır. Son olarak çevresel faktörlerden (deprem, su baskını vb.) korunmaya yönelik ölçekler tasarlanmalı ve uygulanmalıdır. Çevreyi kontrol etmek ve denetlemek için özel malzemeler ve cihazlar kritik alanlara yerleştirilmelidir.

13. *Operasyon yönetimi:*[124] Bilgi teknolojileri operasyonları için standart prosedürler tanımlanmalı, uygulanmalı ve sürdürülmelidir. Operasyonel problemlere karşılık devamlılığını sağlamak için ilgili prosedürler vardiya konusunu da düzenlemek zorundadır. İş gereksinimlerini karşılamak için görevlerin, işlemlerin ve işlerin zamanlaması etkili bir sırada, üretimi ve faydayı en yüksek dereceye çıkaracak biçimde düzenlenmelidir. Bu kapsamda bilgi sistemleri üzerindeki işlerin en uygun sırada çalıştırılması ve çalışma sırasının devamlılığı sağlanmak zorundadır. Ayrıca, bilgi teknolojileri altyapısının ve ilgili olayların gözetimine ilişkin prosedürler tanımlanmalı ve uygulanmalıdır. Bu aşamada performans bozulmasının sıklığının ve etkilerinin azaltılması için donanım altyapısının sürdürebilirliğini sağlayacak prosedürler tanımlanmış olmalıdır. Son olarak bilgi sistemleri operasyonunun yönetimi kapsamında hassas bilgi teknolojileri

[123] ISACA COBIT, **age**, 145
[124] **age**, 149

varlıklarının (kripto anahtarları, özel yazıcılar vb.) korunması ve fiziki güvenliğinin sağlanması gerekmektedir.

4.7.4. İzleme ve Değerlendirme Faaliyetlerinin Denetimi

1. *Bilgi sistemleri performansının izlenmesi ve değerlendirilmesi:*[125] Bu kontrol hedefi kapsamında amaç, metodolojiyi ve bilgi teknolojileri çözümlerini ve dağıtım servislerini ölçecek süreçleri belirlemek ve bilgi teknolojilerinin işe katkısını izlemek için genel bir yaklaşım oluşturmaktır. İş tarafıyla çalışarak, dengeli ve doğru performans hedefleri belirlenmeli ve bunların hem iş hem de paydaşlar tarafından onaylanması sağlanmalıdır. Sonrasında bu hedefleri kayıt eden, ölçümleri yakalayan, bilgi teknolojileri performansı hakkında geniş ve özlü bilgi verecek ve kurum izleme sistemlerine uyumlu bir performans izleme yöntemi uygulanmalıdır. Son olarak performans izlemesini, değerlendirmesini ve raporlamasını temel alan iyileştirme faaliyetleri gerektiği noktalarda başlatılmalıdır.
2. *İç kontrolün izlenmesi ve değerlendirilmesi:*[126] Bilgi teknolojileri ("BT") kontrol ortamının ve kontrol çerçevesinin sürekli olarak izlenmesi sağlanmalıdır. BT kontrol ortamının ve çerçevesinin geliştirilmesi için, sektörün en iyi uygulamaları ile karşılaştırılmalı değerlendirmeler yapılmalıdır. Ayrıca denetimsel gözden geçirme yolu ile BT iç kontrollerinin etkinliğinin izlenmesi ve raporlanması sağlanmalıdır. Bu kapsamda tespit edilen kontrol hataları ile ilgili bilgiler, hataların temelini oluşturan sebeplerin analizine ve düzeltme hareketlerine kaynak teşkil etmesi açısından kaydedilmelidir. Bunun yanında BT bölümü ve yönetimi süregelen bir kendini değerlendirme programı yoluyla, yönetimin BT süreç, politika ve kontratları üzerindeki iç kontrollerinin bütünlüğünün ve etkinliğinin değerlendirilmesi sağlanmalıdır. Son olarak organizasyonun destek aldığı üçüncü taraf hizmet sağlayıcılarının iç kontrol durumu değerlendirilmek zorundadır.
3. *Denetlenenin iç usul ve esasları dahil ilgili mevzuata uyumun sağlanması:*[127] Yasal mevzuat, düzenlemeler ve diğer dış gereksinimler kapsamında organizasyonun bilgi sistemleri politikaları, standartları, prosedürleri ve metodolojileri uyumlu olarak oluşturulmalıdır. Ayrıca mevzuata uyum güvenliği ve ortaya çıkabilecek uyum

[125] ISACA COBIT, **age**, 153
[126] **age**, 157
[127] **age**, 161

boşluklarını düzeltmeye yönelik yapılabilecek faaliyetlerin süreç sahibi tarafından zamanında alındığını doğrulayan ve bunun iç talimatlar veya harici yasal, düzenleyici veya sözleşmeye dayanan gereksinimlerden sağlandığının iç politikalarla uyumu sağlanmalı ve raporlanmalıdır.

4. *Bilgi sistemlerine ilişkin kurumsal yönetişimin temini:*[128] Bilgi teknolojileri ("BT") yönetim çerçevesi oluşturulurken BT süreci ve kontrol modeli üzerinde temellendirilmeli ve dahili kontrollerde bir bozulma ve gözden kaçırmadan kaçınmak için de kesin sorumluluk sağlanmalıdır. Yine bu çerçeve kapsamında, üst kurul ve yönetimin stratejik BT konuları hakkında bilgilenmesinin sağlanması ve organizasyonun stratejileri ile uyumu sağlanmalıdır. Bu yönetim çerçevesi, BT yetkisindeki yatırım programlarının, BT aktiflerinin ve servislerinin kurumun strateji ve hedeflerinin en uygun değerlerde gerçekleşmesini sağlamak amacını taşımalıdır. Bu kapsamda etkin kaynak yönetimini, risk yönetimini ve performans ölçümü adımlarını da içermelidir. Sonuç olarak bu kontrol hedefi kapsamında BT yönetişiminin "CobiT"in hedeflediği gibi stratejik olarak organizasyon genelinde sağlanması istenmektedir.

4.8. Bankaların Bilgi Teknolojilerine Yönelik Destek Alım Faaliyetlerinin Denetimi

14 Eylül 2007 tarihli ve 26643 sayılı "*Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkeler Tebliği*" ve 1 Kasım 2006 tarihli ve 26333 sayılı "*Bankaların Destek Hizmeti Almalarına ve Bu Hizmeti Verecek Kuruluşların Yetkilendirilmesine İlişkin Yönetmelik*" kapsamında denetlenen bankaların bilgi teknolojilerine yönelik destek alım faaliyetlerinde uymaları gereken kurallar belirlenmiştir.

Denetlenen bankaların üst yönetimi tarafından bilgi sistemleri kapsamında alınacak destek hizmetlerine ilişkin olarak, söz konusu hizmetin destek hizmeti alımı yoluyla gerçekleştirilmesinin banka açısından doğuracağı riskler yeterli düzeyde değerlendirilmeli, yönetilmeli ve destek hizmeti kuruluşu ile ilişkilerin etkin bir şekilde yürütülebilmesi gerekmektedir. Bu kapsamda yeterli gözetim mekanizmasının tesis edilmesinde denetlenen bankaların üst yönetimi sorumludur.

Destek hizmeti alımı, planlanması ve sonlandırılması durumlarına ilişkin olarak risklerin yönetilmesi denetlenen bankaların sorumluluğu altındadır. Destek hizmeti alımına ilişkin koşul,

[128] ISACA COBIT, **age**, 165

kapsam ve her türlü diğer tanımlama, ilgili destek hizmeti kuruluşunca da imzalanmış olacak şekilde sözleşmeye bağlamak zorundadır.

Denetlenen bankalar, güvenlik politikasının tanımladığı ilkeler doğrultusunda,[129]

- destek hizmeti alımından kaynaklanan riskleri kontrol altında tutmak üzere gerekli organizasyonel değişiklikleri yapmalı,
- idari prosedürler tanımlamalı ve bu kapsamda alınacak önlemleri ilgili tüm diğer bölümlerin günlük işlemlerine ve sistemlerine entegre etmeli,
- alınan destek hizmetine ilişkin olarak, destek hizmeti kuruluşuyla ilişkileri yürütecek, yeterli bilgi ve tecrübeye sahip bir sorumlu atamalıdır.

Alınan destek hizmeti kapsamında hizmeti veren firmanın bankaların bilgi sistemlerine erişmeleri gerektiği noktalarda destek hizmeti kuruluşlarına verilen erişim hakkı tipleri özel olarak değerlendirilmelidir. Fiziksel veya mantıksal olabilecek bu erişimler için risk değerlendirmesi yapılmalı ve gerekli kontroller tesis edilmek zorundadır. Risk değerlendirmesi yapılırken ihtiyaç duyulan erişim tipi, erişilen verinin değeri, destek hizmeti kurulusu tarafından yürütülmekte olan kontroller ve bu erişimin denetlenen banka bilgilerinin güvenliği üzerindeki etkileri dikkate alınmak zorundadır.

Yukarıdaki yasal kuralların yanı sıra 1 Kasım 2006 tarihli ve 26333 sayılı "*Bankaların Destek Hizmeti Almalarına ve Bu Hizmeti Verecek Kuruluşların Yetkilendirilmesine İlişkin Yönetmelik*" kapsamında bankaların ana hizmetlerinin uzantısı veya tamamlayıcısı niteliğinde hizmet veren destek hizmeti kuruluşlarına ve destek hizmeti alınabilecek konulara ilişkin usul ve esaslar düzenlenmektedir. Bu yönetmelik kapsamında destek hizmeti kapsamına giren hizmetler ve denetlenen bankaların bu kapsama giren hizmetler için uymaları zorunlu olan kurallar belirlenmektedir.

Bağımsız denetim kuruluşları, bilgi sistemleri denetimi kapsamında denetlenen bankaların almış oldukları destek hizmetlerini yukarıda bahsi geçen tebliğ ve yönetmelikteki kurallar gereği değerlendirmek zorunda olup yasal mevzuata uyumluluğunu değerlendirmek zorundadır.

[129] BDDK, "**Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ**" (Madde 8, Sayı 26643; Tarih 14 Eylül 2007), 4

Bağımsız denetim kuruluşları bu kapsamdaki görüşlerini bilgi sistemleri denetim raporuna konu etmek zorundadır.

4.9. Bilgi Sistemleri Denetim Sonuçlarının Değerlendirilmesi ve Olgunluk Seviyesi

Bilgi sistemleri denetim sürecinde genel kontrol alanlarının "CobiT" kapsamında denetlenmesi kapsamında her bir kontrol hedefinin denetim sonuçlarına ve denetçinin değerlendirmesine göre olgunluk seviyeler belirlenmek zorundadır. Aşağıdaki genel kontrol alanları içerisindeki her bir kontrol hedefi için olgunluk seviyelerinin belirlenmesi gerekmektedir.

Tablo 1: Genel Kontrol Alanlarına Yönelik Kontrol Hedefi Sayısı

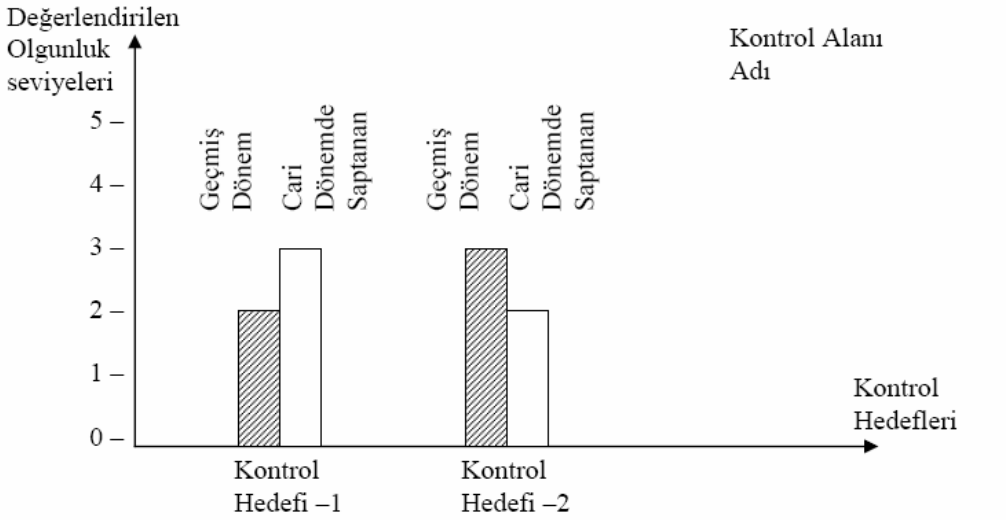
Genel Kontrol Alanı	*Kontrol Hedefi Sayısı*
Planlama ve Organizasyon	10
Tedarik ve Uygulama	13
Hizmet Sunumu ve Destek	7
İzleme ve Değerlendirme	4

Denetlenen bankaların, 1 Kasım 2006 tarihli ve 26333 sayılı "*Bankaların Destek Hizmeti Almalarına ve Bu Hizmeti Verecek Kuruluşların Yetkilendirilmesine İlişkin Yönetmelik*" gereği yapılan bilgi sistemleri denetimine ait genel kontrol hedeflerine ilişkin olgunluk seviyesi grafikleri karşılaştırmalı olarak bilgi sistemleri denetim raporunda sunulmak zorundadır.

Olgunluk seviyeleri Bilgi Sistemleri Denetim ve Kontrol Birliği ("ISACA"), Bilgi Teknolojileri Yönetişim Enstitüsü ("ITGI") tarafından yayınlanmış Bilgi Teknolojilerine İlişkin Kontrol Hedefleri ("CobiT") çerçevesinde yer verilen yöntemlere uygun olarak, bilgi kriterleri, teknoloji kaynakları ve yönetsel ölçütlerin birlikte dikkate alınması suretiyle değerlendirilmek zorundadır. Yönetsel ölçütlerin varlığı, uygunluğu ve bilgi sistemleri gelişimine katkıları da olgunluk seviyesi değerlendirmelerinde dikkate alınmalıdır.

Mevcut olarak bankalarda süren bilgi teknolojileri denetiminde olgunluk seviyeleri "CobiT"in güncel versiyonu (4.1) ve 14 Eylül 2007 tarihli ve 26643 sayılı "*Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ*"in beklentileri dikkate alınarak değerlendirilmektedir.

Bilgi sistemleri denetim raporunda, olgunluk seviyelerinin rakamsal karşılıkları grafiklerde 5 Aralık 2006 tarihli ve 26367 sayılı Resmi Gazete'de yayınlanmış "*Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğine*" göre gösterilmek zorundadır. Buna göre aşağıdaki grafikte bilgi sistemleri denetim raporunda genel kontrol alanlarına ait olgunluk seviyelerinin gösterilme şeklini görebilirsiniz:



Şekil 10: Olgunluk Seviyesi Grafiği

BDDK, "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğine**" (Ek 1, Sayı 26367; Tarih: 5 Aralık 2006), 1

Denetçinin olgunluk seviyesini belirlerken bilgi sistemleri denetim sonuçlarına göre yaptığı değerlendirmeye geçmeden önce olgunluk seviyeleri ve anlamları hakkında CobiT çerçevesine göre bilgi vermek gerekmektedir. Buna göre CobiT çerçevesinin genel tanımlaması kapsamında 5'li ölçek içinde her bir rakamın ne anlama geldiği kısaca aşağıda görülebilmektedir:[130]

[130] ISACA COBIT, **age**, s. 17-18

Tablo 2: CobiT Olgunluk Seviyeleri ve Açıklamaları

Olgunluk Seviyesi Notu	*Olgunluk Seviyesi Açıklaması*
0	Mevcut değil
1	Başlangıç seviyesinde
2	Tekrarlanabilir
3	Tanımlanmış
4	Yönetilen ve ölçülebilir
5	Optimize edilen

Yukarıdaki tabloya göre her bir olgunluk seviyelerinin açıklaması şu şekildedir;[131]

1. ***Mevcut Değil (Seviye 0):*** Kurum genelinde değerlendirilen kontrol hedefine yönelik farkındalığın tespit edilemediği ve dolayısıyla bu kontrol hedefi kapsamında süreç eksikliği bulunan seviyedir.

2. ***Başlangıç Seviyesinde (Seviye 1):*** Kurum genelinde kontrol hedefi ile ilgili olarak farkındalık mevcut olup konuyla ilgili standart bir süreç tanımı mevcut değildir. Bunun yerine kontrol hedefi ile ilgili faaliyetler gerektiğinde kişiye ve/veya duruma bağlı olarak gerçekleştirilmektedir.

3. ***Tekrarlanabilir (Seviye 2):*** Kontrol hedefi ile ilgili süreçlerin geliştirildiği ve farklı kişiler tarafından benzer prosedürlerin izlenerek sürecin yönetildiği fark edilmektedir. Ancak standart prosedürler ile ilgili olarak kurum genelinde eğitim ve duyuruların yapılmadığı ve süreç sorumlularının da açık olarak belirlenmediği tespit edilmektedir. Genel olarak kişilerin tecrübesine ve bilgisine bağlı olarak süreçlerin tanımlarına uygun olarak ve tekrar edilebilir şekilde yönetildiği belirlenmektedir.

4. ***Tanımlanmış (Seviye 3):*** Kontrol hedefi ile ilgili olarak süreçlerin standart prosedürlere bağlı ve dokümante şekilde yönetildiği belirlenmektedir. Standart prosedürler duyurulmaktadır ve bunlara uygun olarak süreçlerin yönetilmesi gerekliliği zorunluluğa bağlanmaktadır. Nadiren standart prosedürlerin uygulanmasında sapmalar tespit edilse de, genel olarak standart prosedürlere uygunluk görülebilmektedir.

5. ***Yönetilen ve Ölçülebilir (Seviye 4):*** Yönetim, kontrol hedefi ile ilgili faaliyetler ve süreçler için tasarlanan standart prosedürlere uyumu izlemekte ve ölçümlemektedir.

[131] ISACA COBIT, **age**, 19

Gerektiği noktalarda, standart prosedürlere uygunsuzlukların tespit edilmekte ve gerekli aksiyonlar alınmaktadır. Süreçlerin iyileşme odaklı olarak yönetildiği ve gereken noktalarda otomatik araçların kullanıldığı tespit edilmektedir.

6. ***Optimize Edilen (Seviye 5):*** Sürekli iyileşme hedeflerine uygun olarak, kontrol hedefi dahilindeki faaliyetler ve süreçler en iyi örneklere bağlı olarak yönetilmekte, izlenmekte ve ölçümlenmektedir. Bilgi teknolojilerinin entegre olarak iş tarafı ile uyumlu yönetildiği, kaliteyi ve etkinliği arttıran araçların da kullanıldığı tespit edilmektedir.

Bilgi sistemleri denetim sonuçlarına bağlı olarak genel kontrol alanları olgunluk seviyelerinin denetçi tarafından nasıl belirlendiğine yönelik bilgiler araştırma kapsamındaki uygulama bölümünde kapsama alınan bir detay kontrol hedefi için gösterilecektir.

4.10. Bilgi Sistemleri Denetim Raporunun Oluşturulması

5 Aralık 2006 tarihli ve 26367 sayılı Resmi Gazete'de yayınlanmış "*Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliği"* kapsamında bilgi sistemleri denetim raporunun içeriği ve şekline ilişkin usul ve esasları yasal kurum olan BDDK tarafından belirlenmiştir. Bağımsız denetim kuruluşları, bilgi sistemleri denetimi ile ilgili olarak uygulama kontrolleri, genel kontrol alanları ve ilkeler tebliği uyumluluk kapsamındaki test sonuçlarına bağlı şekilde denetim raporunu tam olarak hazırlamakla yükümlüdürler.

Bağımsız bilgi sistemleri denetçileri, denetim amaçlarının tamamını karşılayan bilgilere yer vererek; raporlanmış konuları yeterli ve doğru bir şekilde anlaşılmasını sağlayacak biçimde ve yasal gereksinimleri sağlayacak şekilde raporlamakla yükümlüdürler.

Bankalarda gerçekleştirilen bilgi sistemleri denetim faaliyetlerinin sonucu olarak bilgi sistemleri denetim raporu aşağıdaki unsurları içerecek şekilde düzenlenmek zorundadır[132].

1. *Başlık:* Bilgi sistemleri bağımsız denetim raporunun, bir bağımsız denetim kuruluşu tarafından hazırlandığını gösterir açık bir başlık oluşturulması gerekmektedir. Bu başlık, bilgi sistemleri bağımsız denetçilerinin, bağımsızlığa ilişkin etik ilke ve kurallarına uyduğuna ve raporun da bu kişiler tarafından hazırlandığına karine teşkil etmektedir.

[132] BDDK, "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğine**" (Madde 12-20, Sayı 26367; Tarih: 5 Aralık 2006), 6-10

2. *Raporun sunulduğu merci:* Bilgi sistemleri bağımsız denetim raporunun, sözleşmede belirtilen muhataplara hitaben düzenlenmesi gereklidir. Bu kapsamda, bilgi sistemleri bağımsız denetim raporu, bankaların yönetim kurullarına hitaben düzenlenmektedir. Banka yönetim kuruluna hitaben raporun düzenlenip sunulmasının yanında, BDDK ve Türkiye Cumhuriyeti Merkez Bankası'na ("TCMB") da bilgi sistemleri denetim raporunun kopyaları sunulmaktadır. Bunun dışında finansal bağımsız denetim raporundan farklı olarak bilgi sistemleri bağımsız denetim raporları kamuya açık olmayıp gizli nitelik taşımaktadır. BDDK tarafından belirtilen mercilerin dışında bağımsız denetim raporu hiçbir tarafa verilemez, raporlar çoğaltılamaz ve konuyla ilgili diğer taraflarla bilgi paylaşılamaz.
3. *Denetim mektubu:* Bu bölümde bağımsız denetim kuruluşu, bilgi sistemleri denetim faaliyetleri ve testleri sonucunda, bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemler üzerindeki kontroller kapsamındaki görüşe yer vermektedir. Bilgi sistemleri denetçisi denetim raporu kapsamında dört farklı görüş bildirebilmektedir. Buna göre;
    a. *Olumlu görüş:* Bilgi sistemleri denetimi raporunu imzalamaya yetkili kişiler (bilgi sistemleri baş denetçisi ve sorumlu ortak baş denetçi), yapılan denetim sonucunda herhangi bir önemli kontrol eksikliğinin bulunmaması ve denetim kapsamında herhangi bir kısıtlama ya da engelleme ile karşılaşılmaması durumunda, kendilerine bağlı bağımsız denetim ekiplerinin de görüşlerini alarak, raporda olumlu görüş bildirmektedirler.
    b. *Şartlı Görüş:* Yapılan bilgi sistemleri denetimi sonucunda en az bir önemli kontrol eksikliğiyle karsılaşmalarına rağmen, bu eksikliklerin denetlenenin bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemlerinin bütününü veya büyük bir kısmını etkilemediğini düşündükleri durumda denetim mektubunda şartlı görüş bildirilmektedir. Diğer taraftan, görüş bildirmekten kaçınmayı gerektirecek önemde olmamakla birlikte, bilgi sistemleri denetim faaliyetlerini sınırlayan herhangi bir hususun varlığı veya yeni tesis edilmiş bir sistem veya süreç hakkında yeterince bilgi edinememeleri durumunda da denetim mektubunda şartlı görüş bildirilmektedir.

c. *Görüş Bildirmekten Kaçınma:* Bilgi sistemleri denetimi raporunu imzalamaya yetkili kişiler, bağımsız denetim çalışmalarında karşılaşılan belirsizlik ve sınırlamaların görüş belirtilmesini engelleyecek derecede önemli olduğunu düşündükleri durumlarda, kendilerine bağlı bağımsız denetim ekiplerinin de görüşlerini alarak, bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemler üzerindeki kontroller hakkında görüş bildirmekten kaçınabilirler. Ancak görüş bildirmekten kaçınmanın nedenlerinin denetçi tarafından denetim mektubu kapsamında açıklanması şarttır.

d. *Olumsuz Görüş:* Bilgi sistemleri denetimi raporunu imzalamaya yetkili kişiler, yapılan bilgi sistemleri denetimi sonucunda denetlenenin bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemlerinin bütününü veya büyük bir kısmını etkileyen en az bir önemli kontrol eksikliğiyle karşılaşmaları durumunda olumsuz görüş bildirirler. Bu kapsamda önemli kontrol eksikliğinin tanımını anlamak, denetim mektubundaki görüş tiplerinden hangisinin rapora uygun olduğunu anlamak için önem taşımaktadır. Önemli kontrol eksikliği, denetlenen bankanın dönemsel olarak yaptığı finansal raporlamalarında önemli bir yanlışlığın önlenmesini veya düzeltilmesini engelleyecek veya banka bünyesinde yürütülen süreçlerin ve bu süreçlere ilişkin bilgilerin bütünlüğünün ve tutarlılığının, güvenilirliğinin, devamlılığının ve gereken durumlarda gizliliğinin sağlanmasına önemli olumsuz etki yapması yüksek olasılık taşıyan kayda değer kontrol eksikleridir. Kayda değer kontrol eksikliği ise denetlenen bankanın finansal verilerinin bütünlüğünün, tutarlılığının, güvenilirliğinin ve gereken durumlarda gizliliğinin sağlanmasına, faaliyetlerinin devamlılığının teminine olumsuz etki yapması muhtemel bir kontrol zayıflıklarıdır. Bu kapsamda kontrol zayıflıkları ise, bir kontrolün tasarımının veya işletilmesinin, hataları zamanında önleme ve tespit etmeye olanak sağlamaması durumudur. Yukarıdaki açıklanan bilgilerden de anlaşılacağı gibi bilgi sistemleri denetçisinin tespit ettiği bulgular üç kategoride sınıflandırılmak zorunda olup, bu kategoriler kontrol zayıflığı, kayda değer kontrol eksikliği ve önemli kontrol eksikliğidir. Bu aşamada da önemli kontrol eksikliğinin tespiti, denetim mektubu kapsamındaki görüşü etkilemektedir.

4. *Yönetici özeti:* Bilgi sistemleri denetim raporunun bu bölümünde, denetçi denetimin amaçlarından, denetim amaçlarına erişmek için uyguladığı denetimin kapsamından, metodolojisinden ve denetim çalışmasına ilişkin olarak genel bir değerlendirmeden bahseder. Bunun yanında uygulama kontrollerine ve yapıldıysa genel kontrol alanlarına ilişkin denetim sonucunda ortaya çıkan bulgular da dikkate alınarak, denetlenen bankanın durumu hakkında genel bir değerlendirmeye ve öne çıkan bulgulara iş riskleri ile birlikte bu bölümde yer verilir. Son olarak genel kontrol alanlarına yönelik denetim faaliyeti gerçekleştirildiyse "CobiT" kontrol hedeflerine yönelik olarak tespit edilen olgunluk seviyeleri açıklamaları ile birlikte bu bölümde belirtilir.

5. *İçindekiler:* Bilgi sistemleri denetim raporunun içinde yer alan bölümleri gösteren bir içerik sayfası oluşturulur.

6. *Denetim metodolojisi:* Bilgi sistemleri denetçisi denetim metodolojisi kapsamında, denetim amaçlarını gerçekleştirmek için kanıt toplama ve analiz tekniklerini de içerecek şekilde hangi denetim amaçlarının hangi yöntemlerle karşılandığını ifade etmektedir. Bu aşamada, denetim çalışmasındaki önemli varsayımlardan, denetim kanıtı toplama ve analiz tekniklerinden, örnekleme yönteminden ve sonuçların değerlendirilme yönteminde bahsedilmektedir.

7. *Denetlenenin bilgi sistemleri hakkında genel bilgi:* Denetlenen bankanın bilgi teknolojileri çalışan profili, organizasyon yapısı, ana bankacılık faaliyetlerinin yürütülmesinde kullanılan uygulamalar/sistemler, araçlar hakkında genel bilgi, bilgi sistemleri mimarisi, ağ yapısı ve kritik olarak kullanılan yazılım ve araçlar hakkında genel bilgi oluşturularak raporda yer verilmektedir.

8. *Denetlenenin iç kontrol ve iç denetim yapısına ilişkin değerlendirme:* Bu bölümde iç denetim biriminin, finansal raporlama sistemlerine ilişkin iç kontrollerinin denetimi kapsamında yapmış olduğu planlamaların, faaliyetlerin ve denetim sonuçlarının takibinin değerlendirilmesi gerekmektedir. Bunun yanında, yönetimin finansal raporlama sistemlerine ilişkin iç kontrollerin tesis edilmesi ve sağlıklı bir şekilde işletilmesine verdiği önem ve işletilen kontrollerin yeterliğini ve etkinliğini ölçmedeki performansının da değerlendirilmesi gerekmektedir. Son olarak finansal raporlama sistemlerine ilişkin iç

kontrollerle ilgili risk değerlendirme sürecinin değerlendirilmesi ve bilgi sistemleri denetim ekibinin özelliklerinin değerlendirilmesi de bu bölümde yer almaktadır.

9. *Uygulama kontrolleri denetimi bölümü:* Bu bölümde denetlenen bankalarda gerçekleştirilen uygulama kontrollerinin denetimine yönelik faaliyetlerin sonucuna yer verilir. Bilgi sistemleri denetçisi öncelikle uygulama kontrollerinin etkinliğine ve yeterliliğine ilişkin yaptığı denetim sırasında kullandığı önemlilik değerlendirmesini ve bu değerlendirme sonucunda hangi bankacılık süreçlerini seçtiğini açıklamak zorundadır. Önemlilik kriterini kullanarak seçtiği her bir süreç üzerindeki uygulama kontrollerini test ederken kullandığı metodolojiyi de bilgi sistemleri denetçisi açıklamak zorundadır. Bu kapsamda, örneklem boyutunun belirlenmesinden, örneklem seçiminde kullanılan yöntemlerden, test yönteminden, denetimi gerçekleştirdiği denetlenenin birimlerinden, sistemlerinden ve bunların seçim kriterlerinden bahsetmek gerekmektedir. Seçilen süreç ile ilgili olarak uygulama ve sistem üzerindeki anahtar kontroller belirlenir ve bunlara ilişkin testler gerçekleştirilerek denetim sonuçlarına ve tespit edilen bulgulara taşıdıkları iş riskleri ile birlikte yer verilmektedir. Ek olarak denetçi bir önceki yıl yapılan uygulama kontrolleri denetiminde yer alan bütün bulguları da değerlendirmek ve bu bulguların son durumlarını raporlamak zorundadır.

