

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
MUHASEBE FİNANSMAN BİLİM DALI

**SÜREKLİ DENETİMDE DİJİTAL ANALİZ TEKNİĞİNİN
KULLANILMASI VE BİR UYGULAMA**

Doktora Tezi

HÜLYA BOYDAŞ HAZAR

İstanbul, 2013

T.C.
MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
İŞLETME ANABİLİM DALI
MUHASEBE FİNANSMAN BİLİM DALI

**SÜREKLİ DENETİMDE DİJİTAL ANALİZ TEKNİĞİNİN
KULLANILMASI VE BİR UYGULAMA**

Doktora Tezi

HÜLYA BOYDAŞ HAZAR

Danışman: PROF. DR. NEJAT BOZKURT

İstanbul, 2013

MARMARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜ

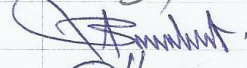
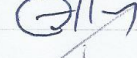
TEZ ONAY BELGESİ

İŞLETME Anabilim Dalı MUHASEBE FİNANSMAN Bilim Dalı DOKTORA öğrencisi HÜLYA BOYDAŞ HAZAR'ın SÜREKLİ DENETİMDE DİJİTAL ANALİZ TEKNİĞİNİN KULLANILMASI VE BİR UYGULAMA adlı tez çalışması, Enstitümüz Yönetim Kurulunun 28.06.2013 tarih ve 2013-24/18 sayılı kararıyla oluşturulan jüri tarafından oy birliği / oy çokluğu ile Doktora Tezi olarak kabul edilmiştir.

Tez Savunma Tarihi 13 / 9 / 2013

Öğretim Üyesi Adı Soyadı

İmzası

1. Tez Danışmanı	Prof. Dr. NEJAT BOZKURT	
2. Jüri Üyesi	Prof. Dr. DOĞAN ARGUN	
3. Jüri Üyesi	Prof. Dr. ŞAHAMET BÜLBÜL	
4. Jüri Üyesi	Doç. Dr. VOLKAN DEMİR	
5. Jüri Üyesi	Prof. Dr. HASAN TÜRELİ	

GENEL BİLGİLER

İsim ve Soyadı	: Hülya Boydaş Hazar
Anabilim Dalı	: İşletme
Programı	: Muhasebe Finansman
Tez Danışmanı	: Prof. Dr. Nejat Bozkurt
Tez Türü ve Tarihi	: Doktora – Eylül 2013
Anahtar Kelimeler	: Sürekli Denetim, Dijital Analiz, CAATTs, ACL

ÖZET

SÜREKLİ DENETİMDE DİJİTAL ANALİZ TEKNİĞİNİN KULLANILMASI VE BİR UYGULAMA

Sürekli denetim bilgisayar ortamındaki verileri dijital analiz teknikleri kullanarak gerçek zamanlı değerlendiren ve doğruluğuna ilişkin yazılı güvence veren bir denetim yöntemidir. Bu çalışmada sürekli denetim kavramı, modelleri, hukuki çerçeve, uygulama geliştirmek için atılması gereken adımlar, veri analizinde kullanılan dijital analiz teknikleri, ilgili bilgisayar teknolojileri ve bugüne kadar geliştirilmiş belli başlı uygulamalar incelenmiştir. Bu bilgilerin ışığında bir sürecin sürekli denetiminin yapılabilmesi için ACL denetim yazılımı ile bir uygulama geliştirilmiştir. Bu çalışmaya konu olan uygulamada bilgi sistemlerinde, iş süreçlerinde ve kurumsal politikalarda değişiklik yapılmadan denetim etkinliğinin sağlanabileceği gösterilmiştir. Bir kurumun çalışma düzeninin herhangi bir aşamasına başlangıçta müdahale edilmeden dijital analiz teknikleri kullanılarak sürekli denetimin yapılabilmesi bilindiği kadarıyla ilk defa bu çalışmada gerçekleşmiştir. Bu da sürekli denetim yönteminin yaygınlaşması yolunda önemli bir adımdır.

GENERAL KNOWLEDGE

Name and Surname : Hülya Boydaş Hazar
Field : Business Administration
Programme : Accounting Finance
Supervisor : Professor Nejat Bozkurt
Degree Awarded and Date : PhD – September 2013
Keywords : Continuous Audit, Digital Analysis, CAATs, ACL

ABSTRACT

USING DIGITAL ANALYSIS TECHNIQUES IN CONTINUOUS AUDIT AND AN APPLICATION

Continuous audit is an auditing technique which makes a real time assessment of the accuracy of digital data using digital analysis techniques and produces a written report. In this thesis continuous audit concept, related models, legal framework, steps to take to develop an application, digital analysis techniques, related computer technologies and applications that were previously developed are analyzed. A continuous audit application is developed for a business process using the digital analysis tools of ACL audit software. Alterations were not made to the related information systems, business processes nor corporate policies to ensure the effectiveness of the application in question. This application is the first application of continuous audit where no adjustments were made to the business proceedings prior to its development. This is an important step towards increasing the usage of continuous audit method.

ÖNSÖZ

Sürekli denetim bilgisayar ortamındaki verileri dijital analiz teknikleri kullanarak gerçek zamanlı değerlendiren ve doğruluğuna ilişkin yazılı güvence veren bir denetim yöntemidir. Bu çalışmamda sürekli denetim kavramını, modellerini, hukuki çerçevesini, uygulama geliştirmek için atılması gereken adımları, veri analizinde kullanılan dijital analiz tekniklerini, ilgili bilgisayar teknolojilerini ve bugüne kadar geliştirilmiş belli başlı uygulamaları inceledim. Bu bilgilerin ışığında bir sürecin sürekli denetiminin yapılabilmesi için ACL denetim yazılımı ile bir uygulama geliştirdim. Bu uygulama yeni bir yaklaşım ile sürekli denetim uygulamaları geliştirirken bilgi sistemlerinde, iş süreçlerinde ve kurumsal politikalarda değişiklik yapılmadan denetim etkinliğinin sağlanabileceğini göstermiştir.

Bu çalışmayı yapmamı öneren ve yönlendiren değerli danışman hocam Prof. Dr. Nejat Bozkurt'a, görüşleri ile katkıda bulunan değerli hocalarım Prof. Dr. Doğan Argun ve Prof. Dr. Şahamet Bülbül'e çok teşekkür ederim.

Kullandığım kaynakçaların önemli bir kısmının temin edilmesinde emeği geçen Dr. Üstün Çelikler'e çok teşekkür ederim.

Uygulama geliştirme sürecinde ihtiyaç duyduğum tüm kurumsal bilgiyi benimle paylaşan Ankara Çelik A.Ş. genel müdürü Ersun Bener'e, iş süreçlerini ayrıntısıyla gösteren satın alma sorumlusu Hüseyin Korkmaz'a, kurumsal veriyi tanıtan muhasebe şefi Gülsen Süslü ve muhasebe sorumlusu Özgür Sönmez'e çok teşekkür ederim.

ACL kullanarak kendi sürekli denetim modelimi oluştururken benden hiçbir desteği esirgemeyen Komtaş Bilgi Yönetimi A.Ş. genel müdürü Yüksel Çomak'a, satış yöneticisi Gizem Yıldırım'a, danışman Mert Şener'e, Ankara Şubesi yönetici ve programcılarına çok teşekkür ederim.

Tüm doktora çalışmam sürecinde her zaman yanımda olan ve desteğini esirgemeyen eşim Op. Dr. Hovsep Hazar'a ve tüm aile bireylerime çok teşekkür ederim.

İstanbul, 2013

Hülya Boydaş Hazar

İÇİNDEKİLER

Sayfa No.

TABLO LİSTESİ	x
ŞEKİL LİSTESİ	xi
KISALTMALAR	xii
1. GİRİŞ	1
2. SÜREKLİ DENETİME İLİŞKİN GENEL BİLGİLER	3
2.1. SÜREKLİ DENETİMİN TANIMI	3
2.2. SÜREKLİ DENETİM İLE GELENEKSEL DENETİM ANLAYIŞI ARASINDAKİ FARKLAR	10
2.3. SÜREKLİ DENETİMİN YARARLARI	11
2.4. SÜREKLİ DENETİMİN TARİHÇESİ.....	14
3. GÜNÜMÜZDE DENETİM ORTAMI VE SÜREKLİ DENETİMİN YERİ	17
3.1. GÜNÜMÜZDE DENETİM ORTAMI	17
3.2. SÜREKLİ DENETİMİN YÖNETİM FAALİYETLERDEKİ ROLÜ	21
3.3. SÜREKLİ GÜVENCE, SÜREKLİ İZLEME VE SÜREKLİ DENETİM İLİŞKİSİ.....	23
3.3.1. Sürekli Güvence	23
3.3.2. Sürekli İzleme	24
3.3.3. Sürekli Denetim	26
3.4. SÜREKLİ DENETİMİN İKİ ANA BİLEŞENİ: KONTROL VE RİSK	30
3.4.1. Sürekli Kontrol Değerlendirmesi (Continuous Control Assessment)	30
3.4.2. Sürekli Risk Değerlendirmesi (Continuous Risk Assessment).....	33
4. DENETİM STANDARTLARI VE HUKUKİ ÇERÇEVE	35
4.1. DENETİM STANDARTLARI.....	35
4.2. ULUSLARARASI DENETİM STANDARTLARINI BELİRLEYEN KURUMLAR.....	36
4.3. SARBANES-OXLEY KANUNU	38
4.4. AMERİKA BİRLEŞİK DEVLETLERİ'NDE DENETİM İLE İLGİLİ KURUMLAR VE UYGULANAN STANDARTLAR	41
4.5. TÜRKİYE'DEKİ DENETİM MEVZUATI VE SÜREKLİ DENETİMİN HUKUKİ ÇERÇEVESİ	43
4.5.1. 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu	44
4.5.2. Sermaye Piyasası Kurulu Düzenlemeleri	45
4.5.3. Bankacılık Kanunu	47
4.5.4. Türk Ticaret Kanunu ve Türkiye Finansal Raporlama Standartları.....	48
5. SÜREKLİ DENETİM MODELLERİNİN DEĞERLENDİRİLMESİ	49
5.1. SÜREKLİ DENETİM MODELLERİ.....	49
5.1.1. Groomer ve Murthy'nin Sürekli Denetim Modeli	49
5.1.2. Woodroof ve Searcy'nin Sürekli Denetim Modeli	51

5.1.3. Rezaee ve Arkadaşlarının Sürekli Denetim Modeli.....	55
5.1.4. Onions'ın Sürekli Denetim Modeli	58
5.1.5. Vasarhelyi, Alles ve Kogan'ın Sürekli Denetim Modeli	61
5.1.6. Coderre'nin Sürekli Denetim Modeli.....	63
5.1.7. Chou, Du ve Lai'nin Sürekli Denetim Modeli	65
5.1.8. Du ve Roohani'nin Sürekli Denetim Modeli.....	69
5.1.9. Yeh ve Shen'nin Sürekli Denetim Modeli	74
5.1.10. Baksa ve Turoff'un Sürekli Denetim Modeli	74
5.1.11. Ye ve Li'nin Sürekli Denetim Modeli.....	78
5.2. SÜREKLİ DENETİM MODELLERİNDE ÖNE ÇIKAN KONULAR.....	80
5.2.1. Sürekli Denetim Sistemlerinde Gömülü Denetim Modüllerinin Kullanılması	80
5.2.2. XML'in Veri Formatı Olarak Benimsenmesi	81
5.2.3. Web Tabanlı Sürekli Denetim Modellerinin Yaygınlaşması.....	82
6. SÜREKLİ DENETİM UYGULAMALARINI GELİŞTİRMEK.....	84
6.1. SÜREKLİ DENETİM UYGULAMALARININ AŞAMALARI.....	84
6.2. SÜREKLİ DENETİM UYGULAMALARINI GELİŞTİRMEK İÇİN ATILMASI GEREKEN ADIMLAR	87
6.2.1. Sürekli Denetim Uygulamalarını Geliştirmek İçin Ön Hazırlık	87
6.2.1.1. Denetim Amaçlarını Tespit Etmek	87
6.2.1.2. Yönetimin Desteğini Almak	89
6.2.1.3. Teknik Bilgiyi Geliştirmek	89
6.2.1.4. Denetim Yazılımını Belirlemek	90
6.2.1.5. İş Süreçlerini Anlamak	90
6.2.1.6. Önemli Kontrol ve Riskleri Belirlemek.....	92
6.2.2. Sürekli Kontrol ve Risk Değerlendirme İlişkisi.....	93
6.2.2.1. Sürekli Kontrol Değerlendirmesi	93
6.2.2.1.1. Kontrol Amaçlarının Tespiti	96
6.2.2.1.2. Önemli Kontrollerin Tespiti	96
6.2.2.1.3. Kontrollerin Test Edilmesi	96
6.2.2.2. Sürekli Risk Değerlendirmesi	97
6.2.2.2.1. Kurumsal Risk Yönetiminin Değerlendirilmesi	98
6.2.2.2.1.1. Olası Riskleri Anlamak	98
6.2.2.2.1.2. Risk Türleri ve Sonuçları	99
6.2.2.2.1.4. Risk Seviyesini Değerlendirmek	101
6.2.2.2.1.5. Veri Toplamak ve Analiz Etmek	102
6.2.3. Sürekli Denetim Modelini Oluşturmak	102
6.2.3.1. Test Kapsamını Belirlemek.....	102
6.2.3.2. Bilgi Kaynaklarını Belirlemek	102
6.2.3.3. Denetim Kanıtlarını Belirlemek	103
6.2.3.4. Denetimin Zamanlaması	104
6.2.4. Veri Erişimi	105
6.2.4.1. Veri Erişim Yöntemleri	105
6.2.4.2. Verinin Yerini Belirlemek	106
6.2.4.3. Veri Talebinde Bulunmak.....	107
6.2.4.4. Verinin Denetim Yazılımına Aktarılması.....	107
6.2.5. Veri Analizi.....	108
6.2.5.1. Veri Bütünlüğünü Sağlamak.....	108
6.2.5.2. Dijital Analizler	110

6.2.6. Sonuçları Değerlendirmek	110
6.2.7. Raporlama.....	112
6.2.7.1. Resmi Raporlama	112
6.2.7.2. Olağandışı Durum Notu.....	113
6.3. SÜREKLİ DENETİM UYGULAMALARINI GELİŞTİRİRKEN KARŞILAŞILAN ZORLUKLAR.....	114
6.3.1. Karşılaşılan Sorunlar	115
6.3.1.1. Güvenli Sistem	115
6.3.1.2. Zamanlama.....	116
6.3.1.3. Verinin Saklanması	116
6.3.1.4. Sistem Verimliliği	117
6.3.1.5. Veri Standardizasyonu	118
6.3.1.6. Otomasyon	118
6.3.1.7. Raporlama	118
6.3.1.8. Bilgi Yüklenmesi.....	119
6.3.1.9. Teknolojik Bilgi	119
6.3.1.10. Sistemin Benimsenmesi	119
6.3.1.11. Maliyet	121
6.3.1.12. İşlemlerin Tamamı Üzerinde Denetim Yapılamaması	121
6.3.2. Karşılaşılan Sorunları Gidermek İçin Yapılması Gerekenler	122
7. SÜREKLİ DENETİMDE KULLANILAN DİJİTAL ANALİZ TEKNİKLERİ.....	124
7.1. VERİ İLE İLGİLİ ANALİZLER.....	127
7.1.1. Veri Bütünlüğüne Yönelik Analizler	127
7.1.1.1. Filtreleme (filter or display criteria)	127
7.1.1.2. Tanımlama ve Denklem (expression/equation)	128
7.1.1.3. Boşlukların Tespiti (gaps).....	129
7.1.1.4. İstatistiksel Analiz (statistical analysis).....	129
7.1.1.5. Eş Kayıtların Tespiti (duplicates).....	131
7.1.1.6. Sınıflama ve Sıralama (sorting and indexing).....	131
7.1.2. Veri Hakkında Bilgi Verici Analizler	133
7.1.2.1. Özetleme (summarization).....	133
7.1.2.2. Katmanlara Ayırmak (stratification)	134
7.1.2.3. Tablolama (cross tabulation/pivot tables).....	134
7.1.2.4. Yaşlandırma (aging)	135
7.1.2.5. Birleştirme ve İlişkilendirme (join/relate)	136
7.1.3. Veride Trendleri Tespit Etmeye Yönelik Analizler	136
7.1.3.1. Trend Analizi (trend analysis).....	136
7.1.3.2. Regresyon Analizi (regression analysis)	137
7.1.3.3. Paralel Simülasyon (parallel simulation).....	137
7.1.4. Gelişmiş Analiz Teknikleri.....	138
7.1.4.1. Veri Profillemesi (data profiling).....	138
7.1.4.2. Benford Kanunu (Benford's Law)	139
7.1.4.3. Rakam Analizi (Digital Analysis)	142
7.1.4.4. Devamlılık Denklemi (continuity equations).....	143
7.1.4.5. Kümeleme Analizi (cluster analysis).....	145
7.1.4.6. Kayıt Günlüklerinin İşlem Madenciliği (process mining of event logs)	146
7.2. FAALİYETLER VE SEKTÖR HAKKINDA BİLGİ VERİCİ ANALİZLER	148
7.2.1. Oran Analizi (ratio analysis).....	148

7.3. ÇEŞİTLİ KONULAR İÇİN DİJİTAL TEKNİKLER.....	149
7.3.1. Otomatik Doğrulama (Automatic Confirmation)	149
7.3.2. Dijital Analizde Kullanılan Örneklem Yöntemleri	149
8. SÜREKLİ DENETİM VE BİLGİ SİSTEMLERİ	150
8.1. SÜREKLİ DENETİMDE ÖNE ÇIKAN TEKNOLOJİK GELİŞMELER	150
8.1.1. Bilgi Girişi	150
8.1.2. Veri Formatında Standardizasyon.....	150
8.1.3. Veri Saklama.....	151
8.1.4. Veri Ambarı (Data Warehouse)	151
8.1.5. Bilgisayar Ağ Teknolojileri	152
8.1.6. Şifreleme.....	153
8.1.7. Yapay Zeka	153
8.1.8. Karar Destek Sistemleri.....	154
8.1.8.1. Karar Destek Sistemleri İle Veri Madenciliği (Data Mining)	155
8.1.8.2. Karar Destek Sistemleri İle Metin Madenciliği (Text Mining)	157
8.1.8.3. Karar Destek Sistemlerinde Veri Profillem Analiz Tekniğinin Kullanılarak Bilgi Sistemlerine İzinsiz Girişlerin Önlenmesi	158
8.1.9. Uzman Sistemler	161
8.2. SÜREKLİ DENETİMDE KULLANILAN DENETİM YAZILIMLARI	162
8.2.1. ACL	163
8.2.2. XBRL	169
8.2.3. R.....	172
9. LİTERATÜRDE SÜREKLİ DENETİM UYGULAMALARI.....	174
9.1. AT&T FATURALAMA SİSTEMİ	174
9.2. KANADA KRALİYET ATLI POLİSİ ÖDEMELER DEPARTMANLARI	175
9.3. SIEMENS'İN SAP GÜVENLİK AYARLARI	179
9.4. HCA INC. SÜREKLİ DENETİM UYGULAMASI	179
9.5. T.C. SAYIŞTAY BAŞKANLIĞI BİLGİSAYAR DESTEKLİ DENETİM SİSTEMİ YAZILIMI PROJESİ.....	184
10. UYGULAMA	187
10.1. GENEL BİLGİLER	187
10.1.1. Konu: Araç Takip Sistemlerinin Üretimine İlişkin Satın Alma Döngüsünün Sürekli Denetimi.....	187
10.1.2. İlgili Kurumun Tanıtımı	187
10.1.3. Araç Takip Sistemleri Hakkında Genel Bilgiler	188
10.1.4. Araç Takip Projeleri Hakkında Genel Bilgiler	188
10.2. SATIN ALMA DÖNGÜSÜ VE DİJİTAL ORTAMDA DENETİMİ.....	189
10.2.1. Satın Alma Döngüsünün Tanımı.....	189
10.2.2. Satın Alma Süreci	189
10.2.2.1. Satın Alma Sürecinin İşleyişi.....	189
10.2.2.2. Satın Alma Sürecinde Hata ve Hilenin İşleyişi.....	191
10.2.3. Denetim Kanıtı Olarak Kullanılabilecek Belge ve Raporlar	193
10.2.4. Satın Alma Döngüsünde Hesapların İşleyişi	197
10.2.5. Satın Alma İşlemlerinde Kontrol Testleri	198

10.2.5.1. Geçerlilik.....	198
10.2.5.2. Tamlık - Bütünlük	198
10.2.5.3. Doğruluk	199
10.2.5.4. Sınıflandırma.....	200
10.2.5.5. Zamanlılık	200
10.2.5.6. Yetkilendirme	201
10.2.5.7. Görev Ayrımları	202
10.2.5.8. Özetleme	203
10.3. SÜREKLİ DENETİM UYGULAMASINI GELİŞTİRMEK İÇİN ÖN HAZIRLIK	204
10.3.1. Denetim Amacı	204
10.3.2. Yönetimin Desteği.....	204
10.3.3. Teknik Bilgi	205
10.3.4. Denetim Yazılımı	205
10.3.5. İş Süreçleri	206
10.3.6. Önemli Kontrol ve Riskleri Belirlemek	211
10.4. SÜREKLİ DENETİM MODELİNİ OLUŞTURMAK	213
10.4.1. Test Kapsamı	213
10.4.2. Bilgi Kaynakları.....	213
10.4.3. Denetim Kanıtları.....	213
10.4.4. Denetimin Zamanlaması.....	216
10.5. VERİ ERİŞİMİ	217
10.5.1. Veri Erişim Yöntemi	217
10.5.2. Verinin Yeri	217
10.5.3. Veri Talebi	218
10.5.4. Verinin ACL Denetim Yazılımına Aktarılması.....	219
10.6. VERİ ANALİZİ	219
10.6.1. Veri Bütünlüğü.....	220
10.6.2. Dijital Analizler.....	225
10.6.2.1. Geçerlilik Kontrol Testleri	225
10.6.2.2. Tamlık – Bütünlük Kontrol Testleri	228
10.6.2.3. Doğruluk Kontrol Testleri.....	230
10.6.2.4. Sınıflandırma Kontrol Testleri	232
10.6.2.5. Zamanlılık Kontrol Testleri	233
10.6.2.6. Yetkilendirme Kontrol Testleri	233
10.6.2.7. Görev Ayrımları Kontrol Testleri.....	234
10.6.2.8. Özetleme Kontrol Testleri.....	235
10.6.2.9. Benford Analizi	235
10.7. VERİ ANALİZ SONUÇLARI VE RAPORLAMA	236
10.7.1. Genel Bakış	236
10.7.2. Satın Alma Döngüsündeki Kontrol Testlerinin ACL Senaryoları ve Dijital Analizlerin Sonuçları	238
10.7.2.1. Geçerlilik Kontrol Testleri	238
10.7.2.2. Tamlık – Bütünlük Kontrol Testleri	240
10.7.2.3. Doğruluk Kontrol Testleri.....	241
10.7.2.4. Sınıflandırma Kontrol Testleri	246
10.7.2.5. Zamanlılık Kontrol Testleri	247
10.7.2.6. Yetkilendirme Kontrol Testleri	248
10.7.2.7. Görev Ayrımları Kontrol Testleri.....	248
10.7.2.8. Özetleme Kontrol Testleri.....	249
10.7.2.9. Benford Analizi	249

10.8. GELİŞTİRİLEN SÜREKLİ DENETİM UYGULAMASININ ETKİNLİĞİ VE ÖNEMİ	251
10.8.1. Geliştirilen Sürekli Denetim Uygulamasının Etkinliği	251
10.8.2. Geliştirilen Sürekli Denetim Uygulamasının Önemi	251
11. SONUÇ.....	253
EKLER	255
EK 1: Denetim Öncesi Veri Bütünlüğü Analizi	256
EK 2: Kaynak Veri Dosyalarındaki Kolon Adları	258
EK 3: Denetim Tablolarının Alan Formatları	260
EK 4: Filtreler.....	262
EK 5: Sürekli Denetim Uygulamasında Yer Alan Dijital Analizlerin Listesi	263
KAYNAKÇA	264

TABLO LİSTESİ

Sayfa No.

Tablo 1: Vasarhelyi, Alles ve Kogan'ın Sürekli Denetim Modeli'nde Belirtilen Dört Seviye İçin Kullanılan Analiz Teknikleri.....	62
Tablo 2: Gerçek Zamanlı Muhasebe Sistemi ve Sürekli Denetim İçin Kontrol Matrisi	94
Tablo 3: Kurumsal Risk Türleri	100
Tablo 4: Sürekli Denetim Modelinin Uygulanmama Nedenleri	115
Tablo 5: Benford Kanunu'na Göre Bir Sayının İlk Dört Basamağındaki Rakamların Ortaya Çıkış Frekansları.....	140
Tablo 6: Bilgi Sistemine Yetkisiz Erişim Sağlamak İsteyen Kişilerin Yaptıkları Eylemler .	159
Tablo 7: Sürekli Denetim Uygulamalarının Karşılaştırılması	183
Tablo 8: Veri Bütünlüğünün Analizi İçin Uygulanan Testler.....	223
Tablo 9: Veri Bütünlüğü Testlerinin Uygulandığı Tablo Alanları.....	224

ŞEKİL LİSTESİ

Sayfa No.

Şekil 1: Sürekli Denetim	6
Şekil 2: Sürekli Güvence, Sürekli İzleme ve Sürekli Denetimin Kavramsal Modeli	24
Şekil 3: Sürekli Denetim İçin Gerekli Koşullar	28
Şekil 4: Sürekli Denetim İle İlgili Kavramlar.....	30
Şekil 5: Woodroof ve Searcy'nin Sürekli Denetim Modeli	52
Şekil 6: Gerçek Zamanlı Muhasebe Sistemi ve İlgili Denetim İşlemi.....	57
Şekil 7: Onions'ın Önerdiği Sürekli Denetim Modeli	60
Şekil 8: Coderre'nin Modelinde Sürekli Denetim Uygulamaları Geliştirmek İçin Atılacak Adımlar	64
Şekil 9: ABCAM - Dijital Ajan Temelli Sürekli Denetim Modeli.....	68
Şekil 10: Genel Bakış - Finansal Tabloların Bağımsız Denetimi İçin Sürekli Denetim Modeli	70
Şekil 11: XML (SOAP) Tabanlı Sürekli Denetim Süreci	72
Şekil 12: CORBA İle Sürekli Denetim Süreci	73
Şekil 13: CAIMOR'un Yapısı	79
Şekil 14: Sürekli Denetim Evreleri ve İşleyişi	86
Şekil 15: Satın Alma Sürecindeki İşlemlerin Akışı	196
Şekil 16: Satın Alma ve Ödeme Döngüsündeki Hesapların İşleyişi.....	197
Şekil 17: Araç Takip Sistemi Projelerinin Üretim Öncesi Hazırlık Dönemini Gösteren İş Akışı	207
Şekil 18: Üretim Sürecinde Yapılan Satın Alma ve Stok Hareketleri	209
Şekil 19: Kurumun Satın Alma Döngüsü.....	210

KISALTMALAR

ACFE	Dolandırıcılık Mfettiřleri Birlięi (Association of Fraud Examiners)
AICPA	Amerikan Sertifikalı Kamu Muhasebecileri Enstits (American Institute of Certified Public Accountants)
CAAT	Bilgisayar Destekli Denetim Teknikleri (Computer Assisted Auditing Tests)
CAATT's	Bilgisayar Destekli Denetim Ara ve Teknikleri (Computer Aided Audit Tools and Techniques)
CICA	Kanadalı Yetkili Muhasebeciler Enstits (Canadian Institute of Chartered Accountants)
CobiT	Bilgi ve İlgili Teknolojiler İin Kontrol Hedefleri (Control objectives for information and related Technology)
COSO	Sponsor Kurumlar Komisyonu'nun (The Committee of Sponsoring Organizations)
CPAS	Srekli İřlem Denetim Sistemi (Continuous Process Auditing System)
EAM	Gml Denetim Modlleri (Embedded Audit Modules)
EDI	Elektronik Veri Alıřveriři (Electronic Data Interchange)
EFT	Elektronik Dosya Transferi (Electronic File Transfer)
GAIN	Global Denetim Bilgi Aęı'nın (Global Audit Information Network)
IAASB	Uluslararası Denetim ve Gvence Standartları Kurulu (International Auditing and Assurance Standards Board)
IAPS	Uluslararası Denetim alıřmaları Aıklamaları (International Auditing Practice Statements)
IFAC	Uluslararası Muhasebeciler Federasyonu (International Federation of Accountants)
INTOSAI	Yce Denetim Kurumları Uluslararası rgt (International Organization of Supreme Audit Institutions)
ISA	Uluslararası Denetim Standartları (International Standards of Auditing)
ISACA	Bilgisayar Sistemleri Denetim ve Kontrol Enstits (Information Systems Audit and Control Association-ISACA)
ISO	Uluslararası Standartlar Kurumu'nun (International Organization for Standardization)
PCAOB	Halka Aık řirketler Muhasebesi Gzetim Komisyonu (Public Company Accounting Oversight Board-PCAOB)
SAS	Denetim Standartları Aıklamaları (Statements of Auditing Standards)
SEC	Sermaye Piyasası Kurulu (Securities and Exchange Commission)

1. GİRİŞ

Yaşanan ekonomik skandallar yatırımcıların büyük kayıplarıyla sonuçlanmış, finansal piyasalara güven sarsılmıştır. Ekonomik skandallar sonrası yaşanan iflaslar önemli miktarlarda işten çıkarmalara neden olmuş ve toplumsal sorunlara yol açmıştır. Bu skandallar toplumun yatırım yapma ve kurumların denetimlerine yönelik algısını değiştirmiştir. 2000’li yıllarda Amerika Birleşik Devletleri’nde yaşanan Enron, WorldCom ve Madoff finansal skandalları tüm dünyayı derinden etkileyen örnekler olmuşlardır. 2001 yılında enerji devi Enron finansal tablolarında yapılan hileler ve usulsüzlükler nedeniyle iflas etmiştir. Enron’un hisseleri 90 USD’den (2000 yılı) 15 cent’e düşmüş, 5600 kişi işini kaybetmiştir. Hissedarların kaybının 60 milyar USD ve çalışanların emeklilik payı olarak kaybının 2 milyar USD olduğu tahmin edilmektedir. Bu skandalın bir diğer vahim tarafı Enron’un bağımsız denetiminden sorumlu Arthur Andersen firmasının hileli işlemlerden haberdar olması ve buna göz yummuş olmasıdır. 2002’de varlıklarının değeri 107 milyar USD’yi bulan telekomünikasyon devi WorldCom’un yöneticilerinin finansal tablolarda 11 milyar USD hile yaptıkları ortaya çıkmıştır. Firma iflasını istedikten sonra 30 bin kişi işsiz kalmıştır. NASDAQ’ın eski başkanı yatırımcı Bernard Madoff 2008 yılında tutuklandığında 4800 müşterisinden yüksek kazançlı yatırım yapma vaadiyle 65 milyar USD civarında para topladığını ancak hiçbir yere yatırım yapmadığını itiraf etmiştir. Aslında Madoff 1990’ların ortalarından beri finansal piyasalarda işlem yapmamış, müşterilerinden yatırım yapması için aldığı parayı bir başka müşterisine faiz kazancı olarak vermiştir. Bu paranın bir bölümü yatırımcılara iade edilmiş olmasına rağmen 18 milyar USD’lik kısmı kayıptır. Madoff skandalı tarihteki en büyük yatırım skandalı olarak kabul edilmekte olup sermaye piyasalarının denetimi ve düzenleyici kurumların etkinliğini tartışmaya açmıştır. Bu üç skandalın sadece maddi kaybı 91 milyar USD¹ olmuştur. Bu da Türkiye’nin 2011 yılı gayri safi yurtiçi hasılasının² %12’si kadardır. Bu skandalların yarattığı işsizlik ve güvensizlik ortamı maliyeti daha da arttırmaktadır.

Finansal piyasaların güvenilirliği ve sağlamlığı ekonomik zenginlik ve gelişme için önemlidir. Bu nedenle ekonomik skandallar sadece birkaç yatırımcının değil küresel ekonominin zarar görmesine yol açmıştır. Finansal tablolardaki hileleri arama, bulma ve raporlama denetimin görevi olduğu için denetim mekanizmasının iyi çalışması yatırımcı

¹ Enron 62 milyar USD + WorldCom 11 milyar USD + Madoff 18 milyar USD = 91 milyar USD

² Türkiye’nin 2011 yılı cari fiyatlarla gayri safi yurtiçi hasılası 772 298 milyon USD. Kaynak: T.C. Türkiye İstatistik Kurumu Haber Bülteni sayı: 66, 2 Nisan 2012.

inancı ve toplumun güvenini sağlayan başlıca değer olarak ortaya çıkmıştır. Ekonomik skandallar denetimin önemini ortaya çıkartmış, denetim anlayışını değiştirmiş ve denetim standartlarının değişmesine yol açmıştır.

İş dünyası 1990’larda gelişen bilgisayar teknolojilerine paralel önemli değişiklikler geçirmiştir. İnternet ve çevrimiçi (online) sistemler bilgi ve belge transferinde kolay, ucuz ve hızlı bir ortam sağladığı için kısa zamanda benimsenmiş ve yaygınlaşmıştır. “Elektronikleşme” ve e-ticaretin gelişmesi ile birlikte “kağıtsız” muhasebe sistemleri dönemine geçilmiştir. Elektronik Veri Alışverişi (Electronic Data Interchange, EDI) ve Elektronik Dosya Transferi (Electronic File Transfer, EFT) teknolojilerinin kullanılmasıyla kağıt üzerindeki muhasebe belgeleri yerini e-belgeye bırakmıştır. Bunun sonucu olarak denetlenen belgelerin kaynakları “kağıt” ortamdan “elektronik” ortama kaymıştır. Denetçiler de elektronik ortamda kanıt toplamak ve test etmek zorunda kalmışlardır.³

Ayrıca, günümüz iş yaşamında hızlı ve doğru karar alabilmek rekabet üstünlüğü yaratmaktadır. “Doğru kararlar verebilmek, bilginin kalitesine ve zamanında elde edilebilmesine bağlıdır.”⁴ Bu nedenle daha kısa sürede daha çok verinin etkin biçimde analizi anlayışı önem kazanmaya başlamıştır. Ancak, bu analizlerin kuruma değer yaratması için analiz edilen verinin doğru ve güvenilir olduğundan emin olunmalıdır. Bu nedenle bu verinin etkin ve hızlı bir denetim sürecinden geçmesi gerekmektedir.