10. *Genel kontroller denetimi bölümü:* Bu bölümde denetlenen bankalarda gerçekleştirilen genel kontrol alanlarının denetimine yönelik faaliyetlerin sonucuna yer verilir. Bilgi sistemleri denetçisi öncelikle, önemlilik kriterini kullanarak CobiT kapsamında seçtiği genel kontrol hedeflerinin denetiminde kullandığı metodolojiyi açıklamaktadır. Metodoloji kapsamında örneklem boyutunun belirlenmesinden, örneklem seçiminde kullandığı yöntemlerden ve test yöntemine ilişkin açıklamalardan bahsedilmektedir. Bilgi sistemleri denetçisi, kapsam dahilinde seçilen kontrol hedeflerine ilişkin denetlenenin durumuna ve yapmış olduğu denetim çalışmasına ilişkin bir genel değerlendirme yapmakta ve her bir genel kontrol alanı kapsamındaki seçilen kontrol hedefleri için denetlenenin kontrollerine, test faaliyetlerine ve sonuçlarına yer vermektedir. Son olarak genel kontrol alanları kapsamında geçmiş dönemlerdeki bulgulardan halen devam edenler ile çözülmüş olanların değerlendirilmesi, geçmiş bulgulara ilişkin denetlenenin görüsüne ve geçmiş dönemlerdeki kontrol hedeflerine ait olgunluk seviyeleri ile denetim

döneminde tespit edilen olgunluk seviyeleri arasındaki karşılaştırmalara da rapor kapsamında yer verilmelidir.

11. *Denetim ekibi ve süresi:* Denetlenen bankalarda, bağımsız denetim kuruluşu tarafından görevlendirilen bilgi sistemleri denetim ekibine ve denetim faaliyetlerinin süresine yer verilmektedir.

12. *Kısaltmalar:* Bu bölümde, bilgi sistemleri denetim raporunda kullanılan kısaltmaların açıklamalarına yer verilmektedir. Örneğin, "BDDK": Bankacılık Denetleme ve Düzenleme Kurulu gibi.

13. *Sözlük:* Bu bölümde, bilgi sistemleri denetim raporunda kullanılan teknik terim ve kavramların açıklamalarına yer verilmektedir. Örneğin, "SWIFT Alliance Sunucusu": SWIFT mesajlarının iletilmesi ve alınması için kullanılan sunucu gibi.

Bilgi sistemleri denetimi kapsamında, gerçekleştirilen denetim faaliyetleri ile finansal veri üretimine ilişkin süreç ve sistemler üzerindeki kontrollerin, kontrol hedeflerini gerçekleştirdiğine dair mutlak bir güvence verilemeyeceği unutulmamalıdır. İnsan faktörünü ve insan muhakemesinin barındırdığı hatalar gibi kontrollerin doğasında bulunan kısıtlar dolayısıyla bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemler üzerinde kontrol zayıflıkları bulunabilir ve zamanında tespit edilemeyebilir. Bu kısıtlar iç kontrol ortamının doğal kısıtları olarak kabul edilmekte ve mutlak güvence verilmesine engel olmaktadır. Bu aşamada bilgi sistemleri denetimi vasıtasıyla bilgi sistemleri iç kontrol ortamı değerlendirilerek ilgili kontrollerin etkin bir şekilde tasarlanması ve işletilmesi sağlanmakta ve önemli yanlışlık riski azaltılmaktadır.

5. UYGULAMA

Türk bankacılık sektöründe gerçekleştirilen bilgi sistemleri denetimi kapsamında uygulama denetimi ve genel kontrol alanları denetimi ile ilgili olarak çeşitli bilgisayar destekli denetim araçlarından ve uygulamalardan yararlanarak denetimin gerçekleştirilmesinin ve raporlanmasının açıklaması istenmektedir.

Tüm bankacılık süreçlerinin ve CobiT kontrol alanlarının bilgi sistemleri denetimi kapsamında açıklaması uygulamanın kapsamını çok genişleteceğinden her bir alanda yeterli açıklamanın sağlanması için kapsam sınırlaması getirilmiştir. Kapsam olarak bilgi sistemleri uygulama denetimi alanında "*Genel Muhasebe Kontrolleri*" sürecinde gerçekleştirilen testlere ve tespitlerin raporlanmasına yer verilirken; bilgi sistemleri genel kontrol alanı denetimi için ise "*DS5: Sistem Güvenliğinin Sağlanması*" sürecinde gerçekleştirilen testlere, tespitlerin raporlanmasına ve olgunluk seviyesinin belirlenmesine yer verilecektir.

Uygulamanın problemi, amacı, önemi ve uygulama yapılırken kullanılan araçlara uygulamanın devam eden bölümlerinde değinilmiştir.

5.1. Uygulamanın Problemi

Bağımsız finansal denetim kapsamında, bağımsız denetim kuruluşlarının ana amacı bağımsızlık ilkesine bağlı olarak finansal tabloların doğruluğu, tutarlılığı, ve tam olarak açıklanmış olması adına makul bir güvence sağlamak için görüş verilmesidir. Bu açıdan değerlendirildiğinde bilgi sistemlerinin yoğun olarak kullanıldığı bankacılık sektöründe, finansal veri üretiminde bilgi sistemlerinin önemi göz önüne çıkmaktadır. Bu sebeple bağımsız finansal denetim faaliyetleri kapsamında bilgi sistemleri denetimi ile entegre olarak denetim faaliyetlerinin yürütülebilmesi günümüz teknolojik gelişmelerine ve bankacılık sektörünün yapısına bağlı olarak kaçınılmaz boyuta gelmiştir. Bu sebepledir ki, bilgi sistemleri denetim faaliyetleri ve testleri sonucunda, bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemler üzerindeki kontroller kapsamında görüş verilmesi gerekmektedir.

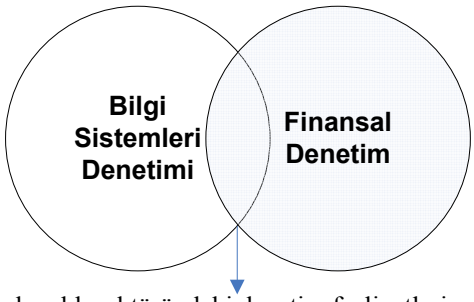
Bu kapsamda uygulamanın ana problemi, bilgi sistemleri denetim faaliyetleri ile finansal denetim faaliyetleri arasındaki entegrasyonun sağlanabilmesi ve denetim faaliyetlerinin denetim amaçlarına uygun olarak bir bütün halinde etkin ve verimli bir şekilde yürütülmesini sağlamaktır.

5.2. Uygulamanın Amacı

Uygulamanın problemine bağlı olarak, uygulamanın amacı iki başlık altında toplanabilmektedir:

- Bağımsız finansal denetim amaçları ile bankacılık sektöründeki bilgi sistemleri uygulama denetimi sonuçlarının nasıl bir arada değerlendirilebileceğini uygulamalı olarak ortaya koymak
- Bankacılık sektöründeki bilgi sistemleri genel kontrol alanları denetim sonuçları ile bilgi sistemleri uygulama denetimi sonuçlarının nasıl bir arada değerlendirilebileceğini uygulamalı olarak ortaya koymak

Genel olarak yukarıdaki iki ayrı başlık ile ulaşılmak istenen ana amaç bilgi sistemleri denetim faaliyetlerinin finansal denetim faaliyetlerine nasıl destek olduğunu, bankacılık sektöründe bilgi sistemleri denetim faaliyetlerinin nasıl yürütülmesi gerektiğini ve aşağıdaki şekilde de gösterildiği gibi entegre bağımsız denetim yaklaşımının gerekliliğini ortaya koymaktır.



Bankacılık sektöründeki denetim faaliyetleri kapsamında ana amaç her iki denetim alanındaki enterasyonun sağlanması ve güvenilir bağımsız görüşün finansal veriler/tablolar üzerinde tesis edilmesidir.

Şekil 11: Bankalarda Entegre Denetim

5.3. Uygulamanın Önemi

Bankacılık sektöründe bilgi sistemleri denetimi kapsamında uygulama denetimine ve genel kontrol alanlarına yönelik seçilen süreçler kapsamında bilgi sistemleri denetiminin nasıl gerçekleştirildiği, sonuçların nasıl yorumlandığı, nasıl raporlandığı ve elde edilen sonuçların nasıl finansal denetim amaçlarına girdi teşkil ettiği ve bu kapsamdaki maddi doğruluk testlerinin kapsamını nasıl belirlediğine yer verilecektir.

Bu kapsamda uygulamanın önemi, bağımsız finansal denetim faaliyetlerinde özellikle bankacılık sektörü gibi bilgi sistemlerinin yoğun kullanıldığı sektörlerde bilgi sistemleri denetiminin önemini vurgulamak ve denetim amaçlarının sağlıklı olarak karşılanması için bilgi sistemleri denetim faaliyetlerinden ve bilgisayar destekli denetim araçlarından yararlanmanın kaçınılmaz olduğunu ortaya koymaktadır.

- Denetimin daha etkin, daha verimli ve daha kısa sürede yapılmasına yardımcı olmak
- Kısa zamanda güvenilirliği yüksek denetimler gerçekleştirmek
- Finansal verilerin yüzde yüzünün işlenmesine olanak sağlamak
- Finansal verileri üreten sistemlerdeki veri bütünlüğünün ve güvenilirliğinin üzerine görüş tesis etmek

bilgi sistemleri denetim faaliyetlerinin ve bilgisayar destekli denetim araçlarının entegre denetim faaliyetleri kapsamında finansal denetim amaçlarına sağladığı faydalardan bazılarıdır. Bu sebeple bilgi sistemlerini denetiminin esaslarını ve uygulamasını öğrenmek hem bağımsız denetim kuruluşlarında bilgi sistemleri denetimini gerçekleştiren denetçiler için hem de finansal verilerden/tablolardan yararlanan bilgi kullanıcılarının güvenilir bilgiye erişmesi için büyük önem taşımaktadır.

5.4. Uygulamanın Kapsamı ve Kısıtları

Bilgi sistemleri denetimi kapsamında, uygulama kontrollerinin denetiminde "*Genel Muhasebe Kontrolleri Süreci*" ve genel kontrol alanlarının denetiminde ise "*DS5: Sistem Güvenliğinin Sağlanması*" kapsam olarak belirlenmiştir.

Bilgi sistemleri denetimi kapsamında denetlenen bankalarda gerçekleştirilen süreç diğer bir adıyla uygulama denetimi ile ilgili olarak üç temel finansal denetim amaç desteklendiğinden her bir finansal denetim amacına uygun olarak uygulama içerisinde örnekler verilerek açıklanmıştır. Bunlar "*Kayıtsal Doğruluk*", "*Eksiksiz Olma*" ve "*Meydana Gelme*" finansal denetim amaçlarıdır.

Genel kontrol alanlarının denetiminde ise kontrollerin değerlendirilmesinden örnekler verilerek genel kontrol alanında "DS5" kontrol hedefinin olgunluk seviyesinin CobiT kapsamında nasıl değerlendirileceği açıklanmaktadır.

Uygulamanın her iki adımında da bilgisayar destekli denetim araçlarından nasıl yararlanılacağına dair bilgi verilmiştir.

Uygulamadaki maliyet ve zaman kısıtları nedeniyle bizzat denetim gerçekleştirilmeyip elde edilen veriler kapsamında "*Genel Muhasebe Kontrolleri Süreci*" ve "*DS5: Sistem Güvenliğinin Sağlanması*" alanlarında bilgi sistemleri denetim sürecini açıklayacak seviyede kontroller değerlendirmeye alınmış olup süreçlerin kapsamındaki tüm kontroller değerlendirilmemiştir.

5.5. Kullanılan Araçlar

Türk bankacılık sektöründeki bilgi sistemleri denetim faaliyetleri ve araştırmamızda belirtilen uygulama kapsamında aşağıdaki araçlardan yararlanılmıştır. Bu araçlardan yararlanılarak denetim faaliyetleri içerisinde elde edilen veriler incelenerek bilgi sistemleri denetim raporunda belirtilen ifadelere ve değerlendirilmelere ulaşılmaktadır.

1. *IDEA (Bilgisayar Destekli Denetim Aracı)*:[133] IDEA, çok çeşitli kaynaklardan verileri alabilen; bu verileri hızlı ve doğru olarak birleştirebilen, analiz edebilen, örnekleyebilen ve kullanıcı odaklı bilgisayar destekli veri analiz aracıdır. IDEA genel olarak, analistlerin, muhasebecilerin ve denetçilerin; görevlerinde etkinliğini arttıran ve önemli analizleri gerçekleştirme olanaklarını sunan bir araçtır. IDEA, bilgi sistemleri denetçileri de uygulama kontrollerinin denetiminde ve bilgi sistemlerinden elde edilen verinin analizinde ve verinin sistemler tarafından doğru olarak işlendiğinden emin olmak için kullandığı bir araçtır. IDEA çok büyük hacimdeki verilere erişmeyi mümkün kılmakta birlikte, verileri de oldukça çabuk olarak işleyebilmektedir. "Excel", "txt" gibi çeşitli formatlarda veri yüklenebildiği gibi, veri almak için herhangi bir sistemin dış veri tabanına bağlanabilme özelliğini de üzerinde bulunduran bir araçtır.
2. *CobiT Olgunluk Seviyesi Değerlendirme Aracı:*[134] Bilgi sistemleri denetim faaliyetleri kapsamında genel kontrol alanları denetim testleri sonuçlarının değerlendirilmesi ve her kontrol hedefi için CobiT standartlarına uygun olarak olgunluk seviyelerinin belirlenmesi için kullanılan bir araçtır. Örneğin "DS5: Sistem Güvenliğinin Sağlanması" kapsamında denetim testlerinin gerçekleştirilmesinden sonra bu kontrol hedefi kapsamında sonuçların

[133] KPMG, **IDEA Training Course Documents** (İstanbul: KPMG Turkey, 2005), 1-4
[134] KPMG, **CobiT Olgunluk Seviyesi Değerlendirme Aracı El Kitabı** (İstanbul: KPMG Turkey, 2005), 5

değerlendirildiği ve 0'dan 5'e kadar uygun olgunluk seviyesinin belirlenmesinde faydalanılan standart bir değerlendirme aracıdır.

3. *Bilgi Sistemleri Güvenlik Ortamı Değerlendirme Aracı*:[135] Uygulamamız kapsamında genel kontrol alanlarının denetimi için CobiT içerisindeki 34 kontrol hedefi içinden "DS5: Sistem Güvenliğinin Sağlanması" seçilmiş bulunmaktadır. Seçilen bu kontrol hedefi kapsamında genel olarak kurumun bilgi sistemleri güvenlik ortamı seviyesini değerlendirmeye yarayan ve detay kontrol testlerinin planlanmasında yol gösteren bir araçtır.

5.6. Uygulamanın Yapılması ve Sonuçları

Türk bankacılık sektöründeki bilgi sistemleri denetiminin uygulaması kapsamında "*Genel Muhasebe Süreci*" uygulama kontrolleri alanı ile "*DS5: Sistem Güvenliğinin Sağlanması*" genel kontrol alanı ile ilgili testlere ve raporlamalara açıklama getirilecek ve finansal denetim ile ilişkisi gösterilecektir.

5.6.1. Uygulama Kontrollerinin Denetimi ve Raporlaması: Genel Muhasebe Kontrolleri Süreci

"Genel Muhasebe Süreci" süreci ile ilgili kapsam altına alınması gereken noktalar kısaca şu şekilde açıklanabilmektedir[136]:

- Muhasebe fişi kesilmesine ilişkin yetkili personelin belirlenmesi ve yetkilendirilmesi süreçleri
- Mizanın oluşumu
- Geriye dönük muhasebe fişi kesilmesi işlemleriyle ilgili yetkilendirmelerin varlığı
- Muhasebe kayıtlarının bütünlüğü ve izlenebilirliği
- Muhasebe işlem numaralarının ardışıklığının korunmasının sağlanması gibi genel muhasebe kontrolleri, işlem limitlerinin ve yetkilerinin kontrolü incelenmelidir.

Bağımsız finansal denetimin amaçları, yukarıdaki kapsam maddeleri ile ilişkilendirilerek uygulama kontrolleri "Genel Muhasebe Süreci" kapsamında belirlenecek ve çeşitli araçlardan yararlanarak test edilecektir.

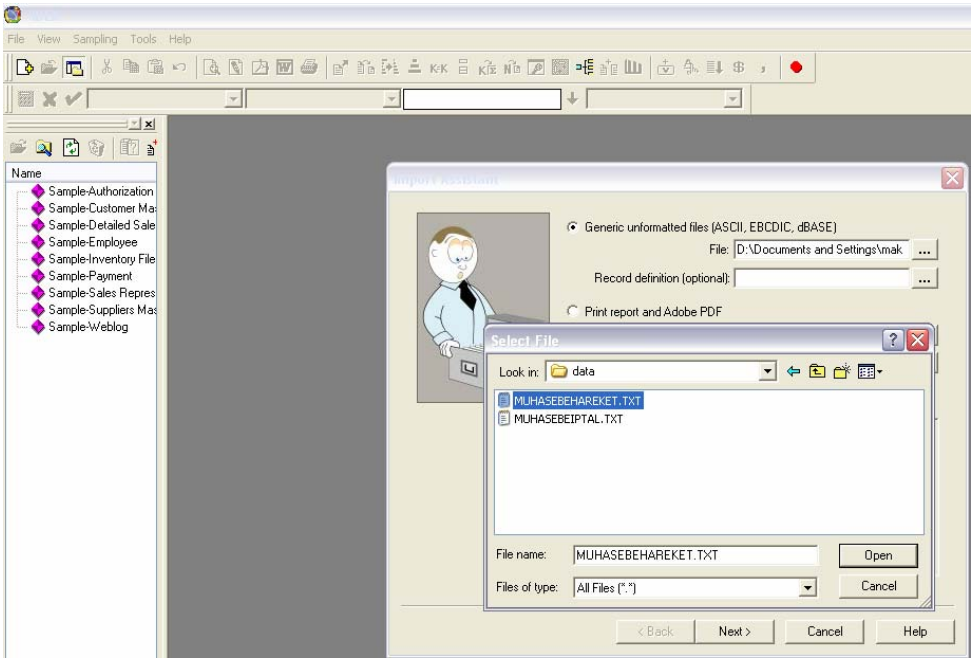
---

[135] Microsoft, **MSAT Tool**, http://technet.microsoft.com/tr-tr/security/cc185712 (en-us).aspx [15.04.2009]

[136] BDDK, "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**" (Madde 18/5, Sayı 26170; Tarih: 16 Mayıs 2006), 9

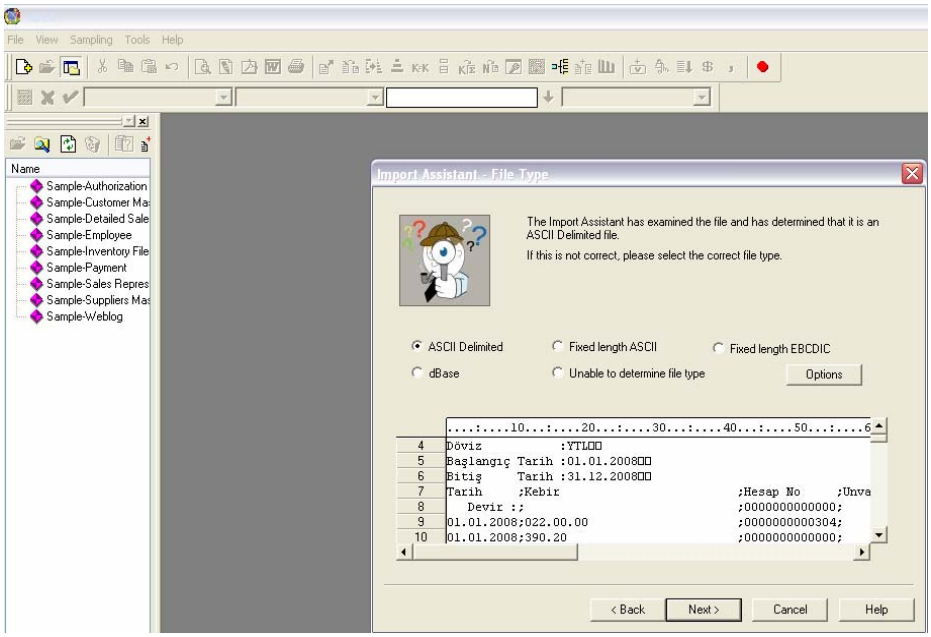
A) Kayıtsal Doğruluk Finansal Denetim Amacına Yönelik Uygulama Denetimi Örneği:

1. *Finansal Denetim Amacı*: Kayıtsal Doğruluk
2. *Sürecin Kapsamı*: Muhasebe kayıtlarının bütünlüğünün sağlanması
3. *Kontrol Alanı*: Girdi Kontrolleri / Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri
4. *Kontrol Tanımı*: Fiş tutar dengesinin korunması amacıyla ana bankacılık sistemi üzerinde oluşturulan muhasebe fişlerinin toplam borç ve alacak tutarlarının eşit olması sistemsel olarak zorlanmaktadır.
5. *Kontrolün Test Yöntemi*: İlgili ekranlar üzerinde örnekleme yöntemiyle otomatik kontrolün test edilmesi ve sistem üzerindeki tüm fişlerin IDEA aracı ile borç alacak dengesinin kontrol edilmesi.
6. *Testin Uygulanması*: Öncelikle serbest muhasebe fişi kesilen ekranlar üzerinde toplam borç ve alacak tutarı eşit olmayacak şekilde muhasebe fişinin sistem üzerinde girişi denerek sistemin girişe izin verip vermediği test edilecektir. Önleyici kontrolün başarılı olduğu tespit edildikten sonra sistem üzerindeki muhasebe hareket dosyasındaki tüm fiş kayıtlarının alınması ve IDEA üzerinde fiş dengelerinin kontrol için analizi gerçekleştirilecektir. Böylelikle üzerinde görüş verilen finansal raporların beslendiği tüm fiş bilgisi üzerinde borç-alacak tutar dengesi tüm kayıtlar üzerinde kontrolü sağlanacaktır.



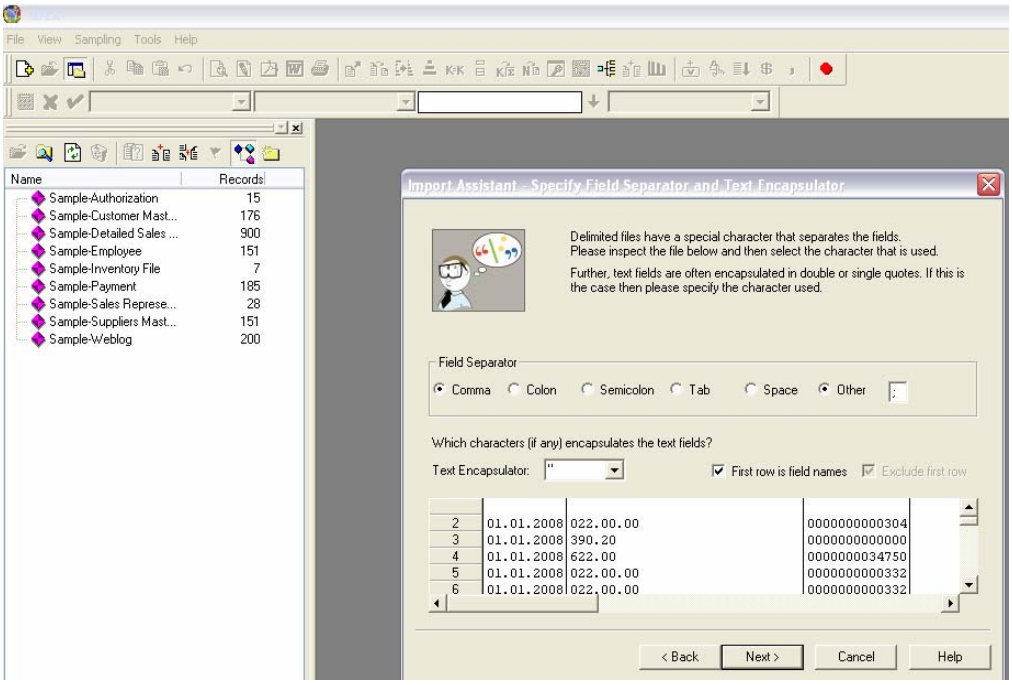
Şekil 12: IDEA Veri Girişi 1

Öncelikle muhasebe verisi "txt" formatında ana bankacılık sisteminden alınarak IDEA üzerine veri girişi sağlanması gerekmektedir. IDEA uygulaması üzerinden "muhasebehareket.txt" dosyası öncelikle seçilmektedir.



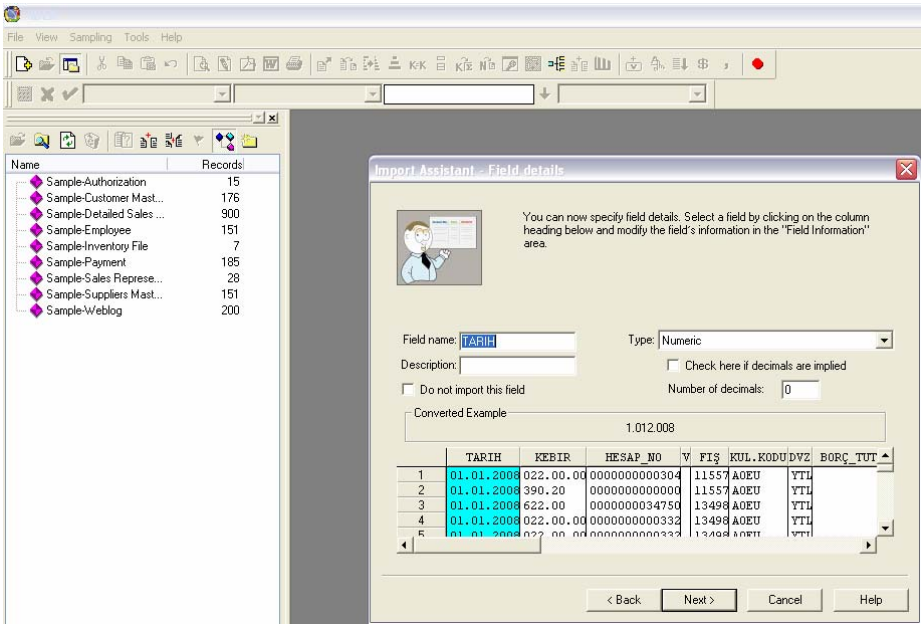
Şekil 13: IDEA Veri Girişi 2

Ana bankacılık sisteminden alınan dosya desenine bağlı olarak “ASCII Delimited” dosya tipi IDEA üzerinde seçilmektedir.



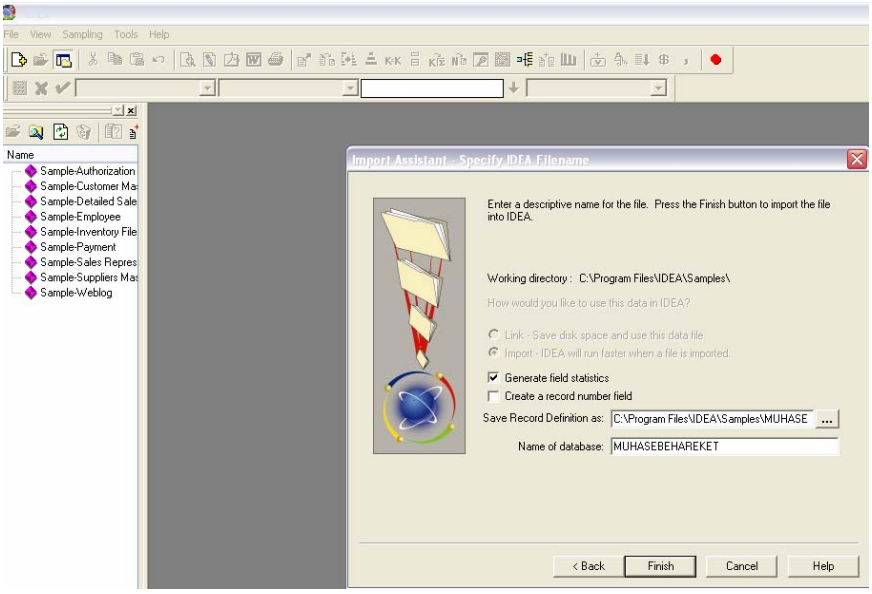
Şekil 14: IDEA Veri Girişi 3

Sonrasında veri deseni üzerindeki her bir kolonu ayırmak için kullanılan “;” işareti seçilerek kolonların tablo olarak IDEA üzerine aktarılması sağlanmaktadır.



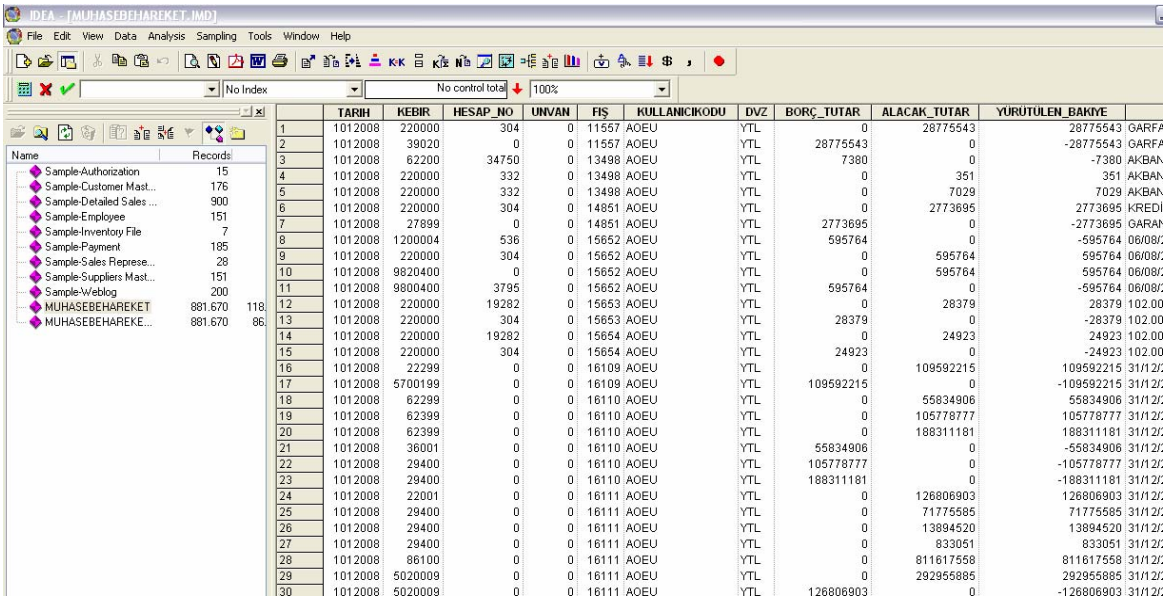
Şekil 15: IDEA Veri Girişi 4

Kolonlar ayrıldıktan sonra ilk satır kolon adları olarak seçilmekte ve verinin ön görünümü IDEA üzerinde görülebilmektedir. Örneğin yukarıdaki ekranda fişin kesildiği tarih, kebir, hesap numarası, fiş numarası, fişi sistem üzerinden kesen kullanıcı kodu ve döviz cinsi görülebilmektedir.



Şekil 16: IDEA Veri Girişi 5

Veri giriş sırasında yapılan ayarlamalar ile birlikte tüm veri "MUHASEBEHAREKET" veritabanına kaydedilmektedir.



	TARIH	KEBIR	HESAP_NO	UNVAN	FIŞ	KULLANICIKODU	DVZ	BORÇ_TUTAR	ALACAK_TUTAR	YÜRÜTÜLEN_BAKIYE
1	1012008	220000	304	0	11557	AOEU	YTL	0	28775543	28775543
2	1012008	39020	0	0	11557	AOEU	YTL	28775543	0	-28775543
3	1012008	62200	34750	0	13498	AOEU	YTL	7380	0	-7380
4	1012008	220000	332	0	13498	AOEU	YTL	0	351	351
5	1012008	220000	332	0	13498	AOEU	YTL	0	7029	7029
6	1012008	220000	304	0	14851	AOEU	YTL	0	2773695	2773695
7	1012008	27899	0	0	14851	AOEU	YTL	2773695	0	-2773695
8	1012008	1200004	536	0	15652	AOEU	YTL	595764	0	-595764
9	1012008	220000	304	0	15652	AOEU	YTL	0	595764	595764
10	1012008	9820400	0	0	15652	AOEU	YTL	0	595764	595764
11	1012008	9800400	3795	0	15652	AOEU	YTL	595764	0	-595764
12	1012008	220000	19282	0	15653	AOEU	YTL	0	28379	28379
13	1012008	220000	304	0	15653	AOEU	YTL	28379	0	-28379
14	1012008	220000	19282	0	15654	AOEU	YTL	0	24923	24923
15	1012008	220000	304	0	15654	AOEU	YTL	24923	0	-24923
16	1012008	22299	0	0	16109	AOEU	YTL	0	109592215	109592215
17	1012008	5700199	0	0	16109	AOEU	YTL	109592215	0	-109592215
18	1012008	62299	0	0	16110	AOEU	YTL	0	55834906	55834906
19	1012008	62399	0	0	16110	AOEU	YTL	0	105778777	105778777
20	1012008	62399	0	0	16110	AOEU	YTL	0	188311181	188311181
21	1012008	36001	0	0	16110	AOEU	YTL	55834906	0	-55834906
22	1012008	29400	0	0	16110	AOEU	YTL	105778777	0	-105778777
23	1012008	29400	0	0	16110	AOEU	YTL	188311181	0	-188311181
24	1012008	22001	0	0	16111	AOEU	YTL	0	126806903	126806903
25	1012008	29400	0	0	16111	AOEU	YTL	0	71775585	71775585
26	1012008	29400	0	0	16111	AOEU	YTL	0	13894520	13894520
27	1012008	29400	0	0	16111	AOEU	YTL	0	833051	833051
28	1012008	86100	0	0	16111	AOEU	YTL	0	811617558	811617558
29	1012008	5020009	0	0	16111	AOEU	YTL	0	292955885	292955885
30	1012008	5020009	0	0	16111	AOEU	YTL	126806903	0	-126806903

Şekil 17: IDEA'ya Transfer Edilen Verinin Görünümü

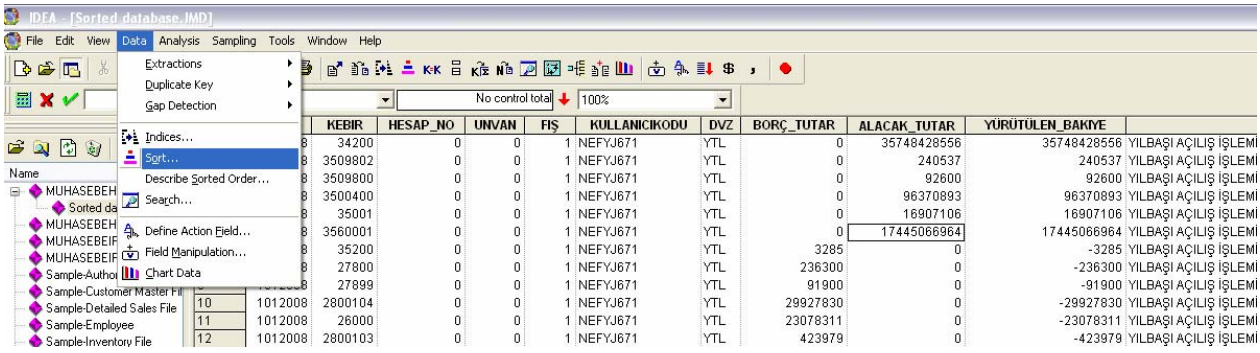
IDEA üzerinde veri girişinin tamamlanması ile birlikte ana bankacılık sisteminden alınan tüm fiş bilgisi kolaylıkla yüklenmiş ve analize hazır hale getirilmiştir.

Veri girişinin tamamlanmasından sonra kontrol testinin uygulaması için tüm fiş bilgisinin borç-alacak tutar dengesinin tüm veri kapsamında IDEA üzerinde analiz edilmesi gerekmektedir.

Numeric Statistics	BORÇ_TUTAR	ALACAK_TUTAR	YÜRÜTÜLEN_BAKIYE
Net Value	72.496.523.690,960	72.497.055.130,362	531.439,402
Absolute Value	72.496.523.690,960	72.497.055.130,362	144.993.578.821,322
# Records	881670	881670	881670
# of Zero Items	390697	490973	0
Positive Value	72.496.523.690,960	72.497.055.130,362	72.497.055.130,362
Negative Value	0	0	-72.496.523.690,960
# of Positive Records	490973	390697	390697
# of Negative Records	0	0	490973
# of Data Errors	0	0	0
# Valid Values	881670	881670	881670
Average Value	82.226.370,06	82.226.972,82	602,76
Minimum Value	0	0	-8.966.005.020,000
Maximum Value	8.966.005.020,000	8.966.005.020,000	8.966.005.020,000
Record Num of Min	1	2	851089
Record Num of Max	851089	851090	851090
Sample Std Dev	13.611.898.078,72	13.611.883.270,44	19.250.471.629,02
Sample Variance	185.283.769.305.429.180.000,00	185.283.366.168.077.600.000,00	370.580.657.939.844.370.000,00

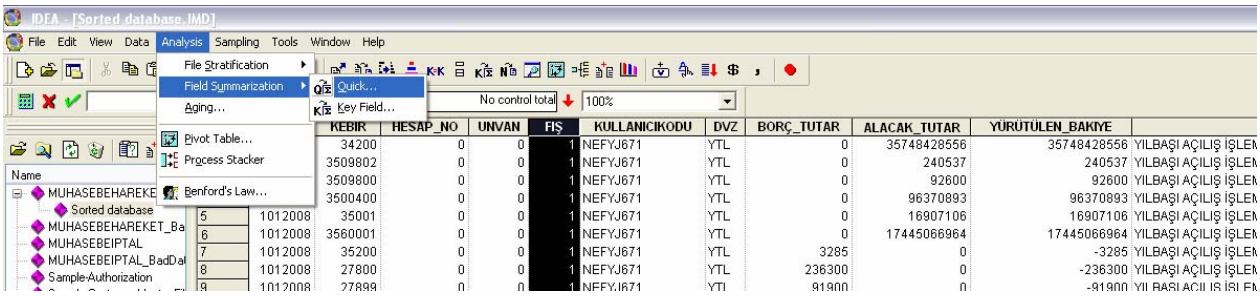
Şekil 18: IDEA İstatistiksel Özel Bilgi

Tüm veri IDEA üzerinde istatistiksel olarak özetlendiğinde, 2008 yılı içerisinde toplam 881.670 adet işlem olduğu tespit edilmiştir. Tüm işlemlerin borç ve alacak toplamları arasında ise yürütülen bakiye kolonunda da görüldüğü gibi 531.439.402 TL fark tespit edilmiştir.



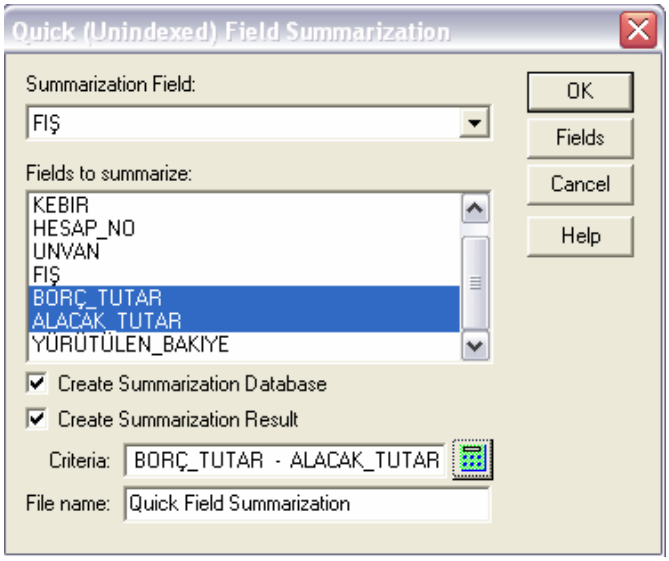
Şekil 19: IDEA Sıralama İşlemi

Öncelikle "*Sort: Sıralama*" alt menüsünden yararlanılarak tüm veri fiş numarasına göre sıralanmaktadır.



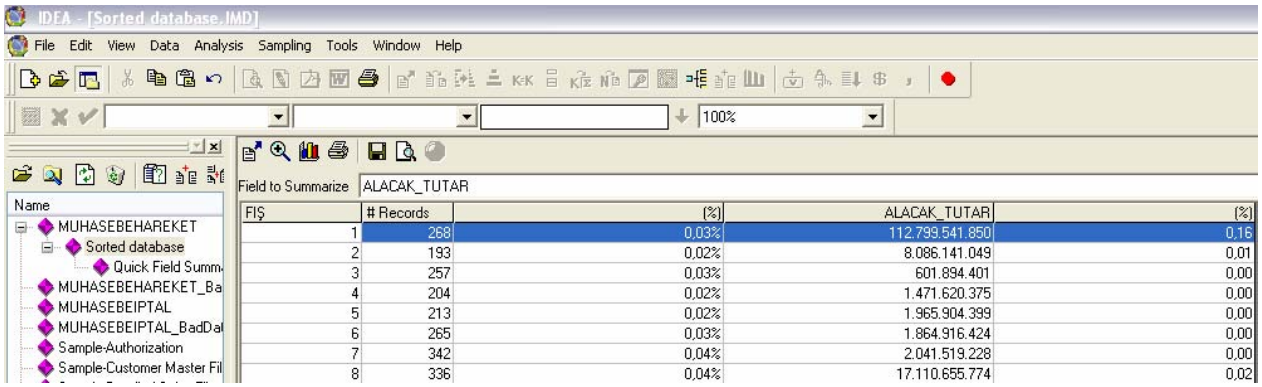
Şekil 20: IDEA "Field Summarization" İşlemi

Toplam borç ve alacak tutar farkını yaratan fiş numaralarının tespiti için "*Field Summarization*" alt menüsünden yararlanılmaktadır.



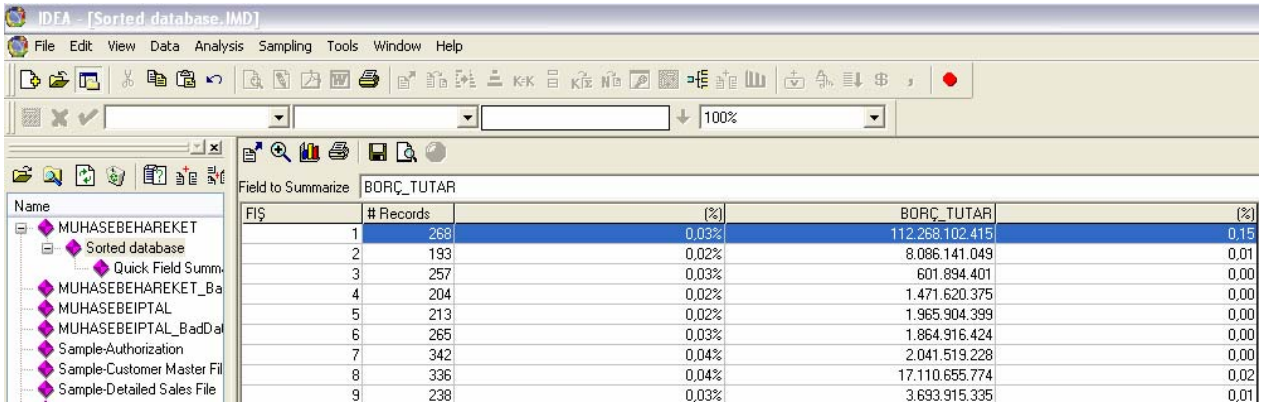
Şekil 21: IDEA "Field Summarization" İşleminde İlgili Kolonların Seçimi

"Fiş" kolonu ile birlikte "Borç Tutarı" ve "Alacak Tutarı" kolonları açılan menü üzerinden seçilmektedir. Böylelikle her bir fiş numarası altındaki işlemlerin toplan borç ve alacak tutarları gruplandırılabilecektir.



Şekil 22: IDEA "Field Summarization" İşleminin Sonucu 1

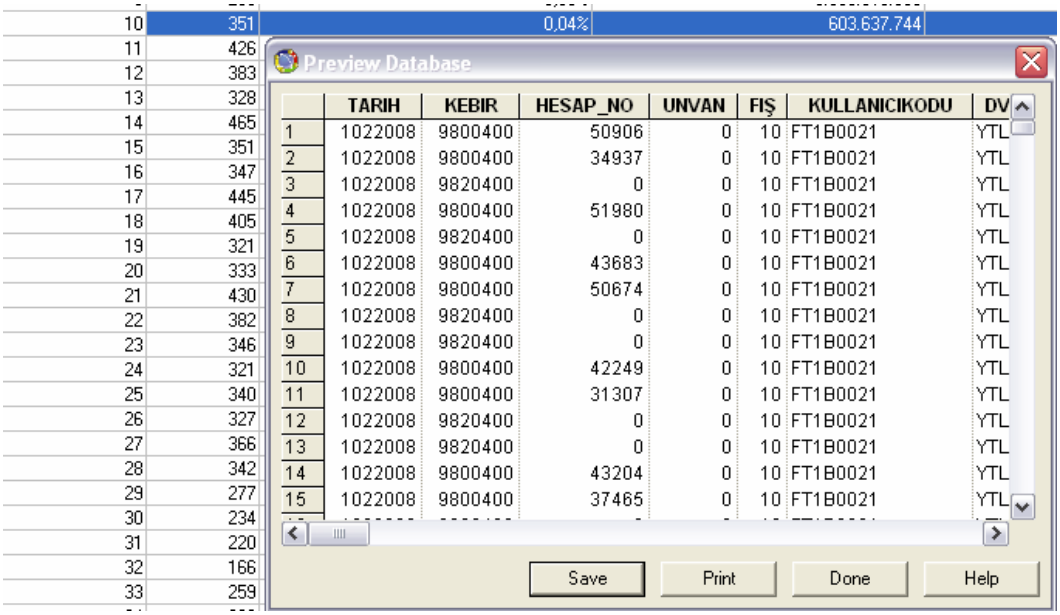
Yukarıdaki ekran görüntüsünden de görülebildiği gibi her bir fiş numarası içerisindeki işlem kaydının sayısı, toplam alacak tutarı ve tüm fişlerin toplam alacak tutarı üzerindeki yüzdelik dilimi görülebilmektedir. Örneğin "1" numaralı fiş içerisinde 268 adet işlem kaydının olduğu ve 112.799.541.850 TL alacak tutarına sahip olduğu görülmektedir. Bu tutar tüm fişlerin alacak tutarının %3'ünü oluşturmaktadır.



Şekil 23: IDEA "Field Summarization" İşleminin Sonucu 2

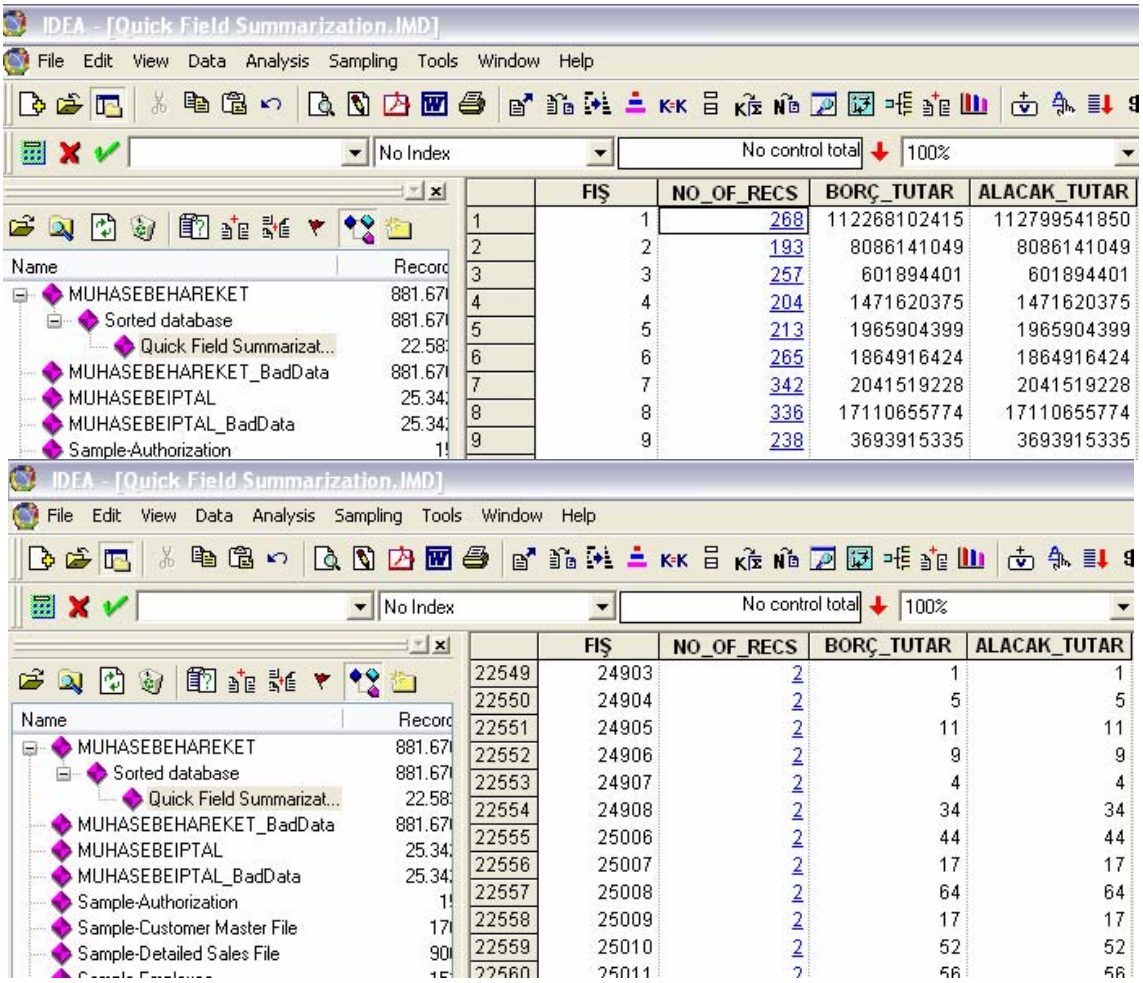
Bir önceki ekran görüntüsüne benzer bir şekilde fişlerin borç tutarı kapsamında gruplandırıldığı yukarıdaki ekran görüntüsünde görülmektedir. Aynı örnek ile ilerlendiğinde "1" numaralı fiş içerisinde 268 adet işlem kaydının olduğu ve

112.268.102.415 TL borç tutarına sahip olduğu görülmektedir. Bu tutar tüm fişlerin alacak tutarının %3'ünü oluşturmaktadır.



Şekil 24: IDEA "Field Summarization" İşleminde Gruplanan Kayıtların Detayı

Yukarıdaki özet bilgilerde gruplanan her bir fiş IDEA üzerinde seçilerek detay işlemlerine bakılabilmektedir. Örneğin, "10" numaralı fiş seçilerek detay 351 adet işleminin görülebildiği yukarıda izlenmektedir.



Şekil 25: IDEA "Field Summarization" İşleminde Fiş Sırası ve Kayıt Miktarları

Fiş numarası kapsamında gruplanan borç ve alacak tutarları birebir eşleştirilerek borç-alacak tutar dengesi bozuk fişler tespit edilebilmektedir. Bu kapsamda borç – alacak tutar dengesi olmayan fiş numaraları aşağıdaki şekilde tespit edilmiştir.

Fiş Numarası	Alt İşlem Say	Toplam Borç Tut	Toplam Alacak Tut	Fark
1	268	112.268.102.415,00	112.799.541.850,00	-531.439.435,00
75	33	14.449.944,00	14.449.943,00	1,00
153	59	17.858.268,00	17.858.267,00	1,00
213	50	40.360.205,00	40.360.206,00	-1,00
246	33	31.814.934,00	31.814.933,00	1,00
247	40	79.336.288,00	79.336.287,00	1,00
248	45	56.380.768,00	56.380.767,00	1,00
249	45	40.832.860,00	40.832.861,00	-1,00
253	42	16.391.793,00	16.391.792,00	1,00
257	44	44.218.486,00	44.218.487,00	-1,00
265	37	652.940.299,00	652.940.298,00	1,00
266	37	35.385.681,00	35.385.680,00	1,00
281	51	69.774.804,00	69.774.803,00	1,00
285	53	43.232.138,00	43.232.139,00	-1,00
298	71	19.429.815,00	19.429.816,00	-1,00
306	36	33.635.765,00	33.635.766,00	-1,00
307	40	2.175.588.467,00	2.175.588.468,00	-1,00
309	47	215.485.608,00	215.485.609,00	-1,00
312	48	19.240.157,00	19.240.156,00	1,00
322	44	27.173.215,00	27.173.216,00	-1,00
709	114	3.685.303.553,00	3.685.303.552,00	1,00
767	37	53.126.974,00	53.126.975,00	-1,00
780	43	30.110.712,00	30.110.713,00	-1,00
857	73	88.448.348,00	88.448.347,00	1,00
883	86	145.407.493,00	145.407.494,00	-1,00
896	92	169.303.925,00	169.303.926,00	-1,00
16877	36	1003735668	1003735669	-1,00
17088	19	8334492	8334493	-1,00
17307	19	242816622	242816623	-1,00
17308	19	370184877	370184878	-1,00
17313	19	23489349	23489348	1,00
17315	17	1307213813	1307213814	-1,00
17317	11	10005927	10005928	-1,00
17398	18	631537550	631537549	1,00
17708	29	11429556297	11429556298	-1,00
17792	17	54742499354	54742499355	-1,00
18188	11	34409446	34409445	1,00
23968	1	1	0	1,00
			Toplam	-531.439.402,00

Şekil 26: IDEA Borç-Alacak Dengesi Analiz Sonucu

Buna göre toplam 431 adet fiş kaydı nedeniyle 531.439.402 TL tutarında alacak tarafının fazla olduğu tespit edilmiştir. Fiş kaydı yapılan ekranlar üzerinde yapılan önleyici kontroller başarılı sonuç verse de sistemdeki mevcut kayıtlar incelendiğinde borç-alacak dengesinin tutturulamadığı fişler tespit edilmiştir. Bu farkın 531.439.435 TL tutarındaki kısmının "1" numaralı fiş nedeniyle olduğu tespit edilmiştir. Böylelikle bilgi sistemleri test sonucuna göre "1" numaralı fiş detayının finansal denetim ekipleri tarafından incelenmesi için bilgi verilmesi gerekmektedir. Yapılan incelemeye göre olası hataların düzeltilmesi denetlenenden talep edilmek durumunda ve mevcut tespitin bilgi sistemleri denetim raporunda belirtilmesi gerekmektedir.

Test sonucunun bilgi sistemleri raporunda ifade edilmesi için bilgilerin aşağıdaki tablo kapsamında rapora eklenmesi gerekmektedir.

Tablo 3: Test Edilen Kontrol Kapsamında Uygulama Kontrol Listesi 1

Kontrol Genel Alanı	Kontrol Noktaları	Kontrol Numarası	Kontrol Tanımı	Anahtar Kontrol	Test
Girdi Kontrolleri	Doğruluk, Bütünlük ve Yetkilendirme Kontrolleri	1	Fiş tutar dengesinin korunması amacıyla ana bankacılık sistemi üzerinde oluşturulan muhasebe fişlerinin toplam borç ve alacak tutarlarının eşit olması sistemsel olarak zorlanmaktadır.	Evet	*Test Edildi – 1* Gözlem ve Sistem Sorgusu *Test Edildi – Tüm Veri* Veri Analizi

Yukarıdaki tablodan da görüleceği gibi ekran üzerinde uygulama ekranlarının test edilmesi ("*Test Edildi – 1* Gözlem ve Sistem Sorgusu") olarak belirtilmişken, tüm muhasebe hareket verisinin kontrol kapsamında analiz edilmesi ("*Test Edildi – Tüm Veri* - Veri Analizi") olarak ifade edilmiştir. Veri analizi sonucunda tespit edilen bulgu, bilgi sistemleri raporunda aşağıdaki tablo kapsamında belirtilmek zorundadır.

Tablo 4: Test Edilen Kontrol Kapsamında Bulgu İfadesi 1

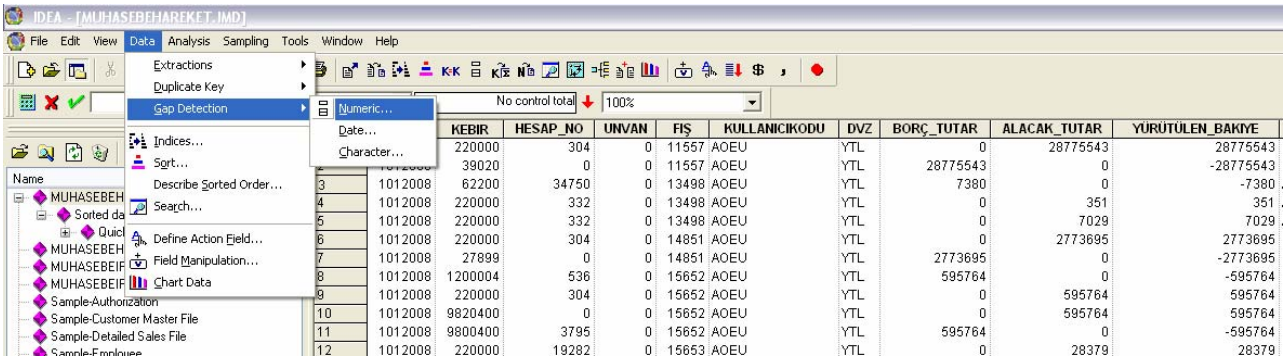
Süreç: Muhasebe Genel Kontrolleri Süreci			
Kontrole İlişkin Bilgiler			
Numarası	1	**Türü**	Otomatik
İşlevi	Fiş tutar dengesinin korunması amacıyla ana bankacılık sistemi	**Çalışma Sıklığı**	İşlem Bazlı

	üzerinde oluşturulan muhasebe fişlerinin toplam borç ve alacak tutarlarının eşit olması sistemsel olarak zorlanmaktadır.		
Aktör	Ana Bankacılık Sistemi	**Sahibi**	Genel Muhasebe Birimi
Bulguya İlişkin Bilgiler			
Bulgu	Tüm muhasebe hareketlerine yönelik fişlerin analizi sonucunda 431 adet fiş kaydı nedeniyle 531.439.402 TL tutarında alacak tarafının fazla olduğu tespit edilmiştir. Dolayısıyla bu fişler nedeniyle borç-alacak tutar dengesinin bozuk olduğu fişlerin sistemde olduğu tespit edilmiştir.		
İş Riski	Borç-alacak tutar dengesi bulunmayan fişlerin sistemde bulunması, sistemden elde edilen finansal tabloların bütünlüğünü ve doğruluğunu olumsuz şekilde etkileyebilmektedir.		