Günümüz koşulları ve denetim anlayışındaki değişiklikler geleneksel denetimden gerçek zamanlı elektronik denetime geçişi hızlandırmıştır. Denetimin gerçek zamanlı ve bilgi sistemleri ile otomatik olarak yapılabilmesi kavramına sürekli denetim adı verilmektedir.

Bu çalışmada sürekli denetim kavramı, modelleri, hukuki çerçeve, uygulama geliştirmek için atılması gereken adımlar, veri analizinde kullanılan dijital analiz teknikleri, ilgili bilgisayar teknolojileri ve bugüne kadar geliştirilmiş belli başlı uygulamalar incelenmiştir. Bu bilgilerin ışığında ACL denetim yazılımı kullanılarak bir sürekli denetim uygulaması geliştirilmiştir.

³ Stephen Flowerday, Adrian Blundell ve Rossouw Von Solms. “Continuous Auditing Technologies and Models: A Discussion”, Computers & Security. 25 (2006):326.

⁴ İsa Cankar, “Denetimin Yeni Paradigması: Sürekli Denetim”. Sayıştay Dergisi 61 (2006): 69.

2. SÜREKLİ DENETİME İLİŞKİN GENEL BİLGİLER

2.1. SÜREKLİ DENETİMİN TANIMI

Literatürde sürekli denetimin tanımı tek değildir. Temel kavramda ortak noktaya gelmelerine karşın araştırmacıların sürekli denetim tanımı birbirinden farklılaşmaktadır.

Miklos Vasarhelyi 1991 tarihli çalışmasında sürekli denetimi “belli bir olay olduktan hemen sonra veya kısa bir süre sonra denetiminin yapılması” olarak tanımlar.

Helms ve Mancino 1999’da sürekli denetimden “gerçek zamanlı veya gerçek zamanlıya yakın ortamlarda işlem gören tüm kayıtlar için denetçilerin olağan dışı durumlarını tespit eden yazılım” diye bahseder. Bu olağan dışı durumlar hemen incelenebildiği gibi denetçinin günlük (log) dosyasına yazılarak daha sonra inceleme yapılmak üzere kaydedilirler.⁵

Sürekli denetim kavramının teorisyenler tarafından literatürde sıkça kullanılmaya başlanması uygulamacıları da harekete geçirmiş, muhasebe mesleğinin dünyadaki en aktif organizasyonlarından ikisi, Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü (American Institute of Certified Public Accountants, AICPA) ile Kanadalı Yetkili Muhasebeciler Enstitüsü (Canadian Institute of Chartered Accountants, CICA) ortak bir çalışma grubu oluşturarak sürekli denetim konusunda bir rapor hazırlamışlardır. Bu raporda sürekli denetim “bağımsız denetçinin, denetim konusunun temelini oluşturan olayların gerçekleşmesi ile eşzamanlı veya bu olayların gerçekleşmesinden kısa bir süre sonra yayınlanan bir dizi denetçi raporunu kullanarak, denetim konusu üzerine yazılı bir güvence vermesine imkan tanıyan bir metodoloji” (CICA, 1999) şeklinde tanımlanmış ve bu tanım literatürde referans olarak kullanılmaya başlanmıştır.⁶

AICPA ve CICA’nın tanımından sonra geliştirilen modellerde de sürekli denetimin bu tanımı temelde kabul edilmesine rağmen bazı konularda farklılıklar göstermiştir.

⁵ Robert Baksa ve Murray Turoff. “The Current State of Continuous Auditing and Emergency Managemet’s Valuable Contribution”, 7th International ISCRAM Conference. Seattle, ABD: Mayıs 2010.

⁶ Ahmet Ağca. “Sürekli Denetim: Denetimde Bir Devrim mi Yoksa Bir Hayal mi?”, MODAV Muhasebe Bilim Dünyası Dergisi 8.1 Mart 2006:63-78. <http://www.muhasebetr.com/ozelbolum/029/> (12 Aralık 2008).

Rezaee 2001’de sürekli denetimi “kağıtsız ve gerçek zamanlı muhasebe sistemi tarafından hazırlanan finansal tabloların doğruluğuna dair görüş oluşturmak için toplam elektronik kanıtların sistematik toplama süreci” olarak tanımlar.

Sürekli denetim, iç ve dış denetçiler için denetim konusuna giren işlemlere ilişkin olarak anında veya işlemler gerçekleştikten kısa bir süre sonra yazılı rapor alınmasını sağlayan yöntemdir.⁷

Sürekli denetim, fiziki belge olmaksızın gerçek zamanlı muhasebe bilgi sisteminde üretilmiş olan finansal tablolarda yer alan finansal karakterli bilgilerin doğruluğuna ve güvenilirliğine ilişkin görüş oluşturmak amacıyla bilgisayar destekli denetim teknikleri ve analitik prosedürleri kullanarak elektronik denetim kanıtlarını toplamaya ve toplanan kanıtlardan ulaşılan görüşü bir denetim raporu ile bilgi kullanıcılarına sunmaya yönelik sistematik bir süreçtir.⁸

Coderre 2005 yılında Global Technology Audit Guide’da (GTAG) sürekli denetimi “genellikle iç denetçilerin sıkça otomatik olarak yaptıkları kontrol ve risk değerlendirmesi için kullandıkları bir yöntem” olarak nitelendirir. Bu çalışmadaki sürekli denetim tanımı gerçek zamanlı veya gerçek zamanlıya yakın gerçekleşen sürekli izleme, sürekli kontrol değerlendirmesi, sürekli risk değerlendirmesi gibi diğer denetim yöntemlerini de içine alır.

Sürekli denetim birleştirici bir çatı olup risk değerlendirme, kontrol, denetim planlama, dijital analiz ve diğer denetim araçları ve tekniklerinin bütünleşmesidir⁹. Analiz sonuçları denetim faaliyetinin tümüne, yani denetim planlamadan geribildirim kadar entegre olmuştur.¹⁰

Sürekli denetim kurumsal yönetim ve risk yönetimine getirdiği sistematik yaklaşımla kurum faaliyetlerini iyileştiren tarafsız, bağımsız güvence ve danışmanlık faaliyetidir.

⁷ ISACA Standards Board, “Continuous Auditing: Is It Fantasy or Reality?”. Information Systems Control Journal 5, 2002.

⁸ Cankar, s.71.

⁹ David Coderre, Internal Audit. A.B.D.: John Wiley & Sons, Inc., 2009, s.70.

¹⁰ David Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide. The Institute of Internal Auditors, USA, 2005:1.

Sürekli denetimin iki ana bileşeni şunlardır:¹¹

a) Sürekli kontrol değerlendirmesi (Continuous control assessment)

Sürekli kontrol değerlendirmesi kontroller üzerinde yapılan denetimleri ifade eder. Yönetimin izleme faaliyetlerinin yeterliliğini denetleyerek bağımsız bir gözle kontrollerin etkinliğinin ölçülmesi ve kurumun muhtemel olumsuzlukları hızlı bir şekilde düzeltmesinin mümkün olup olmadığının araştırılmasıdır.

b) Sürekli risk değerlendirmesi (Continuous risk assessment)

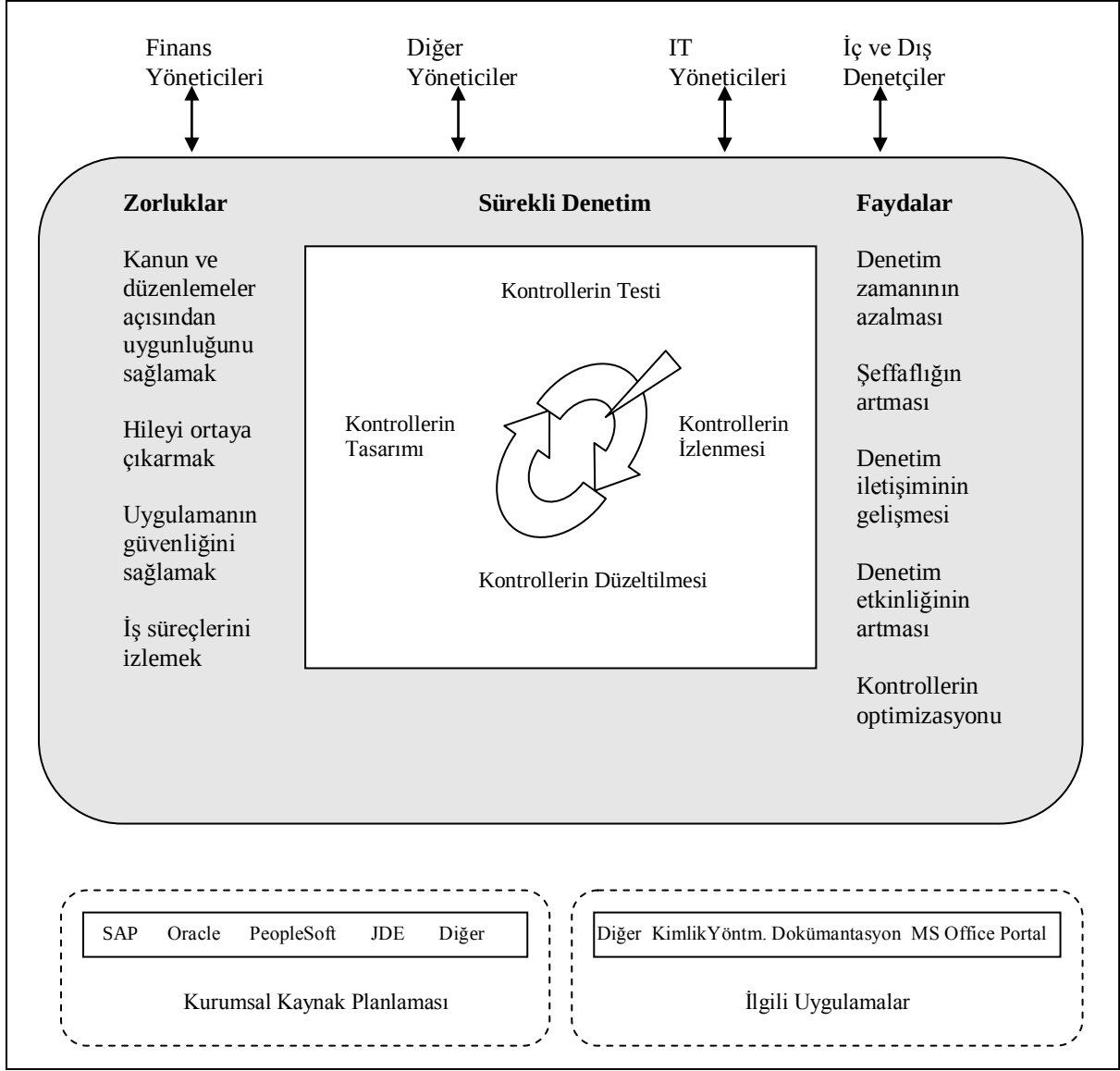
Sürekli risk değerlendirmesi beklenen risk düzeyinin üzerinde riski olan sistem ve süreçlerin belirlenmesini ifade eder. Denetçiler kurumun riskli alanlarını tespit ederek bu riskleri derecelendirir ve önceliklendirirler. Bu sayede sınırlı denetim kaynaklarının daha etkin kullanımını sağlamış olurlar.

Denetçilerin kontrol ve risk değerlendirmelerine ilişkin faaliyetleri, yönetimin izleme faaliyetleri ve risk yönetiminden bağımsızdır. Denetimlerin yapılması yönetimin bu konulardaki sorumluluklarını denetçilere devrettiği anlamına gelmez. Yönetim risk değerlendirmesi, kontrollerin tasarımı, uygulanması ve güncelliğinin korunmasından birinci derecede sorumludur. Denetim bu kurumsal risk yönetim sisteminin etkinliğini yönetimin kurmuş olduğu şekliyle değerlendirir, kanunlara uygunluğunu konusunda görüş bildirir. Denetçilerin tarafsız ve bağımsız kalabilmeleri için ilgili sistemlerin tasarımında yer almamaları gerekir.

Sürekli denetim ve yönetim tarafından yapılan sürekli izleme sonuçları açısından birbirine benzerdir. Her ikisi de kontrol zaafları veya yükselen risk seviyesini bildirir.¹² Ancak, sonrasında atılacak adımlar birbirinden farklıdır. Yönetim kontrol zaaflarını ve hatalı işlemleri düzeltir; denetim ise ilgili konuda hemen denetim başlatır veya daha sonra denetim yapmak üzere işaretler.

¹¹ Cankar, s.71.

¹² David Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide, s.1.



Şekil 1: Sürekli Denetim

Kaynak: Gerard Brennan. "Continuous Auditing Comes of Age". Information Systems Control Journal. 1. 2008. <http://www.isaca.org> (17 Ocak 2009).

Son yirmi yılda yapılan sürekli denetim tanımlarına günümüz teknolojisi ve denetim anlayışıyla baktığımızda sürekli denetim kavramının aşağıdaki unsurları barındırdığını görmekteyiz:

- Yazılı güvence vermek: Sürekli denetim sistemleri denetime konu olan bilginin doğru ve tam olduğunun, ilgili kanun ve kurumsal politikalarla uyumlu olduğunun güvencesini vermek için kurulurlar. Bu güvenceyi verebilmek için bilgi sisteminde destekleyici kanıt ararlar ve dijital analiz teknikleri kullanarak toplanan bilgiyi incelerler. Elde edilen sonuçlar, özellikle de belirlenen olağandışı durumlar ilgili kişilere raporlanır. Hangi olağandışı durumun kime raporlanacağı denetim modeli

geliştirilirken planlanır. Böylece ilgisiz veya yetkisiz kişilerin hassas bilgiye ulaşması önlenmiş olur. Ayrıca, bilgilendirilmesi gereken kişilerin olağandışı durumdan haberdar edilmemesi durumunda doğacak sorunlar da engellenmiş olur. Rapor formatı üzerinde fikir birliği oluşmamıştır. Raporun kapsamı ve formatı tam denetim raporu ile olağandışı durumların listelendiği bilgilendirme notu arasındadır. Önemli olan denetim sonuçlarının amaca uygun ve ihtiyaç duyulan kapsamda açıklanması ve bu açıklamanın doğru kişilere iletilmesidir. Raporların e-posta ile gönderilmesi sürekli denetim modellerinde en yaygın iletişim ortamı olarak görülmektedir. Sürekli denetim sistemlerinde ulaşılmak istenen nokta kurumun finansal raporlarında yer alan bilginin tam ve doğru olduğunun, ilgili yasa ve yönetmeliklerle uyumlu olduğunun güvencesini vermektir. Bu da ancak kurumun tüm faaliyetleri sürekli denetim sistemi tarafından denetlenebildiğinde gerçekleşebilir. İdeal olan kurumun gerçek zamanlı muhasebe sisteminin ürettiği o anki durumunu gösterir finansal tablolarının gerçek zamanlı denetlenmesi ve istendiği anda denetim raporunun sunulmasıdır.

- Gerçek zamanlı: Günümüzde kurum faaliyetini ilgilendiren bir olay gerçekleştiği anda konu ile ilgili finansal veya finansal olmayan tüm işlemler kurumsal bilgi sistemine yansımaktadır. Finansal olaylar gerçek zamanlı muhasebe sistemi aracılığıyla finansal raporlarda yerini almakta, finansal olmayan olaylar da ek bilgi, dipnotlar veya denetim kanıtı olarak kullanılmaktadır. Kurumsal faaliyetlere ilişkin bilgi gerçek zamanlı olarak elektronik ortama aktarılabilirse bu bilginin de gerçek zamanlı denetiminin yapılması ve sonuçların ilgililer ile paylaşılması ideal bir durumdur. Günümüz teknolojisinde bilginin denetiminin gerçek zamanlı yapılması mümkündür. Altyapı yetersizlikleri kurumsal bilgi sisteminin yavaşlamasına neden olduğu için özellikle işlem sayısı yüksek olan kurumlarda denetimin gerçek zamanlı değil de belli aralıklarla yapılması öngörülmektedir. Denetimin hangi sıklıkla yapılacağı risklere ve altyapıya bağlı olarak saat, gün veya ay olarak karşımıza çıkmaktadır. Teknolojik mecburiyetten kaynaklanan bu durum sürekli denetim tanımlarına “gerçek zamanlıya yakın” kavramını sokmuştur. Bir tür dönemselliği ifade eden bu kavram idealden uzak olsa da uygulamada bir mecburiyet olarak karşımıza çıkmaktadır. Teknolojinin gelişimiyle tam anlamıyla gerçek zamanlı denetim mümkün olacaktır.
- Elektronik ortam: Sürekli denetim uygulamalarında denetim faaliyetlerinin tamamı elektronik ortamda ve bilgi sistemleri ile gerçekleşmelidir. Kurumsal veritabanında yer alan bilginin denetimi ya bulunduğu veritabanında ya da başka bir veritabanına aktarılarak yapılır. Sürekli denetim yazılımı amaca ve incelenen bilgiye uygun dijital

analiz tekniklerini kullanarak bilgiyi inceler, değerlendirir ve çıkan sonuçları raporlar. İnceleme, değerlendirme ve raporlama aşamalarının tamamı bilgi sistemi tarafından otomatik olarak gerçekleştirilir. Denetçiler denetim sürecinin modellenmesi, denetim sonuçlarına bağlı olarak denetim modelinde iyileştirmeler yapılması ve gerektiğinde parametrelerin değiştirilmesinden sorumludurlar. Sürekli denetim uygulamalarında ideal olan denetim sürecinin tamamının denetim yazılımı tarafından gerçekleştirilmesidir. Denetçilerin teknik bilgisi ve ellerindeki teknolojik altyapı denetim sürecindeki rollerini belirlemektedir. Denetçiler iş süreçlerinin denetimini modellerken ne kadar gerçeğe yaklaşırlarsa ve bu modeli bir bilgisayar yazılımı haline getirmede ne kadar başarılı olurlarsa o kadar ideal uygulamaya yaklaşırlar.

- İç denetim ve dış denetim: Literatürde çoğu araştırmacının sürekli denetimden bir iç denetim uygulaması olarak söz ettiğini görmekteyiz. İç denetçilerin dış denetçilere göre kurumsal yapı, süreçler ve riskler konularında daha bilgili olmaları, kurumsal veriye daha kolay erişim sağlamaları, denetim modelini geliştirmek için daha çok zamanları olması gibi nedenlerle sürekli denetim uygulamalarının sadece iç denetçiler tarafından geliştirilebileceği inancı doğmuştur. Veri formatlarının ve kurumsal uygulamaların çeşitliliği nedeniyle sürekli denetim uygulaması yaratmak ve kullanmak isteyen dış denetçiler inceledikleri her kurum için ayrı bir yazılım geliştirmek zorundadırlar. Her kurumda ayrı uygulama geliştirmeye çalışmak için harcanacak zaman ve katlanılacak maliyet dış denetim firmaları için ağır bir yüküdür. Yapılan anket çalışmaları da dış denetçilerin sürekli denetim uygulamalarına sıcak bakmadıklarını ortaya koymuştur. Veri ve finansal raporlama formatlarında standardizasyonun artması ve kurumsal bilginin daha şeffaf hale gelmesi dış denetçileri de sürekli denetim uygulamalarına yöneltecektir. Günümüzde XML'in veri formatı, XBRL'in de finansal raporlama formatı olarak öne çıktığını görmekteyiz. Kurumsallaşmaya yönelik çalışmalar ve kanun koyucuların kurumsal bilginin şeffaflığı için aldığı önlemler sayesinde kurumsal veri dış denetçiler tarafından ulaşılabilir hale gelecektir. Dış denetçilerin önündeki engeller kalktıkça sürekli denetim uygulamalarının geliştirilmesi ve kullanılması açısından iç ve dış denetçi ayrımı kalkacaktır.
- Denetlenen nedir: Sürekli denetim sistemlerinin neyi denetlemek için kurulduğu açıklanması gereken bir konudur. Denetim, denetim standartlarının öngördüğü şekilde yapılır. İç Denetçiler Enstitüsü (The Institute of Internal Auditors - IIA) Amerika Birleşik Devletleri'nde iç denetim standartlarını belirleyen bir kuruluştur. Ancak, bu kuruluşun aldığı kararlar birçok ülke için de örnek teşkil ettiğinden etki alanı Türkiye

ve Avrupa Birliđi dahil birçok lkeyi kapsamaktadır. İ Denetim Enstits denetimi i kontrollerin etkinliđinin deđerlendirilmesi olarak tanımladıđı iin srekli denetim sistemleri i kontrollerin denetimi iin geliřtirilmektedir. Kurumsal iř sreleri tek tek ele alınarak ilgili kontroller iin srekli denetim modelleri geliřtirilmeli ve programlanmalıdır. Srekli denetim uygulaması geliřtirmek ve dođru alıřmasını sađlamak maliyetlidir. Bu nedenle uygulamada hedeflenen tm kontrollerin deđil yalnızca en riskli olanların denetlenmesidir. Denetlenen kontrollerin makul seviyede gvence vermek iin yeterli olmasına ve denetlenen kontrollerin neler olduđunun denetim raporunda aıka belirtilmesine dikkat edilmelidir. Denetim kanıtı olarak incelenen iřlemlerin denetime konu olan kontrolle ilgili iřlemlerin tm m yoksa bir blm m olacađı arařtırmacılar arasında ayrı bir tartıřma konusudur. Bazı arařtırmacılar yeterli seviyede gvence verilebilirse iřlemlerin bir blmnn incelenmesinin yeterli olacađı, aksi hale bilgi sistemine gereksiz bir yk bineceđini savunmaktadırlar. İdeal olan denetimin konusu olan kontrolle ilgili tm iřlemlerin denetim srecine dahil edilmesidir. Teknolojik sınırlamalar nedeniyle bunun yapılamadıđı durumlarda rnekleme yntemi ile seilen veri incelemeye alınır.

- Risk: Beklenenin dıřında geliřen olaylar kuruma zarar verme ihtimali olan risklerdir. Duruma bađlı olarak bu risklerin kuruma verebilecekleri zarar deđerşkendir. Denetim standartları denetilerin kurumsal risk ynetimi zerinde grř bildirmelerini ve gerektiđinde ynetime danıřmanlık yapmalarını ngrmektedir. Yasa koyucular ynetim ve denetim birimlerinin oluřabilecek zararın nlenmesi veya en aza indirilmesi iin ortak aba harcamalarını istemektedirler. Bu nedenle srekli denetim uygulamalarının odađında riskli alanları algılamak ve ynetime riskleri azaltacak nlemlerin alınmasında danıřmanlık yapmak vardır. Sınırlı kaynakların etkin kullanımı ve geliřtirilen srekli denetim uygulamalarının kuruma en yksek deđer katması iin denetim uygulaması geliřtirilen alanların risk dzeyi yksek olanlardan seilmesi tercih edilmelidir.

2.2. SÜREKLİ DENETİM İLE GELENEKSEL DENETİM ANLAYIŞI ARASINDAKİ FARKLAR

Sürekli denetim ile geleneksel denetim anlayışı arasındaki farklılıklar vardır ki bunlar:

- a) Sürekli denetim veri, kayıt ve belgelerin elektronik ortamda denetlenme faaliyetidir. Geleneksel denetimde denetim işlemini yapan kişiler, yani denetçiler vardır. Bu kişiler hem elektronik ortamdaki ve hem de kağıt üzerindeki kayıt ve belgeleri incelerler.
- b) Sürekli denetimde sadece dijital analiz araçları ve teknikleri kullanılır. Denetçinin kendisinin geliştireceği veya bir denetim paket programıyla bilgisayar yardımıyla denetim yapılmasını öngörmektedir. Bu paket programlar riskleri belirleyen, iç kontrol sistemini değerleyen, elektronik olarak denetim prosedürlerini yapan, analitik inceleme için gerekli bilgileri indirebilen, kayıtları hesaplayan, büyük defterleri listeleyen, maddi doğruluk ve kontrol testlerine ilişkin örneklemeleri seçebilen normal olmayan işlemleri ve farklılıklar dışında tanımlayabilen ve doğrulamaları yapabilen içeriktedirler. Geleneksel denetimde ise analizi denetçiler yaparlar.
- c) Sürekli denetimde kayıtların tamamına yakını analiz edilirken geleneksel yöntemde çoğunlukla örnekleme yöntemine göre sınırlı sayıda kayıtların yer aldığı bir örnek kayıt kümesi denetlenir.
- d) Geleneksel denetimde belli aralıklarla denetim faaliyeti gerçekleşir ve denetim raporu hazırlanır. Oysa sürekli denetimde kayıtlar eşzamanlı olarak denetlenir, olağandışı durumlar anında denetçilere bildirilir ve denetim raporu istendiği anda hazırlanır.
- e) Sürekli denetimin maliyeti geleneksel denetime göre daha düşüktür. Daha kısa sürede ve daha az kişi ile denetim yapılabilir.
- f) Sürekli denetim uzaktan denetime olanak tanır.
- g) Geleneksel denetimin aşamaları planlama, saha çalışması ve raporlamadan oluşur. Sürekli denetimin aşamaları ise denetim yöntemlerinin otomasyonu, veri modelleme ve karşılaştırmaların geliştirilmesi, veri analizi ve raporlama olarak özetlenebilir.

2.3. SÜREKLİ DENETİMİN YARARLARI

Denetim amaçlarında, güvence seviyelerinde, zamanlamada, denetimde kullanılan araçlarda ve denetim raporlamasında yaşanan anlayış değişikliği sürekli denetimin bir ihtiyaç olduğunu göstermiştir. Ayrıca, sürekli denetim, denetim kalitesini arttıracak sayısız yararlar sağlamaktadır.

Sürekli denetimin yararları aşağıdaki gibi sıralanabilir:

- a) Denetim faaliyetlerinin etkinliğini arttırmak: Otomatik olarak sık sık yapılan veri analizleri kontrol ve risk değerlendirmelerinin gerçek zamanlı yapılmasını sağlar.¹³ Ayrıca, iç denetim faaliyetlerinin iş süreçleriyle eşzamanlı olmasından dolayı risk ve kontrol zaaflarını bulmak kolaylaşır. Hata ve hilelerin bulunmasının yanında etkin bir önleme faaliyetidir. Ampirik çalışmalar standart denetim uygulamaları ile yapılan hilelerin sadece küçük bir bölümünün ortaya çıkartılabildiğini tespit etmişlerdir. Hilelerin tespit edilememesi durumunda yapılan hilelerin devam etmesi olasıdır; bu da kurum için maddi kayıpların devam etmesi anlamına gelir. Ayrıca, hilenin kuruma verdiği ölçülemeyen zararlar da vardır. İş ortamında huzursuzluğun artması, kurumsal etik değerlerin bozulması, kurum adının lekelenmesi, kurumun sermaye piyasalarında değerinin düşmesi gibi birçok ölçülemeyen zararlar verir. Bu nedenle hilenin engellenmesi veya hemen tespit edilmesi kurum için önemlidir.
- b) Katma değer sağlayan faaliyetlerde bulunmak: Denetimin bir görevi de kurum faaliyetleri ile ilgili danışmanlık yapmaktır. Denetim sırasında işlemler ve faaliyetlerin detaylı analizi ve modellemesi yapıldığı için uygulamaların kurumsal politika, hedefler ve iş süreçleri ile uyumluluğunun değerlendirilmesi yapılmaktadır. Denetçiler kurumsal verimliliğin artması ve kurumsal etik değerlerin korunması için önerilerde bulunabilirler. Bu tavsiyeler kuruma değer katar.
- c) Gerçek zamanlı görüşler ortaya koymak: Sürekli denetim gerçek zamanlı bir denetim olduğu için denetçiler olaylar karşısında anında ilgili kişileri bilgilendirme imkanına sahiptirler. Günümüzün rekabetçi ortamında geçmiş bir döneme ait finansal tabloları kullanarak karar vermektense doğru bilgiye zamanında ulaşmaya daha fazla ihtiyaç duyulmaktadır.

¹³ David Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide, s.1.

- d) Denetim kapsamının genişliği: Bilgi sistemlerinin dijital analiz teknikleri ile çok miktarda kaydı kısa sürede inceleyebilme potansiyeli vardır. Sürekli denetim tamamen bilgi teknolojileri kullanılarak yapılan bir denetim türü olduğu için kayıtların tamamı veya tamamına yakını incelenebilir.
- e) Denetimin güvenilirliğini arttırmak: Tüm kayıtların, analizlerin ve raporlamanın elektronik ortamda olması insan hatasını en aza indirmektedir. Verinin doğru ve sistematik bir biçimde incelenmesi, yüksek analiz yeteneği ve denetimde tutarlı uygulamalar denetim güvenilirliğini arttırmaktadır.
- f) Şeffaflığı arttırmak: Sürekli denetim modellerini geliştirirken detaylı belgeleme yapılmaktadır. Böylece, yaklaşımlarda standardizasyon ile değerlendirme ölçütlerinde açıklık ve şeffaflık sağlanmaktadır.
- g) Bilgi işlem bölümünden bağımsız hareket edebilmek: Denetçiler yapacakları çalışmalarda diğer bölümlerden bağımsız hareket edebilmelidirler. Sürekli denetimde kullanılan teknikler sayesinde programcılardan aldıkları desteği azaltabilirler. İş süreçlerinin denetiminde bağımsız hareket edebilecekleri için denetim standartlarını zedelemekten görevlerini yerine getirirler.
- h) Denetim planını geliştirmek: Sürekli risk değerlendirmesi denetimin zamanlaması konusunda yol göstericidir. Süreçlerdeki risk faktörleri göz önüne alınarak denetimin hangi sürede tekrarlanacağına karar verilir. Riskler derecelendirilir ve yüksek risk taşıyan alanlara öncelik verilir. Sürekli risk değerlendirmesi denetimin kapsamını saptarken de yardımcı olur. Hangi kayıtların ne ölçüde incelenmesi gerektiğine ışık tutar.
- i) Özel denetimi desteklemek: Denetçiler sürekli risk değerlendirmesi sonuçlarına göre gerekli durumlarda belli alanlarda özel denetim yapılmasına karar verebilir. Bu denetimin kapsamı, amaçları, incelenecek veri gibi denetime ilişkin unsurlar sürekli risk değerlendirmesinden elde edilen bulgulara göre planlanır.
- j) Denetimin maliyetini düşürmek: Tekrar kullanılabilen bilgisayar teknikleri sayesinde denetim maliyetleri düşmektedir. Sürekli denetim ile kayıtların tamamına yakını çok kısa sürede otomatik olarak denetlendiği için denetim sürecinde ihtiyaç duyulan adam/saat miktarı diğer denetim türlerine göre azdır.

- k) Denetimden kaynaklanan israfı azaltmak: Sürekli denetim uygulamaları denetim israflarını büyük ölçüde azaltır. Denetimden kaynaklanan israflarının yedi farklı türü vardır:¹⁴
- Aşırı denetim: Risk ve önemlilik değerlendirmesinin öngördüğünün çok üzerinde denetim yapmak denetim süresini ve maliyetleri arttırır.
 - Bekleme: Denetçilerin üzerinde denetim yapacakları veriyi beklemeleri büyük bir zaman kaybıdır.
 - Gecikmeler
 - Denetim süreci: Planlamadan raporlamaya kadar olan süreçte etkin olmayan alanlar olabilir.
 - Çalışma dönemi: Denetimin durması ve tekrar başlaması denetim sürecinde sıkça rastlanan bir sorundur.
 - Yeniden gözden geçirmek: Yeniden gözden geçirme bir kalite kontrol unsurudur. Sürekli denetim bu süreyi kısaltabilir.
 - Hatalar: Denetim sırasında ne kadar dikkat edilirse edilsin hata yapılabilir. Bu hataların giderilmesi için emek harcanacaktır.
- l) Standart raporlama yapmak: Denetim raporunun bilgi sistemi tarafından hazırlanarak ilgili kurum ve şahıslara gönderilmesi denetim zamanını kısaltır. Ayrıca, raporun şekli ve içeriğindeki standardizasyon rapor kalitesini arttırır.
- m) Denetim sonuçlarının takibini sağlamak: Denetimin sık aralıklarla yapılması sayesinde denetçiler daha önce yapılmış olan sürekli denetim faaliyetlerinin değerlendirmelerini ve geribildirimlerinin sonuçlarını görme şansına sahiptirler. Önerilerinin ne kadarının uygulandığını ve uygulamaların etkinliğini tespit ederler.
- n) Farklı alanlardaki becerileri birleştirmesi: Farklı alanlardaki becerilerin bütünleşmesine olanak sağlar. Örneğin, denetim faaliyetlerinin planlanması ve denetim sürecinde muhasebe bilgisi ve bilgi işlem teknolojileri bilgisine sahip kişilerin birlikte çalışması gerekmektedir. Bu finansal ve bilgisayar becerilerinin bütünleşmesidir.
- o) Dış denetçiler ile etkin iletişim kurmak: Dış denetçilere sürekli denetim uygulamaları ile ilgili bilgi verilirken kontroller ve bunların denetimi ile ilgili de bilgi verilir. Böylece dış denetçiler test etmeleri gereken kontrolleri kısa sürede tespit edebilirler.

¹⁴ DeWayne L. Searcy ve Jon B. Woodroof. "Continuous Auditing: Leveraging Technology". Mayıs 2003. (17 Ocak 2009).