B) Eksiksiz Olma Finansal Denetim Amacına Yönelik Uygulama Denetimi Örneği:

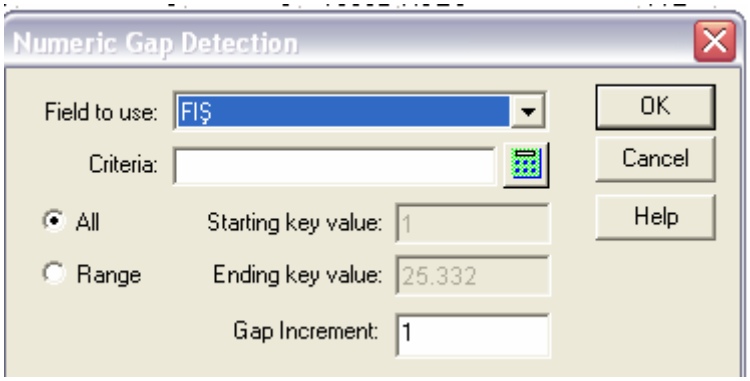
1. *Finansal Denetim Amacı*: Eksiksiz Olma
2. *Sürecin Kapsamı*: Muhasebe işlem numaralarının ardışıklığının korunmasının sağlanması
3. *Kontrol Alanı*: Veri İşleme Kontrolleri / Veri İşlemede Bütünlük
4. *Kontrol Tanımı*: Ana bankacılık sistemi üzerindeki fiş kayıtları atılırken işlem numaraları ardışık, sıralı ve eksiksiz olmak zorundadır.
5. *Kontrolün Test Yöntemi*: Sistem üzerindeki tüm fişlerin IDEA aracı ile analiz edilerek fiş numaralarına göre eksiklik olup olmadığı tespit edilmesi gerekmektedir. Diğer bir ifadeyle fiş numaraları arası atlama ve silinen fiş olup olmadığı kontrol edilmelidir.
6. *Testin Uygulanması*: Muhasebe hareket bilgisi, diğer bir ifadeyle tüm senenin fiş kayıtları ana bankacılık sisteminden alınarak IDEA bilgisayar destekli denetim aracına

yüklenmiştir. Bir önceki uygulama örneğinde bu adımlar detaylı olarak gösterildiğinden direkt olarak test yöntemine uygun olarak IDEA üzerindeki analiz işlemine geçilecektir.



Şekil 27: IDEA "Gap-Detection" Analizi

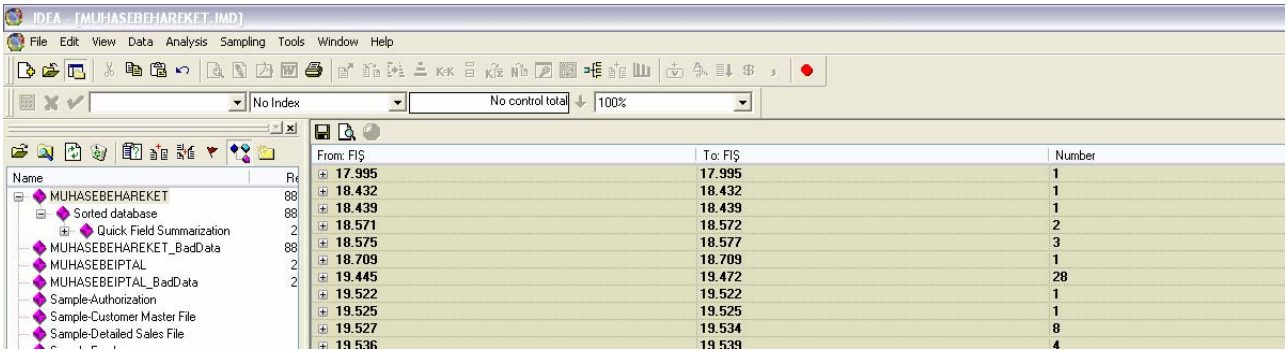
Analizi gerçekleştirmek için IDEA üzerinde "*Gap Detection*" alt menüsünü seçmemiz gerekmektedir. Bu menünün sağladığı fonksiyonla istenilen kolon üzerinde belirtilen kritere göre aralık analizi yapılabilmektedir.



Şekil 28: IDEA "Gap-Detection" Analizinde Fiş Kolonunun Seçilmesi

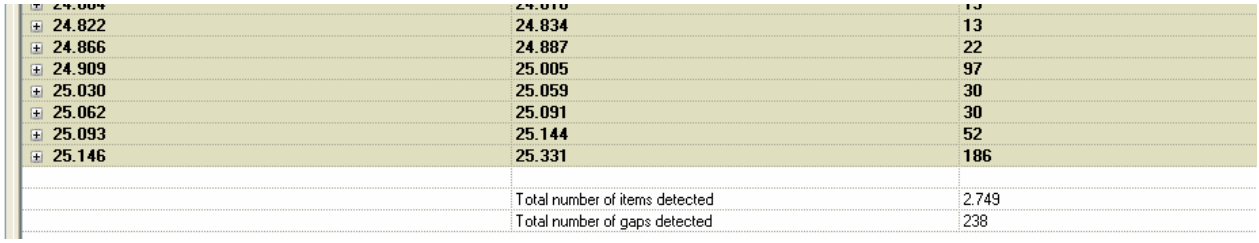
Kontrol tanımımıza göre fiş numarasının ardışık, sıralı ve eksiksiz olmak zorunluluğu incelendiğinden, "FİŞ" kolonu seçilmektedir. Tüm veri kapsamında "1"den "25.332"e kadar fiş bulunduğu da bu ekran üzerinden görülebilmektedir. Veri analizi kapsamında, ana bankacılık sisteminin kayıt yapısı da göz önüne alınarak fişlerin birer artarak ardışık

şekilde kayıt altına alındığından "*gap increment*" alanına "1" sayısı girilmektedir. Böylece birer artarak tüm fişlerin sistemdeki fiş kayıtları arasında olup olmadığı kontrol edilecektir.



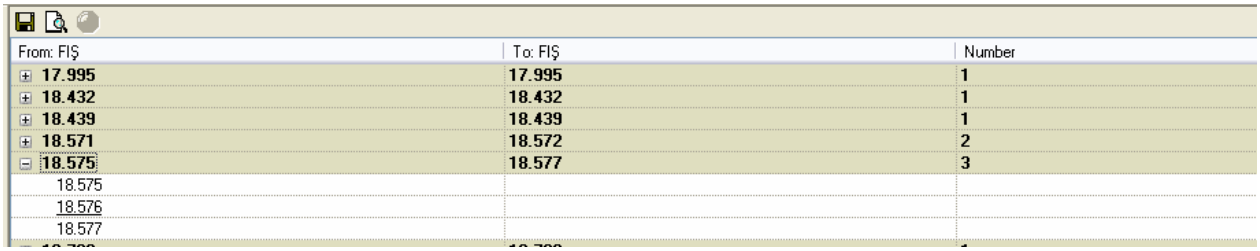
Şekil 29: IDEA "Gap-Detection" Analiz Sonucu 1

Analiz kriterleri girildikten sonra hangi fiş numaraları arasında kaç adet fiş kaydının veri içerisinde bulunamadığını IDEA raporlamaktadır. Örneğin 18.571 ile 18.572 arasında iki adet fişin bulunamadığı yukarıdaki ekran üzerinden görülebilmektedir.



Şekil 30: IDEA "Gap-Detection" Analiz Sonucu 2

Raporun sonuna gelindiğinde toplam 238 farklılığın ve bu farklılıktan kaynaklanan 2.749 fiş kaydının ardışık sıralı olarak sistemdeki fiş verisi üzerinde bulunamadığı tespit edilmiştir.



From: FIŞ	To: FIŞ	Number
17.995	17.995	1
18.432	18.432	1
18.439	18.439	1
18.571	18.572	2
18.575	18.577	3
18.575		
18.576		
18.577		

Şekil 31: IDEA "Gap-Detection" Analiz Sonucu 3

Ek olarak rapor kapsamında her bir farklılığa gelinip incelemek için seçildiğinde hangi fişlerin veri içerisinde eksik olduğu görülebilmektedir. Örneğin 18.575 ve 18.577 fiş aralığı arasında 8.575, 18.576 ve 18.577 olmak üzere üç adet fişin eksik olduğu görülebilmektedir.

Test sonucunun bilgi sistemleri raporunda ifade edilmesi için bilgilerin bir sonraki tablo kapsamında rapora eklenmesi gerekmektedir.

Tablo 5: Test Edilen Kontrol Kapsamında Uygulama Kontrol Listesi 2

Kontrol Genel Alanı	Kontrol Noktaları	Kontrol Numarası	Kontrol Tanımı	Anahtar Kontrol	Test
Veri İşleme Kontrolleri	Veri İşlemede Bütünlük	2	Ana bankacılık sistemi üzerindeki fiş kayıtları atılırken işlem numaraları ardışık, sıralı ve eksiksiz olmak zorundadır.	Evet	*Test Edildi – Tüm Veri* Veri Analizi

Veri analizi sonucunda tespit edilen bulgu, bilgi sistemleri raporunda aşağıdaki tablo kapsamında belirtilmek zorundadır.

Tablo 6: Test Edilen Kontrol Kapsamında Bulgu İfadesi 2

Süreç: Muhasebe Genel Kontrolleri Süreci			
Kontrole İlişkin Bilgiler			
Numarası	2	**Türü**	Otomatik
İşlevi	Ana bankacılık sistemi üzerindeki fiş kayıtları atılırken işlem numaraları ardışık, sıralı ve eksiksiz olmak zorundadır.	**Çalışma Sıklığı**	İşlem Bazlı
Aktör	Ana Bankacılık Sistemi	**Sahibi**	Genel Muhasebe Birimi
Bulguya İlişkin Bilgiler			
Bulgu	Tüm muhasebe hareketlerine yönelik fişlerin analizi sonucunda 238 farklılığın ve bu farklılıktan kaynaklanan 2.749 fiş kaydının ardışık sıralı olarak sistemdeki fiş verisi üzerinde bulunamadığı tespit edilmiştir.		
İş Riski	Fiş kayıtlarının ana bankacılık sistemi üzerinde ardışık ilerleyerek eksik olmaması, sistemden elde edilen finansal tabloların bütünlüğünü ve doğruluğunu olumsuz şekilde etkileyebilmektedir.		

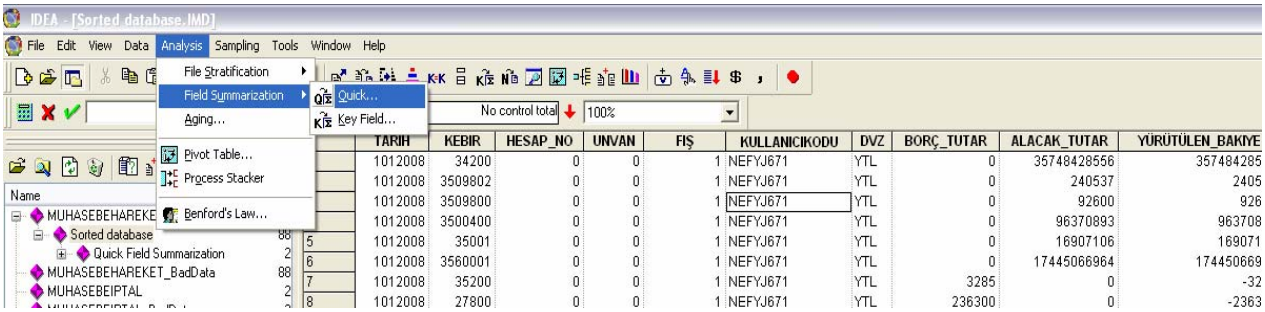
C) Meydana Gelme Finansal Denetim Amacına Yönelik Uygulama Denetimi Örneği:

1. *Finansal Denetim Amacı*: Meydana Gelme
2. *Sürecin Kapsamı*: Muhasebe fişi kesilmesine ilişkin yetkili personelin belirlenmesi ve yetkilerinin kontrolü
3. *Kontrol Alanı*: Girdi Kontrolleri / Doğruluk, bütünlük ve yetkilendirme kontrolleri

4. *Kontrol Tanımı*: Şubeler ve Genel Müdürlük birimleri tarafından sistem üzerinde yapılan serbest fiş girişleri sınırlı ve yetkili uygulama kullanıcıları tarafından yapılmaktadır.

5. *Kontrolün Test Yöntemi*: Sistem üzerinde fiş giriş yetkisine sahip olan kullanıcılar incelenmeli ve yetkili kişiler olup olmadığı sorgulanmalıdır. Ek olarak sistem üzerinde girilmiş olan tüm fişlerin IDEA aracı ile analiz edilerek her bir fiş kaydının hangi kullanıcılar adına sisteme girildiği incelenmelidir.

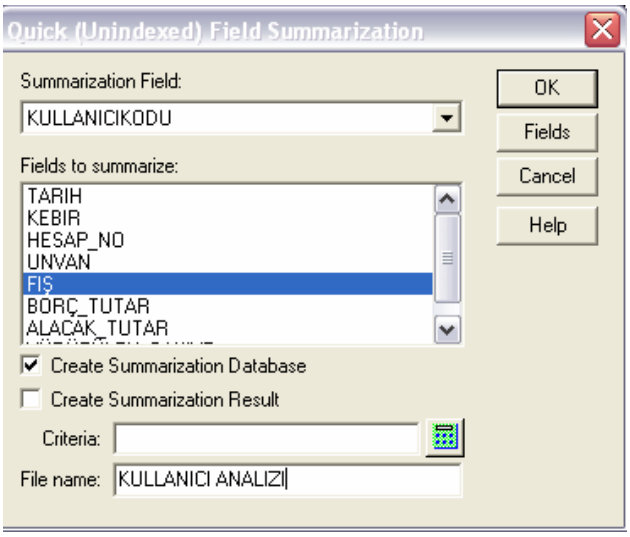
6. *Testin Uygulanması*: Ana bankacılık sistemi üzerinde serbest fiş giriş yetkisine sahip olan son kullanıcılar ve sistem üzerinde otomatik olarak fiş kaydı atan programların kullanıcıları incelenmelidir. Sistem üzerinde yetkilendirilmiş olan kullanıcıların doğru olduğunun tespit edilmesi sonrasında sisteme girişmiş olan tüm fiş bilgileri IDEA üzerinde analiz edilerek yetkili kullanıcılar veya programlar tarafından girildiği test edilmelidir. Böylelikle fişlerin yetkili kullanıcılarla oluşturulduğu kontrol edilebilmekte ve meydana gelme finansal denetim amacına yönelik makul bir güvence elde edilmektedir.



Şekil 32: IDEA "Field Summarization" Analizi

Muhasebe hareket bilgisi, diğer bir ifadeyle tüm senenin fiş kayıtları ana bankacılık sisteminden alınarak IDEA bilgisayar destekli denetim aracına yüklenmiştir. İlk uygulama örneğinde bu adımlar detaylı olarak gösterildiğinden direkt olarak test yöntemine uygun olarak IDEA üzerindeki analiz işlemi açıklanacaktır.

Öncelikle "*Field Summarization*" alt menüsü seçilerek istenen kapsamda IDEA bilgisayar destekli denetim aracına yüklenen verinin gruplanarak özetlenmesi sağlanmaktadır.



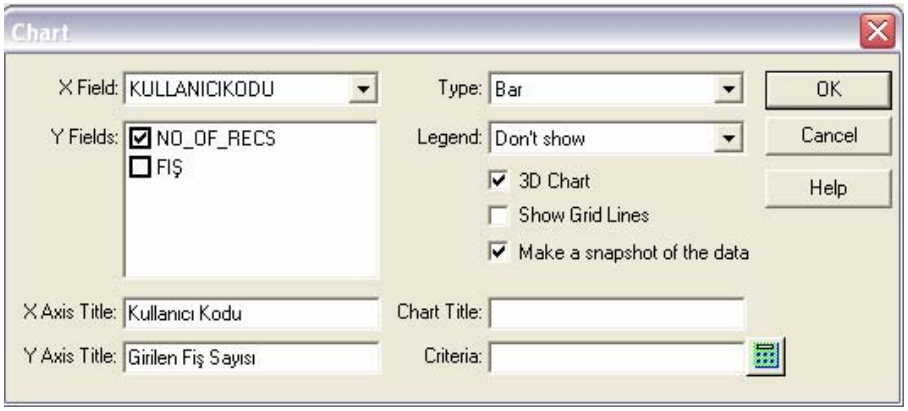
Şekil 33: IDEA "Field Summarization" Analizi Kullanıcı-Fiş Kolonlarının Seçimi

Menü üzerinde "KULLANICI KODU" bazında gruplanması ve "FİŞ" verisinin gruplama sırasında göz önünde bulundurulması sağlanmıştır. Oluşturulacak özet bilginin de "KULLANICI ANALİZİ" olarak IDEA üzerinde dosyada saklanması istenmiştir.

	KULLANICIKODU	NO_OF_RECS	FIŞ
1	A	14255	152449883
2	B	502	7673911
3	C	802290	6733960297
4	D	21639	357941320
5	E	90	90
6	F	22230	224021147
7	G	20664	192117646

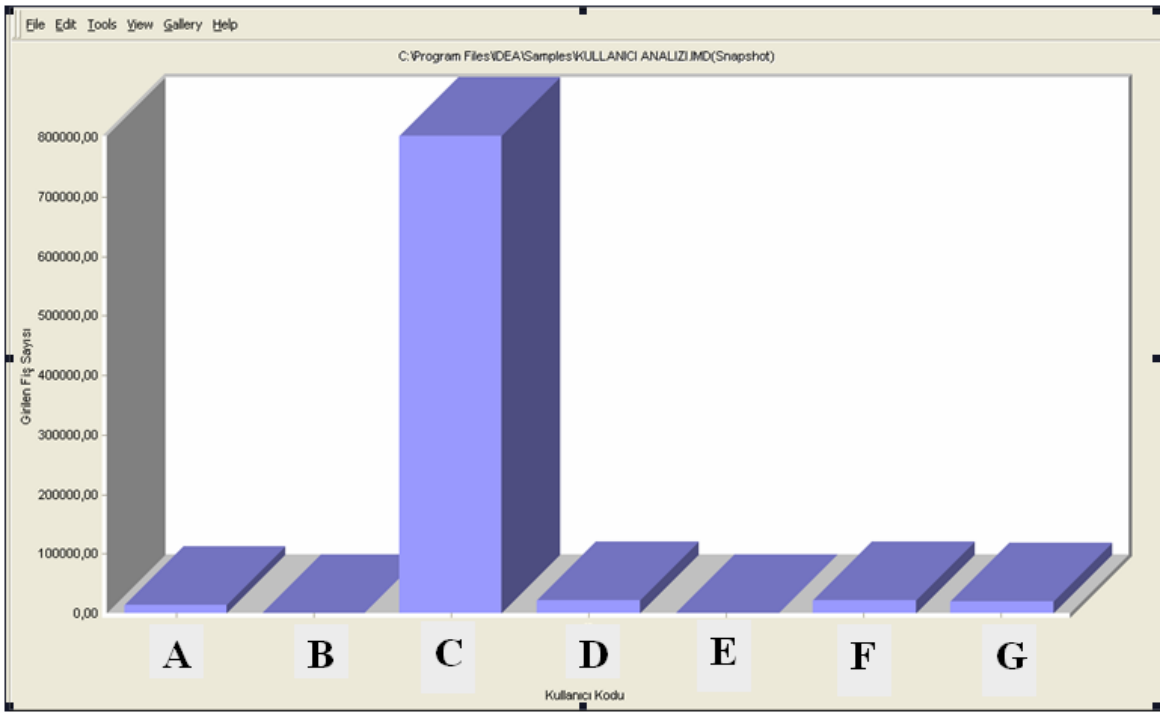
Şekil 34: IDEA "Field Summarization" Kullanıcı-Fiş Girişi Analiz Sonucu

Analiz tamamladığında, fişlerin büyük bir çoğunluğunun "C" program kullanıcısı olduğu tespit edilmiştir. "B" ve "E" kullanıcıları haricinde diğer kullanıcıların da muhasebe fiş kaydı oluşturması gereken program kullanıcıları olduğu, bu iki kullanıcının ise Genel Muhasebe Biriminde Ana Bankacılık Sistemi üzerinde serbest muhasebe fişi kesmeye yetkili kişiler olduğu belirlenmiştir.



Şekil 35: IDEA Kullanıcı-Fiş Girişi Analiz Sonucunun Grafiksel Gösterimi

Elde edilen verinin grafiksel olarak gösterimi de IDEA üzerindeki araçlar kullanılacak yapılabilmektedir. Özet bilgi kapsamında "x" ve "y" eksenlerimdeki veriler tanımlanarak istenen şekilde grafikler oluşturulabilmektedir. Sütun grafiği seçilerek kullanıcı-fiş özet bilgisinin grafiği IDEA üzerinde oluşturulmak istenmiştir.



Şekil 36: IDEA Kullanıcı-Fiş Girişi Grafiği

Yapılan grafik ayarlamalarına ve kullanıcı-fiş özet bilgisine göre yukarıdaki grafik IDEA üzerinde otomatik oluşturulmaktadır. Grafik üzerinde de "C" program kullanıcısının fişlerin çoğunluğunu sisteme girdiği tespit edilebilmektedir.

Bu kapsamda "C" programını bilgi sistemleri denetim kapsamında detay olarak incelemek (kod inceleme, fonksiyonel test vs.) denetim kapsamında makul bir güvence tesis edecektir. Buna ek olarak "B" ve "E" son kullanıcılarının da serbest olarak yaptığı fiş girişlerinin nedenleri finansal denetim ekipleri tarafından incelenebilecektir.

Test sonucunun bilgi sistemleri raporunda ifade edilmesi için bilgilerin aşağıdaki tablo kapsamında rapora eklenmesi gerekmektedir.

Tablo 7: Test Edilen Kontrol Kapsamında Uygulama Kontrol Listesi 3

Kontrol Genel Alanı	Kontrol Noktaları	Kontrol Numarası	Kontrol Tanımı	Anahtar Kontrol	Test
Girdi Kontrolleri	Doğruluk, bütünlük ve yetkilendirme kontrolleri	3	Şubeler ve Genel Müdürlük birimleri tarafından sistem üzerinde yapılan serbest fiş girişleri sınırlı ve yetkili uygulama kullanıcıları tarafından yapılmaktadır.	Evet	*Test Edildi – 1* Gözlem ve Sistem Sorgusu *Test Edildi – Tüm Veri* Veri Analizi

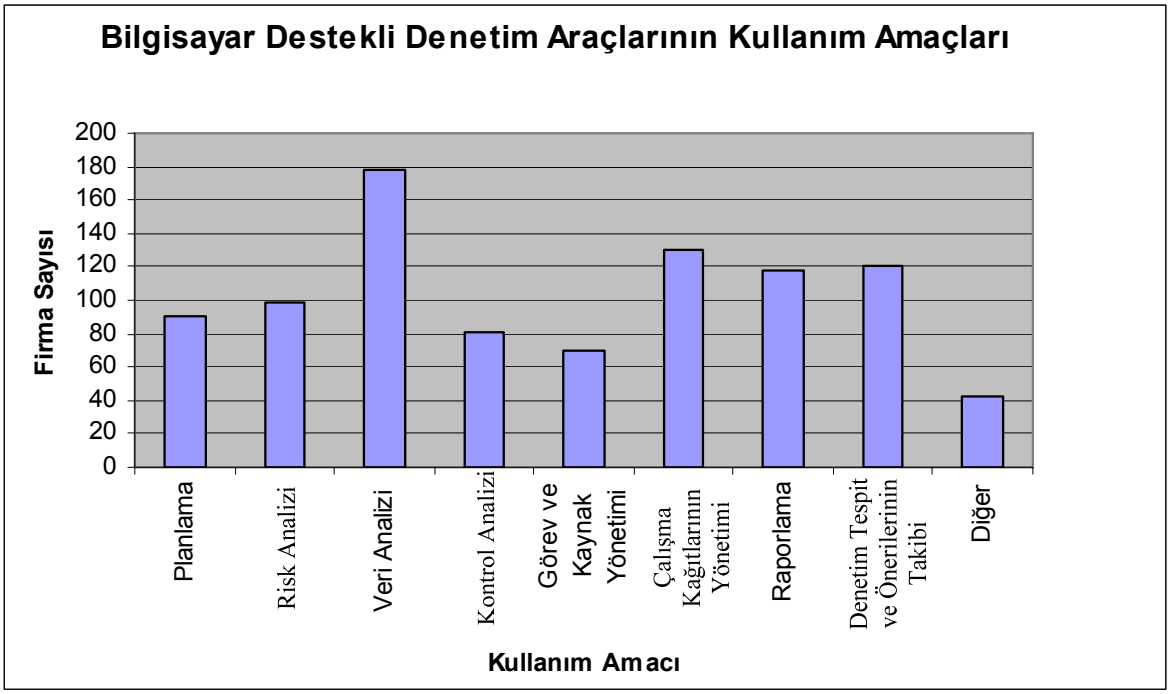
Yukarıdaki tablodan da görüleceği gibi ekran üzerinde uygulama ekranlarının test edilmesi ("*Test Edildi – 1* Gözlem ve Sistem Sorgusu") olarak belirtilmişken, tüm muhasebe hareket verisinin kontrol kapsamında analiz edilmesi ("*Test Edildi – Tüm Veri* - Veri Analizi") olarak ifade edilmiştir. Veri analizi sonucunda tespit edilen bulgu, bilgi sistemleri raporunda aşağıdaki tablo kapsamında belirtilmek zorundadır.

Yaptığımız analiz ve testler sonucunda yetkili kullanıcıların Ana Bankacılık Sistemi üzerinde fiş girişlerini gerçekleştirdiği tespit edildiğinden ve yetkili kişilerin sistemde tanımlandığından bu kontrol kapsamında raporda bulgu ifade edilmeyecektir.

Bilgi sistemleri denetimi kapsamında denetlenen bankalarda gerçekleştirilen süreç diğer bir adıyla uygulama denetimi ile ilgili olarak üç temel finansal denetim amacı desteklenmektedir. Bunlar "*Genel Muhasebe Kontrolleri Süreci*" ile ilgili olarak yukarıda her birisine örnekler verilerek uygulanan "*Kayıtsal Doğruluk*", "*Eksiksiz Olma*" ve "*Meydana Gelme*" denetim amaçlarıdır.

Bu kapsamda test edilen uygulama kontrolleri hem bilgi sistemleri raporuna girdi teşkil etmekte hem de finansal denetim sürecinde gerçekleştirilecek maddi doğruluk testlerinin denetim sürecindeki ağırlığının belirlenmesinde katkıda bulunacaktır. Böylece bilgi sistemleri denetimi ve finansal denetim arasındaki entegrasyon sağlanmış olacaktır. Bilgi sistemleri denetim raporunda her bir kontrolün nasıl ifade edileceği ve tespit edilen bulgu mevcut ise yine raporda nasıl konu edileceği yukarıdaki örnek uygulamalarda gösterilmiştir.

Son olarak bilgi sistemleri denetiminde bilgisayar destekli denetim araçlarının kullanımı hakkında KPMG bağımsız denetim firması tarafından yapılan bir araştırmadan bilgiler verilmek istenmektedir.

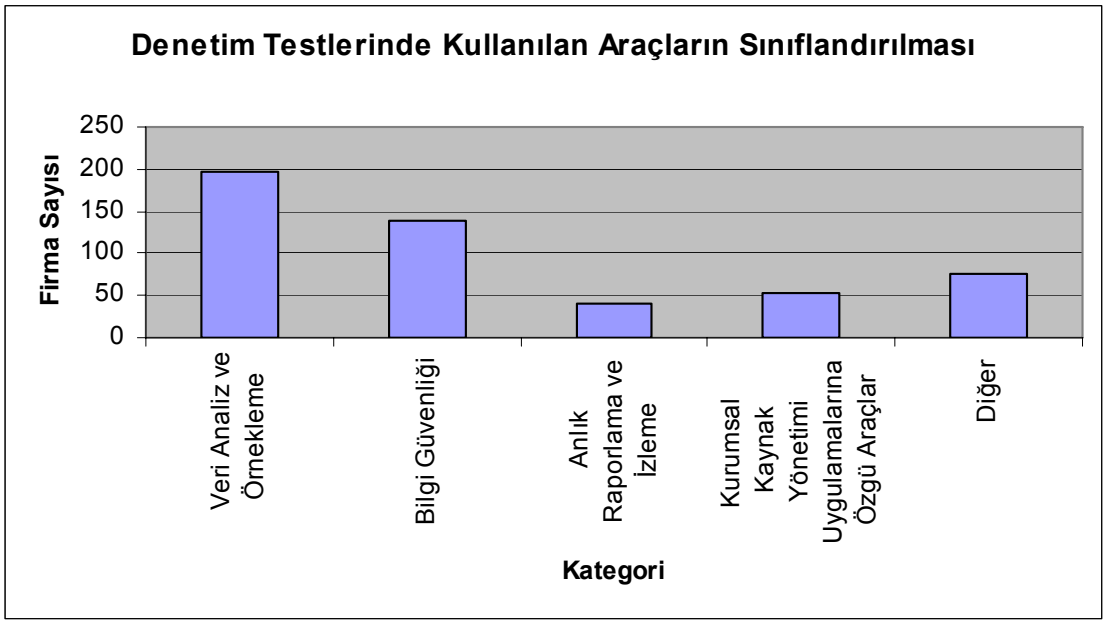


Şekil 37: Bilgisayar Destekli Denetim Araçlarının Kullanım Amaçları

KPMG, "**KPMG's 2009 IT Internal Audit Survey**" (Turkey: KPMG, 2009), 14

Yaklaşık 1000 firma çalışanı ile yapılan araştırma sonucundan görüleceği gibi bilgisayar destekli denetim araçları çoğunlukla veri analizi alanında kullanılmakta olup sırasıyla çalışma kağıtlarının yönetimi, denetim tespit ve önerilerinin takibi, raporlama, risk analizi, planlama, kontrol analizi ve görev-kaynak yönetimi amaçlarında da kullanılmaktadır. Bankalarda uygulama kontrollerinin denetimi kapsamında gerçekleştirdiğimiz araştırma uygulamasında IDEA bilgisayar destekli denetim aracından faydalanılmakla birlikte bu araçtan veri analizi ve kontrol analizi alanların destek alınmıştır.

KPMG tarafından gerçekleştirilen araştırmada firmaların %33'ünün bilgisayar destekli denetim araçlarından faydalanmadığı ortaya çıkmıştır. Kullanan firmaların da gerçekleştirdiği testler kapsamında aşağıdaki tablodaki kategorilere giren araçları kullandığı tespit edilmiştir.

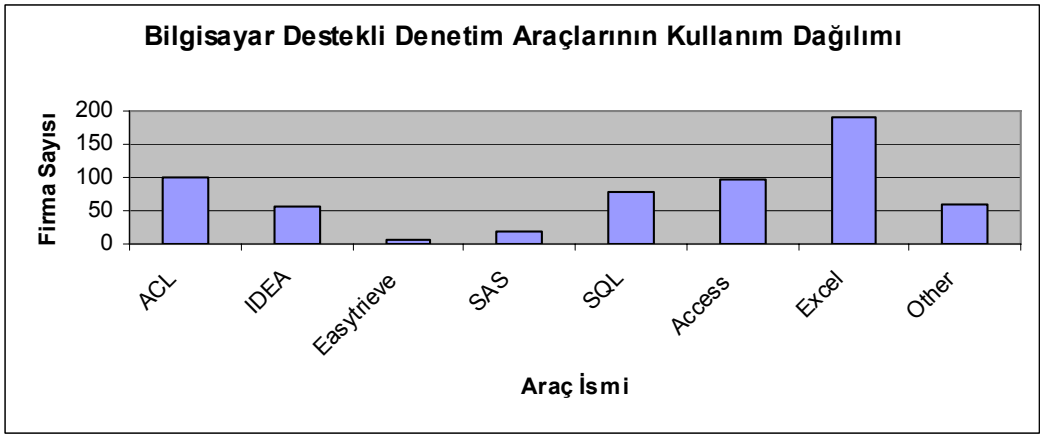


Şekil 38: Bilgisayar Destekli Denetim Araçlarının Sınıflandırılması

KPMG, "**KPMG's 2009 IT Internal Audit Survey**" (Turkey: KPMG, 2009), 14

Yapılan araştırma kapsamında yukarıdaki tablodan görüleceği gibi veri analizi ve örnekleme amaçlı bilgisayar destekli denetim araçlarının kullanımının firmalarda daha yaygın olduğu görülebilmektedir.

Son olarak KPMG tarafından yapılan araştırmada firmalarda bilgi sistemleri denetimi kapsamında hangi araçlardan faydalanıldığı belirlenmeye çalışılmıştır.



Şekil 39: Bilgisayar Destekli Denetim Araçlarının Kullanım Dağılımı

KPMG, "**KPMG's 2009 IT Internal Audit Survey**" (Turkey: KPMG, 2009), 14

Buna göre bilgi sistemleri denetimi kapsamında "*Microsoft Excel*" aracının kullanımın firmalarda yaygın olduğu gözlemlenmektedir. Karmaşık veri analizleri yapılamasa da "*Microsoft Excel*" ve "*Microsoft Access*" gibi araçların kullanım kolaylığı ve kullanıcıların yatkınlığı sebebiyle tercih edildiği gözlenmektedir. Araştırma uygulamamız kapsamında yararlanılan IDEA bilgisayar destekli denetim aracından ise 52 cevaplayıcının faydalandığı tespit edilmiştir.

Sonuç olarak bankalarda uygulama kontrollerinin denetimi kapsamında "*Genel Muhasebe Kontrol Süreci*" seçilerek uygulaması gösterilmiş, testler sırasında bilgisayar destekli denetim araçlarından nasıl yararlanılacağı uygulamalı olarak açıklanmış, finansal denetim ile entegrasyonun nasıl sağlanması gerektiğine değinilmiş ve bilgisayar destekli denetim araçları üzerine yapılan bir araştırmadan bilgiler verilmiştir.

Bir sonraki bölümde ise test edilen uygulama kontrollerinin güvenilir bir bilgi sistemleri kontrol ortamı üzerinde tesis edilip edilmediğini belirlemek için gerçekleştirilen genel kontrol alanlarının denetimine yer verilecektir.

5.6.2. Genel Kontrol Alanı Denetimi ve Raporlaması: Sistem Güvenliğinin Sağlanması (DS5)

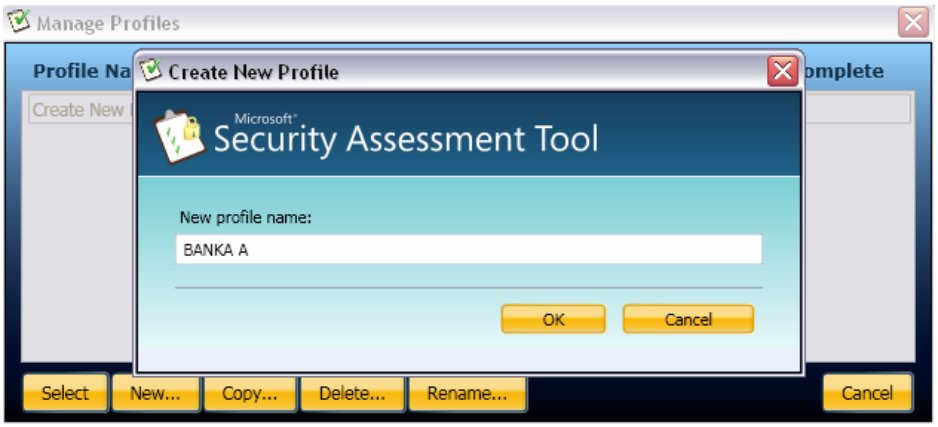
Bankalarda gerçekleştirilen bilgi sistemleri denetim faaliyetleri kapsamına iki senede bir gerçekleştirilmesi zorunlu olan genel kontrol alanlarının denetimi de girmektedir. Bu kapsamda uygulama kontrollerinin üzerine tesis edildiği bilgi teknolojileri genel kontrol ortamının yeterliliğinin diğer bir ifadeyle olgunluk seviyesinin değerlendirilmesi istenmektedir. Zayıf bir kontrol ortamı üzerine tesis edilen uygulama kontrolleri etkin olarak işletilse dahi güvenilirliği azalacaktır. Örneğin, genel muhasebe süreci içerisinde serbest muhasebe fişi girişlerini sınırlı sayıda ve yetkili kişilerin yaptığı uygulama kontrolleri kapsamında incelenebilir ve etkin olduğu sonucuna varılabilir. Ancak ana bankacılık sistemi içerisindeki ekranlara yönelik yetkilendirme sürecinin uygun onaylara ve kontrol ortamına bağlanmadığı bir ortamda bu kontrolün etkinliğinin bozulma riski artacaktır.

Bankalarda genel kontrol alanlarının denetimi 34 CobiT kontrol hedefi kapsamında gerçekleştirilmektedir. Uygulamamızda "*DS5 Sistem Güvenliğinin Sağlanması*" kontrol hedefi kapsamında gerçekleştirilen faaliyetler açıklanacaktır. Bu kapsamda,

- Bilgi güvenliğine yönelik bankalarda ön değerlendirmenin yapılması,
- CobiT detaylı kontrol hedeflerine yönelik test çalışmalarının yapılması ve sonuçların raporlanması,
- "*DS5 Sistem Güvenliğinin Sağlanması*" kontrol hedefine yönelik olgunluk seviyesinin tespiti

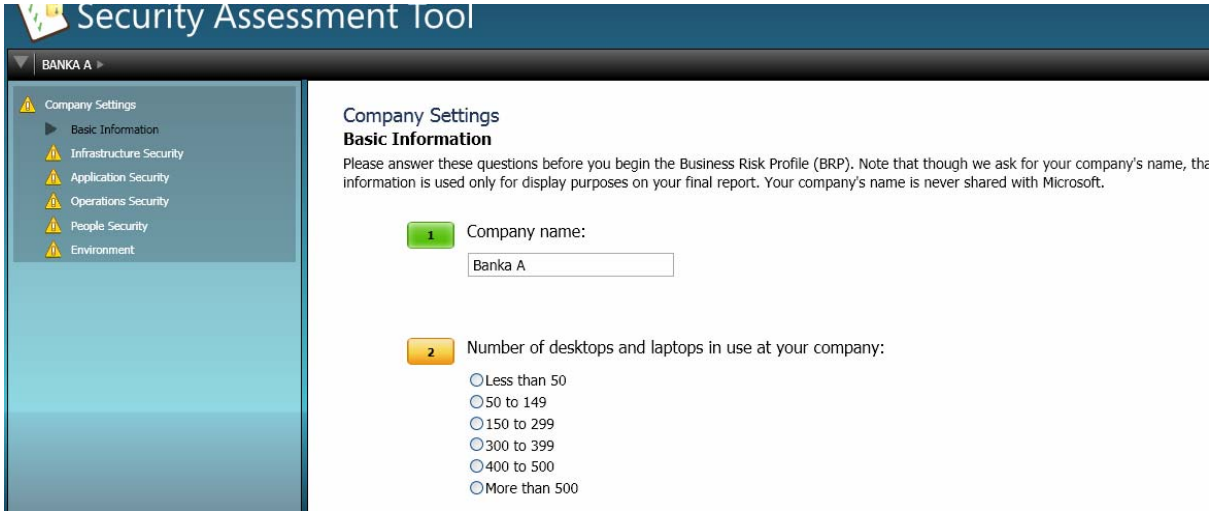
konularına yer verilecektir.

A) Bilgi güvenliğine yönelik bankalarda ön değerlendirmenin yapılması: "*DS5 Sistem Güvenliğinin Sağlanması*" kontrol hedefi kapsamında denetlenen bankanın bilgi teknolojileri güvenlik ortamının ön değerlendirilmesi yapılmalıdır. Kullanılan değerlendirme aracı yardımıyla anket üzerindeki sorular doldurularak bankanın BT güvenlik ortamına yönelik değerlendirme raporu oluşturulmaktadır. Yazılım aracı üzerindeki soruların cevaplanması ve raporun oluşturulması yaklaşık bir saat sürmektedir. Bu ön değerlendirme çalışmasının faydası CobiT detaylı kontrol hedeflerine yönelik test çalışmalarının etkin olarak planlanması ve denetimin riskli kontrol hedeflerine yönlendirilmesidir. Bu adım içerisinde yapılan değerlendirme çalışmaları kullanılan "Bilgi Sistemleri Güvenlik Ortamı Değerlendirme Aracı"ndan alınan ekran görüntüleri ile birlikte açıklanmaya çalışılmıştır.



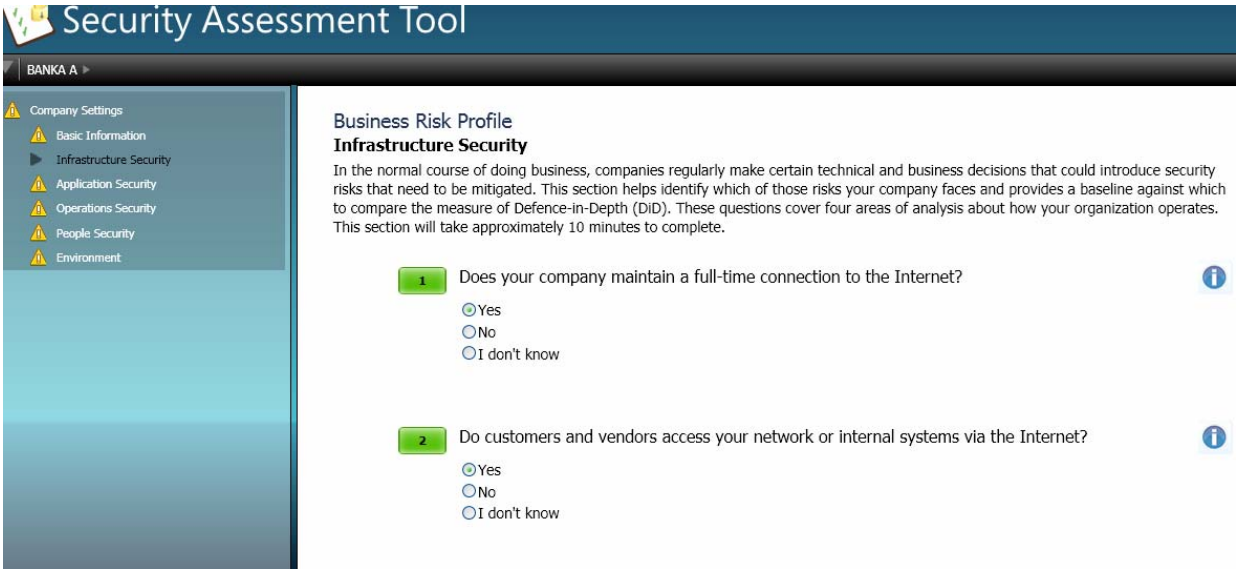
Şekil 40: Bilgi Sistemleri Güvenlik Ortamı Değerlendirme Aracı ("MSAT") Profil Girişi

Öncelikle ön değerlendirmenin yapılacağı bankanın unvanı girilerek risk profilinin oluşturulması gerekmektedir.



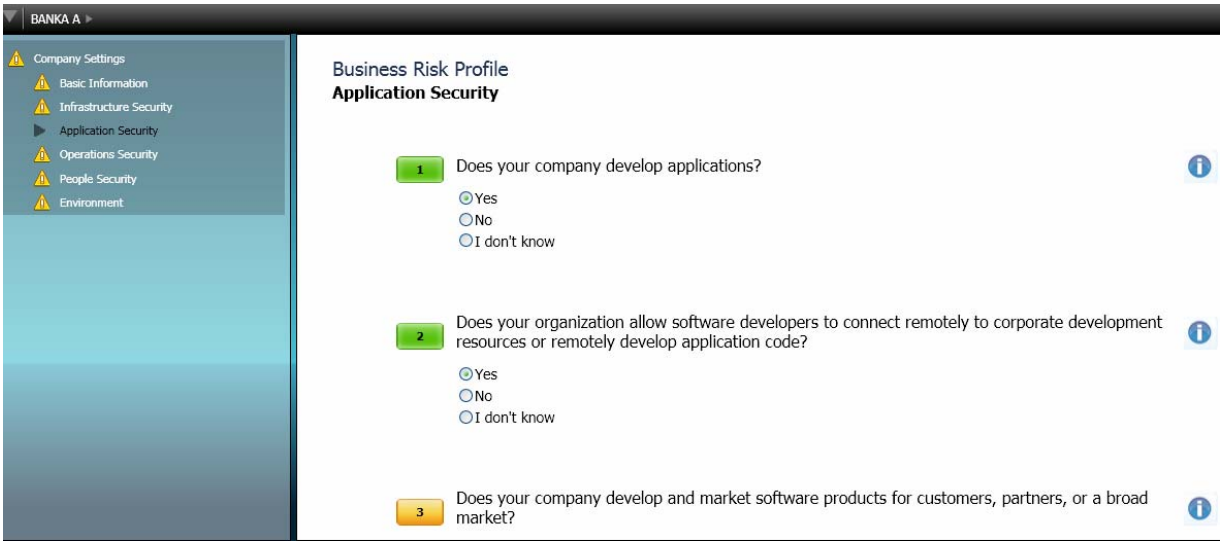
Şekil 41: MSAT Genel Bilgi Girişi

Bankanın unvanı ve mevcut bilgisayar (istemciler ve sunucular) sayısı gibi genel özellikler alınmaktadır. Sonrasında bankanın risk profilini oluşturacak olan altyapı, uygulama, operasyon, çalışan güvenliği ve genel BT ortamı kapsamında sorulara yanıt verilmesi gerekmektedir.



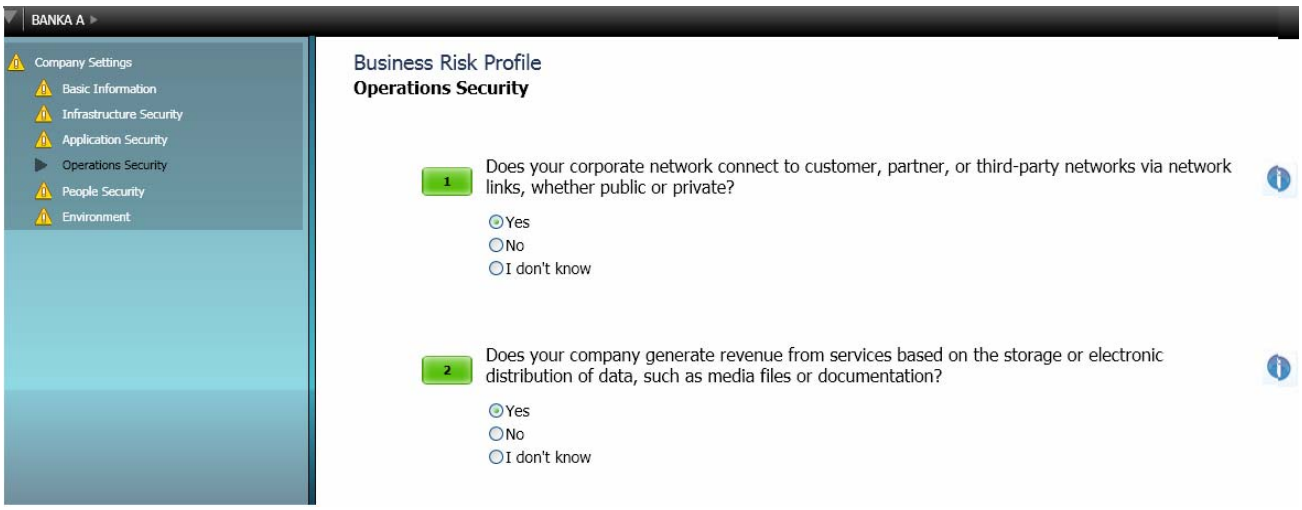
Şekil 42: MSAT Banka Risk Profili Girişi 1

Öncelikle bankanın risk profili kapsamında altyapı güvenliğine yönelik sorulara yanıt verilmesi gerekmektedir. Örneğin yukarıdaki ekran görüntünden de görüleceği gibi bankanın internet bağlantısı kapsamında sorular yöneltilmektedir. Bu gibi sorular ile birlikte bankanın altyapısı hakkında bilgi edinilmeye ve güvenlik açısından altyapı üzerindeki risk seviyesinin belirlenmesi amaçlanmaktadır.



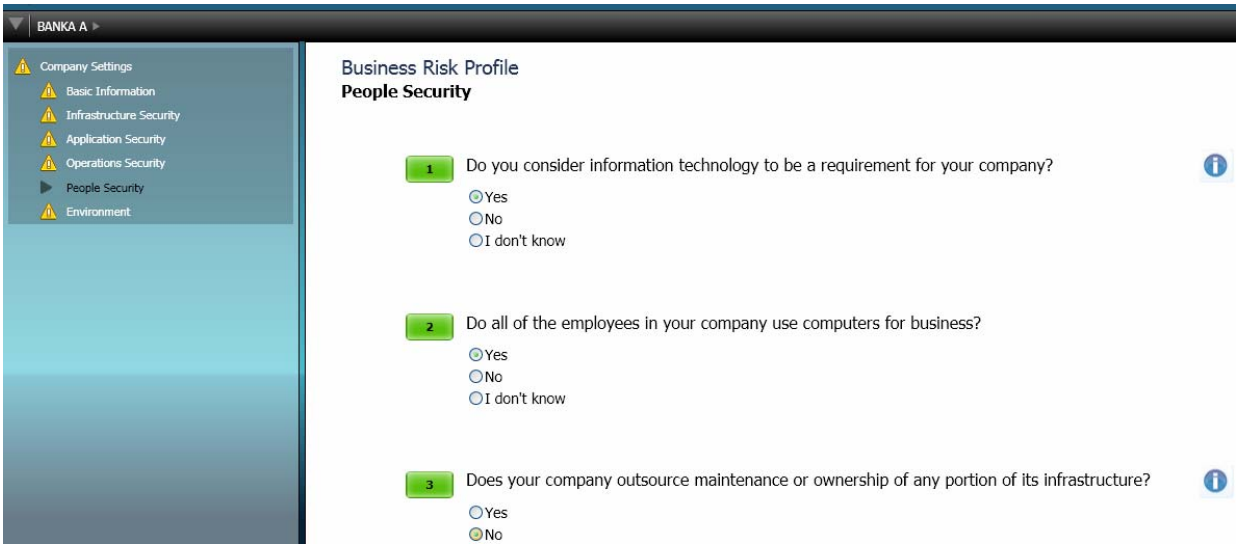
Şekil 43: MSAT Banka Risk Profili Girişi 2

Bir sonraki bölümde ise banka içerisinde kullanılan uygulamaların güvenliği kapsamında sorular sorulmaktadır. Örneğin bankanın kendi uygulamalarını geliştirip geliştirmediği veya yazılımcıların uygulamanın kodlarına erişimi hakkında sorular yukarıdaki ekran görüntüsü üzerinde sorulmaktadır. Buna benzer sorular ile birlikte bankanın uygulama yönetimi ve geliştirme süreci hakkında bilgi edinilmesi ve güvenlik açısından risk seviyesinin belirlenmesi amaçlanmaktadır.



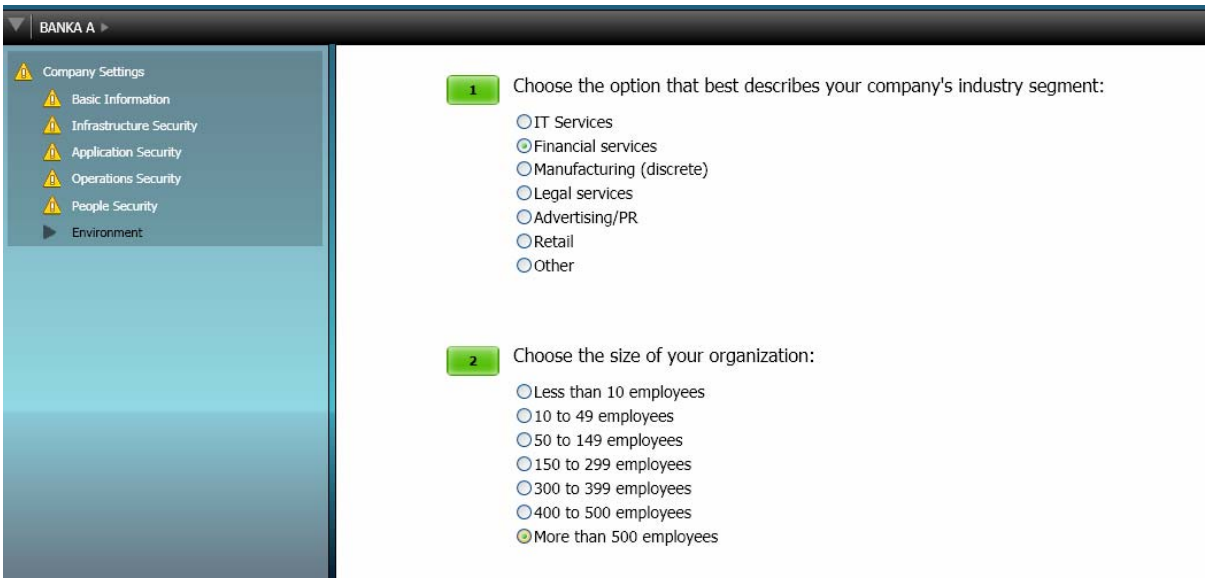
Şekil 44: MSAT Banka Risk Profili Girişi 3

Bir sonraki bölümde ise BT operasyon güvenliği kapsamında bankanın risk seviyesinin belirlenmesine yönelik sorulara cevap verilmektedir. Örneğin kurumsal ağ üzerindeki erişimlerin üçüncü taraflar arasında nasıl olduğu, yedekleme ve saklama gibi servislerden gelir elde edinilip edilmediği gibi sorular cevaplanmaktadır.



Şekil 45: MSAT Banka Risk Profili Girişi 4

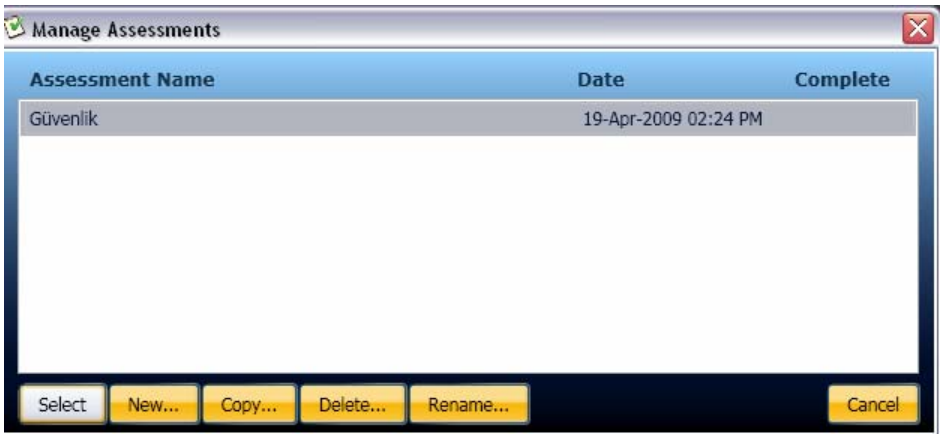
Bir diğer bölümde ise çalışanların güvenliği kapsamında sorular yöneltilmektedir. Bu kapsamda bilgi teknolojilerinin firma için gereklilik olup olmadığı ve bilgisayar kullanımının yaygın olup olmadığı gibi sorular cevaplanmaktadır.



Şekil 46: MSAT Banka Risk Profili Girişi 5

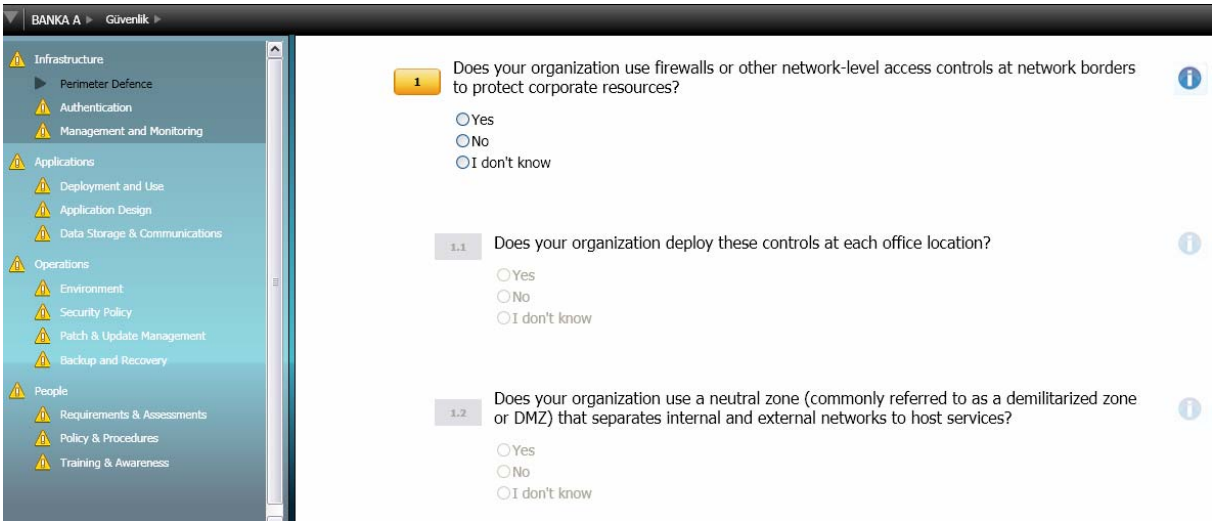
Son olarak firmanın endüstri sınıfı ve işçi sayısı gibi genel ortama yönelik sorular cevaplanmaktadır. Örneğin bankalar kapsamında finansal servisler endüstri kolu altında çalışan sayısının belirtilmesi gerekmektedir. Böylelikle kullanılan araç üzerinde beş ayrı perspektif (altyapı güvenliği, uygulama güvenliği, operasyon güvenliği, çalışan güvenliği ve BT ortamı) açısından bankanın risk profili oluşturulmuştur.

Sonraki adımda ise risk profili oluşturulan banka için çeşitli değerlendirme sorularının bulunduğu anket sorularının bankadaki ilgili kişiler ile konuşularak doldurulması gerekmektedir.