- p) Firma deęerini arttırmak: Srekli denetim yeni bir gvence hizmeti olup firmaya deęer katmaktadır. 2008 yılında yapılan kontroll bir deney ile srekli denetim sistemi kullanımının yatırımcı bakış açısını nasıl etkiledięi zerinde arařtırmalar yapılmış ve srekli denetim uygulamalarına yer veren kurumlar için yatırımcıların firma riski deęerlendirmesi, hisse başına kazanç tahmini ve ilgili kuruma ilişkin tahminlerin gerekleēeęine dair inancı incelenmiştir. Srekli denetim yapılması planlanan kurumlara yatırımcıların yatırım yaparken kendilerini daha gvende hissettikleri ve firma riskini daha dřk olarak deęerlendirdikleri sonucuna varılmıştır.¹⁵

2.4. SREKLİ DENETİMİN TARİHESİ

Kontrollerin test edilmesine ilişkin otomasyon 1960’larda yazılımların içine yerleştirilmiş denetim modlleriyle başlamıştır. O tarihte bu modllerin kullanımındaki zorluklar nedeniyle yaygın bir kullanım alanı bulamamıştır. Hatta 1970’lerin sonlarına doęru kullanımı iyice azalmıştır.¹⁶

1980’lerin başında bazı denetiler dijital analiz tekniklerini genel incelemeler için kullanmaya başlamıştı. O sıralarda srekli izleme kavramı ortaya çıkmıştır. Temel nermesi veri analizinde otomasyonu saęlayarak riskli alanlara odaklanmak olan bu kavrama akademik evrelerce sahip ıkılmıştır. Ancak denetiler o gnn kořullarında gerekli teknolojik altyapıya, analiz tekniklerine ve veri erişimine sahip deęildiler. Ayrıca, bu yeni denetim yaklaşımı ve metotları da onlara yabancı gelmişti.

1990’larda bilgi teknolojilerinin gelişimine paralel olarak iç kontrollerin etkinliğini denetlemek için veri analiz tekniklerinin kullanımı yaygınlaşmaya başlamıştı. 1994’te denetiler arasında yapılan bir ankette, ankete katılanların %93’ bilgisayar teknolojilerinin beř yıl içinde neminin artacağına inandıklarını söylemiştir. Aynı ankette denetilerin en ok ihtiya duydukları ve hedeflerine ulaşmada kendileri için en nemli yazılımların sıralanması istenmiştir. İlk  sırayı alan yazılımlar kelime işlemleri, tablolama ve veri ekmedir¹⁷.

¹⁵ El-Hussein E. El-Masry ve Jacqueline L. Reck. “Continuous online auditing as a response to the Sarbanes-Oxley Act”, Managerial Auditing Journal 23. 8 (2008):795.

¹⁶ David Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide, s.3.

¹⁷ Coderre, Internal Audit, s.104.

1990'lara gelirken iç denetim ve dış denetim birbirinden ayrı ve farklı kaynaklara sahip işlevlerdi. Dış denetim finansal tabloların kurallara uygun şekilde hazırlanması ile ilgilenirken iç denetim yönetime çeşitli konularda hizmet ederdi. 1990'ların başında dış denetim firmaları bazı iç denetim rollerini üstlendi. Bazı büyük kurumlar ana faaliyet alanı dışında kalan konularda iç denetim faaliyetlerini dış denetim firmalarına verdi¹⁸.

2002'de çıkartılan Sarbanes-Oxley kanunları başta Amerika Birleşik Devletleri olmak üzere çoğu ülkenin denetim standartları üzerinde etkili olmuştur. Bu kanunla iç denetimin sorumlulukları artmış, yeni kurumsal yönetim anlayışına paralel olarak iç kontrollerin etkinliğinin denetimi önem kazanmıştır. Günümüzün rekabetçi iş koşulları kurumda meydana gelebilecek risklere karşı önlem almayı ve olumsuzluklara hemen cevap vermeyi gerektirmektedir. Gecikmiş eylemler kayıpların büyümesine yol açabileceği için riskler olmadan veya oluştuğu anda önlemini alma anlayışı önem kazanmaktadır.

Bu gelişmeler denetim mesleği ile ilgili kişileri yeni denetim yaklaşımları aramaya ve denetim yazılımları geliştirmeye itmiştir. Ayrıca, bilgi teknolojilerindeki gelişim sayesinde denetçilerin bilgisayar kullanarak sorular sorabilme, uygun cevaplar alma, yeni yollarla sonuca ulaşma yetenekleri artmıştır. Denetim anlayışındaki değişim ve bilgisayar teknolojilerindeki gelişim sürekli denetim kavramını tekrar gündeme getirmiştir.

Sürekli denetim kavramı ilk kez John Kearns tarafından kullanılmıştır. Kearns, gelişmiş bilgi sistemlerine bağımlılığın artması, büyük hacimli verilerin bu bilgi sistemleri tarafından işlenmesi, yönetimin yeterli iç kontrol için üstlendiği sorumlulukların çoğalması ve denetim teknolojisindeki gelişmeleri gerekçe göstererek sürekli bir süreç denetiminin mümkün olabileceğini ifade etmiştir. Kearns'ün sürekli denetim için gerekçe olarak gösterdiği gelişmelerin zamanla daha da belirginleşmesiyle sürekli denetim konusunda yapılan akademik çalışmalar artmaya başlamıştır. Özellikle Groomer ve Murthy isimli araştırmacıların 1989'da veritabanı uygulamalarının sürekli denetimi ile Vasarhelyi ve Halper isimli araştırmacıların 1991 yılında online sistemlerin sürekli denetimi üzerine yaptıkları çalışmalar, sürekli denetimin akademisyenlerce geleneksel denetime karşı bir alternatif olarak ortaya çıkarıldığı ilk kapsamlı çalışmalar olarak literatürde önemli yer tutmaktadırlar.¹⁹

¹⁸Robert R. Moeller, Brink's Modern Internal Auditing. 7. Basım. A.B.D.: John Wiley & Sons, Inc., 2009, s.60.

¹⁹ Ağca, s. 63-78.

İlk sürekli denetim uygulaması AT&T'nin Bell Laboratuvarı'nda gerçekleşmiştir. O zamanki adıyla sürekli işlem denetim sistemi (continuous process auditing system, CPAS) iç denetim için kağıtsız denetim modeli olarak geliştirilmiştir.²⁰ AT&T'den sonra Siemens, HCA, Itau Unibanco, IBM, HP, MetLife ve Proctor&Gamble gibi kuruluşlar sürekli denetimin ilk uygulayıcıları olmuşlardır.²¹

1999 yılında Amerikan ve Kanadalı muhasebeci birlikleri ortak bir karar alıp sürekli denetim kavramının araştırılması ve ilgili uygulamaların geliştirilmesi için araştırmacılara çağrıda bulunmuşlardır.²² Bu yaklaşım akademik camiada büyük yankı uyandırmış ve 2000'li yıllarda birçok sürekli denetim modeli yaratılmıştır.

²⁰ Chun-Hsiu Yeh ve Wei-Cheng Shen. "Using continuous auditing life cycle management to ensure continuous assurance", African Journal of Business Management 4. 12 (Eylül 2010): 2556.

²¹ David Y. Chan ve Miklos A. Vasarhelyi. "Innovation and Practice of Continuous Auditing (Draft v.8)". <http://www.raw.rutgers.edu> (18 Şubat 2011).

²² Robert L. Onions. "Towards a Paradigm for Continuous Auditing". Ocak 2003. <http://www.auditsoftware.net/community/how/run/tools/Towards%20a%20Paradigm%20for%20Continuous%20Auditin1.doc> (19 Şubat 2011).

3. GÜNÜMÜZDE DENETİM ORTAMI VE SÜREKLİ DENETİMİN YERİ

3.1. GÜNÜMÜZDE DENETİM ORTAMI

Kurumsal yönetim anlayışındaki değişiklikler denetimin kurumsal faaliyetlerde etkinliği ve verimliliği artırıcı yönünü ortaya çıkartmıştır. Hukuki yükümlülüklerin artması da yöneticilerin denetime verdikleri önemi artırıcı bir unsur olmuştur. Finansal piyasaların bilgiyi anında doğrulama ihtiyacı denetim raporlarının en kısa sürede hazırlanıp kamuya açıklanmasını gerekli kılmıştır.

İnternet teknolojilerindeki gelişmeler bu teknolojilerin kurumsal kaynak planlama yazılımlarında kullanılmasını yaygınlaştırmış ve e-ticaretin gündelik yaşama girmesini sağlamıştır. E-ticaret amacıyla kurulan işletmelerin yanında birçok geleneksel yöntemlerle ticaret yapan kuruluşlar da e-ticaret uygulamalarına yer vermeye başlamışlardır. Klasik denetim yöntemleri ile İnternet temelli uygulamaları denetlemek denetim risklerini arttırmaktadır. Bu risklerden bazıları dijital ortamdaki bazı işlemlerin insanlar inceleyemeden tamamlanıyor olması, e-ticaret ve otomatize edilmiş uygulamaların aşamalı gerçekleşiyor olması, bilgisayar virüslerinin yaygınlaşması, birden fazla kurumun kullandığı İnternet uygulamaları, birçok işi taşeronlar aracılığı ile yapmak, İnternet hizmetlerinde kesintiler, ticaret yapılan işletmelerin kimliği belirsiz uluslararası kurumlar olması olarak sıralanabilir.

Bu zorlayıcı etkenler klasik denetim anlayışının geçerliliğini yitirmesine ve sürekli denetim ihtiyacının doğmasına yol açmıştır.²³ Denetim anlayışındaki değişiklikler kayıtların büyük bölümü üzerinde derinlemesine ve gerçek zamanlı analiz ihtiyacı doğurmuştur. Bu da ancak bilgisayar sistemlerinin desteğiyle mümkün olabilmektedir.

Kurumlar farklı ölçülerde de olsa denetimde bilgisayar sistemlerini kullanmaktadırlar. Kurumlarda dört seviyede teknoloji kullanımından söz edilebilir:²⁴

- Başlangıç: Bütçeleme, zaman yönetimi ve raporlama gibi yönetsel amaçlı
- Orta: Veri çekme, sınırlı veri analizi, tablolama ve sunum yazılımlarının kullanımı

²³ Srinivas Sarva. "Continuous Auditing Through Leveraging Technology", Journal Online. 2006. www.isaca.org (17 Ocak 2009).

²⁴ Coderre, Internal Audit, s.28.

- Bütünleyici: Denetimin tüm aşamalarında teknolojinin kullanımı; risk belirleme, incelenecek verileri belirleme, elektronik çalışma kağıtları ve raporlama
- İleri: Sürekli denetim ve Intranet'in kapsamlı kullanımı

Kurumsal faaliyetleri izleme, riskli alanlara odaklanma ve denetime ayrılan kaynakların yönetimi alanlarında yazılımlar geliştirilmektedir. Dijital analiz teknikleri finansal, faaliyet ve uygunluk denetimi de dahil olmak üzere çeşitli denetim faaliyetlerinde yardımcı olmaktadır. Bilgisayar teknolojilerindeki gelişim çok miktardaki veri üzerinde analiz yapılabilme imkanı sağlamaktadır.

İnternet denetçiler için çeşitli olanaklar sağlamaktadır. Gazete ve dergilerin veri tabanlarına girebilmek hem eski tarihli hem de güncel haber ve bilgilere kısa sürede ulaşabilme imkanı vermiştir. Denetim planlaması sırasında yapılan araştırma süresini önemli ölçüde kısaltmaktadır. Denetçiler ve ilgili taraflar arasında e-posta ve elektronik veri transferi kullanımı denetim zamanını azaltmış veri kalitesini arttırmıştır. Ayrıca, sahadaki denetçinin ofisindeki ihtiyacı olan dosyalara uzaktan erişmesi önemli bir kolaylıktır.

Günümüzde denetçilerde devam eden faaliyetlere yönelik gerçek zamanlı değerlendirmeler ve kararlar beklenmektedir. Uygunluk denetiminden ziyade, faaliyetleri geliştirmeye ve verimliliği arttırmaya yönelik talepler artmıştır. Sürekli denetim kavramı bu ihtiyaçlara cevap verebilmek için ortaya çıkmıştır.

Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü (American Institute of Certified Public Accountants, AICPA) ve Kanadalı Yetkili Muhasebeciler Enstitüsü'nün (Canadian Institute of Chartered Accountants, CICA) 1998 yılında sürekli denetim üzerine yaptırdığı araştırmadan üç önemli sonuç çıkmıştır:²⁵

1. Sürekli denetimin yapılabilmesi için uygun şartların gerçekleşmesi gerekmektedir.
2. Sürekli denetimin gelişebilmesi için akademik çevrelerin araştırma yapması, iş dünyasının uygulama yapması ve standartları belirleyen kurumların yol gösterici olması gerekmektedir.
3. Daha güvenilir, konuyla ilgili ve çabuk erişilebilen bilgi kurumların karar alma sürecinde önemli olduğu için sürekli denetim talebini de arttıracaktır. Ancak, denetim

²⁵ Zabihollah Rezaee, Rick Elam, Ahmad Sharbatoghlie. "Continuous auditing: the audit of the future", Managerial Auditing Journal 16. 3 (2001): 151.

mesleğini seçen kişilerin bu ihtiyaca cevap verebilecek şekilde kendilerini konumlandırmaları gerekmektedir.

Bu sonuçlar sürekli denetimin kurumlar açısından ihtiyaç duyulan bir denetim tekniği olabileceğini göstermektedir. Ancak, açıkça görüldüğü üzere hem denetçilerin hem de kullanıcıların bu teknolojiyi olgunlaştırmak ve kullanmak için daha çok emek vermeleri gerektiğidir.

Sürekli denetim kavramının uygulayıcılar tarafından tam anlaşılamadığı ve farklı yorumlandığı görülmektedir. Anketlere verilen cevaplarda denetim faaliyeti ile ilgili kişilerin sürekli denetim kavramını teknik tanımı dışında kullandıkları anlaşılmaktadır. 2006 yılında PricewaterhouseCoopers'ın yaptığı ankette sürekli denetim uygulamalarını kullandıklarını söyleyenlerin %57'si bu uygulamaları üç aylık dönem için yaptıkları denetimlerde, %34'ü ise aylık denetimlerinde kullandıklarını belirtmişlerdir. Ankete katılanların sadece %9'u günlük faaliyetler için sürekli denetim sistemini kullandıklarını belirtmişlerdir.²⁶ Oysa sürekli denetim gerçek zamanlı bir denetim faaliyetidir.

Sürekli denetim başlangıçtan raporlamaya kadar her seviyede bilgisayar sistemlerinin denetim faaliyetleri ile bütünleşmesini gerektirmektedir. Bu bütünleşme bir süreç olup sadece bir yazılım ve donanım satın alma faaliyeti değildir.

Sürekli denetimin ilk adımı olan verinin dijital ortamda bulunuyor olması sorun olmaktan çıkmıştır. 2005 yılında Redgrave tarafından yayınlanan bir araştırmada o tarihte A.B.D.'de kurumların yarattığı bilginin %93'ünün dijital formatta olduğu belirtilmiştir. Yine aynı araştırma kurumların tüm kayıtlarının %70'inin elektronik ortamda olduğunu ve bunların %30'unun hiç basılmadığını tespit etmiştir.²⁷

Ancak, gerçek zamanlı analizler için halen birçok kurumun imkanlarını uygun değildir.²⁸ 2009 yılında KPMG tarafından yapılan bir çalışmada kurumsal kaynak planlama yazılımının tamamen entegre çalıştığı kurumların oranı %16, kontrollerin yarısından çoğunun

²⁶ Ellen M. Heffes. "Theory to Practice: Continuous Auditing Gains", Financial Executive. Eylül 2006: 17. <http://www.fei.org> (18 Şubat 2011).

²⁷ Baksa ve Turoff, s.2.

²⁸ Coderre, Internal Audit, s.69.

otomatize edilmiş olduđu kurumların oranı %20 olarak bulunmuştur.²⁹ Sistem entegrasyonunun az oluşu ve kontrollerin kişilere dayalı oluşu sürekli denetimin gelişmesine engel oluşturmaktadır. Denetçilerin bilgisayar yetkinlikleri de göz önüne alınırsa sürekli denetimin yaygınlaşması için bir süre geçmesi gerekecektir.

İç Denetçiler Enstitüsü'ne (Institute of Internal Auditors-IIA) bağı Global Denetim Bilgi Ağı'nın (Global Audit Information Network-GAIN) 2010 yılında yaptığı ankette 386 katılımcının %57'si sürekli denetim uygulamaları kullanmadıklarını bildirmiştir. Sürekli denetim uygulamaları kullanılan kurumlarda ise bu uygulamaların kullanım alanları sınırlı kalmaktadır. 2007 yılında yapılan bir araştırmada sürekli denetim uygulamalarının kurumsal kaynak planlama sistemlerindeki kullanım alanları aşağıdaki gibi bulunmuştur:³⁰

- satıcılar hesabı %72
- alıcılar hesabı %64
- kebir hesapları %48
- bordro %36

Bağımsız denetim şirketlerinin sürekli denetim uygulamalarını desteklemedikleri anlaşılmaktadır. Sürekli denetimin faydaları konusunda birçok çalışma olmasına karşın bu sistemlerin gerekliliğine şüpheli yaklaşmaktadırlar. Ayrıca, sürekli denetim sistemi olması durumunda bağımsız denetçiler sistemden çıkan sonuçları kullanarak çalışmalarını yapacaklardır. Oysa sistem iç denetçiler, yani bağımsız olmayan kişiler tarafından yaratılmış olduğundan dış denetçiler kendilerine verilen bilginin güvenilirliğini sorgulamaktadırlar.³¹

2007 yılında yapılan bir araştırmada sürekli denetim testlerinin iç denetçiler tarafından kullanılma oranının yöneticilerin iş süreçlerini ve ilgili kontrolleri izleme faaliyetine göre iki kat daha fazla olduğu belirlenmiştir. Bu nedenle sürekli denetim uygulamalarının gelişmesinde en büyük rolün iç denetçilerde olacağı düşünülmektedir.³²

²⁹ Constance Lehmann, Sridhar Ramamoorti ve Marcia Weidenmier Watson. "Maximized Monitoring", Internal Auditor. (Haziran 2010):58.

³⁰ Lehmann, Ramamoorti ve Weidenmier Watson, s.58.

³¹ Tammy Whitehouse. "Whatever Happened to Continuous Auditing?", Compliance Week. 30 Kasım 2010. www.complianceweek.com (Ocak 2011).

³² Lehmann, Ramamoorti ve Weidenmier Watson, s.58.

3.2. SÜREKLİ DENETİMİN YÖNETİM FAALİYETLERDEKİ ROLÜ

Yönetim, kurum hedeflerine ulaşmak için işleri planlar, yönetir ve organize eder. İşlerin sağlıklı biçimde gitmesinden sorumludur. Sahiplerine, çıkar sahiplerine, kanun yapıcılara ve topluma karşı sorumludurlar. Yönetim bu sorumlulukları yerine getirebilmek için finansal ve operasyonel bilginin doğru, zamanlı, etkin ve verimli kullanıldığına emin olmak için uygulamalar geliştirmek, uygulamak ve sürdürmek zorundadır. Yönetim, risklerin belirlenmesi, değerlendirilmesi ve yönetimi ile sorumludur. Yönetim, etik değerlere, kanun ve tüzüklere uyumlu hareket edilmesini sağlamalıdır. Varlıklar doğru şekilde yönetilmelidir. Bütün bu işler birlikte çalıştığında hedeflere ulaşılabilir.

İç denetim, kurumu etkileyen tüm faaliyetleri ve ilgili kayıtları periyodik olarak gözden geçirir ve yönetimin sorumluluklarını yerine getirip getirmediğini denetleyerek güvence verir. Günümüz ihtiyaçlarını göz önüne alan etkin ve hızlı bir denetim faaliyeti için iç denetimin tercih edeceği yöntem sürekli denetim yöntemidir. Sürekli denetim uygulamaları iyi bir kurumsal yönetim ve risk yönetimini destekleyen bir yapı kurulmasına yardımcı olur.

İç denetçilerin kurumsal yönetimdeki rolü ve sorumlulukları altı alanda incelenebilir:³³

1. Etkin iç denetim grubunun en önemli özellikleri:

- Yönetimden bağımsızdır. Denetim komitesine rapor verir.
- Risk değerlendirmesi yapabilecek, hileleri tespit edebilecek ve önleyici tedbirler alabilecek yetkinliklere sahiptir.
- Hilelerde kırmızı bayrakları görebilecek eğitimi, bilgisi ve tecrübesi vardır.
- Risk değerlendirmeleri ışığında denetim planı yapabilir.
- Risk değerlendirme sırasında beyin fırtınası tekniğini kullanır.
- Profesyonel şüpheciliğe sahiptir.
- Önceden tahmin edilemez.
- Gizli anlaşma ve yönetimin geçersiz kıldığı kontrollere ilişkin şüphelere cevap verebilir.
- Kararlarını kanıtlara dayandırır.

³³ Zabiollah Rezaee ve Richard Riley. Financial Statement Fraud Prevention And Detection. 2. Basım. A.B.D.: John Wiley & Sons, Inc., 2010.:225-227.

2. İç denetimin hileye karşı alınacak önlemlerdeki rolü:

- Hile riskini değerlendirir: yönetimin hile riskine ilişkin öngörülerini değerlendirir ve denetler.
- Kurum kültürüne yönelik aşağıdaki konularda denetimler yapar:
 - İç kontrollerin amaçlarını, yeterliliklerini, yetersiz kalmaları durumunda doğacak sonuçları
 - Hedefler, stratejiler, uygulama planları ve bütçe
 - Etik değerler ve yapılmaması gerekenlere yönelik yazılı politikaların varlığı
 - İlgili politikalara uyulmadığında uygulanacak cezalara ilişkin yazılı belge
 - Faaliyetlere ilişkin onay sistemi
 - Uygun izleme politikaları
 - Varlıkların gerektiği şekilde korunması
 - Kurum içi iletişimin etkinliği
 - Yönetim kurulu, denetim komitesi, üst yönetim ve tüm çalışanlara yeterli ve güvenilir bilgi sağlanması

3. Kurumsal etik anlayışı saptamak için iç denetim aşağıdaki konularda anketler düzenler:

- Hatalı davranışa eğilim
- Hatalı davranışı fark eden bir çalışanın bunu bildirme ihtimali
- Hatalı davranışları açıklayan çalışanların yönetimin desteğini alacağına karşı inanç
- Hatalı davranışları bildiren kişilerden intikam alınacağı veya davranışlarından dolayı cezalandırılacakları inancı
- İşe alımlarda kurumsal politikalara uygun şekilde davranma

4. İç denetim hilelerin tespiti için aşağıdaki çalışmaları yapar:

- Hile acil yardım hattının aşağıdaki alanlarda denetimini yapar:
 - Tasarımı
 - Kapsamı: çalışanlar, müşteriler, satıcılar
 - Faaliyetler: plana göre işliyor mu?

- Yönetimin hile tespit etme ve önlemeye ilişkin kurduğu sistemi aşağıdaki alanlarda inceler ve değerlendirir:
 - Tasarımı
 - Uygulaması
- 5. Yönetim kurulu, üst yönetim ve tüm çalışanların iç denetimin işinin bir parçasının da “suçluyu bulma” faaliyeti olduğunu bilmelerini sağlar. İç denetimin:
 - hile aradığını
 - hileye yönelik her tür şikayet, iddia, öneri ve bilgiyi değerlendirdiğini
 - yöneticilere ve çalışanlara sorular sorabileceğinitüm çalışanların bilmelerini sağlar.
- 6. İç denetim hile, yetkiyi kötüye kullanma ve gizli anlaşmalara yönelik iddiaları ve şüpheleri araştırmak için hemen soruşturma başlatır.

3.3. SÜREKLİ GÜVENCE, SÜREKLİ İZLEME VE SÜREKLİ DENETİM İLİŞKİSİ

3.3.1. Sürekli Güvence

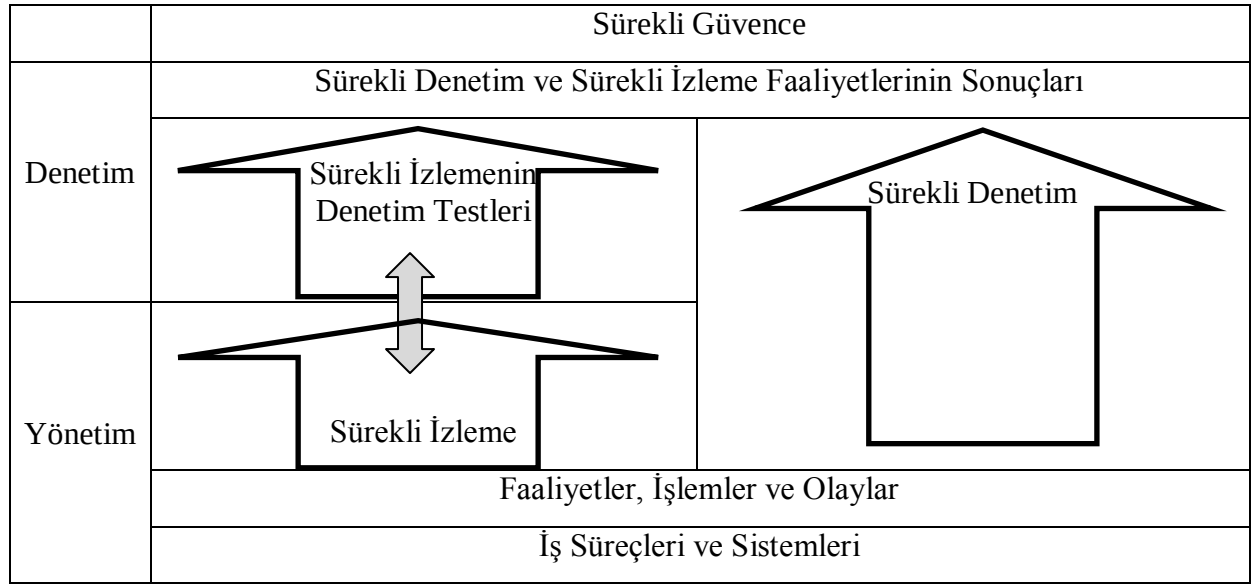
Güvence üçüncü şahıslara bir konu hakkında görüş bildirmektir.³⁴ Bu görüş belli bir işlem, iş süreci, risk veya bir faaliyetin finansal verimliliği ile ilgili olabilir. Denetim güvencesi ise kontrollerin yeterli ve etkin olduğunu, bilginin tam ve doğru olduğunu açıklamaktır.

Denetçiler sürekli güvence faaliyetleri için:

- kanıtları bağımsız bir gözle incelerler,
- risk yönetimine ilişkin stratejileri ve uygulamaları değerlendirirler,
- yönetimin kontrol sistemi ve uygulamalarını değerlendirirler,
- karar verme ve raporlamada kullanılan bilgiyi değerlendirirler.

Denetçiler sürekli kontrol ve risk değerlendirmesi, yani sürekli denetim, sonucunda yönetimin sürekli izleme faaliyetlerinin yeterliliği konusunda görüş bildirerek sürekli güvence sağlamış olurlar.

³⁴ Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide, s. 9.



Şekil 2: Sürekli Güvence, Sürekli İzleme ve Sürekli Denetimin Kavramsal Modeli

Kaynak: Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide, s. 10.

Vasarhelyi ve Alles’in 2004 yılında yazdığı bir makalede sürekli güvencenin dört konudan oluştuğu belirtilmiştir:

1. İşlemlerin doğrulanması
2. İşlemlerin yasalara ve anlaşmalara uygunluğunun doğrulanması
3. Tahminlerin doğrulanması
4. Kararların doğrulanması

Sürekli güvence sistemleri kurumun performansını değerlendirerek başarısına katkıda bulunduğu için güvenceyi veren kişiye bir ölçüde yönetici rolü verir. Denetçi kurum faaliyetlerini yakından izlerler ve öneriler getirir.

3.3.2. Sürekli İzleme

Sürekli izleme yönetimin kontrol amaçlarını ve verilen güvenceleri belirlediği, bunlara uymayan faaliyet ve işlemleri tespit ettiği bilgisayar tarafından otomatik olarak yapılan testlerdir.³⁵

³⁵ Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide, s. 9.

Sürekli izleme kurumun faaliyetlerinin, sistemlerinin veya verilerinin performansının gözlemlenmesine yardımcı olur.³⁶ Örneğin, fatura numaraları, satıcı isimleri ve ödeme miktarlarını karşılaştıran bir sistemin kurulması durumunda bu sistem bir cari hesaplar ve nakit ödemelere ilişkin sürekli izleme sistemi olurdu.

Sürekli izlemenin dayandığı temel ilkeler:³⁷

- İş süreçlerindeki kontrol noktalarını COSO ERM çerçevesinde tespit etmek.
- Her kontrol noktası için amaç ve güvence kapsamını tespit etmek.
- İşlemlerin kontrol amaçlarına ve güvence kapsamına uygunluğunun tespiti için otomatik testleri yapılmak.
- Kontrol testlerini geçemeyen tüm işlemleri incelenmek.
- Uygun olan durumda işlemleri düzeltilmek.
- Uygun olan durumda kontrol zaaflarını düzeltmek.

Kullanılan tekniklerin çoğu sürekli denetimde kullanılan tekniklerdir. Bu sistemler verilerdeki dalgalanmaları ve olağanüstü değişiklikleri rapor ederler.

Sürekli izlemenin sürekli denetimden farkı:

- Sürekli izleme sistemleri bir faaliyet, sistem veya verinin performansı hakkında dolaylı bilgi toplar. Denetçinin fiziki incelemesi, gözlemi, hesaplaması ve kontrolü yoktur. Bilgi dolaylı kanıtlara dayandığı için kanıtların geçerliliği sorgulanabilir. Sürekli denetimde denetçinin amacı denetim raporundaki bilgileri dayandırdığı kanıtların yeterli kalitede olmasıdır.
- Faaliyetlerin ve sistemlerin izlenmesi denetim standartlarına göre yönetimin işlevidir. Yönetimin kontrolleri izlemesi ve planlandığı gibi çalıştığını onaylaması gerekmektedir. Faaliyetlerin, sistemlerin ve verilerin performanslarının izlenmesi denetçiler tarafından yapıldığı takdirde denetçilerin “bağımsızlığı” tehlikeye düşmektedir. Örneğin, yönetim bir sistemin sonuçlarını değerlendirip gerekli düzeltmeleri yaptıktan sonra denetçiler sistemin yöneticiler tarafından kullanımını incelerlerse denetçilerin bağımsızlığı korunmuş olur. Ancak, denetçiler sistemi

³⁶ ISACA Standards Board, s.2.

³⁷ Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide, s. 9.

inceleyip hataları yönetime bildirirlerse denetçiler yönetimin kontrol işlevini yapmış olurlar.

Sürekli izlemenin sürekli denetimden farkını bir örnekle anlatabiliriz: Bir iş biriminin faaliyetlerinin verimliliği yönetim tarafından izlenilmek istenir. Önce iş süreçlerinin faaliyetlerinin detayları raporlanır. Bu detaylarda işlemi yapılan ürünün miktarı, parasal değeri, harcanan işçilik saati gibi verimlilik ölçen önemli göstergeler yer alır. Bu göstergeler önceden belirlenmiş standart değerler veya değer aralıkları ile karşılaştırılır. Bu karşılaştırma sonucunda göstergeler standart değerlerin dışına çıkmıyorsa faaliyetten amaçlanan verim alınıyor ve ilgili kontroller de görevini yapıyor demektir. Sürekli yapılan bu işlem yönetimin sürekli izleme faaliyetidir. Detaylı faaliyet raporlarından yola çıkarak hangi denetim testlerinin yapılacağını belirlemek, sonra da bu testleri sürecin kontrollerine uygulayarak kontrol yapısının yeterli ve işlevsel olduğu güvencesini vermek bir sürekli denetim faaliyetidir.

Sürekli izleme sistemleri sürekli denetimin yapılabilmesine faydalı olurlar. Sürekli izleme sistemleri kontrollerin çalışması, hataların tespit edilmesi ve düzeltilmesi konularında kanıt toplarlar. Denetimin bağımsızlığını zedelemeyen sürekli izleme sistemini sürekli denetimle entegre etmek denetim standartlarına uyarak kısıtlı kaynakların verimli kullanılmasını sağlar.

3.3.3. Sürekli Denetim

Denetimle ilgili faaliyetlerin sürekliliğini sağlayacak her yöntem sürekli denetimdir.³⁸ Sürekli kontrol değerlendirmesinden sürekli risk değerlendirmesi arasında süregelen faaliyetlerdir. Bu sürecin otomasyonunda teknolojinin kullanımı en önemli rolü üstlenir. Farklılıkların veya anomalilerin tespiti, sayısal veriler üzerinde sıralama analizi, trend analizi, hareketlerin analizi, kontrollerin testi ve bir sürecin veya sistemin zamanla veya benzeriyle karşılaştırılması gibi denetim faaliyetleri dijital analiz teknikleri ile bilgisayar tarafından devamlılık arz edecek şekilde tekrarlanır.

³⁸ David Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide, s.7.

Sürekli denetim kontrol güvencesi, risk değerlendirmesi, denetim planlaması, teknoloji, dijital analiz ve diğer denetim tekniklerini birleştiren bir yapıdır.³⁹ Kontrollerin etkinliği konusunda güvence vermek için tüm hareketlerin detaylı incelenmesinden, yıllık denetim planını yapmak için kurumsal risk seviyelerinin tespiti ve değerlendirmesine, denetim amaçlarının belirlenmesine kadar çeşitli amaçlarla kullanılabilir.