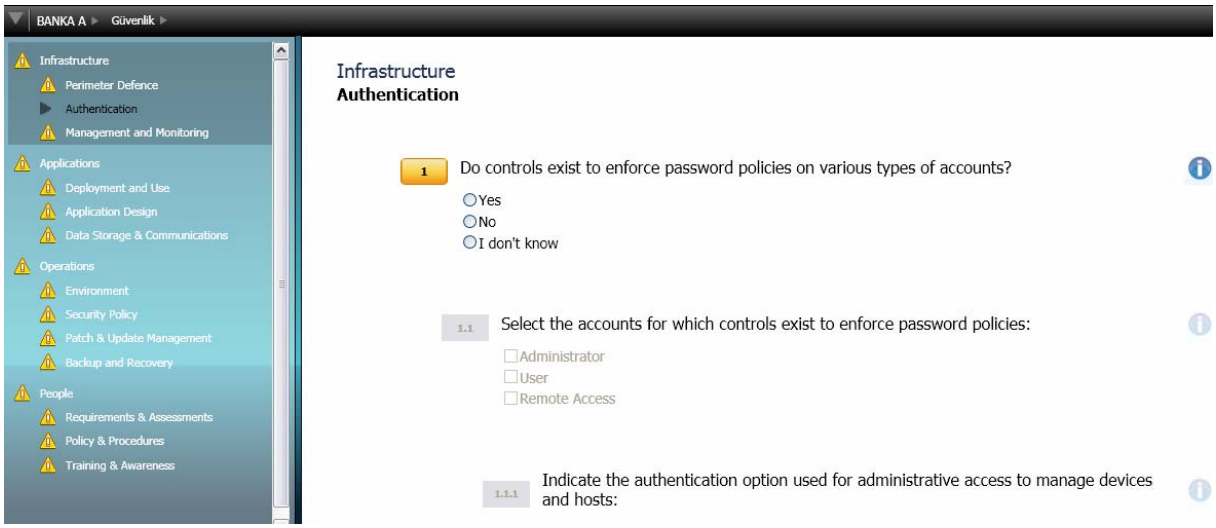
Şekil 47: MSAT Banka Güvenlik Değerlendirme Tanımlaması

İlk önce risk profili oluşturulan banka için araç üzerinde yeni bir değerlendirme açılarak "*Güvenlik*" adı altında kaydedilmiştir. Değerlendirme soruları altyapı, uygulamalar, BT operasyon ve çalışanlar kapsamında dört ana başlık altında sorulmaktadır. Her bir kategori altında örnekler verilerek sonraki ekranlar üzerinde açıklamalar yapılmaktadır.



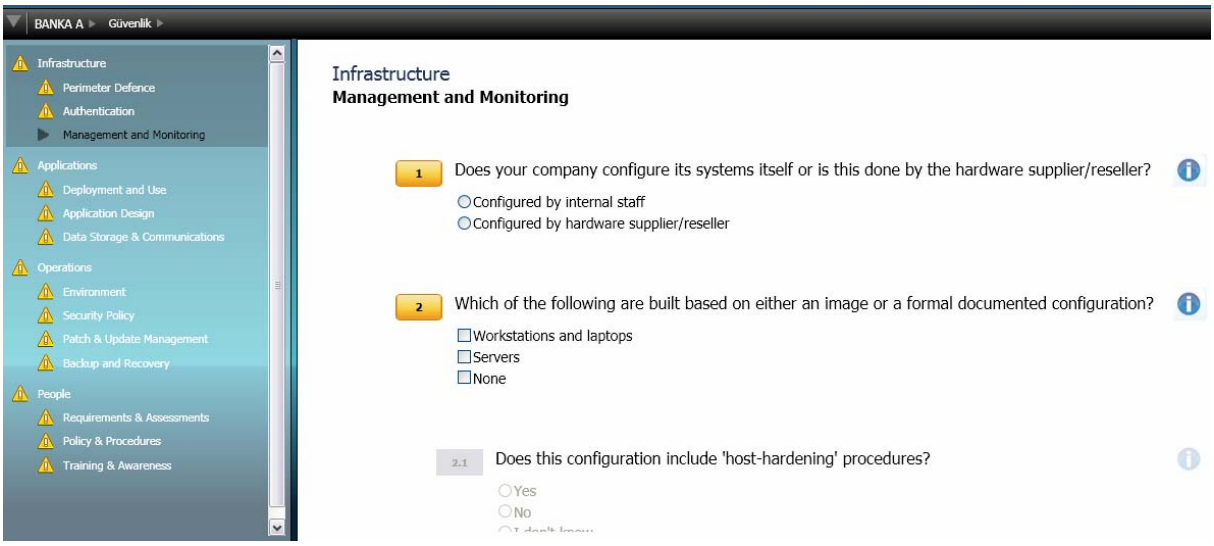
Şekil 48: MSAT Banka Güvenlik Değerlendirme 1

Altyapı kapsamında network güvenliği, iş süreçlerinin BT altyapısı ile nasıl desteklendiği, sunucuların nasıl yönetildiği ve izlendiği kapsamında sorular cevaplanmaktadır. Örneğin yukarıdaki ekranda network üzerinde firewall gibi ağ altyapısına yönelik sınır kontrollerinin uygulanıp uygulanmadığı sorulmaktadır.



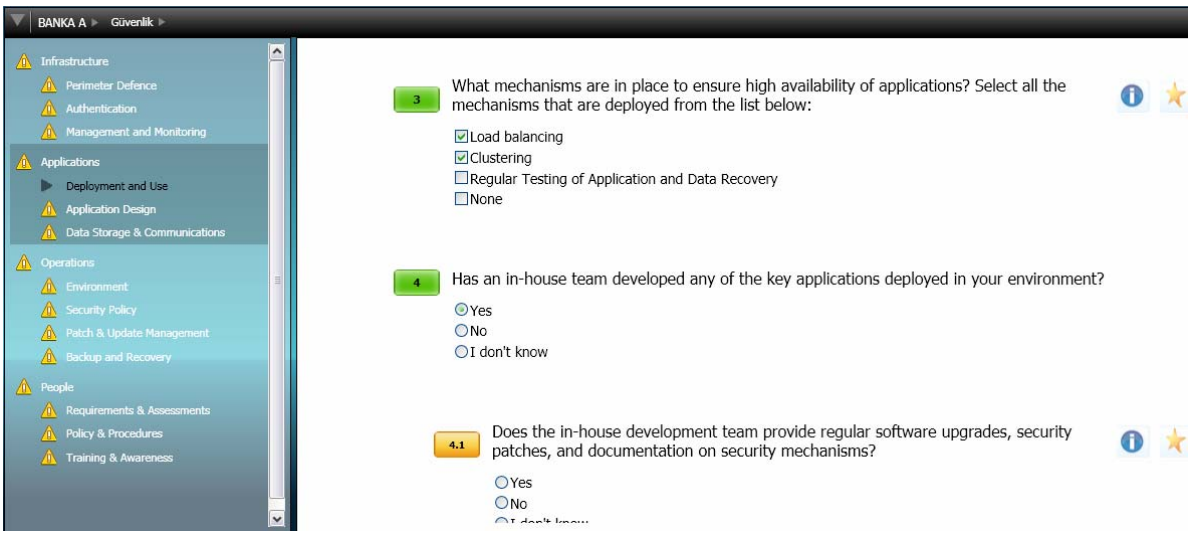
Şekil 49: MSAT Banka Güvenlik Değerlendirme 2

Bir başka bölümde ise altyapı yönetimine yönelik uygulamalar üzerindeki şifre politikaları kapsamında sorular sorulmaktadır.



Şekil 50: MSAT Banka Güvenlik Değerlendirme 3

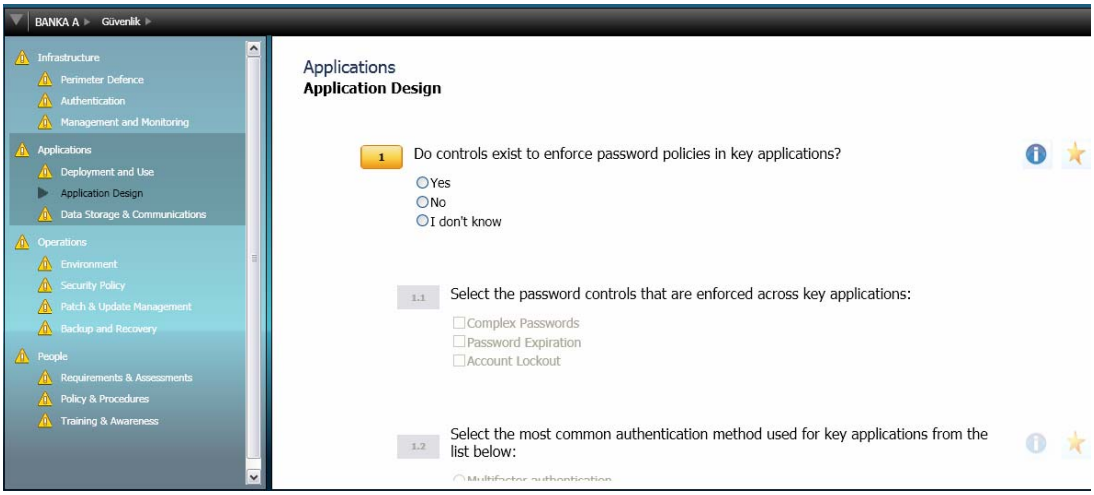
Son olarak altyapı uygulamalarının yönetimi ve izlenmesine yönelik sorular ile altyapı güvelik ortamının değerlendirilmesi tamamlanmaktadır. Örneğin altyapı konfigürasyonunun nasıl yapıldığına yönelik değerlendirme soruları yukarıdaki ekran üzerinde sorulmuştur.



Şekil 51: MSAT Banka Güvenlik Değerlendirme 4

Altyapı güveliğinin değerlendirmesine ek olarak iş süreçlerinin desteklendiği uygulamalara yönelik güvenlik ve erişilebilirlik açısından değerlendirme yapılmaktadır. Uygulamaların

aktarımı, kullanımı, tasarımı, veri saklama ve iletimi gibi konu başlıklarında sorular cevaplanmaktadır. Örneğin yukarıdaki ekranda bankanın kendi uygulamalarını geliştiren BT ekibinin olup olmadığı ve bu şekilde geliştirilen bir uygulamayı kullanıp kullanmadığı sorulmaktadır.

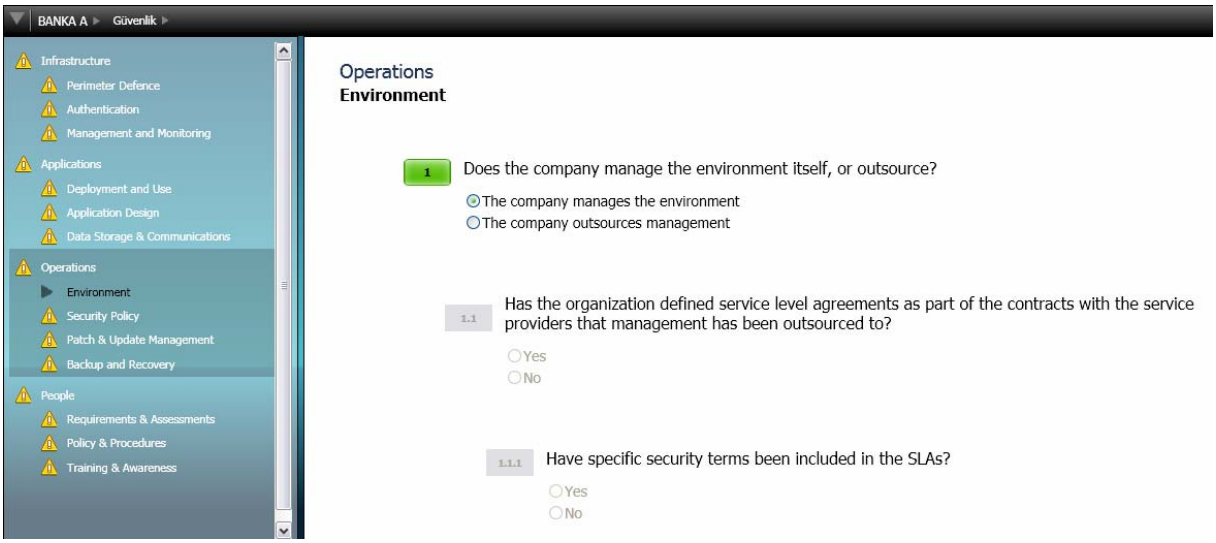


Şekil 52: MSAT Banka Güvenlik Değerlendirme 5

Bir sonraki bölümde ise kritik uygulamaların güvenlik tasarımına yönelik sorular cevaplanmaktadır. Örneğin bu uygulamaların şifre politikaları kapsamında sorular sorulduğu yukarıdaki ekran görüntüsü üzerinden görülebilmektedir.

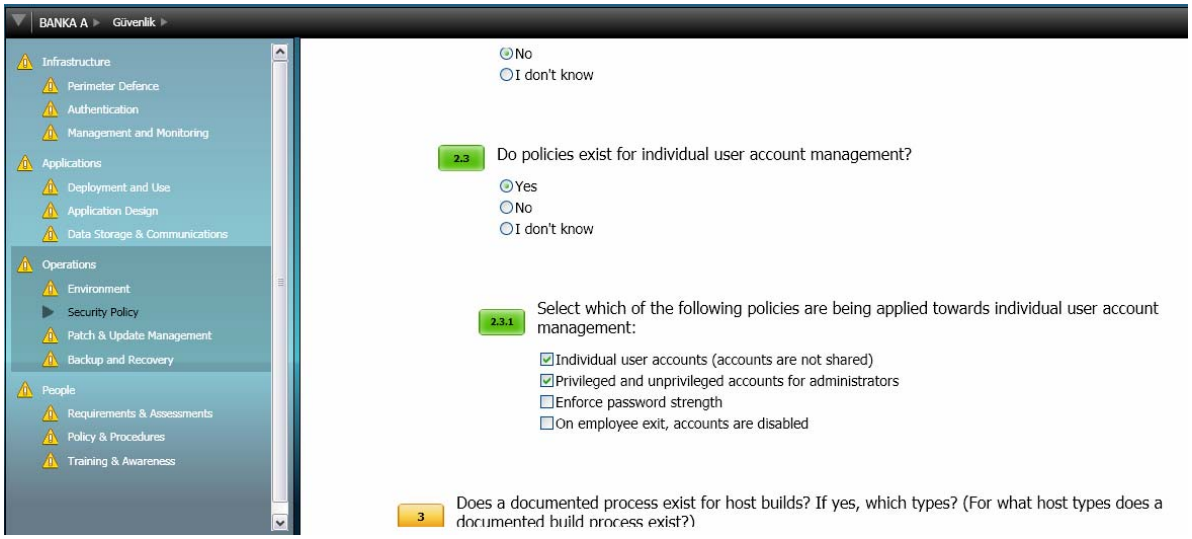
Şekil 53: MSAT Banka Güvenlik Değerlendirme 6

Uygulama güvenliği kapsamında son olarak veri saklama ve iletimi kategorisinde değerlendirme sorularına cevap verilmektedir. Örneğin yukarıdaki ekranda banka tarafından kullanılan kritik uygulamalar (örneğin ana bankacılık sistemi) üzerinde belirlenen hassas verilerin şifreli olarak saklanıp saklanmadığına yönelik değerlendirme soruları sorulmuştur.



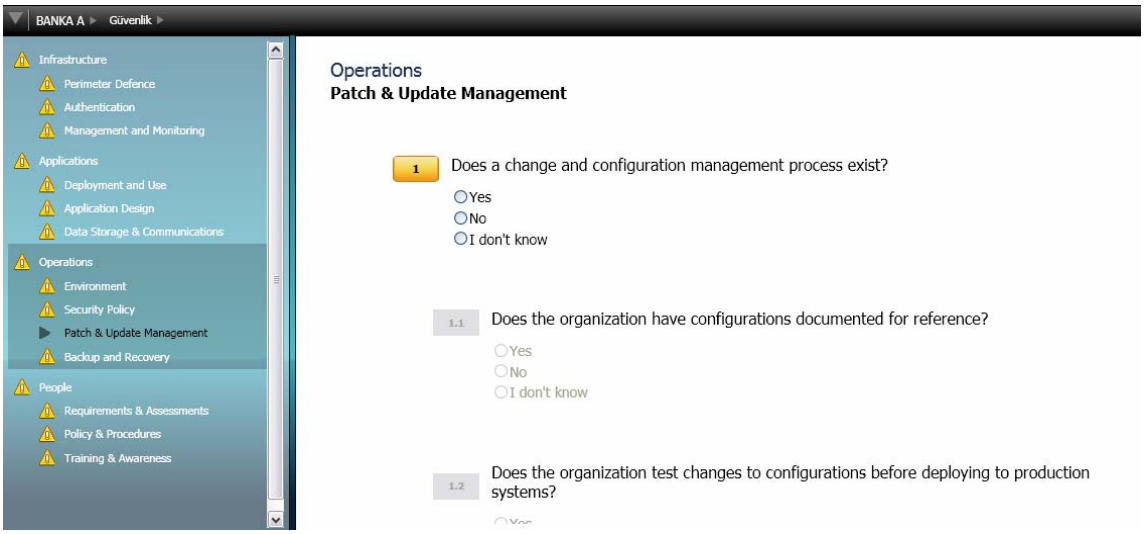
Şekil 54: MSAT Banka Güvenlik Değerlendirme 7

Altyapı ve uygulama güvenliği kapsamındaki soruların cevaplanmasından sonra, BT operasyonuna yönelik değerlendirme sorularının yanıtlanması gerekmektedir. Bu kapsamdaki güvenlik soruları genel BT ortamı, yama yönetimi, güvenlik politikası, yedekleme ve geri dönüş kategorileri altında cevaplanmaktadır. Örneğin, BT operasyonel ortamı ile ilgili olarak BT operasyonunun bankanın kendisi veya dış destek hizmeti vasıtasıyla idare edilip edilmediğinin bilgisi yukarıdaki ekranda sorulmuştur.



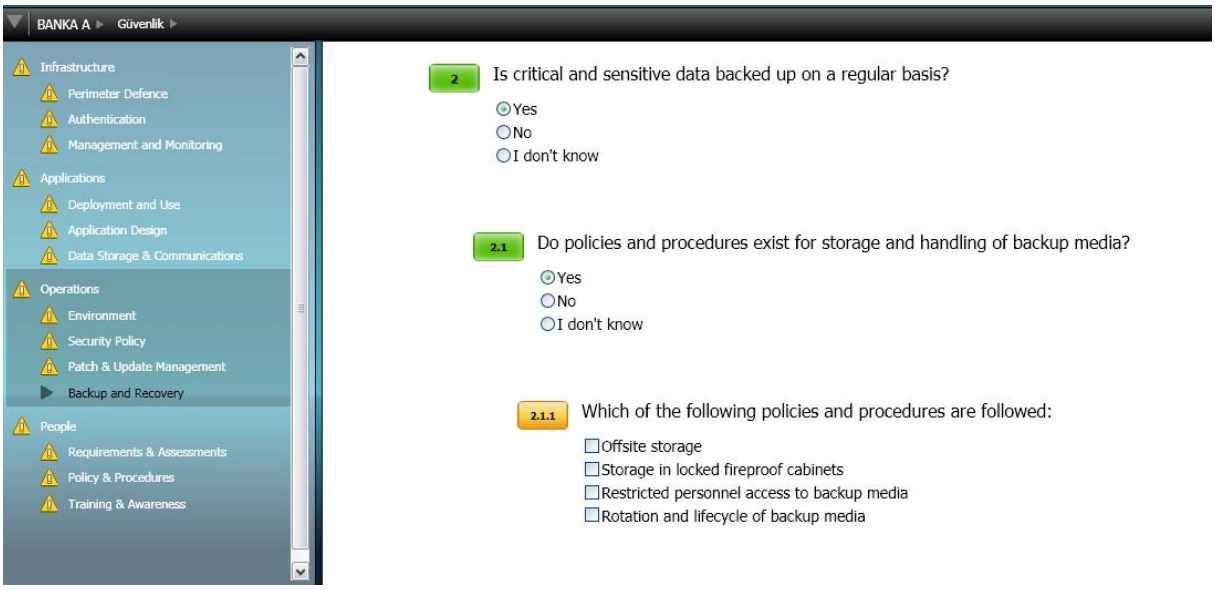
Şekil 55: MSAT Banka Güvenlik Değerlendirme 8

BT operasyonuna ait değerlendirme sorularında güvenlik politikası kategorisi altında da değerlendirme yapılmaktadır. Örneğin yukarıdaki ekranda kullanıcı hesap yönetiminin nasıl yapıldığına ait değerlendirme soruları sorulmuştur.



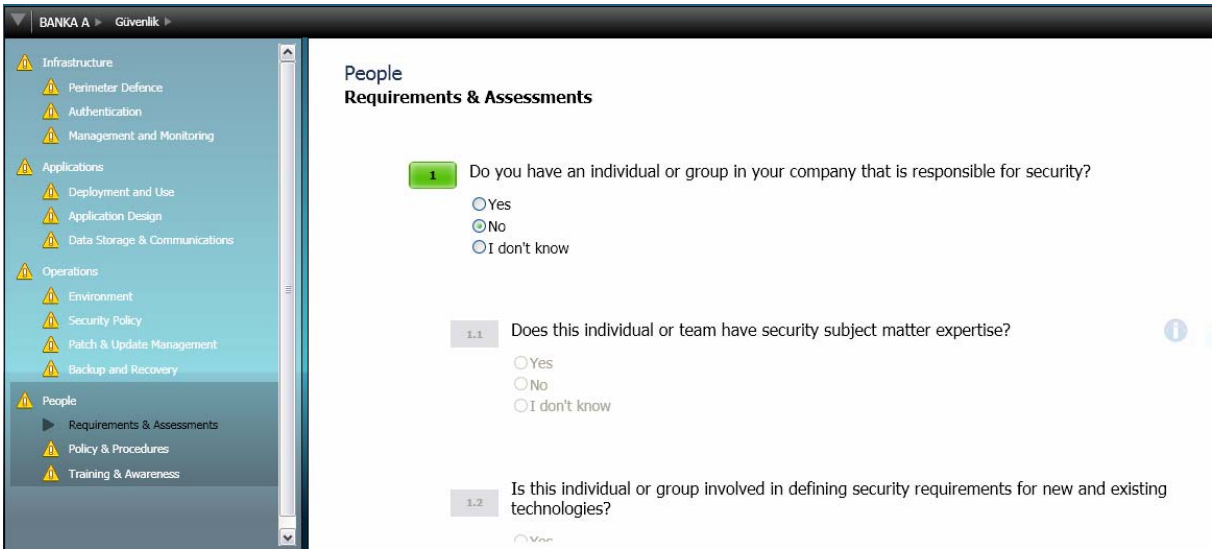
Şekil 56: MSAT Banka Güvenlik Değerlendirme 9

Yama yönetimi kapsamında da benzer değerlendirme soruları cevaplanmıştır. Bu kapsamda konfigürasyon yönetimi ile ilgili olarak çeşitli soruların sorulduğunu da yukarıdaki ekran üzerinden görebilmekteyiz.



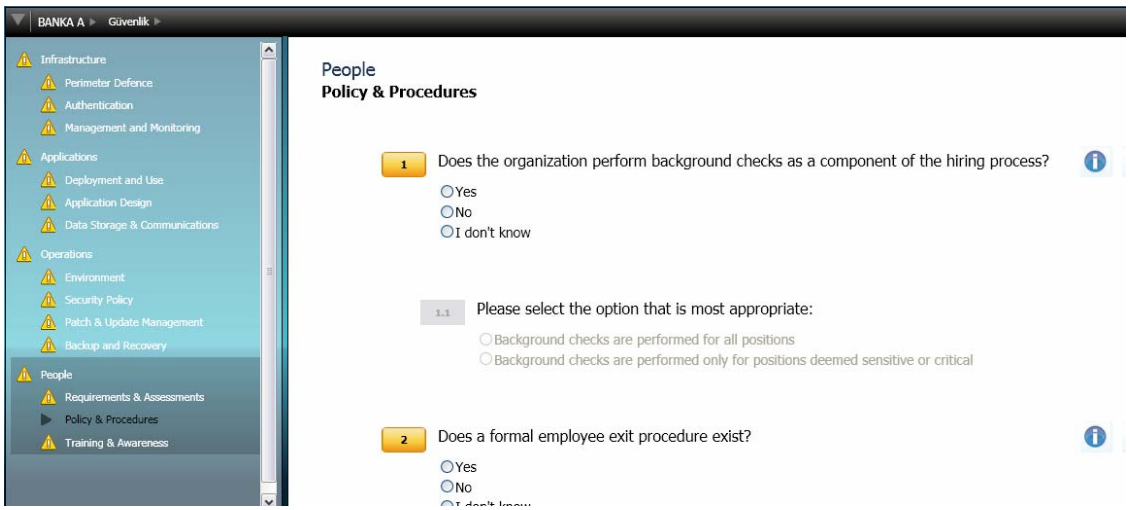
Şekil 57: MSAT Banka Güvenlik Değerlendirme 10

BT operasyonu bölümü kapsamında son olarak yedekleme ve geri dönüş ile ilgili değerlendirme soruları sorulmaktadır. Bu kapsamda kritik ve hassas verinin nasıl yedeklediği ve nasıl saklandığına yönelik sorulara cevap verilmektedir. Kullanılan araç üzerinden alınan ekran görüntüsünden de bu kapsamdaki sorulara yer verildiğini yukarıda görebilmekteyiz.



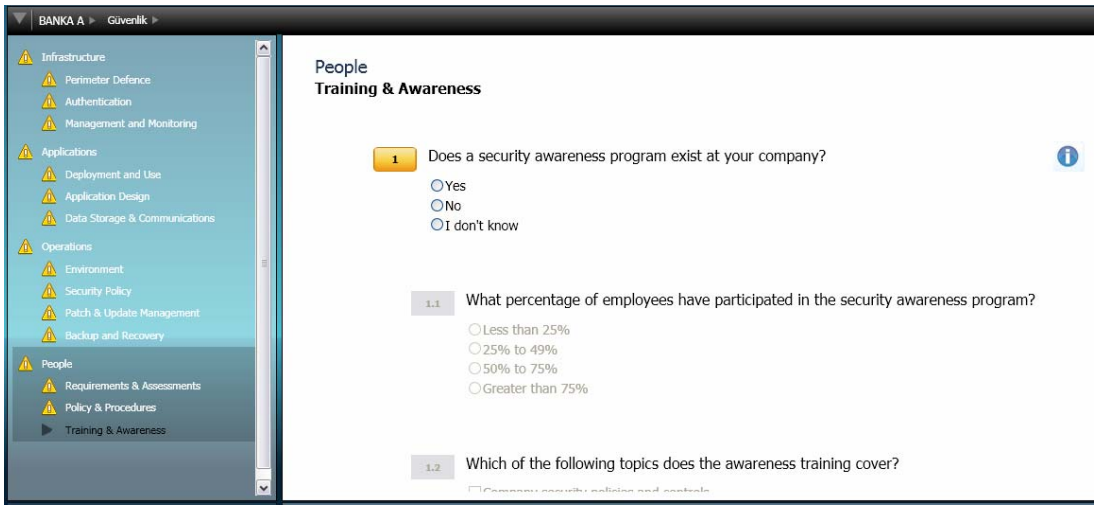
Şekil 58: MSAT Banka Güvenlik Değerlendirme 11

Değerlendirme sorularının son bölümü ise çalışanlar ile ilgili olan sorulardır. Bu kapsamda kurumsal güvenlik politikaları, insan kaynakları süreçleri, BT çalışanlarının ve kullanıcıların bilgi sistemleri güvenliği kapsamdaki farkındalıkları ve eğitim faaliyetleri kapsamındaki sorulara yer verilmektedir. Örneğin ilk kategori altında kurumun çalışanları kapsamında gereksinimleri ve değerlendirmeleri yapılmaktadır. Bu kapsamda bilgi güvenliği ile ilgili olarak ayrı bir bölümün tesis edilip edilmediği ilk soru olarak sorulduğu yukarıdaki ekrandan da görülebilmektedir.



Şekil 59: MSAT Banka Güvenlik Değerlendirme 12

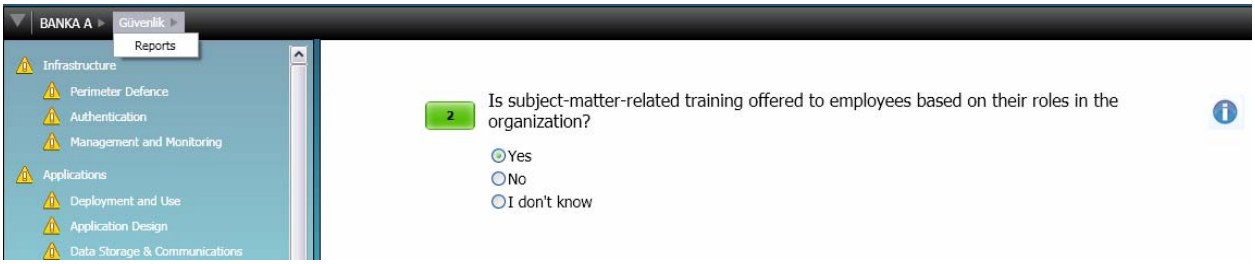
Sonrasında politika ve prosedürler kapsamında çalışanları etkileyen süreçler üzerine bilgi alınmaya ve değerlendirme yapılmaya çalışılmaktadır. Örneğin BT çalışanının işe alınmadan önce öz geçmişinin değerlendirilmesi, işe alma ve işten ayrılma prosedürlerinin BT güvenliği açısından uygunluğunun değerlendirilmesi kapsamındaki sorular cevaplanmaktadır.



Şekil 60: MSAT Banka Güvenlik Değerlendirme 13

Son olarak çalışanların bilgi güvenliği konusunda farkındalığının arttırılması ve bu konuda eğitim faaliyetlerinin organize edilmesine yönelik değerlendirme sorular sorulmaktadır. Örneğin bilgi güvenliği farkındalık programının olup olmadığı ve varsa program hakkındaki bilgiler yukarıdaki ekran üzerinde sorulduğu görülebilmektedir.