Sürekli denetim kavramı 1980'lerden beri araştırmacılar ve ilgili meslek odaları tarafından önem verilen bir konu olmasına rağmen gerçek anlamda uygulanması yaygın olamamıştır.⁴⁰ Bu uygulamaya talebin azlığının başlıca nedenleri teknolojik sorunlar ve kısa vadede faydasının maliyeti karşılayamamasıdır. Sarbanes-Oxley kanunlarından sonra denetim ortamı üzerinde daha fazla baskı oluşmuş ve güvenilir denetim raporlarının en kısa sürede elde edilmesi üzerinde çalışmalar yoğunlaşmıştır.⁴¹ Sürekli denetim bilgi teknolojilerine dayalıdır. Son yıllarda bilgi teknolojilerindeki gelişmeler sürekli denetimi uygulanabilir kılmıştır.⁴²

Sürekli denetim yapılabilmesi için aşağıdaki unsurlar gereklidir:

- Denetçilerin verilere doğrudan erişimi gerekmektedir. Kayıtlara doğrudan erişim hakkını verebilmek için kurum ile denetleyen grup arasında büyük bir güvenin sağlanmış olması gerekir. Bu da özellikle dış denetçiler açısından kolay değildir.
- Kurumun kontrollerinin çok kuvvetli olması gerekmektedir. Bu kontrollerin çoğu bilgisayar sistemleriyle ilgilidir ve kurumsal bilgi sisteminin denetimi yapan kişiler tarafından değerlendirilmesi gerekmektedir. İç kontrolleri kuvvetli ve bilgisayar sistemleri iyi kontrol edilen kurumlar sürekli denetimin uygulanabilmesi için en kuvvetli adaylardır.⁴³
- Sürekli denetimde denetim programları otomatik olarak bilgisayar sistemlerini kullanarak çalışır. Kullanılan bilgi sisteminin güncel olması, yani kayıtların gerçek zamanlı güncelleştirilmeleri gerekmektedir. Örneğin, sistem günde bir defa güncelleştiriliyorsa denetim programının çalışması da günde bir defayla sınırlandırılmış demektir.⁴⁴

³⁹ David Coderre, "Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment", Global Technology Audit Guide, s.8.

⁴⁰ ISACA Standards Board, s.3.

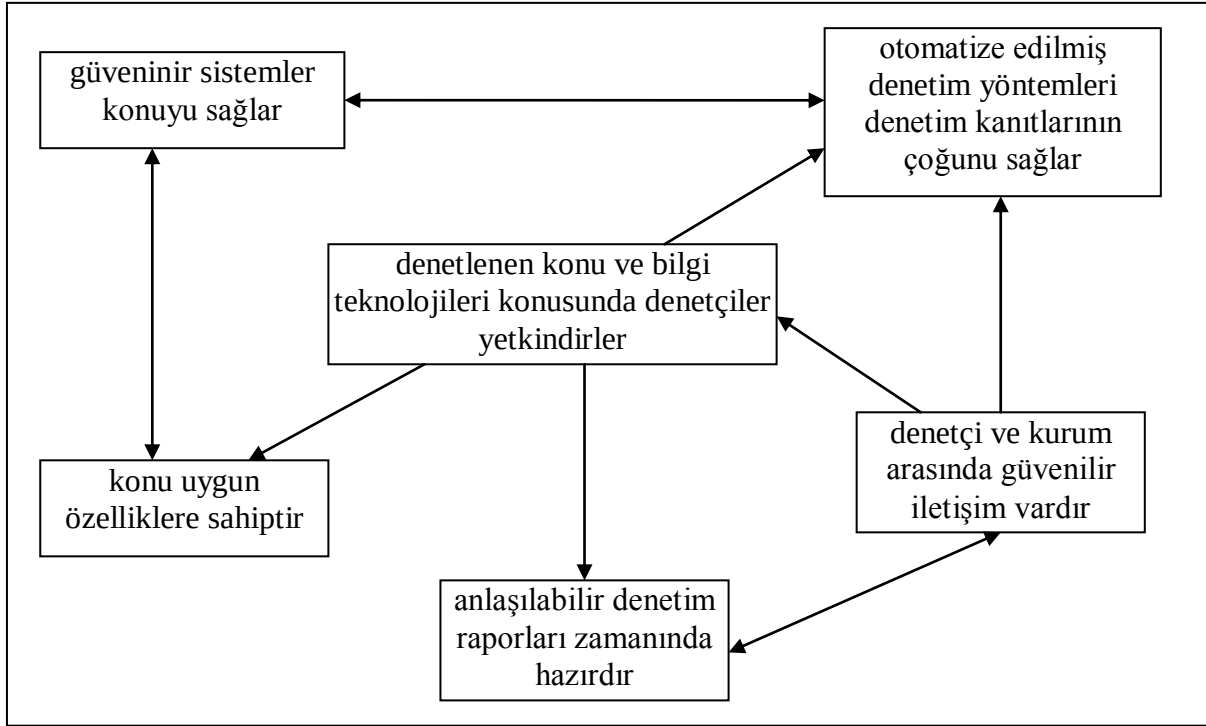
⁴¹ Brennan, s.1.

⁴² Searcy and Woodroof. "Continuous Auditing: Leveraging Technology", s.1.

⁴³ ISACA Standards Board, s.3.

⁴⁴ Searcy and Woodroof. "Continuous Auditing: Leveraging Technology", s.1.

- Sürekli denetim yaklaşımları ve bilgisayar sistemleri hakkında güncel bilgilere sahip olmak çok önemlidir. Bu nedenle ilgili konularda eğitim alınması gerekmektedir.



Şekil 3: Sürekli Denetim İçin Gerekli Koşullar

Kaynak: J. Donald Warren Jr ve L. Murphy Smith. "Continuous Auditing: An Effective Tool For Internal Auditors", Internal Auditing 21. 2 (Mart/Nisan 2006):29.

Bir kuruma sürekli denetim kurmak için aşağıdaki konuları belirlemek gerekir:

- **Konu:** Kapsamı kesin olarak belirlenebilen ve ölçülebilen konularda sürekli denetim yapılması daha kolaydır. Sağduyu veya tahmin yürütmeye dayanan konular ise sürekli denetim için uygun değildir. Bu nedenle sürekli denetim uygulaması geliştiren kurumlar tüm kurum için değil belli alanlarda çalışmalarını yoğunlaştırmayı tercih etmektedirler. Uygulanması kolay alanlardan başlayıp sürekli denetimin kapsamını genişletmek daha iyi bir stratejidir.
- **Çevre:** Faaliyetleri üzerinde kontrolleri kuvvetli olan kurumların, özellikle sürekli izleme sistemleri olanların, sürekli denetim uygulamalarını yürütmeleri daha kolaydır.

- İncelemenin nasıl yapılacağı: Sürekli denetim faaliyetlerinde kullanılmak üzere yeni analiz tekniklerinin keşfedilmesi gerekli değildir. Uygulamalarda geleneksel analizler kullanılır.
- Zamanlama: Uygun zaman dilimlerinin tespit edilmesi gerekir. İki zaman diliminden söz edilebilir. Biri denetlenen kayıtların tarih aralığı, yani raporlama dönemi, diğeri raporu hazırlamak için gereken süredir. Denetim raporunu hazırlama süresi denetim riskini kabul edilebilecek seviyede tutan en kısa zamandır. Amaç, gerçek zamanlı denetim raporları hazırlayabilmektir.

Denetçilerin sürekli denetimden faydalandığı alanlar:

- Yönetimin izleme faaliyetlerinin yeterliliğini değerlendirmek
- Kontrol sistemlerinin etkinliğine ilişkin güvence vermek
- Hata veya hileleri tespit edebilecek denetim faaliyetlerinin varlığının güvencesini vermek
- Verilerin doğruluğu ve bütünlüğüne ilişkin güvence vermek
- Riskli alanları tespit etmek ve değerlendirmek
- Yıllık denetim planını yaparken yüksek risk taşıyan alanlara yoğunlaşarak denetim kaynaklarını verimli kullanmak
- Bağımsız olarak inceleme ve değerlendirme yapmaya olanak sağlamak

Adı geçen kavramların sürekli denetimle ilişkisi aşağıdaki şekilde açıklanmıştır.

Sürekli Denetim						
Sürekli Kontrol Değerlendirmesi						Yaklaşım
Kontrol Tabanlı (kontrollerin çalıştığına dair güvence) Finansal Kontroller						Odak
İşlemlerin gerçek zamanlı ve detaylı testleri (Finansal veriler)						Analiz Teknikleri
Kontrol Güvencesi	Finansal Kanıt	Hile, İsrar, Suistimal	Denetimin Kapsamı ve Amaçları	Denetim Kayıtları Takibi	Yıllık Denetim Planı	İlgili Denetim Faaliyetleri
Kontrol İzleme	Performans İzleme		Kurumsal Karne (Balanced Scorecard)	Toplam Kalite Yönetimi	Kurumsal Risk Yönetimi	İlgili Yönetim Faaliyetleri

Şekil 4: Sürekli Denetim İle İlgili Kavramlar

Kaynak: David Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide, s. 8.

3.4. SÜREKLİ DENETİMİN İKİ ANA BİLEŞENİ: KONTROL VE RİSK

Kontrol ve risk birbirine zıt etkileri olan kavramlardır. Kontrol riskleri azaltmaya yarar. Kontrol zaafılarının tespiti ise riskli alanlara dikkati çeker. Denetçiler riskleri inceleyerek kontrol ihtiyacı olan veya kontrollerin çalışmadığı alanları tespit ederler.

3.4.1. Sürekli Kontrol Değerlendirmesi (Continuous Control Assessment)

Kurumun risklerini yönetmek için uygulanan kurallar, politikalar ve süreçler iç kontroller olarak kabul edilir. 1992 yılında Sponsor Kurumlar Komisyonu’nun (The Committee of Sponsoring Organizations-COSO) tarafından yayınlanan İç Kontroller: Kontrol Yapısı (Internal Controls: Integrated Framework) denetçilere iç kontrolleri nasıl

değerlendirmeleri gerektiğini anlatan bir kılavuz niteliğindedir. Burada yapılan tanıma göre iç kontroller kurumun hedeflerine ulaşabilmesi için aşağıdaki konularda makul güvence verebilecek şekilde tasarlanmalıdır:

- Güvenilir finansal ve operasyonel bilgi
- Yasalar, kurallar, yönetmelikler ve kurumsal politikalarla uyum
- Varlıkların korunması
- Operasyonel etkinlik
- Kurumsal faaliyetlerin amaçlarına ulaşabilmesi
- Bütünlük ve etik değerler

Bu tanıma göre iç kontroller sadece finansal konuları değil kurum faaliyetlerini ilgilendiren tüm süreçleri kapsamaktadır. Ayrıca, kurum çalışanlarının tamamı kendi görev alanına giren iç kontrollerin etkin çalışmasından sorumludur.

İlgili sürece ait iç kontroller etkin ise:

- Süreç hedeflerine etik değerler çerçevesinde ulaşır,
- doğru ve güvenilir veri üretir,
- ilgili kanun ve kurumsal politikalar ile uyumludur,
- kaynakları ekonomik ve etkin kullanır,
- varlıkları uygun biçimde korur.

Sürekli kontrol değerlendirmesi denetçilerin kontrollere ilişkin güvence vermelerini sağlayan faaliyetlerdir. Sürekli denetim kontrollerin işin yapısına uygun tasarlanmış, planlanan şekline sadık kalınarak amaçlanan şekilde çalıştığına dair yeterli güvence sağlar. Kontrol zaafları ve ihlalleri tespit edilerek kontrollerin uygun şekilde çalışıp çalışmadığı raporlanır.

Sürekli kontrol değerlendirmesi yapılan üç temel konu vardır:

1. Kontrollerin işin yapısına uygun tasarlanmış olması: Bir iş sürecine ait kontrollerin uygun tasarlanmış olup olmadığına ilgili sürece ait dokümanlar, kurumsal politikalar ve uygulamalar incelendikten sonra karar verilir. İş sürecinde önemli kontrol noktaları işlevini yapıyorsa ve süreç tamamlandığında amaçlanan görevi yerine getiriyorsa o iş süreci ve kontrolleri uygun tasarlanmış demektir. İlgili sürece ait işlemler çeşitli

kontrol kurallarına göre izlenir, kuraldışı durumlar belirlenir. Uygun tasarlanmış kontrollerin önceden belirlenmiş alt ve üst performans limitleri vardır. Bu limitlerin dışına çıkılması olağandışı durum olarak nitelendirilir. Sürecin verimi bu limitler içinde çalışmasına bağlıdır. Sürecin kontrollerinin aldığı değer bir standartla karşılaştırıldıktan sonra raporlanır. Bu raporlar sürekli denetim testlerinin planlanmasında kullanılır.

2. Kontrollerin planlanan şekline sadık kalınarak kullanılması: Planlanan ve uygulandığı düşünülen sürecin gerçekte kullanılan süreç olduğunun belirlenmesi gerekir. Yönetmelikler ve dokümantasyonda yer alan süreçler zaman içinde uygulama sırasında değişikliğe uğrayabilir. Kontrollerin bu yeni süreci dikkate alarak tekrar düzenlenmesi gerekir. Aksi halede etkinliklerini yitirebilirler.
3. Kontrollerin amaçlanan şekilde çalışması: Kontrollerin amaçlanan şekilde çalışması önemlidir. Her süreç bir sonuç verir. Ancak sonucun beklenen ve kurumsal hedefler doğrultusunda olması gerekir. İyi tarif edilmiş kontrol kuralları bir sistemin amacına uygun şekilde çalışması konusunda ön uyarı sistemi görevini görür.

Kontrollerin izlenmesi, planlanması ve korunması yönetimin görevidir. Ancak, denetim bu faaliyetlerin etkinliğini değerlendirir ve etkinliklerini arttırmak için önerilerde bulunur. Yönetimin izleme faaliyetleri ne kadar kuvvetliyse denetimin kontrollere ilişkin güvence vermek için kontroller üzerinde yapacağı detaylı testlerin miktarı o kadar azalır. Yönetimin izleme görevini yerine getirmediği durumlarda denetimin sürekli kontrol faaliyeti artar. Bu da denetim süreçlerinde ve yöntemlerinde etkisini gösterir.

İşlemler ve süreçler üzerinde yapılan sürekli kontrol değerlendirmesi hata ve anomalilerin kısa sürede ortaya çıkmasını sağlar. Sonuçlar tedbir alınması için yönetime raporlanır. Sürekli kontrol değerlendirmesi bilginin güvenilirliğine, bütünlüğüne ve faaliyetlerin etkinliğine katkıda bulunur. Ayrıca, sürekli risk değerlendirme faaliyetlerinin tamamlayıcısıdır.

Kontrollerin değerlendirilmesine ilişkin sayısız testler geliştirilebilir. Bir anomali tespit edildiğinde denetçiler bir test geliştirerek kanıt ararlar. Hile, israf veya suistimal ihtimali varsa bu testler daha sık tekrarlanır, işlemler detaylı incelenir. Ayrıca, özetleme, karşılaştırmalı analiz, toplamaların kontrolü ve diğer analiz teknikleri de kullanılır.

Hile fırsat olduğunda işlenen bir suçtur. Bu nedenle kontrollerdeki eksiklikler ve zaaflar giderildiği takdirde hile de azalacaktır.

3.4.2. Sürekli Risk Değerlendirmesi (Continuous Risk Assessment)

Risk bir durumun veya faaliyetin gerçekleşmesi durumunda doğabilecek kayıp ihtimalidir. Olası kayıplar da risk olarak adlandırılır. Kurumsal faaliyetlerin hepsi farklı derecelerde risk taşır. Kurumların karşılaşılabileceği riskler çok çeşitlidir. Bunlardan bazılarını şöyle sıralayabiliriz: finansal, operasyonel, sosyal, çevresel, etik. Risk yönetimi kurum yönetiminin gerçekleştirmesi gereken bir faaliyettir. Riskin standart bir tanımı olmadığı için derecelendirilmesi ve yönetimi konularında kurumlar arasında farklılık gözlenir. İç denetim standartları bu risklerin belirlenmesini ve makul seviyede yönetilmesini zorunlu tutmaktadır. Bu nedenle denetçiler kurumsal risk yönetimini değerlendirmek ve görüş bildirmek zorundadırlar.

Sürekli risk değerlendirmesi risk seviyelerinin tespiti ve değerlendirilmesine yönelik denetim faaliyetleridir. Trendler ve benzerlikler incelenir. Geçmiş dönemlere veya diğer sistemlere ait veriler karşılaştırılır. Denetçiler çıkan sonuçları belirlenen risk seviyesi ve riskin yapısına göre değerlendirir ve derecelendirirler. Risk değerlendirmesinin sonuçları, ziyaret edilecek yerleri saptamak, hemen detaylı inceleme başlatmak, yıllık denetim planını hazırlamak veya yönetimin faaliyetlerine ilişkin görüş bildirmek gibi çok çeşitli amaçlarla kullanılabilir.

Sponsor Kurumlar Komisyonu'nun (The Committee of Sponsoring Organizations-COSO) hazırladığı Kurumsal Risk Yönetimi (Enterprise Risk Management-ERM) anlayışı iç denetçilerin faaliyetlerini yönetici benzeri yürütmelerini önermektedir: kontrol çevresi, risk değerlendirmesi, bilgi, iletişim ve risk izleme.⁴⁵ COSO ERM iç kontrollere odaklanırken kurumsal risk yönetimi anlayışını ön planda tutar.

COSO ERM'de amaçlar dört bölüme ayrılır: stratejik, işlemler, raporlama, uyumluluk. Denetçilerin iç kontrol sistemini değerlendirmeleri ve riskleri tespit etmeleri beklenir. Denetçilerin bunları yapabilmeleri için kurumsal hedeflere, stratejilere, risk yönetimine, iş

⁴⁵ David Coderre, "Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment", Global Technology Audit Guide, s. 4.

süreçlerine ve kontrol faaliyetlerine odaklanmaları gerekir. Bu nedenle sürekli denetim sadece iç kontrollere ve kanunlara uyumluluk için kurulmaz; aynı zamanda kurumsal faaliyetlerdeki etkinliğin artması da hedeflenmektedir. Ayrıca, sürekli denetim kurumsal risklerin tespiti ve değerlendirilmesini yaparak yönetime bilgi verir.

COSO ERM iç kontrol sisteminin birbiriyle ilişkili beş bileşenini de şöyle sıralar:⁴⁶

- Kontrol Ortamı (Control Environment)
- Risk Değerlemesi (Risk Assessment)
- Kontrol Eylemleri (Control Activities)
- Bilgi ve İletişim (Information and Communication)
- İzleme (Monitoring)

COSO ERM unsurlarının denetçilere yol gösterebileceği alanlar:⁴⁷

- İç ortam ve amaç belirleme: İç denetimin rolü ve sürekli denetimin amaçları kesin biçimde ortaya konur.
- Olayları tespit etme: Tehlike ve fırsatlar karşısında istenen sonuçları almak için bir süreç belirlenir. Bu tür olayları tespit eden ve raporlayan bir sistem geliştirilir.
- Risk değerlendirme: Riskler analiz edilerek değerlendirilir. İhtimaller ve yaratacağı sonuçlar üzerinde durularak riskler karşısında alınacak önlemler belirlenir.
- Risklerle başa çıkmak: Risk sınıflaması ve faaliyetler göz önüne alınarak risklerle nasıl başa çıkılacağı belirlenir.
- Kontrol faaliyetleri: Kontrollerin değerlendirmesi sürekli yapılması gereken bir faaliyettir. Bu nedenle kontrollerin gerçek zamanlı olarak test edilmesine yönelik otomasyon gereklidir.
- Bilgi ve iletişim: Bilginin doğruluğu ve sorunların zamanında raporlanması sağlanmalıdır.
- İzleme ve gözden geçirme: Yönetim tarafından yürütülen izleme faaliyetlerini bağımsız olarak değerlendirir.

⁴⁶ Niyazi Kurnaz ve Tansel Çetinoğlu. İç Denetim - Güncel Yaklaşımlar. Kocaeli: Umuttepe Yayınları, Mayıs 2010:63.

⁴⁷ David Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide, s. 4.

4. DENETİM STANDARTLARI VE HUKUKİ ÇERÇEVE

Denetimin yapılabilmesi için denetçinin referans standartları veya performans standartları hakkında bilgi sahibi olması gerekir. Bir sistemin uygunluk veya yeterliliği bu standartlar tanımlanmadan ölçülemez. Kurumsal politikalar, ürün/ süreç standartları, kontratlar vb. referans noktalarıdır. Ancak, tüm bunların üzerinde denetçiye yol gösteren kanun ve yönetmelikler vardır. Denetimin yasal dayanağı ilk alınacak referans noktasıdır.⁴⁸

4.1. DENETİM STANDARTLARI

Bağımsız denetim ile sermaye piyasalarının etkinliği ve gelişmesi hedeflenirken yatırımcıların haklarının korunması da ön plana çıkmaktadır. Günümüz ihtiyaçlarıyla şekillenen iç denetim kurumsal faaliyetlerin etkinliğinin ve veriminin artmasını, çalışanların ve ortaklarının haklarının korunmasını amaç edinmiştir.

Denetimin ekonomik ve sosyal faydaları nedeniyle vazgeçilmezliği yadsınamaz. Ancak, denetimin getirdiği maliyetler de küçümsenemez. Kurumların konulan denetim standartlarına uyumu için harcamak zorunda oldukları zaman, para, emek gibi kaynaklar denetimden sağladıkları yararı aşmamalıdır. Bu dengeyi bulmak kanun koyucuların karşılaştıkları belki de en büyük zorluktur.

Kurumların nasıl denetleneceği denetim standartlarıyla belirlenir. Uluslararası kurumlar denetim standartlarının genel çerçevesini belirlerken her ülkenin denetimle ilgili kendi standartları vardır.

Denetim standartlarına uymayanlar ve hileye karışanlar hakkında verilecek cezalar da her ülkenin kendi kanunlarında yer almaktadır. Kanunlar ve verilen cezalar her ülkenin anlayışına göre farklılık göstermektedir. Örneğin, Amerika Birleşik Devletleri ve İngiltere’de küçük hisse sahiplerine tanınan azınlık hakları Almanya’daki azınlık haklarına göre daha fazladır.⁴⁹

⁴⁸ J. P. Russell (Ed.), The Quality Audit Handbook. A.B.D.: American Society For Quality, 2000:46.

⁴⁹ Rezaee ve Riley, Financial Statement Fraud Prevention And Detection, s.132.

4.2. ULUSLARARASI DENETİM STANDARTLARINI BELİRLEYEN KURUMLAR

Uluslararası Muhasebeciler Federasyonu (International Federation of Accountants-IFAC) tarafından kurulmuş olan Uluslararası Denetim ve Güvence Standartları Kurulu (International Auditing and Assurance Standards Board-IAASB) uluslararası denetim standartlarını belirlemektedir. Bu standartları Uluslararası Denetim Standartları (International Standards of Auditing-ISA) ve Uluslararası Denetim Çalışmaları Açıklamaları (International Auditing Practice Statements-IAPS) adıyla yayımlamaktadır. “Bu kurumun değişik komisyonlarında kabul gören düzenlemeler tüm ülkelerde kaynak belgeler olmaktadır.”⁵⁰

Yüce Denetim Kurumları Uluslararası Örgütü (International Organization of Supreme Audit Institutions-INTOSAI) altına faaliyet gösteren Denetim Standartları Komisyonu (Auditing Standards Committee) IAASB’nin çalışmalarına yardımcı olmaktadır.⁵¹

Adı geçen uluslararası kuruluşların yayımladıkları denetime ilişkin standartlar genel çerçeveyi çizen niteliktedir. Uluslar, kendi denetim standartlarını belirlerken bu standartları yol gösterici temel ilkeler olarak kabul eder, belli konulara cevap verecek şekilde detaylandırırlar.

Amerika Birleşik Devletleri’nde kurulmuş olan İç Denetçiler Enstitüsü’nün (Institute of Internal Auditors-IIA) yayınladığı İç Denetçiler İçin Uluslararası Standartlar (International Professional Standards for the Practice of Internal Auditing) iç denetim uygulamaları için uluslararası kabul gören standartlar halini almıştır. Uluslararası Standartlar Kurumu’nun (International Organization for Standardization-ISO) yayınladığı standartlar gün geçtikçe önem kazanmaktadır. ISO standartlarının gün geçtikçe artan etkisi görülmektedir.⁵²

Uluslararası Standartlar Kurumu’nun (International Organization for Standardization-ISO) Denetim Standartları Açısından Önemi:

Uluslararası Standartlar Kurumu (International Organization for Standardization-ISO) Cenevre, İsviçre merkezli birçok ulusun katılımıyla çeşitli konularda uluslararası standartların belirlenmesi amacıyla İkinci Dünya Savaşı’ndan sonra kurulmuştur.

⁵⁰ Hasan Kaval. Muhasebe Denetimi. 2. Basım. Ankara: Gazi Kitabevi, Ekim 2005:28.

⁵¹ Moeller, s.725.

⁵² Moeller, s.728.

ISO standartları ilk aşamada ekonomisini yeniden düzeltmeye çalışan Avrupa ülkeleri ve Japonya tarafından benimsenmiştir. 1950’li ve 1960’lı yıllarda Amerika Birleşik Devletleri’nden bazı bilim adamlarının katkılarıyla bu standartlar geliştirilmiştir. Ancak, bu standartlar Amerika Birleşik Devletleri’nde 1970’li yılların sonlarına doğru Amerika’da Japonya’nın ekonomik başarısı hissedilene kadar ilgi görmemiştir.

ISO standartları birçok ülke için uyum sağlayacakları ve kendi uygulamalarını karşılaştıracakları yol gösterici nitelik taşımaktadır. ISO 19011 denetimin temel ilkelerini beş ana başlıkta açıklamıştır:

1. Etik değerler
2. Dürüst sunum
3. Profesyonelce yaklaşım
4. Bağımsızlık
5. Kanıt temelli yaklaşım

Yıllar içinde kurumsal yönetim ve kalite ile ilgili standartlar da oluşturmuştur. ISO 9001 kalite standartları ve ISO 27001 bilgisayar güvenliği standartları denetçiler için en önemli ISO standartları olmuştur. Amerikan Yeminli Muhasebeciler Odası (American Institute of Certified Public Accountants-AICPA) ISO 9001 belgesi almış dünyadaki ilk meslek kuruluşu olmuştur.⁵³

ISO 9001 ile Sarbanes-Oxley kanunlarının önemli konularda birçok ortak noktası vardır. Bunlardan bazıları şöyle sıralanabilir:

- denetçilerin bağımsızlığı
- finansal raporlarda yöneticilerin sorumluluğu
- kurumsal etik değerlerin oluşmasında yöneticilerin sorumluluğu
- iç kontrollerin etkinliğinde yöneticilerin rolü
- hile tespit edildiğinde yöneticilerin sorumlu tutulması

⁵³ Moeller, s.670.

4.3. SARBANES-OXLEY KANUNU

Amerika Birleşik Devletleri'nde resmi adı Halka Açık Şirketler Muhasebe Reformu ve Yatırımcıyı Koruma Kanunu (Public Accounting Reform and Investor Protection Act) Ağustos 2002'de kanunlaştı. Bu kanuna ilişkin düzenlemelerin tamamlanması 2003 yılı sonuna kadar sürdü. Bu kanun önerisi senatör Paul Sarbanes ve Temsilciler Meclisi üyesi Michael Oxley tarafından gündeme getirildiği için iş çevrelerinde daha ziyade Sarbanes-Oxley Kanunu olarak anılmaktadır.

Temelde üç amacı desteklemektedir: doğruluk, güvenilirlik, sorumluluk⁵⁴. Sarbanes-Oxley kanunlarının amacı finansal verilerin doğruluğunu, bilgilerin güvenilirliğini sağlamak ve yönetimin bu konudaki sorumluluğunu ortaya koymaktır. Toplumun sermaye piyasalarına olan güvenini kazanmak için çıkartılan bu kanun, denetim standartları ve kurumsal yönetim anlayışında büyük değişikliklere yol açmıştır.

Sarbanes-Oxley dış denetim ilkelerini yeniden düzenlerken yönetim kurulu ve üst düzey yöneticilere yeni sorumluluklar vermiştir. Bu kanunda iç denetimin rolü ve sorumlulukları açıkça belirtilmese de iç kontrollere ilişkin değerlendirmeler yer almaktadır. Daha sonra çıkan Denetim Standardı 5'te iç kontrole ilişkin düzenlemeler açıklanmıştır.

Sarbanes-Oxley Kanunu'nun önemli bölümleri aşağıdaki gibidir:

- Bölüm 101: Halka Açık Şirketler Muhasebesi Gözetim Komisyonu'nun (Public Company Accounting Oversight Board-PCAOB) kuruluşu ve üyelik koşullarıyla ilgili bilgiler yer almaktadır. Halka açık şirketlere ilişkin dış denetim standartlarının belirlenmesi ve denetlenmesi Sermaye Piyasası Kurulu (Securities and Exchange Commission-SEC) çatısı altında kurulan bu yeni kurula verilmektedir.
- Bölüm 104: Bağımsız denetim firmalarının PCAOB tarafından kontrol edilmesine ilişkin düzenlemeleri içermektedir.
- Bölüm 108: Denetim standartlarının PCAOB tarafından belirleneceğini açıklamaktadır.
- Bölüm 201: Bağımsız denetim firmalarının inceledikleri firmaların iç denetim faaliyetlerini yürütmelerini, defterlerini tutmalarını, finansal sistemlerini kurmalarını, yatırım danışmanlığı ve diğer danışmanlık hizmetleri vermelerini yasaklamaktadır. İç

⁵⁴ Coderre, Internal Audit, s.80.

denetimin işlevinin bağımsız denetim firmaları aracılığıyla yapılmasının sakıncaları Enron skandalı ile ortaya çıkmıştır. Enron çoğu iç denetim faaliyetini bağımsız denetimini de yaptırdığı Arthur Andersen firmasına vermişti. Soruşturma sırasında iç ve dış denetimin aynı firma tarafından yürütülmesinin denetimin bağımsızlığı ilkesini zedelediği ve sorunların ortaya çıkmasını engellediği tespit edilmiştir.

- Bölüm 203: Bağımsız denetçinin en az beş yılda bir değişmesini öngörmektedir.
- Bölüm 206: Denetçilerin son bir yılda denetimini yaptığı kuruma genel müdür, finans veya muhasebeden sorumlu yönetici olarak atanmaları yasaklanmıştır. Sarbanes-Oxley kanunlarından önce bağımsız denetim firmaları kendi elemanlarını denetledikleri kurumlara yönetici olarak gönderebiliyordu⁵⁵. Bu da bağımsız denetçiler ile yöneticiler arasında arkadaşlık ilişkisinin olmasına ve sorunların ortaya konmasında daha isteksiz davranmalarına yol açabilmekteydi.
- Bölüm 301: Denetim komitesi üyelerinin bağımsız yöneticilerden oluşması gerektiği belirtilmiştir. Bağımsız denetim firması denetim komitesine rapor vermekle yükümlüdür. Denetim faaliyetleri ve anlaşmazlıkların çözümü görevi denetim komitesine verilmiştir.
- Bölüm 302: Finansal tablolardan kurumun sorumlu olmasına ilişkin ilkeler yer almaktadır. Buna göre finansal raporlar yayımlanmadan önce genel müdür ve finans koordinatörü tarafından onaylanmalıdır. Finansal tablolarda sonradan ortaya çıkan hatalardan da kanun karşısında sorumludurlar. Ayrıca, iç kontrollerin doğruluğu ve yeterliliğinden de sorumlu olup tüm kontrol zaaflarını ve ilgili hileleri de açıklamak zorundadırlar.
- Bölüm 305: Yöneticilerin kanunsuz veya hileli işlemlerden edinilen kazanç nedeniyle aldıkları primlerin iadesini öngörmektedir.
- Bölüm 404: İç denetim bölümünün yılda en az bir defa kurumda uygulanan iç kontrolleri değerlendirmesi istenmektedir. İç denetim bölümüne kurumda iç denetim faaliyetlerini düzenleme, test etme görevi verilmiş ve bu incelemelere ilişkin belgelerin bağımsız denetçilere verilmesi istenmiştir. Bağımsız denetçiler de raporlarında bu kontrolleri incelediklerini ve bu kontrollerin doğru ve yeterli olduğunu belirtmek zorundadırlar.
- Bölüm 407: İç denetim bölüm başkanının finansal konularda bilgili bir kişi olmasını öngörmektedir.

⁵⁵ Moeller, s.55.

- Bölüm 408: Sermaye Piyasası Kurulu'nun kurumun açıkladığı bazı bilgilere ilişkin detaylı inceleme yapabileceğine dair düzenlemeleri içermektedir.
- Bölüm: 409: Bağımsız denetim firmalarının finansal raporlara ve kurum faaliyetlerine ilişkin açıklamaları gecikmeden yapmaları gerektiğini belirtmektedir. Bilgilerin güncel olmasını sağlama amaçlı olan bu düzenleme, kuruma ilişkin bilgilerin ortaya çıktığı anda Sermaye Piyasası Kurulu'nun Internet sitesinde yayınlanmasını öngörmektedir.
- Bölüm 802: Bu bölümde kanuni soruşturma sürerken ilgili belgelerin yok edilmesi ve tahrifatı söz konusu olduğunda verilecek cezalar belirtilmiştir. Ayrıca, denetim ve incelemelere ilişkin tüm belgelerin beş yıl süreyle saklanması öngörülmektedir.
- Bölüm 906: Genel müdür ve finans yöneticilerinin onayladıkları finansal raporlarda hileli veya yanıltıcı bilgi bulunmasından kaynaklanan sorumlulukları ve verilecek cezalar belirtilmektedir.
- Bölüm 1105: Suçlu bulunan bir yöneticinin halka açık başka bir kurumda çalışmasının yasaklanmasına ilişkin Sermaye Piyasası Kurulu'na yetki vermektedir.

Enron ve WorldCom'un iflaslarından sonra kabul edilen Sarbanes-Oxley Kanunu denetim kavramını öne çıkartmış ve denetleyen kurumlar üzerindeki kontrolleri arttırmıştır. Araştırmalar 2003 yılından sonra tespit edilen hilelerde büyük artış olduğunu ortaya koymuştur⁵⁶:

- Tespit edilen rüşvet olayları %71 oranında artmıştır.
- Kara para aklama planları %133 oranında artmıştır.
- Finansal verilerde bulunan hatalar % 140 oranında artmıştır.

Son yıllarda tespit edilen hata ve hilelerin oranındaki bu artış Sarbanes-Oxley kanunlarının etkisi olarak görülmektedir.

Denetimin hangi sıklıkla yapılacağı Sarbanes-Oxley Kanunu'nun ele almadığı bir konudur.⁵⁷ Ancak, geliştirilen iç denetim faaliyetleri ve yöneticilerin artan sorumlulukları nedeniyle denetim faaliyetlerine verilen önem sürekli denetim sistemlerinin kurulmasını olumlu etkilemektedir.

⁵⁶ Rezaee ve Riley, Financial Statement Fraud Prevention And Detection, s.8.

⁵⁷ El-Masry ve Reck, s. 780.

Bazı araştırmacılara göre 2008 finansal krizi ve son dönemlerde yaşanan skandallar Sarbanes-Oxley kanunlarının daha ziyade yatırımcılara psikolojik açıdan güven verdiği yolundadır. Tarafsız bakıldığında hukuki çerçeve ve kurumsal yönetimde köklü değişikliklere yol açtığı görülmektedir.

4.4. AMERİKA BİRLEŞİK DEVLETLERİ'NDE DENETİM İLE İLGİLİ KURUMLAR VE UYGULANAN STANDARTLAR

Sarbanes-Oxley kanunları çıkmadan önce bağımsız denetime ilişkin standartların belirlenmesi Amerikan Yeminli Muhasebeciler Odası'nın (American Institute of Certified Public Accountants-AICPA) göreviydi. Genel kabul görmüş denetim standartları uygulanmakta olup yeni çıkartılan standartlar Denetim Standartları Açıklamaları (Statements of Auditing Standards-SASs) adı altında yayınlanmaktaydı.

Sarbanes-Oxley kanunları yürürlüğe girdikten sonra bağımsız denetime ilişkin standartları yapma görevi Sermaye Piyasası Kurulu (Securities and Exchange Commission-SEC) tarafından kurulan Halka Açık Şirketler Muhasebesi Gözetim Komisyonu'na (Public Company Accounting Oversight Board-PCAOB) verilmiştir.

İç Denetçiler Enstitüsü (Institute of Internal Auditors-IIA) iç denetim standartlarını belirleyerek İç Denetçiler İçin Uluslararası Standartlar (International Professional Standards for the Practice of Internal Auditing) adı altında yayımlamıştır.

Sarbanes-Oxley kanunlarından sonra Sponsor Kurumlar Komisyonu'nun (Committee of Sponsoring Organizations-COSO) iç kontrollere ilişkin standartları muhasebe kontrollerini ölçme ve değerlendirme için kullanılmaktadır.

Bilgisayar Sistemleri Denetim ve Kontrol Enstitüsü (Information Systems Audit and Control Association-ISACA) bilgisayarla ilgili faaliyetlerin denetlenmesi amacıyla kurulmuştur. Bilgisayar denetim standartları olan CobiT (Control objectives for information and related Technology) bu kurum tarafından belirlenmektedir. COSO standartlarının bilgisayar teknolojilerinin denetimindeki eksiklikleri CobiT standartları tamamlamaktadır.

Bilgi Teknolojileri Yönetim Enstitüsü (IT Governance Institute) Amerikan Kalite Derneği (American Society for Quality) için iç denetim standartlarını belirlemektedir.

Sürekli Denetimle İlgili Standartlar:

Elektronik ortamlarla birlikte sürekli denetimin gündeme gelmesi ve bu bağlamda elektronik denetim kanıtlarının toplanması gereği Amerika Birleşik Devletleri'nde bu konuda ilgili denetim standartlarının belirlenmesine yol açmıştır. Günümüzde sürekli denetimle ilgili standart bazında düzenlemeler Amerika Birleşik Devletleri'ndeki ve Kanada'daki muhasebe birliklerinde görülmektedir. Yapılan düzenlemeler şöyledir:⁵⁸

- 1996 Denetim Standartları Komitesi (Auditing Standard Board -ASB)
SAS No: 80 “Denetim Kanıtları”
- 2002 Denetim Prosedürleri Çalışmaları (Auditing Procedures Study- APS)
SAS No: 94 “Denetçinin Finansal Tablo Denetiminde Bilgi Teknolojilerinin İç Kontrol Üzerine Etkilerinin Değerlenmesi”

Bu iki standart bazındaki düzenleme denetçilere sürekli denetim konusunda yol gösteren standartlardır. Ancak en iyi açıklama ve en son yapılan düzenleme olması nedeniyle en kapsamlısı SAS No: 94'dür. Bu standartta yapılan düzenlemeler bilgi teknolojilerinin iç kontrol yapısı üzerine olan etkileri, sürekli denetimde kullanılan bilgi teknolojisi kontrollerinin türleri ve gerçek zamanlı muhasebe sistemlerindeki finansal raporların süreci ile ilgilidir.

Sürekli denetimin uygulanabilmesi için kurumun iç kontrol yapısının iyi bir şekilde ele alınması, anlaşılmasına çalışılması ve söz konusu risklerin belirlenmesi gerekir. Sürekli denetimde iç kontrol sistemi üzerine yoğunlaşmak ve sistemin etkinliğini ve verimliliğini ölçmek temel amaçtır. Bu tür sistemlerde aşağıdaki gibi riskler görülebilir:

- Sisteme girilen verinin sürekli olarak güvenilir olamayan şekilde ve hatalı olarak girilmesi nedeniyle bilginin güvenilirliğinin azalması,
- İşlemlere ve kayıtlara sistem dışından yetkisiz kişilerce erişim ve bu nedenle de işlemlerin ve kayıtların bozulması veya uygun olmayan şekilde düzeltilmesi,

⁵⁸ Seval Kardeş. “Denetim Olgusunun Kurumsal Kaynak Planlaması (ERP) Sistemleriyle Bütünleştirilmesi”. <http://archive.ismmmo.org.tr/docs/sempozyum/07Sempozyum/11-SEVAL%20KARDE%20C5%9E%20SEL%20C4%B0MO%20C4%9ELU.doc> (12 Aralık 2008).

- Yetkisiz olarak bilgisayar programlarının deęiřtirilmesi,
- Yapılmak zorunda olan deęiřikler nedeniyle bilgisayar programlarındaki deęiřimlerin başarısızlıkla sonuçlanması,
- Verinin kaybolma olasılıęı,
- Sisteme uygun olmayan bir řekilde verinin elle girilmesi.

Denetçi, sürekli denetim yaparken iç kontrol sistemlerini deęerlendirme ařamasında var olan riskleri tespit etmeli ve kabul edilebilir kontrol riski düzeyini belirleyerek yapacaęı denetime ait denetim planını hazırlamalıdır. Kurumsal kaynak planlaması sistemlerine sahip řiřletmelerde genelde iç kontrol sisteminin güvenilirlięini saęlamak için söz konusu olan bu riskleri azaltmakta SYSTRUST, WebTRUST ve WebTRUST-ISP vb. güvenlik sistemleri kullanılmaktadır. Bu güvenlik sistemlerinin temel amacı bilgi sisteminin güvenilirlięini en üst düzeyde tutacak řekilde korumaktır. (AICPA/CICA) SYSTRUST sistemi Amerika Birleřik Devletleri ve Kanada'daki muhasebeci birliklerinin ortaklařa hazırladıkları bir güvenlik sistemidir. SYSTRUST güvenlik sistemi kurumsal kaynak planlaması sistemi kurulurken řiřletmeye sistemin bir parçası řeklinde entegre olarak kurulmakta ve çalıştırılmaktadır. Denetçi, denetim raporunda kurumun iç kontrol sisteminin güvenilirlięini belirtirken kullanılan SYSTRUST sisteminin ilkeleri ve ölçütlerine uyulmak suretiyle bu güvenilirlięe ulařıldığına ilişkin görüş belirtir.

Bunların yanı sıra SAS No. 94'de denetçinin veri analizinde kullanacaęı bilgisayar destekli denetim tekniklerine de (CAAT- Computer Assisted Auditing Tests) deęinilmektedir. Söz konusu bu tekniklerin kullanılmasıyla da SAS 80'e göre denetçinin sayıca oldukça yüksek miktarda elektronik bilgiye kolayca ulařabilmesi de denetçinin hata ve hileyi tespit edememe riskini azaltacaęı beklenmektedir. Ayrıca toplanacak olan kanıtlara dayanarak denetçi yapacaęı maddi doęruluk testlerinin zamanını, kapsamını ve yapısını belirler.

4.5. TÜRKİYE'DEKİ DENETİM MEVZUATI VE SÜREKLİ DENETİMİN HUKUKİ ÇERÇEVESİ

Günümüzde kullanılan denetime ilişkin standartlar 2003 yılında oluşturulmaya başlanmıştır. Bu standartlar hazırlanırken göz önüne alınan en önemli konu Türk denetim standartlarının uluslararası standartlara ve Avrupa Birlięi mevzuatına uyumunu saęlamak olmuştur.

5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu, SPK düzenlemeleri, Bankacılık Kanunu ve Türk Ticaret Kanunu Türkiye’deki denetimin hukuki dayanağını oluşturmaktadır.

4.5.1. 5018 sayılı Kamu Mali Yönetimi ve Kontrol Kanunu

2003 yılında kabul edilmiş ve 1 Ocak 2006 tarihinde yürürlüğe girmiştir. “Yürürlüğe girdiği şekliyle kanun Avrupa Birliği müktesebatına paraleldir. AB Müktesebatının 32 numaralı başlığı olan Finansal Kontrol; Kamu İç Mali Kontrol Sistemi, Dış Denetim ve AB Fonlarının Korunması alt başlıklarından oluşmaktadır.”⁵⁹

5018 sayılı kanunun 5. kısmı olan ‘İç Kontrol Sistemi’ iç denetimle ilgili düzenlemelerin açıklandığı bölümdür. Bu bölümde iç denetim ile iç denetçinin görevleri, nitelikleri ve atanmasına ilişkin maddeler vardır. İç Denetim Koordinasyon Kurulu ve bu kurulun görevleri de bu bölümde tanımlanmıştır.

5018 sayılı kanunu daha önceki denetimi düzenleyen kanunlardan ayıran en önemli fark kurumsal risk yönetimine bakış açısıdır. Bu kanunda kurumsal risk yönetiminin etkinliğinin denetimi iç denetimin görevi kabul edilmektedir. Bu nedenle risk yönetim süreçlerinin denetimi zorunlu hale gelmektedir. Bu durum Uluslararası İç Denetim Enstitüsü’nün açıkladığı iç denetimin görev tanımıyla örtüşmektedir.

Bu kanunla birlikte kamu yönetimi bağlamında iç denetim gelecek hedefli, riskleri daha fazla dikkate alan, risk yönetimi süreçlerinin değerlendirilmesi faaliyetini kapsayan ve risk odaklı denetimden risk yönetimi temelli denetime geçişin ilk adımlarını atan bir niteliktedir.⁶⁰

5018 sayılı kanunda yer alan maddeler çoğunlukla uluslararası standartlar gözetilerek hazırlanmıştır. Ancak, denetimin raporlanması ile ilgili düzenleme uluslararası standartlara uymamaktadır. Kanunda iç denetçilerin raporlarını ‘doğrudan üst yöneticiye sunması’ beklenmektedir. Bu da yine aynı kanunda vurgulanan ‘iç denetçilerin bağımsızlığı’ ilkesi ile ters düşmektedir.

⁵⁹ Davut Pehlivanlı, Modern İç Denetim. İstanbul: Beta Basım, 2010, s.24.

⁶⁰ Pehlivanlı, Modern İç Denetim, s.24.

5018 sayılı kanunla ‘kamu idarelerinin iç denetim sistemlerini izlemek, bağımsız ve tarafsız bir organ olarak hizmet vermek’ amacıyla İç Denetim Koordinasyon Kurulu kurulmuştur. Bu kanunda bu kurulun görevleri açıklanmıştır. “Bu kurul kanunda sıralanan görev çerçevesi ve amaçları itibarıyla Uluslararası İç Denetim Enstitüsü’nü anımsatır bir yapıdadır.”⁶¹ İç Denetim Koordinasyon Kurulu 2006 yılında Kamu İç Denetim Standartları ve Kamuda İç Denetçileri Meslek Ahlak Kuralları’nı yayınlamıştır.

Maliye Bakanlığı tarafından 2006 yılında yayınlanan İç Denetçiler Çalışma Usul ve Esasları Hakkında Yönetmelik 5018 sayılı kanunun 65. maddesine göre düzenlenmiştir. Bu yönetmelikte kurumsal risklerin değerlendirilmesi ve sıralanması gerektiğinden bahsedilmektedir. Ayrıca, denetim planını hazırlarken bu risklerin göz önüne alınması gerektiği vurgulanmaktadır.

4.5.2. Sermaye Piyasası Kurulu Düzenlemeleri

Sermaye Piyasası Kurulu (SPK) denetimi ilgilendiren düzenlemeleri Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ (Seri: X, No: 22) ile yapmıştır. Bu tebliğ 2006 yılında çıkmıştır. Sonraki yıllarda bazı düzenlemeler yapılmış ve Seri X’un 23, 24, 25, 26, 27 numaralı tebliğleri olarak yayınlanmıştır. Bu tebliğin amacı “sermaye piyasasında bağımsız denetim faaliyetine, bu faaliyette bulunmak üzere Kurulca yetkilendirilecek bağımsız denetim kuruluşlarına ve bağımsız denetçilere ilişkin standart, ilke, usul ve esasları belirlemektir”.

Bu tebliğde sürekli denetime ilişkin esaslar açıkça belirtilmese de elektronik ortamda denetimin yapılması ve elektronik ortamda çalışma kağıtlarının tutulmasına yönelik açıklamalar bulunmaktadır.

Belgelendirmenin kapsamı ve şekli; işletmenin yapısı, büyüklüğü ve faaliyetlerinin karmaşıklığı ile iç kontrol sistemine, işletmeye ait bilgilerin elde edilebilirliğine, bağımsız denetim metodolojisi ve bağımsız denetim sırasında kullanılan teknolojilere bağlı olarak biçimlenir. Bu kapsamda, işlemleri ağırlıklı olarak elektronik ortamda gerçekleşen, kaydedilen, işlenen ve raporlanan karmaşık bir bilgi sistemi hakkındaki

⁶¹ Pehlivanlı, Modern İç Denetim, s.25.

saptamaların belgelendirilmesi iş akış şemaları, formlar ve karar tablolarını içerebilir.⁶²

Çalışma kâğıtları kâğıt ya da elektronik ortam veya diğer şekillerde tutulabilir. Bu kapsamda bağımsız denetim programları, analizler, önemli konuların özeti, doğrulama mektupları, işletme yönetimi teyit mektupları, kontrol listeleri, elektronik posta dahil önemli konularla ilgili yazışmalar çalışma kâğıtları olarak sınıflandırılabilir. Gerekli görüldüğü takdirde önemli ve özellik arz eden sözleşmelerin kopyaları çalışma kâğıtları olarak saklanabilir.⁶³

Bilgisayar destekli bağımsız denetim teknikleri elektronik işlem ve hesapların daha geniş kapsamlı testine imkan verir. Bu tür teknikler, örnek işlemlerin veritabanından seçilmesi, özelliklerine göre sınıflandırılması veya örnekler yerine verilerin tamamının teste tabi tutulmasına olanak sağlar.⁶⁴

Bilgiler elektronik formda ise, bağımsız denetçi bazı bağımsız denetim tekniklerini bilgisayar destekli programları kullanarak gerçekleştirebilir.⁶⁵

Sürekli denetimin yapılabilmesi için denetim kanıtlarının bilgisayar ortamında tutulması, analizlerin ve raporlamanın bilgisayar kullanılarak yapılması gerekmektedir. SPK tebliğinde yer alan bu maddeler elektronik ortamda yapılacak denetimlerin hukuki dayanağını oluşturmaktadır. Yukarıda belirtilen maddeler esas alındığında denetim kanıtlarının elektronik ortamda tutulması, bilgisayar destekli analiz tekniklerinin kullanılması ve denetim sonuçlarının elektronik ortamda raporlanması denetim standartları ile uyumludur.

SPK tebliğinde elektronik ortamda denetim yapmanın riskleri açıklanmış ve veri bütünlüğünün sağlanmasına dikkat çekilmiştir. “Bilgi sisteminden gelen bilgiler bağımsız

⁶² Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ (Seri: X, No: 22) Onuncu Kısım: İşletmenin, Faaliyet Koşullarının ve Çevresiyle Olan İlişkilerinin Anlaşılması ve Bu Konulara İlişkin Önemli Yanlışlık Riskinin Değerlendirilmesi, Dördüncü Bölüm: İşletme Yönetimi ve Yönetimden Sorumlu Kişilerle İletişim ve Belgelendirme, Madde 26: Belgelendirme.

⁶³ Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ (Seri: X, No: 22) Beşinci Kısım: Bağımsız Denetim Çalışmasının Belgelendirilmesi, Birinci Bölüm: Çalışma Kâğıtları ve Nitelikleri, Madde 5: Çalışma kâğıtlarının niteliği.

⁶⁴ Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ (Seri: X, No: 22) Onikinci Kısım: Değerlendirilmiş Risklere Karşı Uygulanacak Bağımsız Denetim Teknikleri, Birinci Bölüm: Finansal Tablolardaki Önemli Yanlışlık Risklerine Karşı Yapılacak İşlemlerin ve Uygulanacak Ek Bağımsız Denetim Tekniklerinin Belirlenmesi, Madde 7: Ek bağımsız denetim tekniklerinin kapsamı.

⁶⁵ Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ (Seri: X, No: 22) Ondördüncü Kısım: Bağımsız Denetim Kanıtı, İkinci Bölüm: Bağımsız Denetim Kanıtları Toplamak Amacıyla Uygulanan Bağımsız Denetim Teknikleri, Madde 6: Bağımsız denetim teknikleri.

denetim sırasında kullanılıyorsa, bağımsız denetçinin bilgi sisteminin doğruluğu ve bütünlüğü hakkında da kanıt toplaması gerekir.”⁶⁶

4.5.3. Bankacılık Kanunu

2005 yılında yürürlüğe giren 5411 sayılı Bankacılık Kanunu’nun Kurumsal Yönetim başlığını taşıyan üçüncü kısmı bankalardaki iç denetim uygulamalarının nasıl yapılması gerektiğini açıklar. Bu bölümde sürekli kontrol değerlendirmesinin önemli olduğu ve bu denetimi yönetim kuruluna bağlı bağımsız bir birimin yapması gerektiği belirtilmiştir.

Bankalar, iç kontrol sistemi kapsamında, faaliyetlerinin mevzuata, iç düzenlemelerine ve bankacılık teamüllerine uygun olarak yürütülmesini, muhasebe ve raporlama sisteminin bütünlüğünü, güvenilirliğini ve bilgilerin zamanında elde edilebilirliğini her seviyedeki personeli tarafından uyulacak ve uygulanacak sürekli kontrol faaliyetleri ile sağlamak, görevlerin fonksiyonel ayrımlarını, yetki ve sorumlulukların paylaşımını, fon ödemelerini, banka işlemlerinin mutabakatını, varlıkların korunmasını ve yükümlülüklerin kontrol altında tutulmasını temin etmek, maruz kalınan her türlü riskin tanınması, değerlendirilmesi ve yönetimi için gerekli alt yapıyı hazırlamak ve yeterli iletişim ağını oluşturmak zorundadır. İç kontrol faaliyetleri yönetim kuruluna bağlı olarak çalışacak iç kontrol birimi ve personeli tarafından yürütülür.⁶⁷

Bankacılık Kanunu’nda sürekli denetime ilişkin belirgin bir hüküm bulunmamaktadır. Ancak, bu kanunda yer alan sürekli kontrol faaliyetlerinin desteklenmesi yönündeki maddeler sürekli denetim uygulamalarını destekleyici niteliktedir.

Bankacılık Düzenleme ve Denetleme Kurumu tarafından yayınlanan Bankaların İç Sistemleri Hakkında Yönetmelik, bankaların denetlenmesine ilişkin düzenlemelere açıklık getirmiştir. Bu yönetmelikte yer alan maddeler uluslararası standartlarla uyum içinde olup risk yönetimi sisteminin etkinliğinin denetlenmesine vurgu yapmaktadır.

⁶⁶ Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ (Seri: X, No: 22) Onikinci Kısım: Değerlendirilmiş Risklere Karşı Uygulanacak Bağımsız Denetim Teknikleri, Birinci Bölüm: Finansal Tablolardaki Önemli Yanlışlık Risklerine Karşı Yapılacak İşlemlerin ve Uygulanacak Ek Bağımsız Denetim Tekniklerinin Belirlenmesi, MADDE 5: Ek bağımsız denetim tekniklerinin yapısı.

⁶⁷ 5411 sayılı Bankacılık Kanunu, Üçüncü Kısım: Kurumsal Yönetim, İkinci Bölüm: İç Sistemler, Madde 30: İç kontrol sistemi.

5.5.4. Türk Ticaret Kanunu ve Türkiye Finansal Raporlama Standartları

2011 yılında kabul edilen 6102 sayılı Türk Ticaret Kanunu muhasebe ve finansal raporlama konularında standartları belirlemeyi Türkiye Muhasebe Standartları Kurumu'na bırakmıştır. “Anonim şirketin ve şirketler topluluğunun finansal tabloları denetçi tarafından, uluslararası denetim standartlarıyla uyumlu Türkiye Denetim Standartlarına göre denetlenir.” (Madde 397)

Dayanağını 6102 sayılı Türk Ticaret Kanunu'ndan alan ve 2011 yılında kabul edilen 660 sayılı Kamu Gözetimi, Muhasebe ve Denetim Standartları Kurumunun Teşkilat ve Görevleri Hakkında Kanun Hükmünde Kararname “bağımsız denetime, bağımsız denetim kuruluşlarına ve bağımsız denetçilere ilişkin usul ve esasları düzenlemektir”. Bu kararnamede bilgisayar ortamında yapılan herhangi bir denetim şekline ilişkin açık bir düzenleme bulunmamaktadır. Ancak, 660 sayılı kararnamenin 38. maddesinde yer alan “elektronik, manyetik ve benzeri ortamlarda tutulanlar dahil tüm kayıtlar” ibaresi bilgisayar ortamında bulunan belgelerin denetim kanıtı olarak kullanılabilmesine olanak sağlamaktadır.

Türkiye Muhasebe Standartları Kurumu tarafından yayınlanan Türkiye Finansal Raporlama Standartları Uluslararası Finansal Raporlama Standartları ile uyumludur. Sanayileşmiş ülkelerle aynı finansal raporlama standartlarını uygulamak Türk piyasalarına uluslararası nitelik kazandırmakta ve Türk işletmelerinin uluslararası piyasalarda işlem görmesini kolaylaştırmaktadır.

5. SÜREKLİ DENETİM MODELLERİNİN DEĞERLENDİRİLMESİ

Akademisyenler tarafından birçok sürekli denetim modeli geliştirilse de bu modeller birbirlerinden sadece detaylarda farklılaşmaktadır. Bütün bu geliştirilen modellerde aşağıda belirtilen üç unsur mutlaka yer almaktadır:⁶⁸

1. Kurumun faaliyetleri neticesinde ortaya çıkan işlemlere ilişkin verileri eşzamanlı veya bu verilerin ortaya çıkmasından çok kısa bir süre sonra tanımlayıp veri işleme sürecine dahil edebilen, muhasebe bilgi sistemini de içine alan elektronik temelli “Kurumsal Bilgi Sistemi”,
2. Denetlenen işletmenin faaliyetleri neticesinde ortaya çıkan işlemlere ilişkin verileri eşzamanlı veya bu verilerin ortaya çıkmasından çok kısa bir süre sonra izleyip, denetimle ilgili işlemlerin gerçekleştirilmesine imkan tanıyacak ve aynı hızla denetim raporunu oluşturabilecek elektronik temelli bir “Denetçi Bilgi Sistemi”,
3. Bu iki sistemi ve üretilen denetim raporuna ulaşmak isteyenleri birbirine bağlayacak bir “ağ” ve ağ üzerinde yer alan “sunucular (server)”.

Gerçek zamanlı sistemlere uygulanan ilk sürekli denetim modellerinden biri Sürekli İşlem Denetim Sistemi (Continuous Process Auditing System, CPAS) olup AT&T Bell Laboratuvarı’nda geliştirilmiştir.⁶⁹ CPAS büyük “kâğıtsız” gerçek zamanlı sistemlerin iç denetimi için geliştirilmiş bir yöntemdir. CPAS kendinden sonraki modeller için bir temel teşkil etmiştir. Bu modeller birbirinden farklı yaklaşımlar sergilemiş ve farklı teknolojileri kullanmışlardır.

5.1. SÜREKLİ DENETİM MODELLERİ

5.1.1. Groomer ve Murthy’nin Sürekli Denetim Modeli

1989 yılında Groomer ve Murthy yazdıkları makalede⁷⁰ sürekli denetimin kavramsal çerçevesini belirlemişler ve kendilerinden sonra gelen akademisyenlere temel oluşturmuşlardır. Bu model sürekli denetimin muhasebe veritabanının içine yerleştirilen denetim modülleri ile yapılmasını öngörür. Veritabanı içinde yer alan bu denetim

⁶⁸ Ağca, s. 63-78.

⁶⁹ Flowerday, Blundell ve Von Solms, s. 327.

⁷⁰ S. Michael Groomer ve Uday S. Murthy. “Continuous Auditing of Database Applications: An Embedded Audit Module Approach”, Journal of Information Systems. 3 (İlkbahar 1989):53–69.

modüllerinin işlemlerin kaydı esnasında hataları tespit etmesi, hataya ilişkin bilgiyi saklaması ve denetçilerin bu bilgiye bir uygulama programı ile ulaşmaları bu modelin temel amacıdır.

Bu modelde denetim modüllerinin veritabanına yerleştirilme süreci aşağıdaki adımlardan oluşmaktadır:

1. Denetlenecek uygulamanın belirlenmesi
2. Denetim amaçlarının belirlenmesi
3. Alarmların belirlenmesi
4. Denetim ile ilişkili bilginin tespiti
5. Denetim modüllerinin yazılması
6. Yazılımın alarm bildirme kurallarının belirlenmesi
7. Denetim bilgisinin veritabanında saklanmasına ilişkin düzenlemenin yapılması
8. Denetim modüllerinin testi
9. Uygulamaya geçilmesi

Bu modelde süreçlerin doğruluğunun tespiti görevlerin ayrılığı ilkesinin bozulup bozulmadığının kontrolü ile gerçekleşmektedir. Bu da muhasebe veritabanında yer alan kayıtların yetkili kişilerce erişilip erişilmediğinin kontrolü ile yapılmaktadır. Kullanıcılara verilen şifreler ve bu şifrelerin kontrolü anahtar rol oynamaktadır.

Kurallara uyulup uyulmadığının tespiti ise kural tabanlı kontroller ile sağlanmaktadır. Örneğin, belli bir miktarın üzerindeki faturalar için ön onay alınması gerektiği halde alınmamışsa bu faturalara ilişkin hata kayıtlarının tutulması. Kayıtlar üzerinde yapılacak analizlerin bilgisayar destekli teknikler (CAT's) ile yapılması öngörülmüştür.

Hatalı olan işlemlere ilişkin bilgiler bir dosyada saklanır ve denetçiler tarafından bir arayüz yazılımı ile görülebilir.

2004 yılında bu model bazı değişikliklere uğramıştır. IBM tarafından geliştirilen Business Process Execution Language for Web Services (BPEL4WS) yazılımını temel alınarak XML (eXtensible Markup Language) veri formatındaki muhasebe sistemleri için Internet üzerinden sürekli denetim yapılmak üzere geliştirilmiştir.

5.1.2. Woodroof ve Searcy'nin Sürekli Denetim Modeli

Woodroof ve Searcy'nin 2001 yılında ortaya koyduğu bu model⁷¹ sürekli denetimin kavramsal modelidir. Sınırlı bir kapsamı vardır. Daha ziyade kişi ve kurumlar arasındaki borç alacak işlemlerine yönelik güvence vermek için tasarlanmıştır. Bu modelde Web tabanlı teknolojiler kullanılmakta olup sistem güvenliğine dikkat çekilmektedir. Denetim uygulamaları sistemin içine entegre olmuştur. Raporlar anında istek üzerine üretilir ve genellikle bir Web sitesi aracılığı ile görüntülenir. Bu modelde işlemler bir veritabanında tutulur ve denetçi bir web arayüzü ile bu veritabanını kullanır. Woodroof ve Searcy birbirinden farklı kurumlardan veriyi sürekli birleştirebilme kabiliyetini eklemiştir.

Woodroof ve Searcy'nin sürekli denetim modelinin bileşenleri:

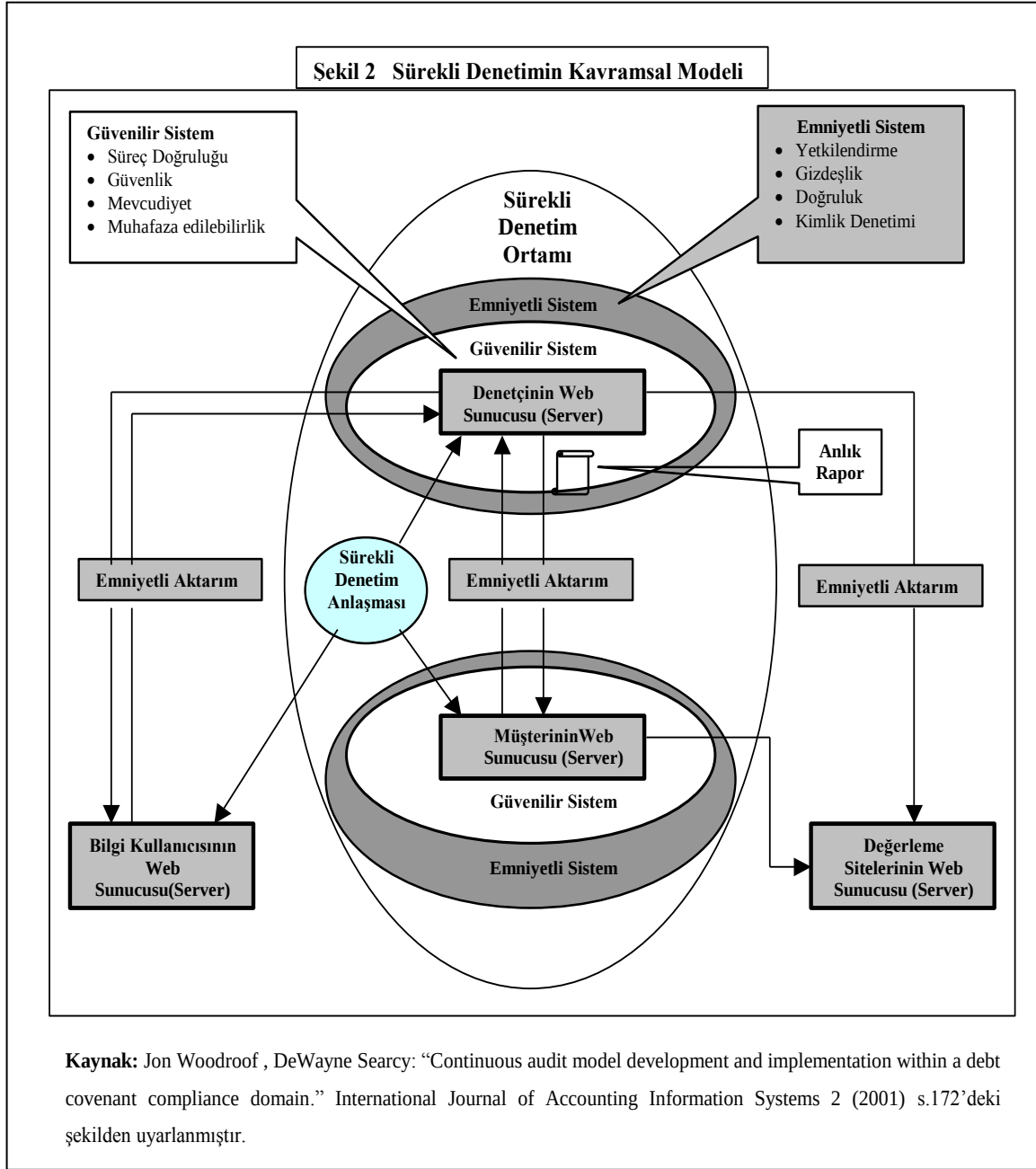
1. Birbirleriyle bağlantılı Web sunucuları:

Bu modelin temelinde sürekli denetim ile ilgili olan tüm sistemlerin birbirleriyle iletişimi öngörülür. Denetimi yapılan kurumun Web sunucusu denetçinin denetlenen kurumun veritabanına belli ölçüde erişebilmesine olanak vermelidir. Denetlenen kurumun ilişkide bulunduğu müşterilerin, satıcıların ve finansal kurumların Web sunucuları vasıtasıyla onların veritabanlarına sınırlı erişimin sağlanması gerekir. Hesap bakiyelerinin doğruluğunun teyit edilmesi bu sayede elektronik ortamda otomatik olarak gerçekleşir.

2. Sürekli denetim ortamı:

Denetlenen kurumun sistemi sürekli izlenir ve sistemin içine yerleştirilen yöntemlerle analiz edilir. Sistem denetçinin önceden belirlediği normlara uymayan veri tespit ederse sistem “alarm” verir; yani sistem denetçiye Internet aracılığı ile bilgi verir. Bu “alarm” sistemin bozulması veya veride bir anomali olduğunun göstergesidir.

⁷¹ Jon Woodroof ve DeWayne Searcy. “Continuous audit: Model development and implementation within a debt covenant compliance domain”, International Journal of Accounting Information Systems 2. (2001): 169-191.



Şekil 5: Woodroof ve Searcy’nin Sürekli Denetim Modeli

Kaynak: Ağca, s. 63-78.

Bu modelde sürekli denetim ortamı üç seviyede güvence sağlar:

- Seviye 1: denetlenen kurumun sisteminin güvenilirliği ve veri iletiminin emniyeti.
- Seviye 2: gerçek zamanlı finansal tabloların doğru olduğu ve gerçeği yansıttığına ilişkin görüş.
- Seviye 3: denetlenen kurum ile üçüncü şahıslar arasındaki özellikli durumun (borç akdi gibi) analiz sonuçlarına ilişkin güvence vermek.