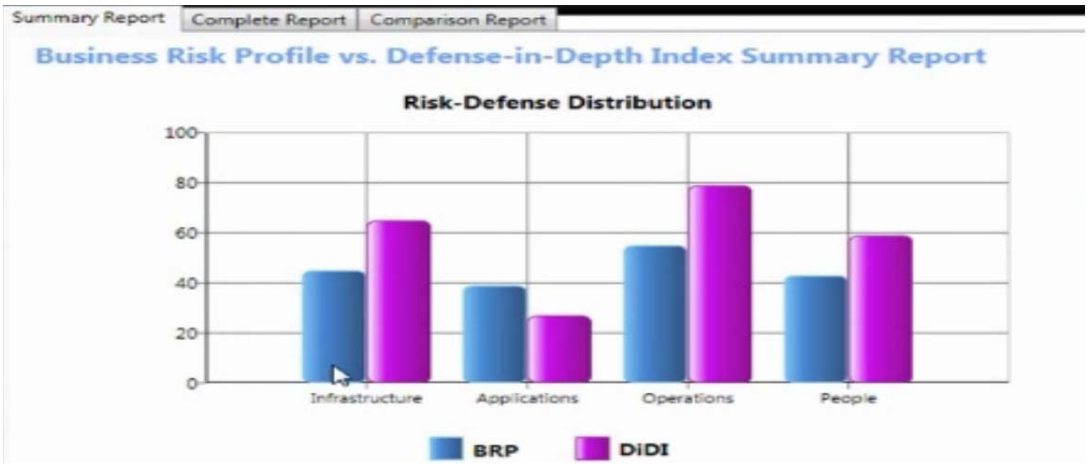
Dört ana bölüm altındaki tüm değerlendirme soruları cevaplandıktan sonra banka için öncelikle doldurulmuş olan risk profili de göz önünde bulundurularak bilgi güvenliği açısından bir ön değerlendirme raporu yazılım aracı vasıtasıyla otomatik olarak oluşturulmaktadır.



Şekil 61: MSAT Banka Güvenlik Değerlendirme Raporlaması

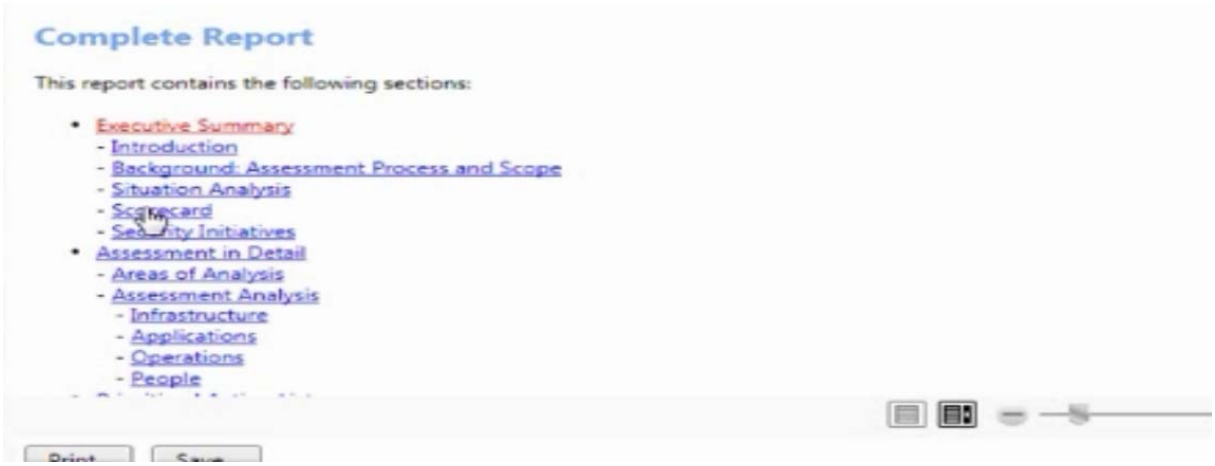
Yazılım aracı üzerinde "Güvenlik" değerlendirme sorularına ve banka risk profiline istinaden raporun çalıştırılması yeterli olacaktır. Bu kapsamda özet rapor, detaylı tüm rapor ve karşılaştırılmalı raporlar otomatik olarak araçtan alınabilmektedir. Raporlar değerlendirilerek

CobiT detay kontrol hedefleri kapsamında yapılan test aktivitelerinin planlanmasında yol gösterecektir.



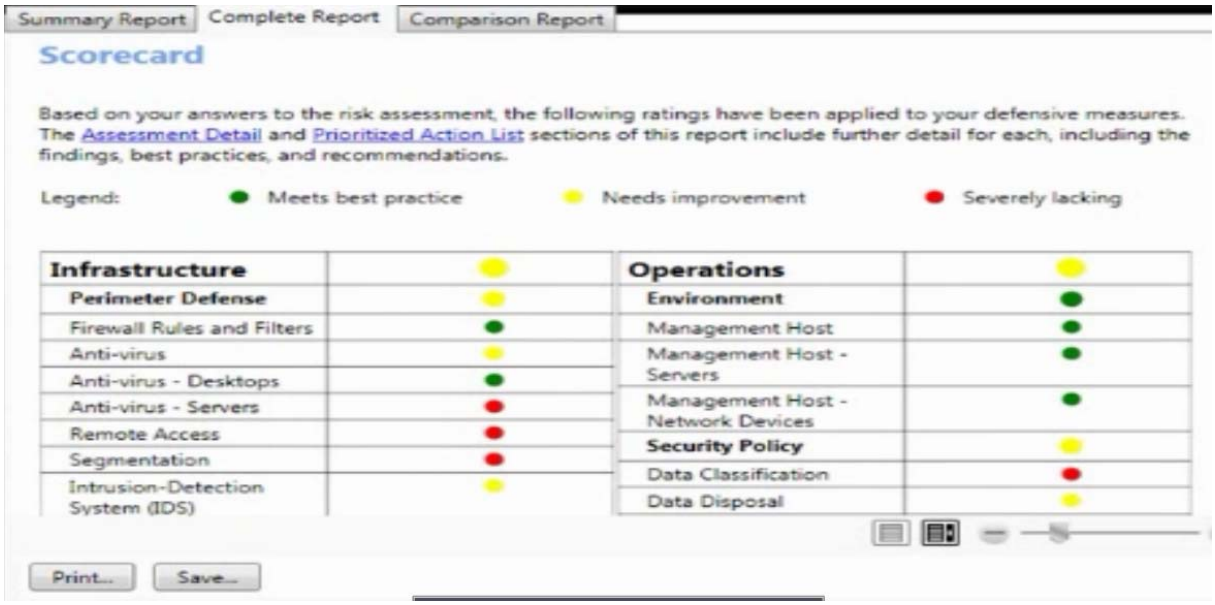
Şekil 62: MSAT Banka Güvenlik Değerlendirme Özet Rapor

Özet raporu yukarıdaki ekran görüntüsü üzerinde görebilmekteyiz. Bu kapsamda bankanın risk profiline karşılık risk seviyesi mavi ile değerlendirme sorularına karşılık öngörülen koruma seviyesi ise mor ile gösterilmektedir. Örneğin uygulamaların güvenliği alanında riskin koruma seviyesinden yüksek olduğu göz önüne alınarak ileriki test faaliyetlerinde bu alana ağırlık verilmesi planlanmalıdır.



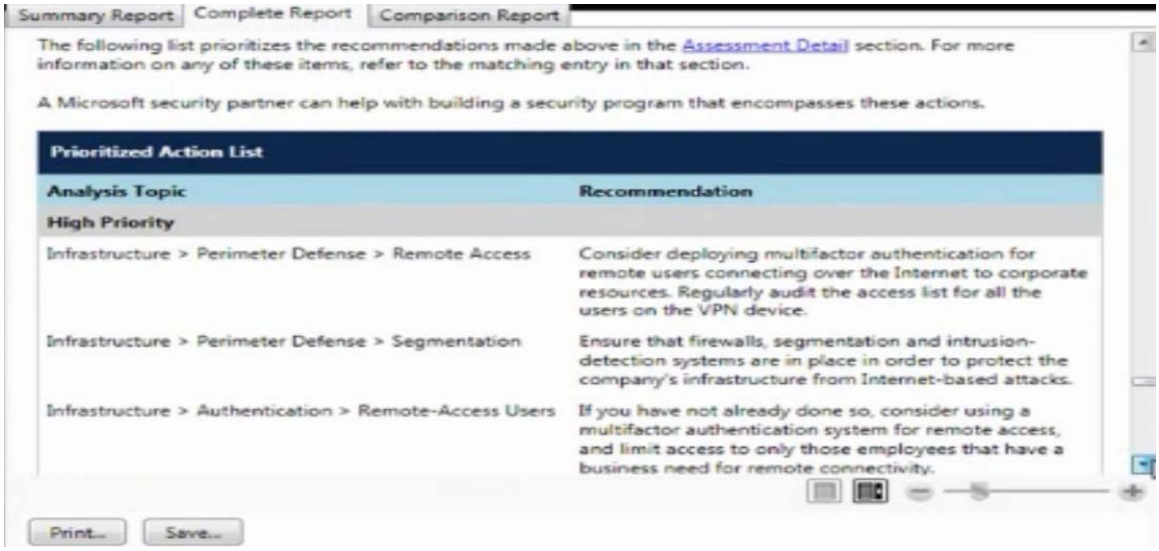
Şekil 63: MSAT Banka Güvenlik Değerlendirme Detay Rapor

Detay değerlendirme raporunda ise durum analizi, karne ve tavsiyeler kapsamında detaylı bilgilere yer verilmektedir. Özellikle bankalardaki BT çalışanlarının kendilerinin yapacağı değerlendirmelerde iş planlarını güvenlik açısından daha iyiye gitmede yol gösterecek şekilde revize etmelerini sağlayacak rapor oluşturulmaktadır.



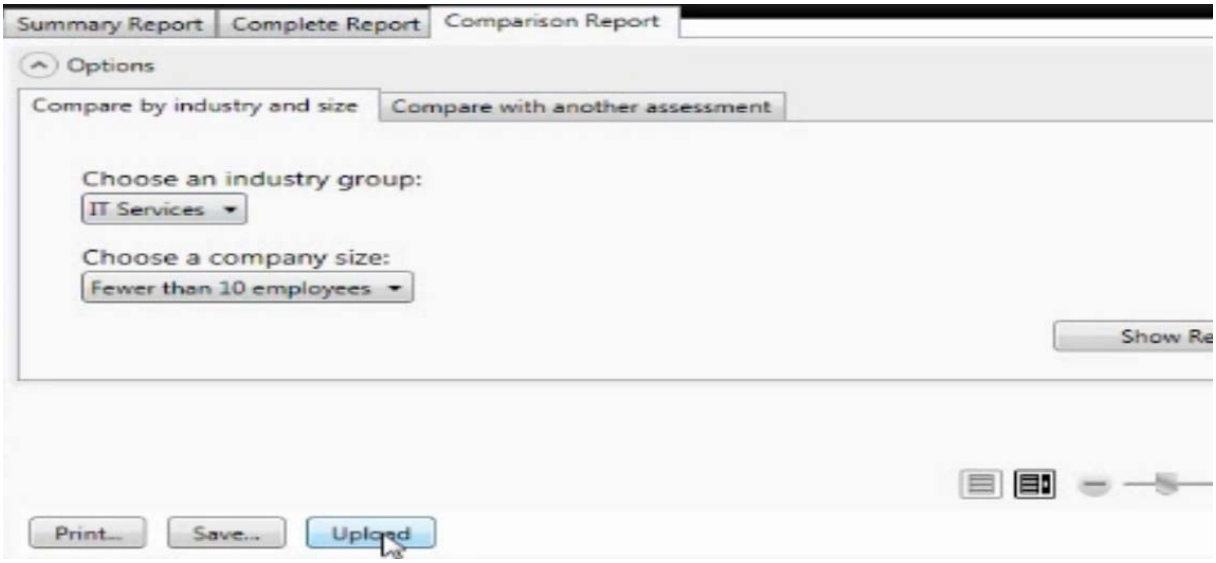
Şekil 64: MSAT Banka Güvenlik Değerlendirme Detay Rapor: Karne Gösterimi

Örneğin detay rapor üzerinde hangi bölümde hangi konu ile ilgili zayıf kalındığı ve iyileştirme gerektiği karne şeklinde görülebilmektedir. Örneğin altyapı değerlendirme soruları ile ilgili olarak anti virüs sunucuları kapsamında zayıflık bulunduğu görülebilmektedir.



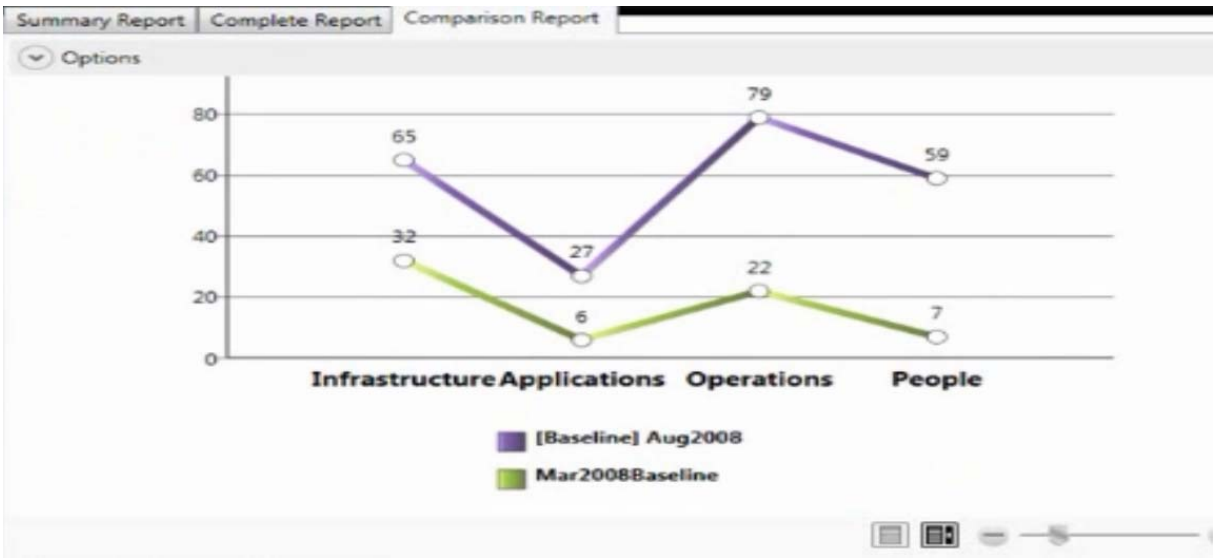
Şekil 65: MSAT Banka Güvenlik Değerlendirme Detay Rapor: Tavsiyeler

Bunun yanında güvenlik açısında zayıf kalınan noktalara veya iyileştirme gereken noktalara yönelik yazılım aracı kapsamında en iyi örneklerden yararlanarak öneriler de otomatik olarak getirilmektedir.



Şekil 66: MSAT Banka Güvenlik Değerlendirme Karşılaştırmalı Rapor 1

Son olarak benzer bankalar kapsamında yapılan değerlendirme raporlarının karşılaştırılması da otomatik olarak yazalım aracı vasıtasıyla yapılabilmektedir.



Şekil 67: MSAT Banka Güvenlik Değerlendirme Karşılaştırmalı Rapor 2

Endüstri kapsamında yapılan karşılaştırmaların yanı sıra zaman süresinde yapılan değerlendirmeler arasında da karşılaştırma otomatik olarak yapılabilmektedir. Örneğin, Ağustos 2008'de yapılan değerlendirme ile Mart 2008 değerlendirme sonuçları grafik üzerinde karşılaştırılabilmektedir.

Bankadaki doğru kişilerden değerlendirme sorularının cevapları alınarak kısa sürede güvenlik ortamı kapsamında bir ön değerlendirme raporu oluşturulabilmekte ve CobiT detay kontrol hedeflerine yönelik test faaliyetlerinin planlaması yapılabilmektedir.

B) CobiT detaylı kontrol hedeflerine yönelik test çalışmalarının yapılması ve sonuçların raporlanması: CobiT (DS5) sistem güvenliğinin sağlanmasına yönelik 11 detaylı kontrol hedefi kapsamında test çalışmalarının bankalarda gerçekleştirilmesi, her bir detaylı kontrol hedefi için kontrollerin belirlenmesi, bu kontrollerin test edilmesi ve sonuçlarının raporlanması gerekmektedir. Bu adım kapsamında her bir detaylı kontrol hedefinin incelenmesinde nelere dikkat edilmesi gerektiğine ve nasıl raporlanması gerektiğine yer verilecektir. Her bir detaylı kontrol hedefinin incelenmesine ve elde edilen sonuçlara bağlı olarak son adımda "*DS5 Sistem Güvenliğinin Sağlanması*" kontrol hedefi için olgunluk seviyesi belirlenecektir. Buna göre DS5 kapsamındaki detaylı kontrol hedefleri şu şekildedir:

- Bilgi Teknolojileri ("BT") Güvenliği Yönetimi (DS5.1): BT güvenliği bankaların en yüksek organizasyon seviyesi, diğer bir ifadeyle üst yönetim, tarafından yönetilmelidir. Bu kapsamda güvenlik aksiyonlarının yönetimi iş gereksinimleri ile uyum hale getirilmelidir.
- BT Güvenlik Planı (DS5.2): Bankalarda yürürlükte bulunan bir BT güvenlik planı olmalıdır. Bu plan kurumsal bilgi işlem kullanımı, BT yapılanışı, bilgi risk ve hareket planları ile bilgi güvenlik kültürünü içermelidir. BT güvenlik planı, bankaların güvenlik politika ve prosedürlerinde uygulanmalı; şirket hizmet, personel, yazılım ve donanıma gerekli yatırımı yaparken bu plan göz önüne alınmalıdır. Güvenlik politika ve prosedürleri kullanıcılara ve diğer ilgili kişilere bildirilmelidir.
- Kimlik Yönetimi (DS5.3): Tüm sistem kullanıcıları (iç, dış, veya geçici) ve BT sistemleri üzerindeki aktiviteleri (iş uygulamaları, sistem operasyon, geliştirme ve bakım) tek başlarına tanımlanabilir olmalıdır. Kullanıcıların sistemlere ve veriye erişim hakları; tanımlanmış ve yazılı hale getirilmiş iş ihtiyaçları ve görev gereksinimleri ile uyumlu olmalıdır. Kullanıcı erişim hakları; kullanıcının yöneticisi tarafından talep edilmeli, sistem sahibi tarafından onaylanmalı ve güvenlikten sorumlu kişi tarafından uygulanmalıdır. Kullanıcı kimlikleri ve erişim hakları, merkezi bir arşivde korunmalıdır. Maliyet etkili teknik ve yasal ölçümlemeler yapılmalı ve kullanıcı tanımını oluşturmak, kimlik denetimini yapmak ve erişim haklarını kuvvetlendirmek için mevcut durum devam ettirilmelidir.
- Kullanıcı Hesap Yönetimi (DS5.4): Kullanıcı hesaplarının ve ilgili kullanıcı haklarının talep edilmesi, oluşturulması, kullanıcılara atanması, askıya alınması ve kapatılması işlemlerinin ne şekilde gerçekleştirileceği kullanıcı hesapları yönetimi sürecinde belirlenmiş olmalıdır. Veri veya sistem sahiplerinin onayıyla talep edilen erişim haklarının kullanıcılara verilmesi süreci kullanıcı hesapları yönetimi dâhilinde olmalıdır. Bu prosedürler sistem yöneticileri, iç ve dış kullanıcıları da kapsayacak şekilde tüm kullanıcılar için olağan ve acil durumlarda uygulanıyor olmalıdır. Kurumsal sistemler ve bilgi kaynaklarına erişim ile ilgili haklar ve yükümlülükler her tip kullanıcı için sözleşmeye dayalı olarak düzenlenmelidir. Tüm hesaplar ve ilgili erişim hakları düzenli olarak yönetim tarafından gözden geçirilmelidir.
- Güvenlik Testleri, gözetimi ve izlenmesi (DS5.5): BT güvenlik uygulamaları test edilmeli ve aktif olarak gözlemlenmelidir. BT güvenliğinin; onaylanmış güvenlik seviyesinin sürdürülmesini sağlamak için düzenli aralıklarla kalitesi arttırılmalıdır. Arşivleme ve

fonksiyon gözlemlenmesi; tespit edilmeye gerek duyabilecek seyrek veya olağandışı aktivitelerin erken tanısını mümkün kılmalıdır. Arşiv verisine erişim; erişim hakları ve alıkoyma gereksinimleri açısından, iş gereksinimleri ile uyumlu olmalıdır.

- Güvenlik vakasının tanımı (DS5.6): Potansiyel güvenlik vakalarının karakteristikleri açık şekilde tanımlanmalıdır. Bu şekilde güvenlik vakaları, vaka ve problem yönetimi süreci vasıtasıyla uygun şekilde yönetilmelidir. Karakteristikler, neyin güvenlik vakası olarak tanımlanacağını ve etki seviyesini içermelidir[137]. Kısıtlı sayıdaki etki seviyeleri açıklanmalı ve ihtiyaç duyulan her belirli aksiyon ve bildirime ihtiyaç duyulan kişiler için tanımlanmalıdır.
- Güvenlik teknolojilerinin korunması (DS5.7): Güvenlik ile ilişkili önemli teknolojilerin zarar görmesine karşılık dirençli olması ve ilgili güvenlik dokümantasyonun da gerekmiyorsa yetkili olmayan kişilere açıklanmaması gerekmektedir.
- Kriptografik anahtar yönetimi (DS5.8): Meydana getirme, değiştirme, geçersiz kılma, dağıtım, sertifikasyon, saklama, giriş, kullanım ve değişiklik, yetkisiz açıklamaya karşın anahtar korumasının sağlanması için kriptografik anahtarların arşivlenmesi ile ilgili politikalar ve prosedürler tanımlanmalıdır
- Zararlı Yazılımların Önlenmesi, Belirlenmesi ve Düzeltilmesi (DS5.9): Bankaların bünyesinde BT sistemlerini, virüs, solucan, casus yazılımlar, iç veya dış kullanıcılar tarafından geliştirilmiş diğer zararlı yazılımlardan koruyacak, önleyici, tespit edici ve düzeltici sistemlerin mevcut olması gerekmektedir.
- Ağ güvenliği (DS5.10): Güvenlik tekniklerinin ve ilgili yönetim prosedürlerinin (örneğin firewall, güvenlik cihazları, ağların bölümlenmesi ve istenmeyen girişlerin tespiti) girişleri onaylamak ve ağ içinde akan bilginin kontrol edilmesi için kullanılması sağlanmalıdır.
- Hassas verilerin alışverişi (DS5.11): Hassas işlemlere ait verilerin taraflar arasında aktarımı sırasında güvenli yolla iletilmesi ve içerik doğruluğunun kanıtlaması için çeşitli kontrollerin bankalar tarafından tesis edilmesi gerekmektedir.

Yukarıdaki detaylı kontrol hedefleri kapsamında test faaliyetleri gerçekleştirilerek kontroller tespit edilmekte, tasarım ve etkinlik açısından değerlendirilmektedir. Bu kapsamda "*Kullanıcı*

[137] Steven J. Ross, "Reliable Security", Information Systems Control Journal, volume 5 (2008), 9

Hesap Yönetimi (DS5.4)" örnek olarak alınarak kontrollerin nasıl tespit edildiği ve sonuçlarının bilgi sistemleri denetim raporuna nasıl konu edildiği hakkında bilgi verilecektir.

Tablo 7: Detaylı Kontrol Hedeflerine İlişkin Tablo

<table>
<tr><th colspan="3">Detaylı Kontrol Hedeflerine İlişkin Tablo</th></tr>
<tr><td colspan="3">Kontrol Hedefi: Hizmet Sunumu ve Destek: Sistem Güvenliğinin Sağlanması</td></tr>
<tr><td colspan="3">Detaylı Kontrol Hedefi: Kullanıcı Hesap Yönetimi (DS5.4)</td></tr>
<tr><td rowspan="3">Kontroller ve Testler</td><td>Denetlenenin Kontrolleri</td><td>• Ana bankacılık sistemi kapsamında gerçekleştirilen tüm kullanıcı yetkilendirmeleri iş akışı uygulaması üzerinden onaylanarak gerçekleştirilmektedir.</td></tr>
<tr><td>Gerçekleştirilen Testler</td><td>Yeterlilik Testi
• Ana bankacılık sistemi kullanıcı hesap yönetimine ait prosedür alınarak incelenmiş ve yetkilendirme işlemlerini gerçekleştiren çalışanlar ile görüşme yapılmıştır.
Etkinlik Testi
• Ana bankacılık sistemi üzerinde yetki değişikliğine uğrayan kullanıcıların sistem kayıtların alınmış ve iş akış uygulaması üzerindeki onay kayıtları ile kullanıcı ve tarih bazlı olarak karşılaştırılmıştır.</td></tr>
<tr><td>Test Sonuçları</td><td>Yeterlilik Testi
• Ana bankacılık sistemi üzerindeki yeni kullanıcı yaratma, mevcut kullanıcıda yetki değişikliği gibi ek yetkilendirme işlemleri doğuran durumların ancak iş akış uygulaması üzerinde gerekli onaylar alındığında</td></tr>
</table>

		gerçekleştirildiği belirlenmiştir. ***Etkinlik Testi*** • Denetim dönemi kapsamında ana bankacılık sistemi üzerindeki tüm yetkilendirme işlemlerinin onay dahilinde gerçekleştirildiği tespit edilmiştir.
Sonuç	Bulgular	-
	Riskler	-
	Denetlenenin Görüşü	
	Sonuç Değerlendirmesi	

Yukarıdaki tablo üzerinde "*Kullanıcı Hesap Yönetimi (DS5.4)*" kapsamında tek bir kontrolün nasıl test edildiği ve rapora konu edildiğini görebilmekteyiz. Her detay kontrol hedefi kapsamında tespit edilen tüm kontroller bu şekilde yazıya dökülecek ve tespit edilen olası bulgular riskleri ile birlikte yukarıdaki tablonun "*Bulgular*" ve "*Riskler*" alanlarına yazılacaktır. *"DS5 Sistem Güvenliğinin Sağlanması"* kontrol hedefi kapsamındaki tüm detay kontrol hedefleri üzerindeki kontroller test edilerek CobiT kapsamındaki DS5 denetim faaliyetleri tamamlanmış olacaktır. Bu test işlemleri ve raporlama tamamlandıktan sonra sonuçlar değerlendirilerek *"DS5 Sistem Güvenliğinin Sağlanması"* kontrol hedefi için olgunluk seviyesi belirlenecektir.

C) "DS5 Sistem Güvenliğinin Sağlanması" kontrol hedefine yönelik olgunluk seviyesinin tespiti: "*DS5 Sistem Güvenliğinin Sağlanması*" kapsamında tüm detaylı kontrol hedeflerinin test edilmesinden sonra elde edilen sonuçlara göre "*CobiT Olgunluk Seviyesi Değerlendirme Aracı"*ndan faydalanılarak değerlendirme soruları cevaplanmakta ve denetlenen bankanın olgunluk seviyesi otomatik olarak belirlenmektedir.

Tablo 8: Olgunluk Seviyesi "0" için Anket Soruları

DS5: Olgunluk Seviyesi 0 için Anket Soruları						
		Hangi seviyede katılıyorsunuz?				
Seviye	İfadeler	Hiç	Biraz	Oldukça	Tamamiyle	İfadelerin uygunluğuna yönelik değerler
1	Bilgi teknolojileri güvenliğinin gerekliliği konusu kurum tarafından anlaşılmamıştır. Güvenlik konusunda görev ve sorumluluklar kurum içinde belirlenmemiştir.	x				0,00
2	Bilgi teknolojileri güvenlik yönetiminin oluşturulmasına yönelik gerekli adımlar uygulanmamıştır.		x			0,33
3	Bilgi teknolojileri güvenlik raporlaması mevcut olmayıp güvelik açıklarına yönelik aksiyonların belirlenmesine yönelik süreç de mevcut değildir.	x				0,00
4	Sistem güvelik yönetimi kapsamında tanımlı bir süreç eksikliği mevcuttur.	x				0,00
Toplam Değer						**0,33**

Bilgi sistemleri denetçisi testlerden elde ettiği sonuçlara göre DS5 kontrol hedefine yönelik olgunluk seviyesi "0" ile ilgili ifadelere ne ölçüde katıldığını göstermek için cevaplar vermektedir. Örneğin yukarıdaki örnek üzerinde "Bilgi teknolojileri güvenlik yönetiminin oluşturulmasına yönelik gerekli adımlar uygulanmamıştır" ifadesine denetçi biraz katılmaktadır. Her bir soruya verilen cevaba göre "0" olgunluk seviyesindeki ifadelerin uygunluğuna yönelik değer belirlenmektedir. Örneğin "0" olgunluk seviyesinden elde edilen değer "0,33"tür.

Bu kapsamda her bir olgunluk seviyesi için "*CobiT Olgunluk Seviyesi Değerlendirme Aracı"*nda belirlenmiş olan ifadelere denetçinin test sonuçlarına göre ne ölçüde katıldığı belirlenmektedir. Böylece her bir olgunluk seviyesi için toplam değer belirlenmekte ve bankanın DS5 kontrol hedefi kapsamında olgunluk seviyesi hesaplanabilmektedir. Araştırma uygulaması kapsamında tüm olgunluk seviyelerine ait ifadelere ve cevaplarına bu bölümde yer verilmeyip "*CobiT Olgunluk Seviyesi Değerlendirme Aracı"* kapsamındaki tüm olgunluk seviyelerine yönelik sorulara araştırmanın ekler kısmında yer verilecektir.