Her seviyenin önem derecesi farklıdır. Ayrıca, denetçinin yapması gerekenler de her seviyede birbirinden farklıdır.

Bu model üç kategoride verinin otomasyonunu gerektirir:

- Alışılmış belirli veri: Net bir şekilde tarif edilebilen, kolaylıkla yorumlanan ve ölçülebilen veri (örnek: fiyatlar).
- Alışılmamış belirli veri: Yorumlayabilmek ve ölçebilmek için başka kaynaklardan bilgi alınması gereken veri (örnek: artış miktarı). Bu tür veriyi analiz etmek için çeşitli sistemlerin entegrasyonuna ihtiyaç vardır.
- Belirsiz veri: Yoruma açık ve varsayımlara dayalı veri (örnek: stokların o anki piyasa değeri). Bu tür veriyi analiz etmek için yapay zeka uygulamalarına ihtiyaç duyulmaktadır.

Bu modelde denetim uygulamaları “dijital ajan” (digital agent) denilen yazılımlarla yapılmaktadır. Dijital ajanlar denetçiler tarafından Internet’e gönderildikten sonra kendi başlarına hareket eden ve belli emirleri yerine getiren yazılımlardır. Bunlar çeşitli Web sunucularını ziyaret eder ve ilgili veritabanlarındaki işlemlere ve kontrollere ilişkin analizleri yaparak sonuçlarını denetçiye ulaştırır. Dijital ajanların kendi başlarına verilen emirleri yerine getirebiliyor olmaları denetim testlerinin ilgili veritabanı üzerinde uzaktan yapılabilmesini sağlar. Bu modelde verinin denetçinin bilgisayarına transfer edilmesi gerekmez.

3. İlgili taraflar arasında yapılan sürekli denetim anlaşması:

Sürekli denetimin kapsamına göre ilgili taraflar sitemlerinin kullanımı ve veritabanlarına erişim gibi teknik konular üzerinde anlaşma sağlarlar. Denetim ilişkisi denetleyen ve denetlenen kurumlar arasında gibi düşünülse de üçüncü şahısların veritabanlarıyla otomatik veri alış verişi söz konusu olduğu için denetlenen kurumun müşterileri, satıcıları ve ilişkide olduğu finansal kurumlar da bu anlaşmaya taraftır.

4. Güvenilir (reliable) sistemin özellikleri:

Sürekli denetimin yapılabilmesi birbiriyle iletişim içinde olan sistemlerin güvenilir olmasına bağlıdır. Denetçilerin finansal bilgilerin doğruluğu konusunda güvence verebilmesi için ilgili bilgiyi yaratan muhasebe sisteminin güvenilir olması gerekmektedir. Elektronik ortamda ve tamamen otomatik olarak gerçekleştirilen uygulamalar güvenilir olmalıdır.

Güvenilirliğin dört temel ilkesi vardır:

- Süreç doğruluğu (integrity): Sistemin ilgili konuda bilgiyi doğru, tam ve gerçek zamanlı olarak toplama, saklama ve raporlama kabiliyetidir.

- Güvenlik (security): Veri ve uygulamalara yetkisiz kişilerin erişememesi için gerekli kontrollerin sağlanmasıdır.
- Mevcudiyet (availability): Raporların istendiği an alınmasının sağlanmasıdır. Raporların çıkmasını engelleyici teknik sorunlara karşı önlemler alınmalıdır.
- Muhafaza edilebilirlik (maintainability): Bakım veya diğer nedenlerle sistem erişimi kesintiye uğrayacaksa ilgili tarafların süre ve zaman konularında anlaşmaya varmaları gerekir. Sürekli denetimin yapılabilmesi için ilgili sistemlere erişimin kesintisiz sağlanması gerekir.

5. Emniyetli (secure) sistemin özellikleri:

Bilginin taraflar arasında transferi yetkilendirilmiş kişilerce bilginin gizliliği korunarak doğruluğundan ödün vermeden yapılmalıdır. Bu emniyetli sistemin oluşmasında dört temel unsur vardır:

- Yetkilendirme (authorization): Transfer edilen bilgiye sadece yetkilendirilmiş kişilerin ulaşması.
- Gizlilik (confidentiality): Transfer edilen bilginin gizli kalması.
- Doğruluk (integrity): Transfer edilen bilgiye izinsiz girilmesi veya bilginin değiştirilmesi durumunu tespit edebilmek.
- Kimlik denetimi (authentication): İletişimin kaynağını doğrulamak.

6. Anlık (evergreen) raporlar:

Sürekli denetim ortamına Web sayfası aracılığı ile bağlanan kullanıcılara sağlanan denetlenmiş raporlardır. Bu raporlar kullanıcıya daha önce belirtilen üç seviyede güvence sağlarlar:

- Seviye 1 güvencesi veri transferinin güvenilirliği ve emniyeti ile ilgilidir. Bu seviyedeki olağandışı durum denetçinin konu ile hemen ilgilenmesini gerektirir.
- Seviye 2 güvencesi finansal raporların tam ve doğru olarak finansal durumu, kayıtları ve nakit akımlarını yansıttığını ve genel kabul görmüş muhasebe standartlarıyla uyumlu olduğunu teyit eder. Finansal tabloları oluşturan kayıtların sürekli izlenmesi sonucu denetçiler güvence verirler. Kayıtlardaki anomaliler dijital ajanlar tarafından yapılan testlerin sonucunda tespit edilir. Denetçi, olağandışı durumun kaynaklandığı hesabı dikkate alarak yapılması gerekeni belirler.

- Seviye 3 güvencesi, denetimi yapılan kurumun işlemlerinin kurumun yapmış olduğu anlaşmalarla uyumlu olduğunun güvencesidir. Bu anlaşmalara aykırı davranıldığında sistem olağandışı işlemleri belirler. Bu işlemler e-posta yoluyla denetçiye raporlanır. Denetçi duruma göre ya hiçbir şey yapmaz veya denetlenen kurumun anlaşmalara uygun davranması için gerekli çabayı harcar.

Raporlar gerçek zamanlı hazırlanır.

Bu model beş aşamada uygulanır:

1. Bir raporun hazırlanması talep edilir.
2. Kullanıcı veritabanındaki işlemlerin önceden belirlenmiş kurallara uygunluğu sistem içine yerleştirilmiş yazılımlarla izlenir. Belirlenen kurallara uymayan işlemler olağandışı işlemler olarak denetçiye bildirilir. Kurallar sistem güvenilirliği, finansal raporların doğruluğu ve üçüncü şahıslarla yapılan anlaşmalara uygunluk ile ilgilidir.
3. Denetçinin sistemi kullanıcının veritabanından gerçek zamanlı hesap bakiyelerini ister.
4. Gelen bakiyenin üçüncü şahıslarla borç alacak ilişkisini düzenleyen anlaşmalara uygunluğu ve işlemlerin standart işlemlere benzerliği kontrol edilir. Anomaliler denetçilere bildirilir.
5. Gerçek zamanlı rapor üretilir. Bu raporlar üç alanda güvence verir. Birincisi güvenilirlik güvencesidir, daha detaylı analiz gerektirmez. İkincisi gerçek zamanlı finansal tabloların doğruluğuna ilişkin görüş bildirmektir. Üçüncüsü ise üçüncü kişilerle yapılan anlaşmaların ihlal edilip edilmediğine dair analizdir. Raporlar anlık üretildiği için XBRL tabanlı raporlamaya uygun değildir.

5.1.3. Rezaee ve Arkadaşlarının Sürekli Denetim Modeli

Rezaee, Elam ve Sharbatoghile 2001 yılında yaptıkları çalışmada gerçek zamanlı muhasebe sisteminde denetimin nasıl yapılabileceğini adım adım açıklamışlardır.⁷² Rezaee ve arkadaşlarına göre gerçek zamanlı muhasebe sistemi aşağıdaki süreçlerden oluşmaktadır:

1. işlemlerin ve diğer ekonomik olayların belirlenmesi
2. işlemlerin gerçek zamanlı muhasebe sisteminde ölçülmesi, tanınması ve raporlanması
3. yeterli ve etkin iç kontrol yapısının varlığı
4. kayıtların elektronik olarak işlenmesi

⁷² Rezaee, Elam, Sharbatoghlie, s. 150-158.

5. ana ve alt kebir hesaplarının bakiyelerinin her an görülebilmesi
6. gerçek zamanlı finansal tablolara her an ulaşılabilmesi

Rezaee ve arkadaşları 2001 yılındaki çalışmalarında sürekli denetimi beş aşamada tanımlamışlardır:

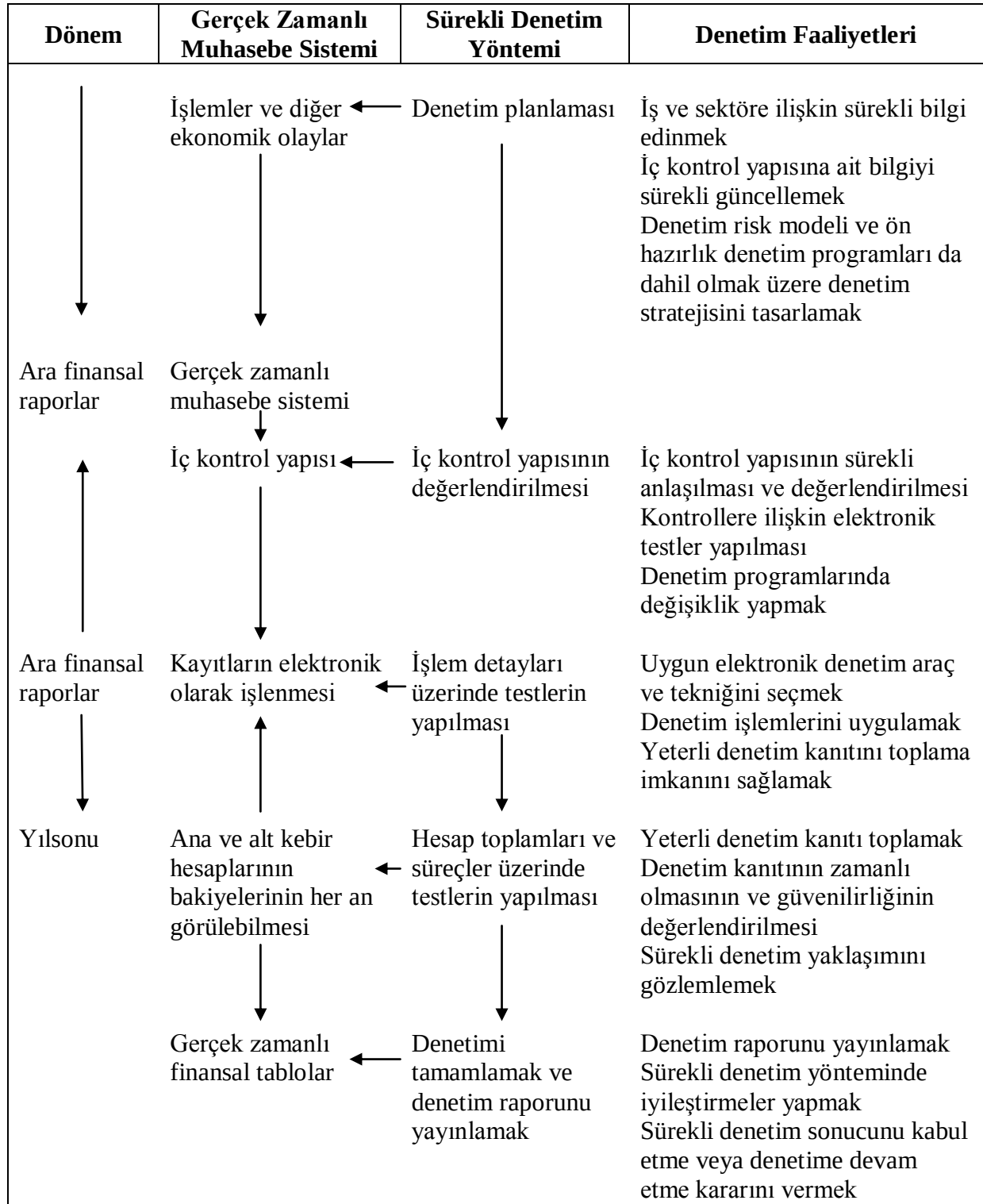
1. yapılacak analizler de dahil denetimin planlanması
2. kontrollerin performanslarına ait testler ve kontrollerin risklerine ait değerlendirmeler de dahil olmak üzere gerçek zamanlı muhasebe sisteminin iç kontrol yapısının değerlendirilmesi
3. işlemlerin detayları üzerinde testlerin yapılması
4. hesap toplamları ve genel sonuçlar üzerinde sene sonu testlerinin ve analizlerinin yapılması
5. denetimin tamamlaması ve denetim raporunun yayınlanması

Rezaee, Sharbatoghlie, Elam ve McMicle'nin 2002 yılında yazdığı makalede bu model olgunlaştırılmış ve sürekli denetim sistemlerinin kavramsal çerçevesi oluşturulmuştur.⁷³ Rezaee ve arkadaşları sürekli denetimin aşağıdaki beş soru için denetim bulgularını topladığını öngörmektedir:

1. Elektronik ortamda veri nasıl toplandı?
2. Veri nasıl, nereden ve kim tarafından yaratıldı?
3. Hangi doğrulama teknikleri kullanıldı?
4. Verinin ilk kaydı ve dağıtımı için hangi bilgisayar sistemleri kullanıldı?
5. Veri nasıl işlendi?

Denetim yazılımının bu sorulara ilişkin bulguları toplarken dijital analiz teknikleri ve veri madenciliği yöntemlerini kullanarak olağandışı işlemleri tespit etmesi ve denetçileri uyarması öngörülmektedir.

⁷³ Zabihollah Rezaee ve diğerleri. "Continuous Auditing: Building Automated Auditing Capability", A Journal of Practice & Theory 21. 1 (Mart 2002): 147-163.



Şekil 6: Gerçek Zamanlı Muhasebe Sistemi ve İlgili Denetim İşlemi

Kaynak: Zabihollah Rezaee, Rick Elam, Ahmad Sharbatoghlie. "Continuous auditing: the audit of the future", Managerial Auditing Journal 16. 3 (2001): 152.

Bu model birkaç adımdan oluşmaktadır. İlk adım ihtiyaç duyulan bilginin farklı veritabanlarında yer alan kayıtlardan Web tabanlı bir yazılımla denetçinin bilgisayarına aktarılmasıdır. Daha sonra bu bilgi belli bir standart format geliştirilerek saklanır, yani denetim veritabanı oluşturulur. Veri temizlenir, geçerliliği tespit edilir ve yeniden yapılandırılır. Son olarak bu veritabanında çalışacak standart testler geliştirilir. Bu testler sürekli veya önceden belirlenen aralıklarla çalışır.

5.1.4. Onions'ın Sürekli Denetim Modeli

Onions 2003 yılında yazdığı bir makalede⁷⁴ o günkü mevcut yazılım ve donanımlarla tamamen otomatik gerçek zamanlı denetim anlayışının nasıl hayata geçirilebileceğini yorumlamıştır. Onions Bilgisayar Destekli Denetim Araç ve Teknikleri (Computer Aided Audit Tools and Techniques, CAATT's) ve uzman sistemlerin (expert systems) gerçek zamanlı kullanımı ile sürekli denetimin başarılabileceğine inanmaktadır. Ayrıca, bu makalede sürekli denetim raporlamasında evrensel bir dil oluşmasının öneminden de bahseder. Raporlamanın standardizasyonu için XBRL (Extensible Business Reporting Language) kullanımını önerir.

Veri bütünlüğü ve doğruluğunun güvencesini verebilmek için kayıtların ilk sisteme girişlerinden itibaren izlenmesinin gerekliliği kavramını ortaya atmıştır. Hesapların doğruluğunun güvencesinin klavyeden yapılan her giriş, her yöntem ve her şablonun izlenmesi ile mümkün olabileceğini savunur.

Onions'ın modeline göre etkin ve kapsamlı denetim için üç alanda veri incelemesi yapılmalıdır:

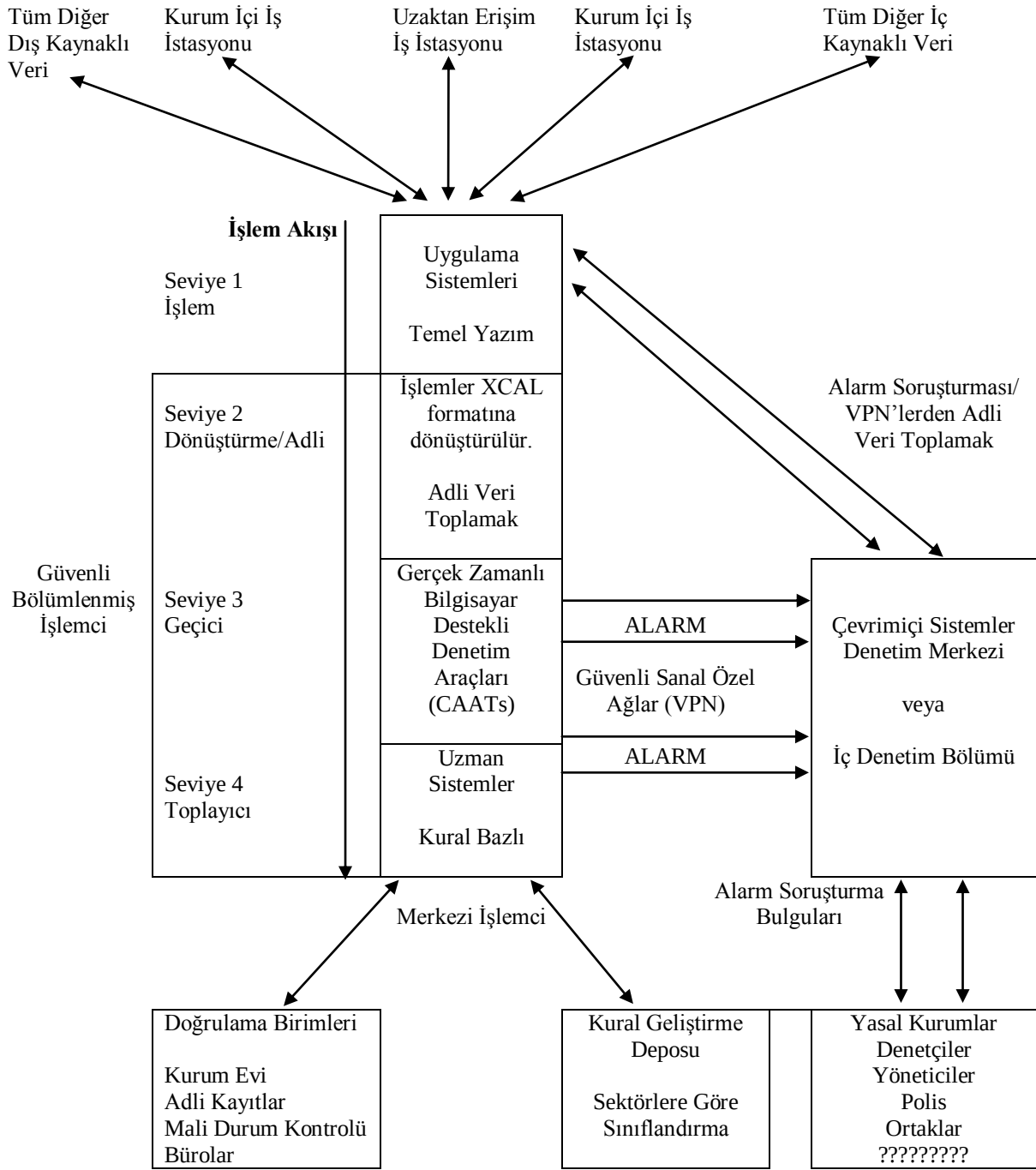
- Tuşa basma seviyesi (keystroke level): Çoğu veritabanı yazılımı giriş şifresi olan kişilerin kayıtlar üzerinde değişiklik yapmalarına ve bu değişiklikleri saklamalarına olanak vermektedir. Güncellenebilen kayıt sistemi hata ve hilelere açıktır. Bu tür sistemlerde kullanıcıların kayıtlar üzerinde hangi işlemleri yapabileceklerine dair yetkilerin tespit edilmesi, kullanıcı şifrelerinin gizliliği ve güncel olması önemlidir.

⁷⁴ Robert L Onions. "Towards a Paradigm for Continuous Auditing". Ocak 2003.
<http://www.auditsoftware.net/community/how/run/tools/Towards%20a%20Paradigm%20for%20Continuous%20Auditin1.doc> (19 Şubat 2011).

- İşlem seviyesi (transaction level): Veri girişi sırasında her işlem diğer işlemlerden bağımsız olarak denetlenir ve raporlanır. Buna işlem seviyesinde veri incelemesi denir. İşlemin önceden belirlenmiş kurallara uygunluğu tespit edilir. Uygulama yazılımları genellikle kayıtları ilk girildikleri anda kontrol ederler. Örneğin, bilgi girilmesi gereken tüm alanların dolu olması, belirlenen standartlarda girişlerin yapılmış olması gibi basit kontroller yapılır. Bilgisayar Destekli Denetim Araç ve Teknikleri (Computer Aided Audit Tools and Techniques, CAATT's) bu seviye analizler için uygundur. Ancak, bu tür analizler veritabanından seçilen ve belli bir dönemi kapsayan kayıtlar üzerinde yapılmaktadır. Bu analizler gerçek zamanlı yapılabilirse sürekli denetim ruhu yakalanmış olur.
- Şablon işlem seviyesi (transaction pattern level): Bazı hile türleri işlemlerin bir bütün içinde uzun bir süreye yayılmış olarak incelenmesi sonucunda tespit edilebilir. Bu incelemede işlemler arasında benzerlikler aranır ve tekrarlanan yöntemler veya işlemler araştırılır. Çeşitli kurallar ölçüt olarak kullanılır. Bu nedenle verinin uzman sistemlerce (expert systems) ve kural tabanlı ölçütlerle belli bir dönem izlenmesi gerekir. Uzman sistemler kurumun kayıtlarının tutulduğu veritabanlarını devamlı dolaşarak işlemlerde şablon ararlar. Farklı sektörler için kuralların tanımları değişebilir. Bu nedenle uzman sistemler işkoluna özel geliştirilmelidir. Ancak, uzman sistemler kurumda kullanılan yazılımlardan farklı veri formatları kullanır. Her uygulamayı kullanan uzman sistemin anlayacağı formata çevirmek çok maliyetli ve zaman alıcıdır. Bu nedenle kullanılan uygulamalardan bağımsız bir veritabanı formatı ile çalışmak önemlidir. Bu modelde kurumsal veritabanında XML tabanlı Geliştirilebilir Sürekli Denetim Dili'nin (eXtensible Continuous Auditing Language, XCAL) kullanılması önerilmektedir.

Onions modelinin işleyişi dört seviyeden oluşmaktadır:

1. Farklı kaynaklardan girişler yapılır.
2. Girişler gerçek zamanlı olarak XCAL veri formatına çevrilir.
3. Gerçek zamanlı Bilgisayar Destekli Denetim Araç ve Teknikleri (Computer Aided Audit Tools and Techniques, CAATT's) kullanılarak işlemler kontrol edilir. Uyarılar denetim merkezine gönderilir. İşlemler dördüncü seviye incelemesi için yıllarca saklanır.
4. Uzman sistemler işlemler arasında benzerlik ararlar.



Şekil 7: Onions'ın Önerdiği Sürekli Denetim Modeli

Kaynak: Robert L Onions. "Towards a Paradigm for Continuous Auditing". Ocak 2003. <http://www.auditsoftware.net/community/how/run/tools/Towards%20a%20Paradigm%20for%20Continuous%20Auditin1.doc> (19 Şubat 2011).

5.1.5. Vasarhelyi, Alles ve Kogan'ın Sürekli Denetim Modeli

Vasarhelyi, Alles ve Kogan 2004 yılında yazdıkları bir makalede⁷⁵ sürekli denetimin kavramsal modelini anlatırlar. Model, Internet tabanlı bir yapıda çalışan veritabanları ile kurumsal kaynak planlama yazılımının ürettiği XML (Extensible Markup Language) formatındaki finansal ve finansal olmayan bilgi ile ilgili güvencenin verilmesi üzerine kurulmuştur.

Bu modelde dört seviyede güvence verilmektedir:

- Seviye 1 İşlem Doğrulama: İşlemlerde yer alan tüm verinin doğrulanması (örnek: para hareketi, bilgi).
- Seviye 2 Uygunluk Doğrulama: İşlemleri değerlendirmede kullanılan ölçütlerin uygunluğuna güvence vermek (örnek: gelirlerin genel kabul görmüş muhasebe ilkelerine uygun şekilde kaydedilmiş olması).
- Seviye 3 Tahmin Doğrulama: Kullanılan tahminlerin ve varsayımların yeterliliği ve üst seviye ölçümlerin tutarlılığı (örnek: işin bitme oranı, şüpheli alacaklara karşılık ayrılması gibi ölçülmesi zor durumlar için finansal değerler tahmin yöntemiyle belirlenir).
- Seviye 4 Karar Doğrulama: Kuruma ilişkin üst seviye değerlendirmelerin ve kararların denetlenmesi ve sorgulanması. Kurumsal kaynak planlaması gibi üst düzey analiz yeteneği olan yazılımları kullanan kurumlar bu yazılımlardan elde edilen bilgilere göre karar verirler. Ancak bu kararların da incelenmesi ve doğrulanması gerekir.

Sürekli güvencenin verilebilmesi için çeşitli analiz tekniklerinin uygulanması gerekir. Bu analizler çoğunlukla otomatik olarak gerçek zamanlı veya işlemin oluşuna yakın bir zamanda yapılmalıdır. Ancak, analizlerin zamanlaması anlamlı sonuç elde edebilmek için denetlenen iş süreçlerine ve analiz tekniğine bağlı olmaktadır.

⁷⁵ Miklos A. Vasarhelyi, Michael G. Alles ve Alexander Kogan. "Principles of Analytic Monitoring for Continuous Assurance", Journal of Emerging Technologies in Accounting 1. (2004):1-21.

Tablo 1

**Vasarhelyi, Alles ve Kogan’ın Sürekli Denetim Modeli’nde Belirtilen Dört Seviye İçin
Kullanılan Analiz Teknikleri**

	Seviye 1 İşlem Doğrulama	Seviye 2 Uygunluk Doğrulama	Seviye 3 Tahmin Doğrulama	Seviye 4 Karar Doğrulama
Yöntemler	Kural/şelale tarzı veri incelemesi	XML türevi ile standart ilişkiyi biçimlendirme	Yukarı ve aşağı akım doğrulaması	
	Süreç kesintisi	Devamlılık denklemi	Devamlılık denklemi	Devamlılık denklemi
	Değer zinciri işlem takibi	Yapısal bilgi	Değer zinciri ilişkileri	Uzman sistemler
Otomasyon seviyesi	Yüksek	Karışık	Karışık	Düşük
Yeni yöntemler, teknikler	Sürekli uzlaşma	Devamlılık denklemi	Devamlılık denklemi	Devamlılık denklemi
	Görünmez izleme/ saydam işaretleme		Büyük ölçüde dış kaynaklı veri kullanımı	Büyük ölçüde dış kaynaklı veri kullanımı
	Otomatik doğrulamalar			
	Kural tabanlı işlem değerlendirmesi			
		Zaman serisi/ kesit analizleri	Zaman serisi/ kesit analizleri	Zaman serisi/ kesit analizleri

Kaynak: Miklos A. Vasarhelyi, Michael G. Alles ve Alexander Kogan. “Principles of Analytic Monitoring for Continuous Assurance”, Journal of Emerging Technologies in Accounting 1. (2004):6.

Vasarhelyi, Alles ve Kogan modelinde izleme ve kontrol faaliyetlerinin yapısı aşağıdaki katmanlardan oluşur:

1. veri toplama (data capture)
2. veri arındırma (data filtering)
3. ilişkisel saklama (relational storage)
4. ölçme standartları (measurement standards)
5. çıkarsama motoru (inference engine)
6. analiz (analytic)
7. alarm ve uyarma (alarms and alerting)
8. raporlama (reporting)

5.1.6. Coderre'nin Sürekli Denetim Modeli

David Coderre'nin sürekli denetim tanımı incelenen modeller içinde kapsamı en geniş olanıdır. 2005 yılında İç Denetçiler Enstitüsü (The Institute of Internal Auditors) için hazırladığı kitapçıkta ("Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment", Global Technology Audit Guide) modeli olgunluğa ulaşmıştır. Coderre sürekli denetimin risk ve kontrol değerlendirmesi, denetim planlaması, dijital analiz ve diğer denetim teknoloji ve tekniklerini bir araya getiren bir yapısı olduğunu savunmuştur. Coderre sürekli denetim sistemlerinin kurumsal riskleri tespit etme ve önemini değerlendirme yeteneğinin yapılacak denetimin kapsamını ve amaçlarını belirlemede önemli bir rol üstlendiğine inanmıştır. Sürekli denetimin esnek yapısının hem geniş hem de dar kapsamlı denetim faaliyetleri için kullanılabileceğini belirtmiştir. Örneğin, kurumsal risk unsurlarını değerlendirerek denetim planlaması yapılması geniş kapsamlı bir denetim faaliyeti iken belli bir olayın araştırılması dar kapsamlı bir denetim faaliyeti olarak kabul edilmektedir.

Coderre'nin modelinde işlemler sadece önceden belirlenmiş bir değer ile karşılaştırılmamakta, daha önce gerçekleşmiş diğer benzer işlemler ile de karşılaştırılmaktadır. Ayrıca, bu model işlem setlerinin birbirleriyle karşılaştırılmasına da olanak tanımaktadır. Örneğin, iki tarih arası gerçekleşen belli bir konudaki finansal işlemlerin diğer bir şubedeki aynı tarih aralığında ve aynı konuda yapılmış olan işlemlerle karşılaştırılması iki işlem setinin (veya kümesinin) karşılaştırılmasıdır. İşlem setlerinin karşılaştırılmasından yararlanılarak ölçülen değişkenlik süreçlerin tutarlılığını test etmek için kullanılmaktadır.

Sürekli Denetimin Amaçları • Sürekli denetimin amaçlarını saptamak • Üst yönetimin desteğini almak • Yönetimin izleme görevini ne derecede yerine getirdiğini anlamak • Ele alınacak konuları ve denetim çeşidini tespit etmek ve derecelendirmek • Önemli bilgi sistemleri ve veri kaynaklarını tespit etmek • İlgili iş süreçleri ve uygulamaları anlamak • Bilgi teknolojileri bölümü ile ilişkileri geliştirmek	
Verilere Ulaşım ve Kullanımı • Analiz programlarını seçmek ve satın almak • Erişim ve analiz olanaklarını geliştirmek • Denetçilerin analiz yetkinliklerini ve tekniklerini geliştirmelerini sağlamak • Veri bütünlüğü ve güvenilirliğini tespit etmek • Veriyi temizlemek ve hazırlamak	
Sürekli Kontrol Değerlendirmesi • Kritik kontrol noktalarını tespit etmek • Kontrol kurallarını belirlemek • Sıradışı durumları belirlemek • Kontrollerin testi ve zaafıların tespiti için dijital analiz tekniklerini kullanmak	Sürekli Risk Değerlendirmesi • İncelenecek konuları tespit etmek • Risk kategorilerini belirlemek • Risk/performans göstergelerini belirlemek • Yükselen risk seviyelerini ölçecek analitik testler planlamak
Raporlama ve Sonuçların Yönetimi • Sonuçları önceliklendirmek ve sürekli denetim faaliyetlerinin sıklığını tespit etmek • Testleri düzenli ve zamanında yapmak • Kontrol zaafıların ve yükselen risk seviyelerini belirlemek • Sonuçları önceliklendirmek • Denetimin sonuçlarını yönetime bildirmek • Sonuçların yönetimi – takip, raporlama, izleme • Alınan önlemlerin sonuçlarını değerlendirmek • Sürekli denetim yöntemlerinin etkinliğini izlemek ve değerlendirmek – analizler, sonuçlar, test parametreleri • Sürekli denetim yöntemlerinin güvenliğini sağlamak, kurumsal risk yönetimi, izleme ve performans ölçümü gibi yönetim faaliyetleriyle ilişkilendirmek	

Şekil 8: Coderre'nin Modelinde Sürekli Denetim Uygulamaları Geliştirmek İçin Atılacak Adımlar

Kaynak: David Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide. The Institute of Internal Auditors, USA, 2005: 17.

5.1.7. Chou, Du ve Lai'nin Sürekli Denetim Modeli

Charles Ling-yu Chou, Timon Du ve Vincent Lai 2006 yılında dijital ajan (digital agent) temelli sürekli denetim modeli (agent based continuous audit model – ABCAM) geliştirmişlerdir.⁷⁶ Bu modelin temelinde denetim kanıtlarının dijital ajanlar tarafından toplanması yatmaktadır. Her denetim kanıtı için programlanmış farklı dijital ajanlar ilgili bilgi sistemine gönderilir. Bu dijital ajanlar sistemde programlandıkları denetim kanıtlarını ararlar ve bulgularını kullanıcıya bildirirler.

Dijital ajanlar değişken ortamlarda kendi başlarına hareket edebilen ve önceden belirlenmiş bir eylemi gerçekleştirmek için programlanmış akıllı yazılımlardır. Belirlenmiş eylemleri gerçekleştirmek için bilgi sisteminin bir bölümünden diğerine geçebilen yapay zeka uygulamalarıdır. Sisteme yüklendikten sonra bağımsız hareket ederler. Örneğin, belli bir veri ile ilişkili dosyaları bulmak için programlanan bir dijital ajan kurumsal kaynak planlama yazılımına gönderildiğinde bu yazılımın desteklediği tüm bilgisayarları dolaşarak sabit disklerinde bulunan tüm dosyalar ve veri tabanlarında ilgili veriyi arar, ilgili bulunduğu dosyaları kullanıcıya bildirir. Akıllı dijital ajanlar uzak mesafelerdeki birbirinden farklı platformlardaki bilgi sistemlerinde gelişmiş analizler yapabilirler. Dijital ajanlar bir bütünün parçaları gibi birlikte çalışmak için programlanabilirler.