Tablo 9: Olgunluk Seviyesinin Hesaplanma Yöntemi

DS5: Olgunluk Seviyesinin Hesaplanma Yöntemi					
Olgunluk Seviyesi (N)	İfadelerin Uygunluğuna Yönelik Değerlerin Toplamı (A)	Olgunluk Seviyelerinin Değerlendirilmesi Yönelik İfadelerin Toplamı (B)	Olgunluk Seviyesi Uygunluk Değeri =X (A/B)	Normalize Edilen Uygunluk Değeri = Y X/∑X	Olgunluk Seviyesine Yapılan Katkı (N*Y)
0	0,33	4	0,08	0,05	0,00
1	1,67	4	0,42	0,27	0,27
2	4,00	7	0,57	0,37	0,73
3	2,00	7	0,29	0,18	0,55
4	2,00	10	0,20	0,13	0,51
5	0,00	12	0,00	0,00	0,00
Toplam X ve Y Değerleri			1,56	1,00	
Olgunluk Seviyesi					**2,07**

Tüm olgunluk seviyeleri (N) için ifadeler denetçinin test sonuçlarına göre cevaplanmış ve her bir seviyenin olgunluk seviyesinin hesaplanmasındaki katkısı (A) otomatik olarak hesaplanmıştır. Yukarıdaki tablodan da görüleceği gibi bu uygunluk değerleri (A) her bir olgunluk seviyesi fazında cevaplanan ifadelerin toplam sayısına (B) bölünerek olgunluk seviyesi uygunluk değeri (X) belirlenmektedir. Son olarak olgunluk seviyesi uygunluk değeri (X) bir üzerinden ifade edilerek (Y) mevcut seviye ile çarpılması sonucu bankanın DS5 kontrol hedefi kapsamındaki olgunluk seviyesi (2,07) objektif olarak hesaplanmaktadır.

Örneğin yukarıdaki değerlendirme kapsamında denetlenen bankanın olgunluk seviyesi "2" olarak tespit edilmiş olup aşağıdaki sonucu işaret etmekte ve bilgi sistemleri raporunda yer verilmektedir:

Bilgi güvenliğine yönelik prosedürler oluşturulmuş olmasına rağmen, banka tarafında güvenlik farkındalığı kısıtlı olarak mevcut olmakla birlikte, banka için yürürlükte bulunan yazılı bir "Bilgi

Güvenliği Politikası" ve beklentileri karşılayacak düzeyde bir güvenlik planı mevcut değildir. Bunun yanında kritik sistemler de dâhil olmak üzere, güvenlik kayıtlarını işleyip derleyecek ve üst yönetime raporlayacak bir yapı mevcut değildir.

Böylece "DS5" kontrol hedefi kapsamındaki genel kontrol alanının denetimi tamamlanmış olup bilgi sistemleri denetim raporunun ilgili bölümü yönetmeliğe uygun olarak hazırlanmaktadır.

6. SONUÇ

Bağımsız finansal denetim kapsamında, bağımsız denetim kuruluşlarının ana amacı bağımsızlık ilkesine bağlı olarak finansal tabloların doğruluğu, tutarlılığı, ve tam olarak açıklanmış olması adına makul bir güvence sağlamak için görüş verilmesidir. Bu açıdan değerlendirildiğinde bilgi sistemlerinin yoğun olarak kullanıldığı bankacılık sektöründe, finansal veri üretiminde bilgi sistemlerinin önemi göz önüne çıkmaktadır. Bu sebeple bağımsız finansal denetim faaliyetleri kapsamında bilgi sistemleri denetimi ile entegre olarak denetim faaliyetlerinin yürütülebilmesi günümüz teknolojik gelişmelerine ve bankacılık sektörünün yapısına bağlı olarak kaçınılmaz boyuta gelmiştir.

Bilgi sistemleri denetiminin finansal denetimi ile entegre olarak yürütülmesi gerektiğini ortaya koymak için araştırmanın uygulaması vasıtasıyla "Genel Muhasebe Süreci" uygulama kontrol alanı ve "DS5: Sistem Güvenliğinin Sağlanması" genel kontrol alanı kapsamında testler gerçekleştirilmiş ve sonuçlar raporlanmıştır.

Örneğin "Genel Muhasebe Süreci" kapsamında ve finansal denetimin kayıtsal doğruluk amacına göre fişlerdeki borç-alacak dengesinin sağlanması gerektiği bilinmektedir. Bu amaç ile ilgili olarak süreç içinde fiş tutar dengesinin korunması amacıyla ana bankacılık sistemi üzerinde oluşturulan muhasebe fişlerinin toplam borç ve alacak tutarlarının eşit olması sistemsel olarak kontrol ile zorlandığı öğrenilmiştir. Böylelikle ana bankacılık uygulaması kapsamında bu uygulama kontrolünün finansal denetim için kritikliği değerlendirilerek bilgi sistemleri denetiminde test edilmesi gerekmektedir. Bununla birlikte test sonucuna göre bilgisayar destekli denetim aracından da yararlanarak tüm muhasebe hareketlerine yönelik fişlerin analizi sonucunda 431 adet fiş kaydı nedeniyle 531.439.402 TL tutarında alacak tarafının fazla olduğu tespit edilmiştir. Dolayısıyla bu fişler nedeniyle borç-alacak tutar dengesinin bozuk olduğu fişlerin sistemde olduğu tespit edilmiştir. Bunun sonucu olarak borç-alacak tutar dengesi bulunmayan fişlerin sistemde bulunması, sistemden elde edilen finansal tabloların bütünlüğünü ve doğruluğunu olumsuz şekilde etkileyebilmektedir.

Bilgi sistemleri yoğun iş süreçleri olan bankalarda iç kontrollerin de bankaların sistemleri üzerinde olmasından dolayı iç kontrol ortamının değerlendirilmesinde bilgi sistemleri denetiminin önemi artmaktadır. Bir önceki paragraftaki örneğimizde de olduğu gibi finansal

denetimin amacına uygun olarak bilgi sistemleri denetiminin yürütülmesi finansal denetim aracılığıyla tespit edilemeyen kontrol zayıflıklarının tespit edilebilmesini sağlamaktadır.

- Denetimin daha etkin, daha verimli ve daha kısa sürede yapılmasına yardımcı olmak
- Kısa zamanda güvenilirliği yüksek denetimler gerçekleştirmek
- Finansal verilerin yüzde yüzünün işlenmesine olanak sağlamak
- Finansal verileri üreten sistemlerdeki veri bütünlüğünün ve güvenilirliğinin üzerine görüş tesis etmek

bilgi sistemleri denetim faaliyetlerinin ve bilgisayar destekli denetim araçlarının entegre denetim faaliyetleri kapsamında finansal denetim amaçlarına sağladığı faydalardan bazılarıdır

Araştırmanın uygulamasında olduğu gibi bankacılık sistemi üzerindeki tüm fişlerin ardışık ve sıralı olarak kayıt altına alındığını finansal denetim kapsamında manüel olarak incelemek ve makul bir güvence vermek mümkün olmayabilmektedir. Ancak bilgi sistemleri denetimi kapsamında sistem üzerinde fişlerin nasıl sistemsel olarak kayıt altına alındığı incelenebilmekle (program ve ekran inceleme vs.) birlikte tüm fişler bilgisayar destekli denetim araçları vasıtasıyla incelenip makul bir güvence de verilebilmektedir. Bu kapsamdaki yaptığımız örnekte ise tüm muhasebe hareketlerine yönelik fişlerin analizi sonucunda 238 farklılığın ve bu farklılıktan kaynaklanan 2.749 fiş kaydının ardışık sıralı olarak sistemdeki fiş verisi üzerinde bulunmadığı tespit edilmiştir. Bu sonuca göre sistemden elde edilen finansal tabloların bütünlüğünün ve doğruluğunun olumsuz şekilde etkilenebileceği ortaya çıkmaktadır.

Bilgi sistemleri denetimi kapsamında gerçekleştirilen uygulama kontrolleri alanı denetimi finansal denetim ile ilişkilendirilerek bankaların teknoloji yoğun iş süreçlerini ve iç kontrol ortamını değerlendirmek için gerekli noktaları kapatmakta ve günümüz gereği olan entegre denetimin gerçekleşmesini sağlamaktadır.

Ancak uygulama kontrolleri alanının denetimi bilgi sistemleri denetiminin başarılı olarak tamamlanması, diğer bir ifadeyle finansal denetim amaçlarının bilgi sistemleri denetim amaçları ile eksiksiz olarak desteklenmesi anlamına gelmemektedir. Bu kapsamda bilgi teknolojileri genel kontrol alanlarının da denetiminin gerçekleştirilmesi gerekmektedir. Bankalar tarafından kullanılan uygulamalar üzerinde tasarlanan kontroller etkin bir bilgi teknolojileri genel kontrol ortamı üzerinde çalışma gereği duymaktadırlar. Güvenli olmayan bir bilgi teknolojileri genel

kontrol ortamı üzerinde tesis edilen uygulama kontrolleri etkin olarak çalışsa bile güvenilir olmayacaktır. Örneğin araştırmanın uygulaması kapsamında "Şubeler ve Genel Müdürlük birimleri tarafından sistem üzerinde yapılan serbest fiş girişleri sınırlı ve yetkili uygulama kullanıcıları tarafından yapılmaktadır" kontrolü uygulama kontrolleri alanında test edilen ve başarılı sonuç veren bir kontroldür. Ancak "DS5: Sistem Güvenliğinin Sağlanması" sağlanması genel kontrol alanında sistem üzerindeki yetkilendirme sürecinin etkin olarak işletilememesi veya sistem yöneticilerinin uygulamanın önyüzü dışında arka taraftan veritabanında fişleri değiştirebilmesi gibi tespitler genel kontrol ortamının güvenilirliğini düşürecektir. Böylelikle etkilenen uygulama kontrollerinin de güvenilirliği azalacak ve finansal denetim amaçları bilgi sistemleri denetim amaçları ile yeterince desteklenemeyecektir. Bu sebeple uygulama kontrol alanının yanında bilgi teknolojileri genel kontrol ortamı da bilgi sistemleri denetim kapsamında değerlendirilmelidir.

Araştırmanın uygulaması kapsamında yapılan örnekler ve analizler ile aşağıdaki sonuç ve önerilere varılabilmektedir:

- Bağımsız finansal denetim amaçları ile bankacılık sektöründeki bilgi sistemleri denetim faaliyetleri kapsamındaki uygulama denetimi sonuçlarının bir arada değerlendirmesi sağlanmalı ve entegre denetim faaliyetleri desteklenmelidir.
- Bankacılık sektöründeki bilgi sistemleri denetim faaliyetleri kapsamındaki genel kontrol alanları denetim sonuçları ile uygulama denetimi sonuçları bir arada değerlendirilmeli ve uygulama kontrolleri üzerindeki etkileri belirlenmelidir.
- Bilgisayar destekli denetim araçları ile verinin tümünün daha kısa sürede etkin olarak analiz edilmesi sağlanmalı ve denetim sonuçlarının güvenilirliği arttırılmalıdır.

Sonuç olarak bilgi sistemleri denetimi ve bilgisayar destekli denetim araçlarının kullanımı günümüz teknolojisinin iş süreçleri üzerindeki etkisine paralel olarak bağımsız finansal denetim süreci üzerinde de vazgeçilmez bir yere sahip olmuştur. Kısaca banka sektörü gibi verinin miktarının yüksek ve bilgi sistemleri kullanımının yoğun olduğu sektörlerde bilgi sistemleri denetimi, bağımsız finansal denetim amaçlarının desteklenmesi açısında çok önemli bir yere sahip olduğu sonucu çıkarılabilmektedir. Araştırma ve uygulama kapsamda ise bilgi sistemleri denetimi ile bağımsız finansal denetim arasındaki ilişkinin nasıl kurulabileceğine dair entegre denetim anlayışına teorik olarak da katkıda bulunulduğu düşünülmektedir.

KAYNAKÇA

Kitaplar

Bozkurt, Nejat. **Muhasebe Denetimi**. 3. Baskı (İstanbul: Alfa Basım Yayım, 2000)

Devlin, Edward S. Cole H. Emerson ve diğerleri. **Business Resumption Planning** (USA: AUERBACH, 2000)

Duman, Ömer. **SM, SMMM, ve YMM Sınavları için Muhasebe Denetimi ve Raporlama**. 2. baskı (Ankara: Siyasal Kitabevi, 2008)

Erdoğan, Melih. **Denetim Kavramsal ve Teknolojik Yapı.** 3. baskı (Ankara: Maliye ve Hukuk Yayınları, 2006)

ISACA. **IT Assurance Guide** (USA: 2007)

ISACA. **Control Objectives for Information and related Technology 4.1** (USA, 2007)

ISACA. **Control Objectives for Information and related Technology 4.0** (USA, 2005)

Johnson, Everett C. Robert D. Johnson. **CISA Review Manual 2007.** (USA: ISACA, 2007)

Kepekçi, Celal. **Bağımsız Denetim**. 5. baskı (İstanbul: AVCIOL Basım Yayın, 2007)

Porter, Brenda, Jon Simon, David Hatherly. **Principles of External Auditing** (USA: John Wiley & Sons, 1996)

Rosenblatt, Shelly Cashman. **System Analysis and Design.** 5. Edition (USA: Thomson Learning, 2002)

Saka, Tamer. **Türk Bankacılık Sektöründe Bilgi Teknolojileri Denetimi.** Yayın:224 (İstanbul: Türkiye Bankalar Birliği, 2001)

Sommerville, Ian. **Software Engineering**. 6. Edition (England: Pearson Educated Limited, 2001)

Makaleler

Bağcı, Barış. **Bilgi Teknolojileri Risk Yönetimine Genel Bakış**. (İstanbul: Deloitte Touche Tohmatsu, 2007)

Bakman, Alex. "If Compliance is so critical , Why are we still failing audits?", **Information Systems Control Journal**, volume 5 (2007): s. 37

Gallegos, Frederick. **Information Technology Control and Audit**. (USA: Auerbach Publications, 2004)

Lawton, Robert. "Transitioning IT From a Compliance to a Value-driven Enterprise Using CobiT", **Information Systems Control Journal**, volume 6 (2007): s. 43

Pironti, John P. "Key Elements of an Information Risk Management Program", **Information Systems Control Journal**, volume 2 (2008): s. 43

Ross, Steven J. "Reliable Security", **Information Systems Control Journal**, volume 5 (2008): s. 9

Swaroop, Shankar. "Managing Multiple Medium and Small Scale Projects in Large IT Organization", **Information Systems Control Journal**, volume 4 (2007): s. 24

Türkiye İç Denetim Enstitüsü. **Uluslararası İç Denetim Standartları ve Mesleki Uygulama Çerçevesi.** (İstanbul: Print Center, 2008)

Diğer Yayınlar

AICPA. **Audit Standards**. www.aicpa.org [03.03.2009]

BDDK. "**Bilgi Sistemleri Denetim Yetkisi Verilen Kuruluşlar**". www.bddk.org.tr [28.03.2009]

BDDK. "**Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ**" (Sayı 26643; Tarih 14 Eylül 2007)

BDDK. "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik**" (Sayı 26170; Tarih: 16 Mayıs 2006)

BDDK. "**Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimine İlişkin Rapor Formatı Hakkında Tebliğine**" (Sayı 26367; Tarih: 5 Aralık 2006)

BDDK. "**Bankaların Destek Hizmeti Almalarına ve Bu Hizmeti Verecek Kuruluşların Yetkilendirilmesine İlişkin Yönetmelik**" (Sayı 26333; Tarih: 1 Kasım 2006)

ISACA. **IT Continuity Planning Audit/Assurance Program**. www.isaca.org [01.03.2009]

ISACA. **IT Audit Standards**. http://www.isaca.org/Template.cfm? Section=Standards& CONTENTID=47286&TEMPLATE=/ContentManagement/ContentDisplay.cfm [03.03.2009]

KPMG. **IDEA Training Course Documents.** (İstanbul: KPMG Turkey, 2005)

KPMG. **CobiT Olgunluk Seviyesi Değerlendirme Aracı El Kitabı.** (İstanbul: KPMG Turkey, 2005)

KPMG. **KPMG's 2009 IT Internal Audit Survey**. (Turkey: KPMG, 2009)

KPMG. **KPMG IT Audit Methodology (KAM)**. www.kworld.com [23.03.2009]

Microsoft. **MSAT Tool**. http://technet.microsoft.com/tr-tr/security/cc185712 (en-us).aspx [15.04.2009]

Önal, Mehmet Zeki. "**An Aggregated Information Technology Checklist for Operational Risk Management**". Yüksek Lisans Tezi. Boğaziçi Üniversitesi Sosyal Bilimler Enstitüsü, 2007.

SPK, "**Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ"** (Seri: X, No: 22)

TUBİTAK UEKAE. **Yedekleme ve İş Sürekliliği Kontrol Listesi**. (Ankara: TUBİTAK, 2007)

EKLER

Ek 1. CobiT Olgunluk Seviyesi Değerlendirme Aracı

DS5: Olgunluk Seviyesi 0 için Anket Soruları						
		Hangi seviyede katılıyorsunuz?				
Seviye	İfadeler	Hiç	Biraz	Oldukça	Tamamiyle	İfadelerin uygunluğuna yönelik değerler
1	Bilgi teknolojileri güvenliğinin gerekliliği konusu kurum tarafından anlaşılmamıştır. Güvenlik konusunda görev ve sorumluluklar kurum içinde belirlenmemiştir.	x				0,00
2	Bilgi teknolojileri güvenlik yönetiminin oluşturulmasına yönelik gerekli adımlar uygulanmamıştır.		x			0,33
3	Bilgi teknolojileri güvenlik raporlaması mevcut olmayıp güvelik açıklarına yönelik aksiyonların belirlenmesine yönelik süreç de mevcut değildir.	x				0,00
4	Sistem güvelik yönetimi kapsamında tanımlı bir süreç eksikliği mevcuttur.	x				0,00
Toplam Değer						**0,33**

DS5: Olgunluk Seviyesi 1 için Anket Soruları						
		Hangi seviyede katılıyorsunuz?				
Seviye	İfadeler	Hiç	Biraz	Oldukça	Tamamiyle	İfadelerin uygunluğuna yönelik değerler
1	Bilgi teknolojileri güvenliğinin gerekliliği konusu kurum tarafından anlaşılmıştır. Bu konudaki farkındalık temel olarak BT çalışanlarının kişisel faaliyetlerine özgüdür.			x		0,67
2	Bilgi teknolojileri güvenliği kapsamındaki faaliyetler reaktif olarak sağlanmaktadır.			x		0,67
3	Bilgi teknolojileri güvenlik seviyesi ölçümlenmemektedir. Sorumluluklar açık olarak belirlenmediğinden, tespit edilen güvenlik vakaları atanan kişiler vasıtasıyla çözümlenmektedir.		x			0,33
4	Güvenlik vakalarının çözümüne yönelik cevaplar standart ve önceden öngörülebilen çözümler değildir.	x				0,00
Toplam Değer						**1,67**

DS5: Olgunluk Seviyesi 2 için Anket Soruları						
		Hangi seviyede katılıyorsunuz?				
Seviye	İfadeler	Hiç	Biraz	Oldukça	Tamamiyle	İfadelerin uygunluğuna yönelik değerler
1	Bilgi teknolojileri güvenliğine yönelik görev ve sorumluluklar belirlenmiş olup güvenlikten sorumlu bir koordinatöre atama yapılmıştır. Ancak koordinatörün yönetim otoritesi sınırlı tutulmuştur.	x				0,00
2	Bilgi teknolojileri güvenlik ihtiyacına yönelik farkındalık sınırlı olmak kaydıyla kurumda oluşmuştur.			x		0,67
3	gereken bilgiler oluşturulmasına rağmen bilgilere yönelik güvenlik ihtiyaçları analiz edilmemektedir.		x			0,33
4	Services from third parties may not address the specific security needs of the organisation. Security policies are being developed, but skills and tools are inadequate.				x	1,00
5	Bilgi teknolojileri güvenliğine yönelik raporlama eksik, yanıltıcı ve sürekli değildir.			x		0,67
6	Bilgi güvenliğine yönelik eğitim mevcut olmasına rağmen, sadece başlangıç seviyesinde yeni çalışanlara verilmektedir.		x			0,33
7	Bilgi teknolojileri güvenliğinin sağlanması ve yönetimi temel olarak Bilgi Teknolojileri bölümünün görev sorumlulukları altında görülmektedir. İş tarafının bu konu kapsamında katkısı mevcut değildir.				x	1,00
Toplam Değer						**4,00**

DS5: Olgunluk Seviyesi 3 için Anket Soruları						
		Hangi seviyede katılıyorsunuz?				
Seviye	İfadeler	Hiç	Biraz	Oldukça	Tamamiyle	İfadelerin uygunluğuna yönelik değerler
1	Bilgi güvenliğine yönelik farkındalık mevcut olup yönetim tarafından desteklenmektedir.			x		0,67
2	Bilgi teknolojileri güvenliğine yönelik prosedürler tanımlanmış ve bilgi güvenliği politikasına uyumlu hale getirilmiştir.		x			0,33
3	Bilgi teknolojileri güvenliğine yönelik sorumluluklar ve kurallar belirlenmiş, atanmış ve anlaşılmıştır. Ancak kurum genelinde uygulanmasına yönelik zorundalıklar tesis edilmemiştir.		x			0,33
4	Risk analizi kapsamında bilgi teknlojileri güvenlik planı ve çözümleri oluşturulmuştur.	x				0,00
5	Bilgi güvenliğine yönelik raporlama, iş tarafına ait konulara açık bir şekilde odaklanmamıştır.			x		0,67
6	İhtiyaca yönelik güvenlik testleri (sızma testi vb.) gerçekleştirilmektedir.	x				0,00
7	Bilgi güvenliği eğitimi, Bilgi Teknolojileri bölümü ve iş tarafı için mevcut olup düzenli olarak zamanlanmamakta ve yönetilmemektedir.	x				0,00
Toplam Değer						**2,00**

DS5: Olgunluk Seviyesi 4 için Anket Soruları						
		seviyede katılıyorsunuz				
Seviye	İfadeler	Hiç	Biraz	Oldukça	Tamamiyle	İfadelerin uygunluğuna yönelik değerler
1	Bilgi güvenliğine yönelik sorumluluklar açık olarak belirlenmiş, zorunlu hale getirilmiş ve yönetilebilir seviyeye getirilmiştir.		×			0,33
2	Bilgi teknolojileri güvenliğine yönelik risk ve etki analizi düzenli olarak yapılmaktadır.		×			0,33
3	Spesifik güvenlik temellerine bağlanarak güvenlik politika ve prosedürleri tamamlanmıştır.		×			0,33
4	Bilgi güvenliğine yönelik farkındalığın kurum genelinde arttırılmasına yönelik uygulamalar zorunlu hale getirilmiştir.	×				0,00
5	Kullanıcı belirleme, kimlik doğrulama ve yetkilendirme süreçleri standart hale getirilmiştir.			×		0,67
6	Güvenlik denetimine ve yönetimine yönelik sorumlu tutulan çalışanlardan sertifikasyon aranmaktadır.	×				0,00
7	Güvenlik testleri düzenli ve standart olarak gerçekleştirilmekte ve sonuçlar kurum genelinde güvenlik seviyesinin arttırılmasında yardımcı		×			0,33
8	Bilgi teknolojileri güvenlik birimi kurum genelinde oluşturulmuş olup bilgi güvenliğine yönelik süreçler bu bölüm tarafından koordine edilmektedir.	×				0,00
9	İş hedefleri ile uygun olarak bilgi teknolojileri güvenlik raporlaması yapılmaktadır.	×				0,00
10	İş tarafı ve BT bölümü kapsamında bilgi teknolojileri güvenlik eğitimleri yapılmaktadır.	×				0,00
11	Bilgi teknolojileri güvenlik eğitimleri planlanmakta ve düzenli olarak ilgili eğitim faaliyetleri yönetilmektedir. Eğitimler iş ihtiyaçlarına ve risk profiline cevap verecek şekilde oluşturulmaktadır.	×				0,00
12	Bilgi güvenliği yönetimi kapsamında performans kriterleri ve anahtar hedefler belirlenmiş, fakat ölçümlenmemektedir.	×				0,00
Toplam Değer						2,00

DS5: Olgunluk Seviyesi 5 için Anket Soruları						
		Hangi seviyede katılıyorsunuz				
Seviye	İfadeler	Hiç	Biraz	Oldukça	Tamamiyle	İfadelerin uygunluğuna yönelik değerler
1	Bilgi teknolojileri güvenliği BT ve iş tarafının ortak sorumluluğu olup entegre olarak kurumun güvenlik hedeflerine uygun olarak yönetilmektedir.	x				0,00
2	Bilgi teknolojileri güvenlik gereksinimleri açık olarak tanımlanmış ve optimize edilmiştir. Bu gereksinimler, bilgi teknolojileri güvenlik planına da dahil edilmiştir.	x				0,00
3	Kullanıcıları ve müşteriler güvenlik gereksinimlerinin belirlenmesinde dahil edilmekte ve geliştirilen uygulamaların tasarım aşamasında güvenlik fonsiyonalitesi sağlanmaktadır.	x				0,00
4	Güvenlik vakaları vaka yönetim sürecine entegre olarak otomatik yazılım araçları ile takip edilmektedir.	x				0,00
5	Bilgi teknolojileri güvelik planının uygulanmasındaki etkinliğin değerlendirilmesi açısından periyodik olarak güvenlik değerlendirmesi yapılmaktadır.	x				0,00
6	Bilgi güvenliğine yönelik tehdit ve zayıflıklara karşı bilgiler kurum genelinde sistematik olarak toplanmakta ve gerekli önlemler için analiz	x				0,00
7	Güvenlik risklerini azaltmak için yeterli kontroller belirlenmekte, duyurulmakta ve uygulanmaktadır.	x				0,00
8	Sürekli iyileşme için güvenlik testleri, ana sebep analizi ve vakalara karşı proaktif çözümler	x				0,00
9	Güvenlik süreçleri ve teknolojileri organizasyon seviyesinde entegre edilmiştir. Bu kapsamdaki performans kriterleri ve hedefler incelenmekte, analiz edilmekte ve sonuçlar ilgililere duyurulmaktadır.	x				0,00
10	Yönetim performans göstergelerinden ve hedeflerinden faydalanarak güvenlik planının sürekli iyileşme kapsamında uygulanmasını sağlamaktadır.	x				0,00
Toplam Değer						0,00

DS5: Olgunluk Seviyesinin Hesaplanma Yöntemi					
Olgunluk Seviyesi (N)	İfadelerin Uygunluğuna Yönelik Değerlerin Toplamı (A)	Olgunluk Seviyelerinin Değerlendirilmesi Yönelik İfadelerin Toplamı (B)	Olgunluk Seviyesi Uygunluk Değeri =X (A/B)	Normalize Edilen Uygunluk Değeri = Y X/∑X	Olgunluk Seviyesine Yapılan Katkı (N*Y)
0	0,33	4	0,08	0,05	0,00
1	1,67	4	0,42	0,27	0,27
2	4,00	7	0,57	0,37	0,73
3	2,00	7	0,29	0,18	0,55
4	2,00	10	0,20	0,13	0,51
5	0,00	12	0,00	0,00	0,00
Toplam X ve Y Değerleri			1,56	1,00	
Olgunluk Seviyesi					**2,07**

ÖZGEÇMİŞ

Kişisel Bilgi

Cinsiyet	Erkek
Doğum Tarihi ve Yeri	08.03.1982/ İstanbul
Sürücü Belgesi	B sınıfı

Eğitim

Üniversite (Yüksek Lisans)	Yıldız Teknik Üniversitesi 1- İşletme Yönetimi (Halen devam ediyor)
Üniversite (Lisans)	Boğaziçi Üniversitesi 1- Yönetim ve Bilişim Sistemleri 2- Uluslararası Ticaret (Çift Ana Dal Programı)

Nitelikler

Yabancı Dil	İngilizce - Akıcı Almanca - Başlangıç Düzeyi
Bilgisayar Bilgisi	Microsoft Office Tools, C, C++, Java, HTML, DHTML, XML, ASP, MS FrontPage, VBScript, JavaScript, Flash, Adobe Photoshop, SPPS, Dome, Sybase, Expert Choice, MS SQL Server, UML, Network Systems: LAN, WAN. ERP sistemleri hakkında genel bilgi: SAP, Microsoft AXAPTA
Sertifikalar / Eğitimler	* Bilgi Sistemleri Denetçisi Sertifikası (CISA) * Bilgi Sistemleri Denetimi ve Kontrolü Kurumu Üyeliği (ISACA) * Mainframe/RACF ve AS400 konulu eğitim sertifikaları

İş Tecrübesi

KPMG

Ağustos 2005 tarihinde KPMG firmasında çalışmaya başlamış bulunmakta ve bilgi sistemleri denetimi, bilgi riskleri yönetimi ve bilgi sistemleri danışmanlığı alanlarında tecrübe sahibidir. BDDK'nın bilgi sistemleri denetimi konulu tebliğine yönelik BS denetimi, BT genel kontrolleri, uygulama kontrolleri ve süreç analizine yönelik denetimler, Sarbanes-Oxley (SOX) denetimleri ve bu konulara yönelik danışmanlık servislerinde tecrübe sahibidir. Bunun yanında tecrübe sahibi olduğu sektörler, bankacılık ve finansal servisler, telekomünikasyon, perakende ve çeşitli üretim sektörleridir.

Referanslar

Tanıl Durkaya	KPMG, Manager
Erol Lengerli	KPMG, Partner