Denetim alanında yeni olmakla birlikte günümüzde özellikle telekomünikasyon ve Internet alanlarında dijital ajanları içeren başarılı uygulamalar vardır. Elektronik ticaret, farklı sistemlerden bilgi çekmek ve izleme konularında dijital ajanlarla yapılmış Internet uygulamalarından başarılı sonuçlar alınmaktadır. Bu nedenle bu model sadece kavramsal değil şu anki teknolojiyle uygulanabilir bir model olarak karşımıza çıkmaktadır.

Bu modelin uygulanabilmesi için kuruma ilişkin her türlü bilginin elektronik formatta ve birbirleri arasında ağ bağlantısı olan bilgi sistemlerinde olması gerekir. Dijital ajanlar yüklendikleri bilgisayar sistemini ve ona bağlı bilgi sistemlerini tarayabildikleri için ağ bağlantısı içinde olmayan bilgisayarları göremezler. Kağıt gibi dijital olmayan ortamlardaki denetim kanıtlarına da ulaşmaları mümkün değildir. Günümüzde kurumsal bilginin çoğu

⁷⁶ Charles Ling-yu Chou, Timon Du ve Vincent S. Lai. "Continuous Auditing with a multi-agent system", Decision Support Systems, 42 (2007): 2274-2292.

dijital ortamda olduğundan bu konu modelin uygulanmasında fazla bir sorun oluşturmayacaktır.

Denetim kanıtları yedi gruba ayrılır:

- Varlıkların fiziki incelemesi
- Doğrulama: belgelerin doğruluğunun teyit edilmesi. Örneğin, kayıtlarda yer alan belli bir alımın satıcısı tarafından teyit edilmesi.
- Belgeleme: bir veri değişik belgelerde yer alıyorsa, bu belgelerin birbirleriyle olan ilişkisi.
- Gözlem
- Soruşturma
- Tekrar hesaplama
- Analiz yöntemleri

Dijital ajanlar yedi gruptan gözlem ve soruşturma haricindeki beş gruba ait denetim kanıtlarını toplayabilirler. Hesaplarda yer alan muhasebe verisinin doğruluğunu kanıtlamak için kurumsal kaynak planlama yazılımında ilgili veriyi destekleyici belgeler dijital ajanlar tarafından aranabilir. Toplamların ve formüllerin tekrar hesaplanması ve veri üzerinde dijital analiz yapmak için de dijital ajanlar kullanılabilir. Denetlenen kurumla ilişki içinde olan müşteriler, satıcılar, bankalar gibi diğer kuruluşlarla elektronik iletişim kurulabilir. Bu iletişim hattı üzerinden dijital ajanlar denetim verisinin doğruluğunu teyit edebilir. Ayrıca, dijital ajanlar hesaplarda yer alan varlıkların gerçekten var olup olmadıkları hakkında bilgiyi diğer sistemlerle iletişime geçerek öğrenebilirler. Örneğin, stokların varlığını stok yönetim programından elde edecekleri bilgi ile kanıtlayabilirler.

ABCAM modelindeki dijital ajan platformu soyut sınıflama kümelerinden ve uygulama programlarından oluşmaktadır. Programlama dili Internet uygulamalarında kullanılan Java'dır. Denetçi dijital ajanın davranış modelini kendisi tanımlayabilir. Yani dijital ajanları denetçiler kendi ihtiyaçları doğrultusunda bir arayüz kullanarak programlayabilirler.

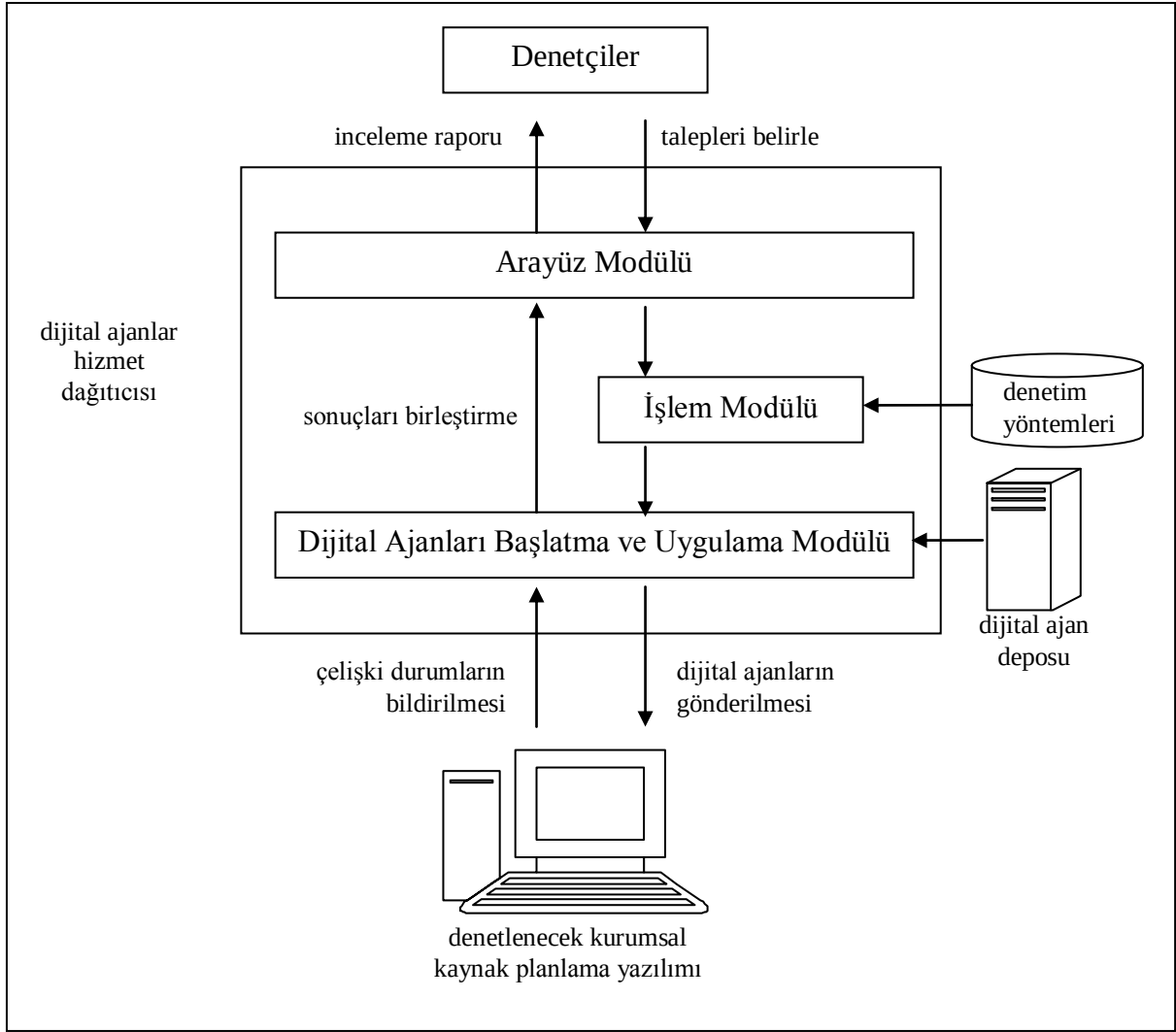
ABCAM modeli çeşitli modüllerin birlikte çalışmasını öngörür:

- Arayüz modülü (interface module) kullanıcıya dijital ajanları yönetme olanağı verir. Kullanıcı bu modülü kullanarak dijital ajanları denetime ilişkin eylemleri yapmaları

iin programlar. Dijital ajanların elde ettikleri sonuçlar da arayüz modülü ile kullanıcı tarafından görülür.

- İşlem modülü (procedures module) arayüz modülü ile kullanıcı tarafından istenen denetim eylemini gerçekleştirmek için yapılması gereken faaliyetleri planlar. Toplanması istenen denetim kanıtı, gönderilecek dijital ajanlar ve bu dijital ajanların çalışmalarına ilişkin düzenlemeler işlem modülü tarafından planlanır. İşlem modülü dijital ajanların ulaşması gereken bilgi kaynaklarını ve bunlar üzerinde yapacakları işlemleri belirler. Bu modül denetimle ilgili detaylı faaliyet planını oluşturan bir veritabanı ile desteklenir. Chou ve arkadaşları modellerini test etmek için MySQL veritabanını kullanmışlardır. Veri formatı ise XML'dir.
- Dijital ajanları başlatma ve uygulama modülü (agent invocation and execution module) dijital ajanların faaliyetlerini başlatır ve programlanan eylemlerin gerçekleşmesi aşamasını yönetir. Dijital ajanlar planlanan işleri bitirdikçe bu modül sonuçları arayüz modülüne aktarır.

Aşağıdaki şekilde ABCAM modelinin çalışma şekli grafik olarak anlatılmaktadır.



Şekil 9: ABCAM - Dijital Ajan Temelli Sürekli Denetim Modeli

Kaynak: Charles Ling-yu Chou, Timon Du ve Vincent S. Lai. "Continuous Auditing with a multi-agent system", Decision Support Systems. 42 (2007):2278.

ABCAM modelinin faydaları:

- ABCAM modelinin getirdiği en büyük yenilik kurumsal kaynak planlama yazılımına gömülü denetim modülleri (embedded audit modules - EAM) olmadan veya denetlenecek veriyi denetim veritabanına transfer etmeden denetim yapabiliyor olmasıdır. Gömülü denetim modülleri kullanan modellerde denetçi bağımsızlığı, denetim veritabanı kullanan modellerde çok fazla sabit disk ihtiyacı sorun olurken dijital ajanlar kavramı sürekli denetim modellerine yeni bir soluk getirmiştir.

- Dijital ajanların deęişiklik ve yeniliklere uyarlanabilen esnek yapısı, bir kez sisteme gönderildikten sonra kendi başına izleme faaliyetine devam edebilmesi denetimin süreklilięi açısından deęerli özelliklerdir.

ABCAM modelinin olumsuz yanları:

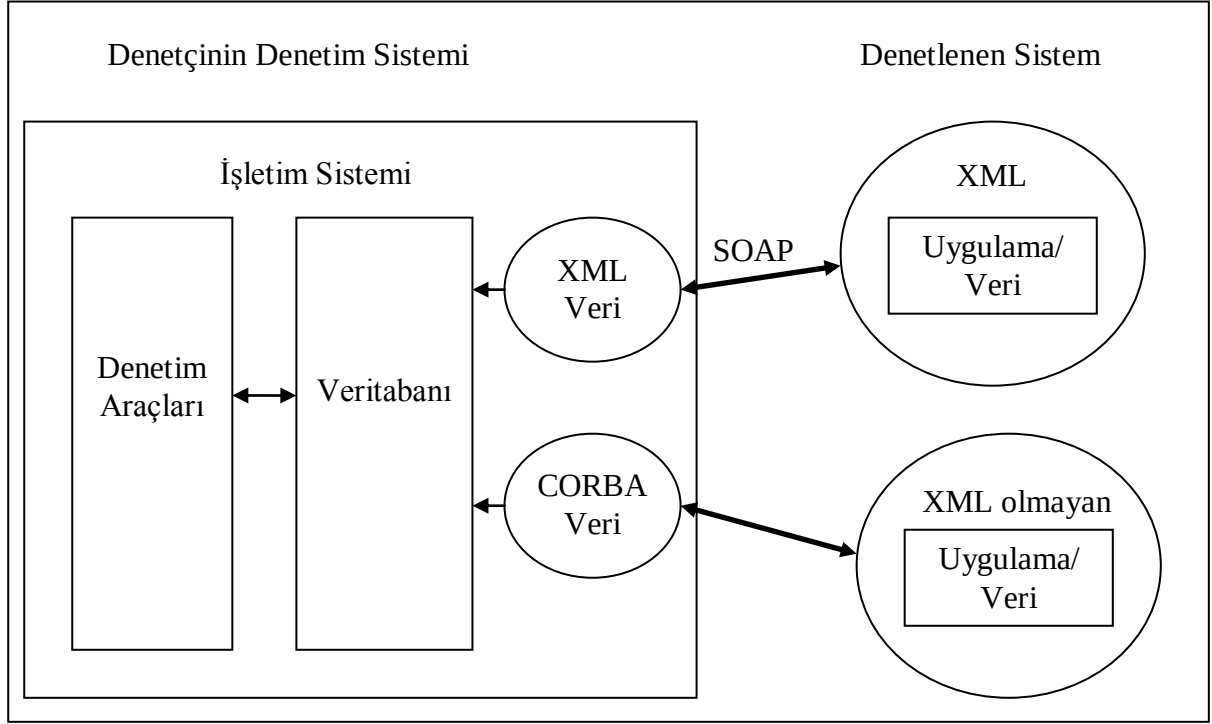
- Dijital ajanlar sistem performansını olumsuz etkileyebilirler. Dijital ajanlar denetim kanıtlarını toplayabilmek için sistem ve uygulama yazılımları ile sürekli ilişkide olmak zorundadırlar. Bu da sistem kaynaklarının bir bölümünün sürekli olarak denetim faaliyetine ayrılması demektir. Donanımda yapılacak iyileştirme çalışmaları sistemin yavaşlamasının önüne bir ölçüde geçse bile maliyeti arttırıcı bir unsurdur.
- Dijital ajanların çalışması için denetlenen kurumun bilgi sisteminin tamamına denetçilerin erişimlerinin olması gereklidir. Dijital ajanlar sistemi dolaşarak ve farklı platformdaki bilgileri toplayarak denetim kanıtlarını topladıęı için kurumun tüm bilgisayarları, sunucuları ve veritabanlarına ulaşabilmeleri gerekir. Kurum yöneticilerinin içeriğini bilmedikleri yazılımların bilgisayar sistemlerinde serbestçe dolaşmalarına izin vermeleri sistem güvenliğine aykırı olduęu için uzak bir ihtimaldir.

5.1.8. Du ve Roohani'nin Sürekli Denetim Modeli

Hui Du ve Saeed Roohani 2007 yılında finansal tabloların bağımsız denetimi için bir sürekli denetim modeli geliştirmişlerdir.⁷⁷ O tarihe kadar sürekli denetim modellerinin birçoęu yazılımın içine gömülmüş modüllerden (embedded audit modules, EAM) yararlanmaktadır. Du ve Roohani bu durumun bağımsız denetçiler açısından bazı sakıncalar yarattığını öngörmüşlerdir. Denetlenen kurumun yazılımlarının içinde denetim modüllerinin yer alması için ilgili kurumun bilgisayar uzmanlarının planlama, programlama ve test aşamalarında denetçilere yardımcı olmaları gerekmektedir. İç denetçiler için daha kolay olan bu durum dış denetçiler için uygulamada zorluk getirmektedir. Denetçilerin sisteminin denetlenen kurumların sistemiyle iç içe olması denetimin bağımsızlığı konusunda şüphe uyandırmaktadır. Ayrıca, bu uygulama her sistem için ayrı bir yazılımın yaratılmasını gerektirmektedir. Bağımsız denetim yapan kuruluşların müşterilerinin her biri için ayrı ayrı yazılım geliştirmeleri çok maliyetli olacaktır.

⁷⁷ Hui Du ve Saeed Roohani. "Meeting Challenges and Expectations of Continuous Auditing in the Context of Independent Audits of Financial Statements", International Journal of Auditing. 11 (2007):133-146.

Du ve Roohani'nin geliřtirdiđi model özellikle dıř denetilerin bu sorunlarını zmek iin tasarlanmıřtır. En nemli zelliđi her trl veri formatını kullanabilmesi ve denetim yapılan kurumun sisteminden tamamen bađımsız olmasıdır. Sistem mhendisliđi aısından bakıldıđında tařınabilir bir yapıya sahiptir. Yani, denetim dneminin bařlangıcında denetlenen kurumun sistemine kolayca bađlanabilir ve denetim dneminin sonunda sorunsuz ayrılabilir.



řekil 10: Genel Bakıř - Finansal Tabloların Bađımsız Denetimi İin Srekli Denetim Modeli

Kaynak: Hui Du ve Saeed Roohani. "Meeting Challenges and Expectations of Continuous Auditing in the Context of Independent Audits of Financial Statements", International Journal of Auditing, 11 (2007):139.

İletiřim:

Srekli denetim iin denetinin sistemi ile denetlenen sistem arasında srekli veri transferi yapılmalıdır. Bunun iin iki sistem arasında iletiřimin srekliliđinin sađlanması gerekir. Denetinin sistemi en az maliyetle ve en kısa zamanda ilgili veriyi ekebilmelidir.

Veri formatı:

Du ve Roohani srekli denetim faaliyetini XBRL kullanarak gerekleřtirmeyi dřndrkleri iin XML veri formatını standart format olarak kabul etmektedirler. Bu nedenle onlar iin veri formatı iki trldr: XML olan ve olmayan. Modellerinde bu iki tr veri iin

çözüm önermişlerdir. Bu model XML formatındaki veri için XML tabanlı SOAP⁷⁸ (Simple Object Access Protocol - Basit Nesne Erişim Protokolü) veri protokolünün kullanılarak iletişim sağlanmasını önermektedir. XML formatında olmayan, farklı formatlardaki veri için CORBA⁷⁹ (Common Object Request Broker Architecture - Ortak Nesne İstem Aracısı Mimarisi) veri protokolünün kullanılması önerilmektedir.

Sürekli denetim dönemi:

Du ve Roohani ‘sürekli denetim dönemi’ diye bir kavram ortaya atmışlardır. Klasik denetimde olan denetim dönemi kavramını sürekli denetime uyarlamışlardır. Amaçlarının bir ölçüde düzenleyici kurumların da yaptırımlarını göz önüne alarak “ne sıklıkla denetim yapmalı” sorusuna cevap bulmak olduğunu belirtmektedirler. Bu modelde denetim dönemi başında denetlenen sistem denetçinin sistemine bağlanır ve denetim dönemi sonunda iletişimi sonlandırılır. Dönem içinde iletişim ve denetim sürekli ve gerçek zamanlıdır. Dönem zaman (dakika, saat, ay vb.) olarak tanımlanabileceği gibi işlem sayısı (bir aydaki ilk yüz işlem vb.) olarak da tanımlanabilir. Denetim kurumunun yöneticileri ile denetlenen kurumun yöneticileri sürekli denetim dönemine, başlangıç ve bitiş tarihlerine karar verirler.

⁷⁸ SOAP (Basit Nesne Erişim Protokolü) dağıtık uygulamalarda ve web servislerinin haberleşmesinde kullanılmak üzere tasarlanan, RPC (Remote Procedure Call) modelini kullanan, istemci/sunucu mantığına dayalı bir protokoldür. Daha genel olarak SOAP, web üzerinden fonksiyonları kullanmak için geliştirilmiş bir sistemin XML tabanlı kurallar topluluğudur.

⁷⁹ Common Object Request Broker Architecture, kısaca CORBA, (Ortak Nesne İstem Aracısı Mimarisi), Nesne Yönetim Grubunun'nun (OMG) Nesne Yönetim Mimarisi'nin (OMA) ana bileşenlerinden birisidir. Nesne Yönetim Mimarisi Nesne Modeli ve Referans Modelinden oluşur. Nesne Modeli heterojen bir ortamda dağılmış nesnelerin nasıl tanımlanabileceğini belirler. Referans Modeli ise nesneler arası etkileşimleri tanımlar. Dolayısıyla Nesne Yönetim Mimarisi heterojen ortamlara dağılmış beraber işleyebilen dağıtık nesnelerin geliştirilmesine ve konuşlandırılmasına yardımcı olur. CORBA sayesinde programcılar kullandıkları nesnelerin hangi dilde yazıldığına, dağıtık olup olmadıklarına, işletim sistemlerine ve iletişim protokollerine bakmaksızın programları geliştirebilirler. CORBA'nın ana bileşenleri ORB çekirdeği, OMG arayüz dili (OMG IDL), taşınabilir nesne adaptörüdür (POA).

5.1.9. Yeh ve Shen'nin Sürekli Denetim Modeli

Yeh ve Shen'in 2010 yılındaki makalelerinde⁸⁰ tartıştığı sürekli denetim modeli günümüz anlayışına örnektir. Kendilerinden önceki modellerin günümüz teknolojisiyle uygulanabilirliği en etkin yönlerini alan araştırmacılar XML (Extensible Markup Language) veri formatı olan Internet tabanlı ve üç katmanlı bir yapı önermişlerdir.

1. Veri erişim katmanı: Veri girişi sırasında denetim faaliyetlerinde kullanılacak olanlar tespit edilip ayrı bir veritabanına (data mart) alınır. Bu aşamada veritabanı programının özellikleri kullanılır.
2. Veri analiz katmanı: Veri, çeşitli bilgisayar destekli denetim yazılımları ile otomatik olarak incelenir. Karar destek sistemleri (Decision Support Systems, DSS) ve uzman sistemler (Expert Systems, ES) kullanılarak hızlı ve doğru denetim sonuçları elde edilir. Genel amaçlı denetim yazılımları ise denetçinin kendi programını yazmasına olanak vererek denetim etkinliğini artırır. Verinin bütünlüğü, doğruluğu ve güncelliği denetlenir. Veri analiz katmanı sürekli denetimin en önemli aşamasıdır.
3. Veri sunum katmanı: Veri analiz sonuçlarının görüntülediği bu aşamada denetim raporlarının Web sitesinde yayınlanması öngörülmüştür.

5.1.10. Baksa ve Turoff'un Sürekli Denetim Modeli

Robert Baksa ve Murray Turoff 2010 yılında yayınladıkları makalede⁸¹ acil durum yönetimi sistemlerini inceleyerek bir sürekli denetim modeli geliştirmişlerdir.

Baksa ve Turoff'a göre sürekli denetim sistemleri denetçi kararlarının bilgisayar sistemlerinde kullanılabilecek şekilde biçimlenmiş bir modelidir. Baksa ve Turoff sürekli denetim sistemlerinin Acil Durum Yönetimi⁸² (Emergency Management and Response) sistemleri ile benzerlik taşıdığını düşünmüşlerdir. Bu araştırmacılar sürekli denetimin

⁸⁰ Chun-Hsiu Yeh ve Wei-Cheng Shen. "Using continuous auditing life cycle management to ensure continuous assurance", African Journal of Business Management 4. 12 (Eylül 2010): 2554-2570.

⁸¹ Baksa ve Turoff, s.1.

⁸² Acil durum yönetimi kurum için hayati önem taşıyan varlıkların riskli durumlara karşı korunmasını ve bu varlıkların planlanan ekonomik ömürleri boyunca çalışmasını sağlamak amacıyla uygulanan stratejik yönetim süreçlerine verilen addır. Varlıklar ve olası felaketler kategorilere ayrılır. Her kategori için riskleri azaltmak, bir felaketin gerçekleşmesi halinde varlıkları bu duruma hazırlamak, felaketin gerçekleşmesi durumunda yapılacaklar, hasarı sınırlandırmak ve varlıkları felaket öncesindeki durumlarına getirebilmek için yapılacaklar planlanır.

karmaşık modellemesinin üstesinden acil durum yönetimi sistemlerini inceleyerek gelebileceklerini söylemişlerdir.

Sürekli denetim sistemini kurabilmek için kurumun iş süreçlerinin, önemli kontrol noktalarının, ölçme işlevinin ve kural dışı kabul edilen durumların modelinin yaratılması gerekir. İş süreçlerini analiz ederek işlem bazında anomalileri bulmak, sistemin ürettiği alarmları raporlamak, gerçek zamanlı kontrol ve risk değerlendirmesi yaparak kurumun kontrol zaafılarını ve artan risklerini göstermek sürekli denetim sisteminin kuruluş amacıdır. Bu seviyede bir otomasyonu sağlayabilmek için denetçinin yapacağı inceleme, değerlendirme ve karar verme faaliyetlerinin tamamen sürekli denetim sistemi tarafından yapılabiliyor olması gerekir.

Ancak, Baksa ve Turoff karar verme faaliyetinin bilgisayar sistemleri aracılığıyla yapılmaya çalışılmasının sürekli denetim uygulamalarının yaygınlaşması önünde bir engel olarak görmektedirler. Bu engeli aşmak için sürekli denetimin anomalileri belirleme ve bilgilendirme faaliyeti ile acil durum yönetimi araştırmaları sonucu geliştirilen karar verme tekniklerini birleştiren karma bir sistem geliştirilmesini önermektedirler. Turoff 2004 yılında yayınladığı bir makalede analizlerin bilgisayar tarafından, karar verme faaliyetinin ise denetçi tarafından yapılacağı karma bir model üzerinde durmuş, bu alandaki araştırmalara öncülük etmiştir.

Modelin Yapısı:

“En basit sürekli denetim sistem yapısı dijital veri kaynağı, iyi tanımlanmış veri onaylama motoru ve kurallar çiğnendiğinde ilgili tarafları bilgilendirecek alarm ve/veya raporlama mekanizmasından oluşur.”⁸³

Dijital Veri Kaynağı:

Baksa ve Turoff dijital veri kaynağını temin etmek için Groomer ve Murthy'den (1989) esinlenmiştir. Groomer ve Murthy'nin tarif ettiği şekilde ilgili kayıtların farklı bir veritabanına çekilerek bu veritabanı üzerinde denetimin gerçekleşmesini önermişlerdir. Kayıtları denetim yapılacak veritabanına çekmek için yazılımın içine gömülmüş modüllerden (embedded audit modules, EAM) yararlanmayı düşünmüşlerdir. EAM'lar önemli iş

⁸³ Baksa ve Turoff, s.2.

süreçlerinden denetlenmesi planlanan veriyi çekmek için yazılmış olup kurumun kayıtlarının tamamını çekmezler. Araştırmacılar EAM kullanımını sistemin hızının düşmesi, kayıtların sabit sürücüde çok yer tutması ve network bant genişliğinin yoğun kullanımı gibi donanımsal sınırlamaları en aza indirmek için önermişlerdir.

Veri Onaylama Motoru:

Bu modelde veri onaylama motorunun girdisi dijital formatta kaydedilmiş işlemler olup çıktısı ise denetim sırasında olağan dışı olarak belirlenen kayıtlardan kaynaklanan bir tür alarm veya rapordur.

Baksa ve Turoff aşağıdaki matematik teorileri ve bilgisayar sistemlerini kullanarak veri onaylama motoru için algoritmalar geliştirmeyi önermişlerdir:

- güven fonksiyonları (belief functions)⁸⁴
- devamlılık denklemi (continuity equations)
- uzman sistemler (expert systems)
- sinirsel ağlar (neural networks)
- regresyon temelli istatistik teknikleri

Ayrıca, veri onaylama motorunun birbirinin tamamlayıcısı olarak birden fazla algoritmayı kullanabileceğini belirtmişlerdir.

Bu yöntemlerin ortak noktaları gerçek zamanlı veya gerçek zamana yakın bir sürede olayları gözlemlemek, denetimde ortaya çıkan olağandışı durumlarda alarm vermek veya rapor düzenlemek, testleri hızlı, az maliyetli ve sürekli tekrarlayabilmektir.

Uygulamada Karşılaşılan Zorluklar:

Baksa ve Turoff'a göre uygulamalar sürekli denetimin olağan dışı durumları tespit etmesine yöneliktir; ancak, sürekli denetimin gerçek zamanlı tepki verme unsuruna odaklanılmamıştır.

Baksa ve Turoff'a göre Acil Durum Yönetimi (Emergency Management and Response) sistemi ile mevcut sürekli denetim sistemleri birleştirilirse bu sorun ortadan

⁸⁴ Dempster ve Shafer teorisi diye de anılan bu matematik modelinde birçok farklı kaynaktan toplanan bulgular değerlendirilir ve ilgili bulguya dair bir güven fonksiyonu yaratılır.

kalkacaktır. Uzmanların karar ve sonuçlarının modellendiği gerçek zamanlı karar destek sistemi ve/veya insan davranışlarını iş süreçlerine entegre eden bir model geliştirmenin bir çözüm olacağını savunmaktadırlar. Örneğin, olağandışı durumlar için iş akış modelleri geliştirilerek her aşama ve durum için denetçi kararlarının ne olacağı belirlenir ve sistemin ona göre karar alması sağlanabilir.

İş Süreçlerini Modelleme:

Sürekli denetim sistemlerinin kurulabilmesi için iş süreçleri, kontroller ve olağandışı durumlara ilişkin modellerin bilgisayarın anlaması için dijital ortamda yaratılması gerekir. Bu da ilgili konulara ilişkin algoritmaların geliştirilmesi ile yapılmaktadır.

Geleneksel denetimin dijital ortama aktarılması Baksa ve Turoff'a göre zor bir iştir. Karmaşık işlemlere ilişkin karar verme çok sayıda ölçütün birlikte kullanılmasını gerektirebilir. Farklı kaynaklardan veri elde edildiği durumlarda sık rastlanan bir konu da bu ölçütlerin birbirleriyle çelişmesidir. Geleneksel denetim tamamen dijital ortama aktarılmak üzere planlanmamış da olabilir. Bir ölçüde otomasyon sağlanmış ancak karar verme denetçiye bırakılmış olabilir. Bu durumda Baksa ve Turoff'un önerisi var olan denetim uygulamalarını bir kenara bırakıp denetimi yeniden planlayıp düzenlemektir.

Baksa ve Turoff modelini uygulamak için atılacak adımlar:⁸⁵

1. Sürekli denetim sistemini sağlam bir altyapının üzerine kurun.
2. Modellemesi ve otomasyonu en kolay süreçleri ele alın. Başta kapsamı dar tutun.
3. Sürekli denetim sistemi
 - kabul edilebilir bir sistem performansı olmalı
 - görülebilen belirgin sonuçlara ulaşmalı
 - kullanımı ve anlaması kolay olmalı
4. Yeni bir sistemi kullanmanın getireceği isteksizliği gidermek için üst yönetimin desteğini alın.

⁸⁵ Baksa ve Turoff, s.4.

5.1.11. Ye ve Li'nin Sürekli Denetim Modeli

Huanzhuo Ye ve Ye Li 2010 yılında insanlardaki bağışıklık sisteminden esinlenerek yeni bir sürekli denetim modeli geliştirmişlerdir. Bu modeli Nesneye Dayalı Kural Tabanı'na dayanarak Sürekli Denetimde Bağışıklık Modeli (Continuous Auditing Immune Model based on Object-Oriented Rule Base – CAIMOR) olarak adlandırmışlardır.⁸⁶

Biyolojide bağışıklık sistemi insanı hastalıklara karşı korumak için yabancı hücreleri tanımlar ve yok eder. Bağışıklık kendinden olanı tanımak ve kendinden olmayanı sonlandırmak esasına dayanır. CAIMOR da benzer bir mantık çerçevesinde çalışan yapay bir bağışıklık sistemidir. Bu model sistemin veriyi çekmesi, değerlendirmesi ve olağandışı durumları raporlaması aşamalarından oluşur.

Veri çekme:

Bu model gerçek zamanlı verinin tamamının denetlenmesi esasına dayanır. Bu nedenle transfer edilen bilgi tam ve gerçek zamanlıdır.

Veri değerlendirme:

CAIMOR'un veriyi değerlendirebilmesi için aşağıdaki adımların gerçekleştirilmesi gerekir:

1. Veri ile ilgili kural tabanını oluşturmak: Bu aşamada veri üzerindeki iş kuralları belirlenir. Kural tabanlı sürekli denetimi kurabilmek için normal denetim kurallarını belirlemek, denetim verisini ve kurallarını ilişkilendirmek gerekir. Nesneye dayalı programlama ilkeleri ile uyumlu özellikler, davranışlar ve veri işleme yöntemleri tanımlanır. Verinin birbiri arasındaki ilişkileri gösteren fonksiyonlar ve standart iş süreçleri şablonları belirlenir.
2. Yapay bağışıklık ile antikor⁸⁷ (antibody) tanıyıcı üretmek: Veri grupları içindeki her öğenin “kendi” veya “kendi değil” kümelerine ait olduğu varsayılır. Hangi verinin “kendi” hangisinin “kendi değil” kümesine ait olduğunu belirlenir. İlk aşamada “kendi” kümesinin küçük bir alt kümesi “kendi değil” kümesini belli ölçüde tanımlayabilir. CAIMOR kendi kendine öğrenen dinamik bir model olduğu için model

⁸⁶ Huanzhuo Ye ve Ye Li. “Research of Continuous Auditing Immune Model based on Object-Oriented Rule Base”, 2nd International Conference on Computer Engineering and Technology. Chengdu, Çin: 17 Haziran 2010: V4-148 - V4-152.

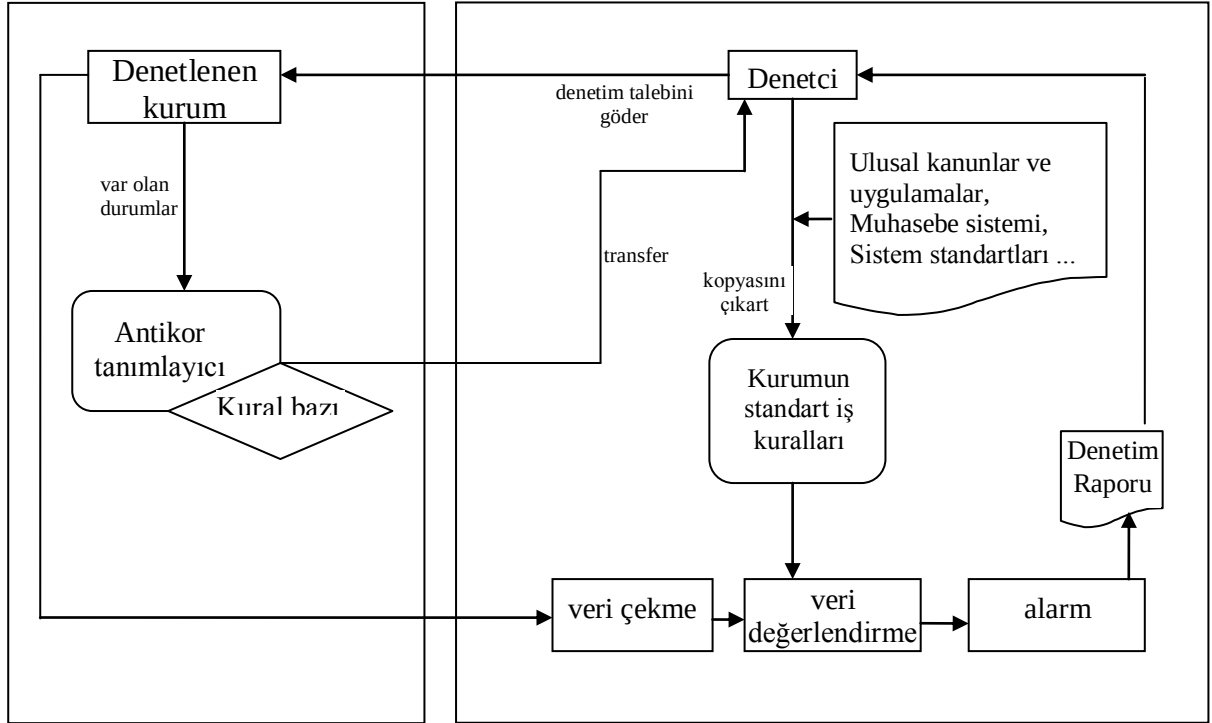
⁸⁷ Antikor: kana dışarıdan giren yabancı cisimlere karşı koyan madde.

kullanıldıkça “kendi değil” kümesi daha doğru ve kapsamlı olacaktır. “Kendi değil” kümesi olağandışı veri ve uygulamaları içeren bir bilgi grubudur. Denetlenen kuruma ilişkin anomalilerin tespit edildiği bu bilgi grubu yapay bağışıklık sistemi (artificial immune system) uygulamalarının geliştirilebilmesine zemin hazırlar ve kendinden olmayanı tanımlayabilecek “antikorların” üretilmesini sağlar.

3. Bilgisayarın yeni gelen verinin normal olup olmadığına karar vermesi: Yapay bağışıklığın kendini değerlendirme ve kendi kendine uyum sağlama gibi dinamik olanaklarını kullanarak olağandışı durumları belirler.

Raporlama:

Anomaliler “antikorlar” sayesinde bulunduktan sonra ilgililere raporlanır.



Şekil 13: CAIMOR'un Yapısı

Kaynak: Huanzhuo Ye ve Ye Li. “Research of Continuous Auditing Immune Model based on Object-Oriented Rule Base”, 2nd International Conference on Computer Engineering and Technology. Chengdu, Çin: 17 Haziran 2010: V4-152.

5.2. SÜREKLİ DENETİM MODELLERİNDE ÖNE ÇIKAN KONULAR

5.2.1. Sürekli Denetim Sistemlerinde Gömülü Denetim Modüllerinin Kullanılması

İlk olarak Groomer ve Murthy'nin ortaya attıkları gömülü denetim modülleri (Embedded Audit Modules-EAM) ile denetimin yapılması kavramı kendilerinden sonra gelen pek çok akademisyen tarafından benimsenmiştir. Bu modelde denetim kurumsal kaynak planlama yazılımının içine yerleştirilen denetim modülleri ile yapılmaktadır. Bir başka deyişle, kurumun kullandığı yazılım kodlarının içine ilgili konunun denetimine ilişkin kodlar eklenmiştir. Bu denetim modüllerinin kullanımı ve kontrolü bir arayüz yazılımı ile denetçiler tarafından gerçekleşir. Arayüz yazılımı kurumun yazılımlarının bir parçası değildir; bağımsız çalışan ve kurumun bilgi sistemine bağlanabilen bir yazılımdır. Bu sistemde denetim yazılım kodları kurumsal kaynak planlama yazılımına bağlıdır. Ancak, kullanım ve kontrolü bağımsızdır.

Bazı araştırmacılar gömülü denetim modülleri yönteminin denetimin bağımsızlığını zedelediği görüşündedirler. Bu nedenle kurumsal veriyi denetim veritabanına çekip ilgili testleri bağımsız bir bilgisayarda yapmanın daha doğru olacağını savunmaktadırlar.

Günümüzde bu iki ana görüşün savunucuları araştırmalarını farklı yönlerde yapmaktadırlar. Gömülü denetim modülleri yaklaşımını benimseyenler kurumsal kaynak planlama yazılımlarının geliştirilmesine yardımcı olurken denetim yazılımlarının bağımsızlığını savunanlar her tür veritabanından her formatta veriyi çekip inceleyebilen bağımsız yazılımlar üzerinde çalışmaktadırlar.

“EAM Ghosting” (gömülü denetim modülü gölgesi) denilen sistem gömülü denetim modülleri kullanan sistemler için denetimin bağımsızlığı sorununa çözüm olarak görülebilir. “EAM Ghosting” kurumsal kaynak planlama yazılımına yapılan tüm girişlerin bir kopyasını çıkartır ve farklı bir bilgisayara aktarır. Denetçiler çalışmalarını bu kopyalanmış veri üzerinde yaparlar. Bu bilgisayar kurumsal bilgi sisteminden bağımsız çalışır. İşlemlerin kopyası veri girişi sırasında çıkartıldığı için bu sistem gerçek zamanlı sürekli denetim uygulamaları için de uygundur.

Gömülü denetim modülleri kullanan sürekli denetim sistemleri önceden tanımlanmış ölçütlere göre veriyi ve işlemleri analiz ederler. Bir veri veya işlemin olağandışı olup olmadığı bu önceden tanımlanmış ölçütlere bağlıdır. Bu ölçütlerin zaman içinde değişimi denetimin etkinliğini olumsuz etkileyecektir. Ölçütlerde veya analiz tekniklerinde değişiklik yapılması kurumsal kaynak planlama yazılım kodlarında değişiklik yapılmasını gerektirir.

Bir yazılımın kaynak kodunda değişiklik yapmak için bu yazılıma tam erişim sağlanması gerekir. Kurumlar genel olarak iç veya dış denetçilere bilgi sistemleri üzerinde tam yetki vermedikleri için kurumsal kaynak planlaması yazılımlarında değişiklik bilgi işleminden sorumlu kişiler tarafından gerekli onaylar alındıktan sonra yapılabilir. Bu da kurum çalışanlarının denetçilerin kullanacağı testler ve algoritmalar hakkında bilgi sahibi olmalarına yol açacaktır.

Gerçek zamanlı denetim gömülü denetim modülleriyle kolaylıkla sağlanabilmektedir. Kurumsal kaynak planlama yazılımının denetim modülleri istenirse gerçek zamanlı olarak çalıştırılabilir. Sistemin yoğun olarak kullanıldığı zamanlarda denetim modüllerinin çalışıyor olması belli bir yük getirecektir. Ancak, gelişen ağ ve bilgisayar teknolojileri bu yavaşlamayı uzun vadede dengeleyebilecektir.

Gömülü denetim modülleri kullanan sürekli denetim sistemleri veriyi saklamak veya analiz etmek için ayrı bir bilgisayar sistemine ihtiyaç duymaz. Kurumsal faaliyetler ve denetimi aynı bilgisayarda yapılır. Bu nedenle veriye erişim ve saklanması ile ilgili herhangi bir sorun yaşanmaz. Veriyi başka bir bilgisayara çekip orada denetim yapan sistemlerde veri formatının denetim yazılımı ile uyumluluğuna, veri transferi sırasında veri bütünlüğünün sağlanmasına ve verinin saklanması için gerekli donanımların hazır olmasına dikkat edilmelidir.

5.2.2. XML'in Veri Formatı Olarak Benimsenmesi

Tüm sürekli denetim modelleri için kurumsal kaynak planlama yazılımının kullandığı veri formatı ile denetim yazılımının veri formatı arasındaki uyumluluk öncelikli bir konudur. Denetim verisi kurumsal faaliyetlerin işlendiği kurumsal kaynak planlama sisteminin veritabanından alınır. Bu veritabanının kullandığı veri formatı denetim yazılımı tarafından okunamaz ise denetim testlerini yapmak mümkün olmayacaktır.

Sürekli denetim modelleri ilk ortaya atılmaya başlandığı dönemlerde kurumsal kaynak planlama sistemleri ve denetim yazılımları kendi veri formatlarını yaratmışlardı. Bunlar çoğunlukla birbirleriyle uyum sağlamadıkları için “dönüştürme yazılımları” ile veri formatları değiştirilerek uyumlu hale getirilirdi. Bu “dönüştürme yazılımları” iki sistemin veri formatları incelenerek her kurum için ayrı ayrı yazılması gereken yazılımlardı.

Zaman alan ve belli bir maliyeti olan bu “dönüştürme yazılımları” veri bütünlüğünün korunması açısından da sorun yaratmaktaydı. Yazılımda olabilecek kod hataları kaynak veriyi dönüştürme sırasında kayıt alanlarının karışmasına veya belli alanların denetim sistemine hiç alınmamasına yol açabiliyordu.

Sürekli denetim modellerini ortaya çıkış tarihlerine göre sıralayarak incelediğimizde araştırmacıların bu soruna XML (eXtensible Markup Language) veri formatı ile çare aradıkları gözlemlenmektedir. Web tabanlı yazılımların yaygınlaşması ile XML veri formatı bilgi teknolojilerinde altın standart haline gelmiştir. Bu nedenle birçok kurumsal kaynak planlama yazılımı XML veri formatını kullanmaktadır. Yakın dönemde yaratılan sürekli denetim modellerine baktığımızda da veri formatı olarak XML’in tercih edildiğini görmekteyiz.

5.2.3. Web Tabanlı Sürekli Denetim Modellerinin Yaygınlaşması

Son yirmi yılda Internet kullanımındaki artış bilgi teknolojilerinde önemli gelişmelere yol açmıştır. Internet altyapısı kurumlar için ucuz ağ bağlantısı sağladığı için kurumsal yazılımlar ve veritabanları Internet üzerinden ulaşılmaya başlanmıştır. Böylece kurumsal yazılım kullanarak ilgili kurumun veritabanında işlem yapan kişiler özel ağlar kullanmak yerine Internet altyapısını kullanarak zaman ve mekan sınırlaması olmadan düşük maliyetle kurumsal kaynak planlama yazılımları ile çalışma imkanı bulmuşlardır.

Bu gelişme kurumsal kaynak planlama yazılımlarının Web tabanlı olmasına neden olmuştur. Bu yazılımlarla uyumlu olarak çalışması gereken denetim yazılımları da Web tabanlı üretilmeye başlanmıştır.

Denetim yazılımlarının Web tabanlı olması sadece uyumluluk sorunundan ileri gelmemektedir. Günümüzde Internet denetçilerin ilgili veriye ucuz ve kolay bir şekilde uzaktan erişim sağladığı bir ağ bağlantısıdır. Bu sayede denetlenen veri ile denetim yazılımının birbirinden farklı bilgisayarlarda hatta farklı mekanlarda olması bir sorun yaratmamaktadır.

Kavramsal sürekli denetim modellerinden uygulamaya geçilebilmesi için bu modellerin güncel teknolojiler düşünülerek yaratılması gerekmektedir. Internet kullanımındaki gelişmeler ışığında son yıllarda ortaya atılan sürekli denetim modellerinin Internet tabanlı olduğu gözlemlenmektedir.

6. SÜREKLİ DENETİM UYGULAMALARINI GELİŞTİRMEK

6.1. SÜREKLİ DENETİM UYGULAMALARININ AŞAMALARI

Araştırmalara baktığımızda sürekli denetim uygulamalarının genellikle altı adımda geliştirildiğini görmekteyiz.⁸⁸

1. Öncelikli denetim alanlarının tespiti

Hangi alanlarda denetim yapılacağı aşağıdaki konulara verilecek yanıtlarla mümkün olacaktır:

- Risklerin sınıflaması ve derecelendirmesi ile kritik iş süreçlerinin tespiti.
- Her bir risk için sürekli denetim verisine ulaşılabilirlik.
- Her bir risk için sürekli denetim uygulamasının getireceği fayda ve maliyet analizini yapmak.
- Denetim sonuçlarının kuruma katkısının en yüksek olduğu risk alanının seçilmesi.

2. Kuralların tespiti ve sürekli denetim modelini oluşturmak

Sürekli denetim faaliyetine yön veren kurallar tespit edilir. Bu kurallar programlanacak, sıkça tekrar edilecek ve gerektiğinde yeniden şekillendirilecektir.

3. Uygulamanın tekrarlanma sıklığı

Sürekli denetim uygulamasının hangi sıklıkla çalıştırılacağı önceden belirlenir. Sürekli denetimin amaçları ve denetim maliyeti denetimin hangi sürelerde tekrarlanması gerektiğini belirler.

4. Parametreleri ayarlamak

Olağandışı olarak sistemin tespit edeceği kayıtlar üzerinde yapılacak denetimin fayda maliyetine göre parametreler ayarlanır. Başlangıç parametreleri gerektiği zaman düzeltilir.

5. Denetim sonuçlarının takibi

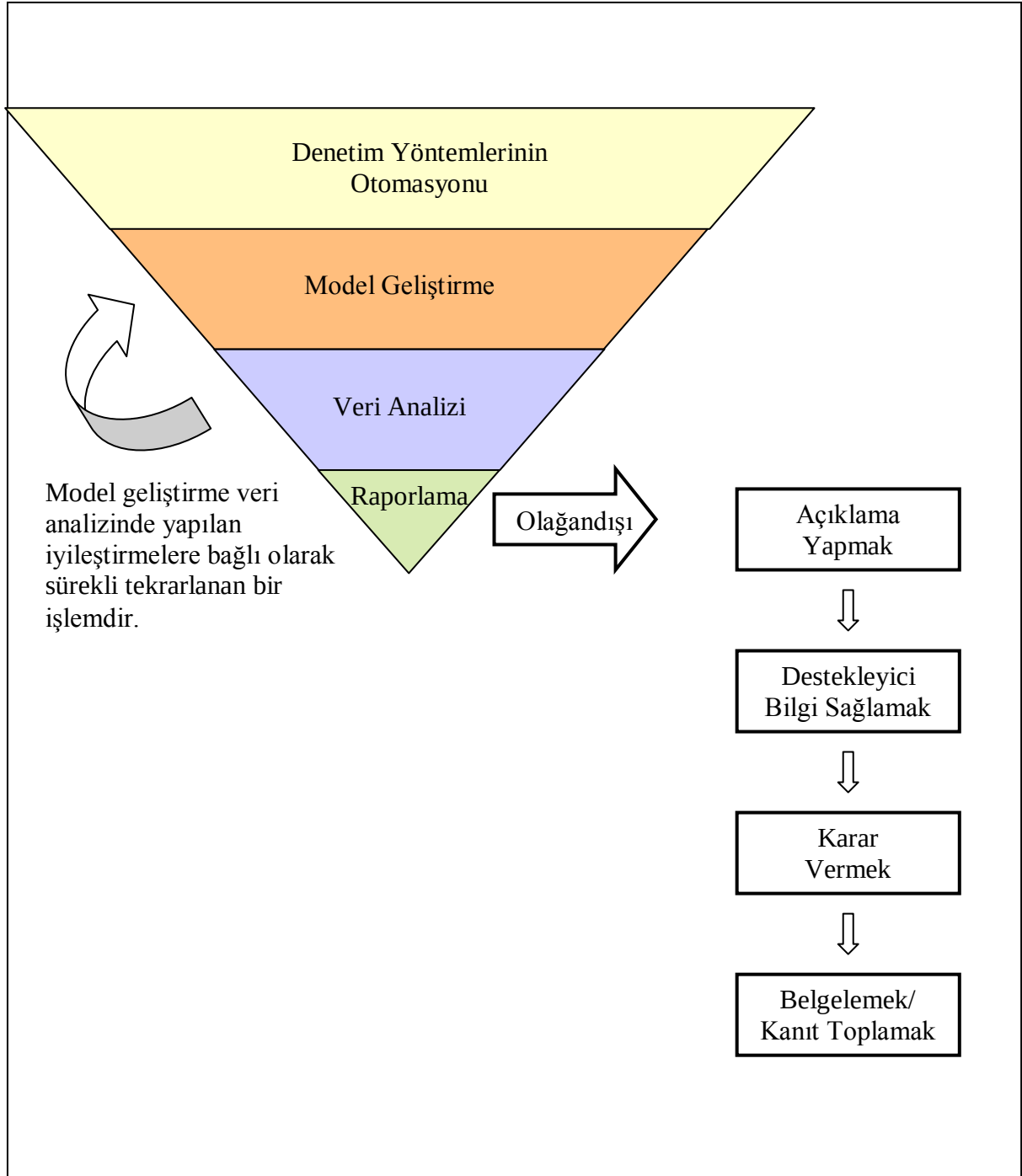
Olağandışı kayıtlar ve hataların tespiti durumunda yapılması gerekenler belirlenir.

⁸⁸ Carlos Elder Maciel De Aquino, Washington Lopes Da Silva and Miklos A. Vasarhelyi. "Moving Toward Continuous Auditing: Establishing Audit Priority Areas Can Lead To A More Effective Continuous Audit Process", Tech Forum (Ağustos 2008). <http://www.entrepreneur.com/tradejournals/article/183444836.html> (17 Ocak 2009).

6. Geribildirim

Denetim sonuçlarının kimlerle ve nasıl paylaşılacağı planlanır. Bu kişiler tarafından yapılması gereken çalışmalar varsa takip edilir.

Araştırmacılar farklı sürekli denetim modelleri üzerinde dursalar da bu modelleri kullanarak geliştirilecek uygulamaların evreleri konusunda benzer görüşler ortaya koymuşlardır. Denetimin amacının ve kapsamının belirlendiği ön hazırlık aşamaları tamamlandıktan sonra sürekli denetim uygulaması geliştirmenin evreleri (denetim yöntemlerinin otomasyonu, model geliştirme, veri analizi, raporlama) ve olağandışı durumlarda atılması gereken adımlar aşağıdaki şekilde görülmektedir:



Şekil 14: Sürekli Denetim Evreleri ve İşleyişi

Kaynak: David Y. Chan ve Miklos A. Vasarhelyi. "Innovation and Practice of Continuous Auditing". <http://www.raw.rutgers.edu> (18 Şubat 2011).

6.2. SÜREKLİ DENETİM UYGULAMALARINI GELİŞTİRMEK İÇİN ATILMASI GEREKEN ADIMLAR

6.2.1. Sürekli Denetim Uygulamalarını Geliştirmek İçin Ön Hazırlık

6.2.1.1. Denetim Amaçlarını Tespit Etmek

Sürekli denetim uygulamalarını geliştirmek için bir amaç olması gerekir. Amaç incelenen konuyu veya varılmak istenen noktayı ortaya koyar. Bu amacın tanımı ilgili uygulamanın neden yaratıldığının ve nasıl kullanılacağına açıklamasıdır.

Denetimin amaç açıklaması yapılacak denetim faaliyetinin genel çerçevesini tanımlar. Denetim planlaması sırasında ön hazırlık sürecinde kurumsal iş süreçleri incelendikçe kuruma, iş koluna ve genel ekonomiye bağlı riskler daha iyi anlaşılacak ve denetim faaliyetinin detayları ortaya çıkacaktır. Ancak, denetimin amaç açıklaması büyük resmi çizmelidir.

Amaç açıklaması yapılacakların detaylı bir dökümü olmasa da denetimin sonucunda ulaşılmak istenen noktayı açıkça ortaya koyması gerekir. Amaç açıklaması aşağıdaki örneklerde görüldüğü gibi olabilir:

- Kurumun merkez ve şubelerindeki satın alma süreçlerindeki iç kontrollerin yeterliliğini denetlemek.
- Duran varlıklara ilişkin yapılan kayıtların muhasebe standartlarına uygunluğunu denetlemek.
- Kurumsal kaynak planlama yazılımı kullanıcılarının işlemlerini kendilerine tanımlanmış yetkileri aşmadan gerçekleştirmiş olduklarını denetlemek.

Denetim amaç açıklamasına test kapsamı hakkında bilgi eklenebilir. Örneğin, denetimin belli bir şubeyi veya belli bir coğrafi bölgeyi kapsayacağı durumlarda denetime konu olan alan amaç açıklamasında yer alırsa ilgili taraflar açısından daha bilgilendirici olur.

Analize başlamadan amaçların net olarak belirlenmesi gerekir. Amaçları ortaya koymadan denetim stratejileri belirlemek imkansızdır. Amaçların belirlenmesi zamanın ve kaynakların etkin kullanılmasını sağlar.

Bir kurumda iş birimlerinin yaptıkları işlerden ve yapılarından kaynaklanan farklı ihtiyaçları vardır. Bu nedenle farklı birimlerin, hatta süreçlerin denetim amaçları birbirinden farklı olabilir. Amaçların gerçekçi olması, erişilmesi beklenen sonuçların ilgili kişilere ve kuruma değer katması gerekir.

Sürekli denetim uygulamalarını geliştirmek için denetimin amaçlarının beklentileri karşılayacak şekilde ortaya koyması gerekir. Denetimin planlaması, yapılacak testler ve analizler ilgili denetimden beklentiler doğrultusunda şekillenir. Dolandırıcılık Müfettişleri Birliği'nin (Association of Fraud Examiners - ACFE) son yıllarda yayınladığı raporlarda tespit edilen hilelerin sadece %10-%12'sinin finansal denetim sırasında ortaya çıktığını belirtmiştir. Bunun nedenini de finansal denetimin odağının hile denetimine göre farklı olduğu ve yapılan testlerin de farklılaşması olarak göstermiştir.⁸⁹

Denetimin amacının detaylı ama net olarak ortaya konması hangi kontrollerin denetlendiğinin tam olarak anlaşılmasını sağlayacaktır. Sürekli denetimin kapsamadığı bir kontrol varsa açıkça görülebilecektir.

Denetim amaçlarının yönetimin katkılarıyla iç ve dış denetçiler tarafından tespit edilmesi gerekir. Amaçların saptanmasında söz sahibi olan denetçiler sektör, kurum, iş süreçleri, kontroller ve bilgisayar destekli denetim teknolojileri konularında bilgi sahibi olmalıdırlar.

Denetim amaçlarını belirlerken aşağıdaki hatalardan kaçınmak gerekir:⁹⁰

- İletişim eksikliği: Denetçiler kendi içlerinde ve kurum çalışanları ile iyi iletişim içinde olmalıdırlar. Denetimin kapsamının ve yapılacak testlerin gerekçelerinin ilgili kişiler tarafından anlaşılması için denetimin amaçlarının kurum çalışanlarına anlatılması gerekir. Denetim amaçlarının iyi anlatılmaması kurum çalışanlarının denetçilere karşı güvensizlik duymalarına neden olabilir.
- Yetersiz açıklama: Denetim amaçları ilgili sürekli denetim uygulamasının neden geliştirildiğine dair yeterli derecede bilgi vermelidir. Konu hakkında daha önce bilgi

⁸⁹ Timothy A. Pearson ve Tommie W. Singleton. "Fraud and Forensic Accounting in the Digital Environment", Issues In Accounting Education 23. 4 (Kasım 2008): 547.

⁹⁰ Robert L. Mainardi. Harnessing the Power of Continuous Auditing: Developing and Implementing a Practical Methodology. A.B.D.: John Wiley & Sons, Inc., 2011:67-69.

sahibi olmayan bir kişinin bile denetimin gerekçelerini anlayabileceği ölçüde detay verilmelidir.

- Kayıp bağlantı: Denetim amaçlarının kurumsal hedeflerle bağlantılı olması gerekir. Denetim amaçlarını belirlerken denetimi yapılan bölümün kurumsal hedefleri gerçekleştirmedeki rolü ve faaliyetlerinin kuruma etkisi göz önüne alınmalıdır.
- Gerçekleştirmesi olanaksız sürekli denetim amaçları belirlemek: Denetim kapsamının geniş tutulmasının daha başarılı bir sürekli denetim uygulaması yaratacağı inancı vardır. Ancak, bu durum odaklı ve doğrudan yaklaşımı olanaksız hale getirir. Sürekli denetimin amaçları çok fazla ve birçok farklı faaliyet süreçlerini kapsıyorsa geliştirilen uygulamayı yönetmek ve raporlamak zorlaşır. Denetçilerin ve kurum yönetiminin uygulamayı geliştirme sürecinde olumsuz bir durum yaşamamaları için sürekli denetim amaçlarının gerçekleştirilebilir ve kurumsal hedeflerle uyum içinde olması gerekir.

6.2.1.2. Yönetimin Desteğini Almak

Sürekli denetimin amaçları tespit edildikten sonra üst yönetimin desteği sağlanmalıdır. Üst yönetim veri erişimi, değerlendirme yöntemleri, raporlamanın nasıl ve ne zaman yapılacağı da dahil tüm aşamalarla ilgili bilgilendirilmelidir. Bu yapılmadığı takdirde kaynak veriye ulaşma sürecinde ve işlemlerde anomaliler tespit edilip yöneticilerden açıklama istendiğinde sürekli denetime karşı tepki oluşabilir, denetim faaliyetlerinin yavaşlamasına yol açabilir.

6.2.1.3. Teknik Bilgiyi Geliştirmek

Veriyi bulmak ve analiz etmek için veri ile ilgili temel bilgilerin kavranması gerekir. Bu temel bilgi verinin bulunduğu dosya formatı, veri erişim ve dosya transfer yöntemlerini de içerir. Bu tür temel teknik bilginin ilgili denetim projesinde çalışacak kişiler tarafından bilinmesi özellikle veriye erişim sürecinde veri bütünlüğünün sağlanması açısından önemlidir.

Sürekli denetim uygulamaları kurarken kurumun teknolojik altyapısını göz önüne almak gerekir. Bilgi sistemine yapılan ilaveler ve değişiklikler her zaman iyi belgelenmemiş olabilir. Kullanılmakta olan yazılım ve donanım belgelenenden farklı olabilir. Denetim

projesinde çalışan kişilerin bu konudaki değişiklikleri fark etmeleri ve iş süreçlerine etkilerini değerlendirebilmeleri gerekir.

Sürekli denetim uygulaması ilk kurulduğunda denetim yazılımının hatalı oluşunu belirttiği kayıtların bir bölümü aslında hatalı olmayabilir. Yazılım kullanılan hatalı parametreler nedeniyle veriler ve raporlara ilişkin hatalı yorumlama yapılabilir. Kullanılan parametreler ve kontroller zamanla düzeltilerek bu hatalar giderilir. Denetçiler kurumsal bilgi sistemini daha iyi tanıdıkça bu sorun ortadan kalkacaktır.

6.2.1.4. Denetim Yazılımını Belirlemek

Sürekli denetim yapabilmek için veriye elektronik olarak ulaşabilmek ve analiz edebilmek gerekir. Bu nedenle denetimde kullanılacak bilgisayar programlarının seçimi uzun vadeli başarıda önemli rol oynar. Veri kaynakları, formatları ve miktarı göz önüne alınarak denetim programının seçilmesi gerekir. Kurumun o anki bilgisayar sistemleri ve bilgi teknolojileri ile ilgili gelecek planları da dikkate alınmalıdır. Günümüzde denetim amaçlı yazılmış programlar farklı veri türlerindeki bilgiyi farklı işletim sistemlerinden alabilme ve analiz edebilme yeteneğine sahiptir. Veriye ulaşım konusundaki engeller teknolojik olmaktan çok denetçilere verilen erişim hakları ile ilgilidir. Sürekli denetim yapabilmek için denetçilerin kurum verilerine ve uygulamalarına doğrudan erişim hakkına sahip olmaları gerekir.

6.2.1.5. İş Süreçlerini Anlamak

Denetimin amacını tespit edip ilgili bilgisayar uygulamaları hakkında bilgilendikten sonra kaynak verinin yaratılmasına neden olan iş süreçlerini de anlamak gerekir. İş süreçleri hakkında bilgi sahibi olmayan bir denetçinin işlemler ve kontroller konusunda görüş bildirecek bir uygulama geliştirmesi düşünülemez.

İş süreçleri hakkında bilgiye aşağıdaki yöntemlerle ulaşılabilir:

- Araştırma: Belli bir sürece ait genel bilgiye sahip olmak için parçası olduğu ana faaliyet konusunda araştırma yapılmalıdır. Özellikle daha önce ilgili faaliyet alanında bir denetim uygulaması yapılmamışsa bu araştırma daha büyük önem taşır. Kütüphane veya Internet’te yapılan araştırmalar denetçilere faaliyet alanına ait temel bilgileri, istatistikleri, güncel haber ve duyuruları sağlar.

- Önceki denetim faaliyetleri ve sonuçları: İlgili birimde veya faaliyet alanında daha önce denetim yapılmışsa önceki denetimlere ilişkin dokümantasyon ve geribildirim değerlendirilir. Eski denetimlere ait bilgilerden faydalanılacak alanlar aşağıdaki gibidir:
 - Amaçlar: İlgili iş biriminin kuruluş amacı, denetimin yapılma nedeni ve uygulanmış analizlerin seçilme nedeni ilgili faaliyet konusunda önemli bilgiler verir.
 - Kapsam: İşin kapsamı analiz aşamasında incelenen konuların detayları hakkında bilgi verir.
 - Riskler ve kontroller: Önceki denetim dokümanlarından belirlenmiş riskler, bu risklerin gerçekleşme olasılığı ve yaratacağı sonuçlar görülür. Sürekli denetim uygulamalarının önemli risklere karşı kontrollerin etkin ve çalışır durumda olduğunun güvencesini vermesi gerekir. Geçmiş denetimlerin sonuçları göz önüne alınarak güncel riskler önem sırasına göre sıralanır. Yeni sürekli denetim uygulamasının ilk analiz edeceği alanlar önemli risklere karşı alınan önlemler olmalıdır.
 - Analizler: Denetim planı incelenerek yapılmış olan analizler hakkında bilgi edinilir. Kontrollerin risklerin gerçekleşmesini önlemede etkinliğini test eden bu analiz teknikleri faaliyetlere ilişkin süreçler hakkında önemli bilgiler verir. Kontrolleri test etmede etkin olan analizlere yeni kurulacak sürekli denetim uygulamasında da yer verilir.
 - Sonuçlar: Denetim sonuçları kontrol yapısının ne kadar etkin ve verimli çalıştığı hakkında bilgi verir.
- Süreci incelemek: İlgili birimde şahsen bulunup faaliyet sürecini gözlemlemek sürece ilişkin konuların daha iyi anlaşılmasına olanak verir. Olayları yerinde görmek, yöneticilerle görüşmek, soruları bizzat işi yapana sormak tarafsız bir gözle sürecin incelenmesini sağlar.
- Süreç şeması çıkarmak: Faaliyet sürecinde yapılan işlemler adım adım detaylı bir şekilde belirlenir. Belirlenen işlemler şematik olarak gerçekleşme sırasına göre yerleştirilir. Süreç haritası hazırlama aşamasında riskler ve ilgili kontroller de şema üzerinde gösterilir. Böylece iş biriminin faaliyetleri detaylı bir şekilde açıklanmış ve sürekli denetim uygulaması geliştirecek denetçiler için odaklanacakları önemli kontroller belirlenmiş olur. Süreç haritası hazırlamak süreci genel hatlarıyla tarif

etmekten daha fazla zaman alsa da sürece ilişkin denetimin otomasyonunu kolaylaştırır.

- Bilgi sistemini incelemek:
 - Bilgi sistemine ait dokümantasyonu incelemek: program kullanım kılavuzu, sistem akış şeması, örnek çıktılar, veritabanına ilişkin bilgi, sistem kontrolleri hakkında bilgi vs.
 - Bilgi sistemi kullanıcıları ve programcıları ile görüşmek
 - Standart raporları ve hata raporlarını incelemek
- Tedarikçilerden müşterilere kadar uzanan yolu takip etmek: Tedarikçiler, girdiler, işlemler, çıktılar ve müşteriler hakkında bilgi toplamak faaliyet konusunda ve iş birimlerinin birbirleriyle olan ilişkileri hakkında tamamlayıcı bilgi verir. Tedarikçiler malzeme, bilgi, form ve eleman sağlayan kişi veya kurumlardır. Girdiler hammadde, raporlar, süreç bilgisi veya personel gibi süreci tamamlamaya yönelik unsurlardır. İşlemler sürecin parçalarıdır ve başlangıçtan sona kadar belgelenmelidirler. Çıktılar rapor, onay, bitmiş bir montaj veya bilgi olabilir. İlgili çıktıları alan kişi veya kurumlar da müşterileri oluşturur.
- Düzenleyici kurallar: Kurumsal politikalar ve uygulamalar, yasalar, düzenleyici kurumların kararları gibi iç ve dış kurallar süreçler üzerinde etkilidir. Bu kuralların değişikliğe uğraması gelecekte süreçlerin uygulanmasında değişiklik yaratabilir. Süreçleri denetleyecek yazılımlar hazırlanırken bu kurallar ve değişiklik riski de dikkate alınmalıdır.

İş süreçlerini öğrenirken ilgili bilgi sistemi, kontroller ve veri hakkında da daha derin bilgi edinilmiş olur.

6.2.1.6. Önemli Kontrol ve Riskleri Belirlemek

Sürekli denetimin amacı kontrollerin etkinliği arttırmak ve riskleri azaltmaktır. Bunu yapabilmek için önemli kontrolleri ve risk kategorilerini tespit etmek gerekir. Denetçiler risk değerlendirmesi yaparak hangi kontrollerin incelenmesi gerektiğine karar verirler.

Denetçiler kontroller hakkında görüş bildirmek için ilk önce kurumun iç yapısını anlamalıdır. İç kontrol yapısı Sponsor Kurumlar Komisyonu'nun (The Committee of Sponsoring Organizations-COSO) yaptığı çalışmalara paralel olarak tanımlanabilir. 1992

COSO raporunda iç kontrol yapısının beş bileşeninden söz edilmektedir: kontrol ortamı, risk değerlendirmesi, bilgi ve iletişim, kontrol faaliyetleri ve izleme. İç kontrollerinin yeterliliği bu beş bileşenin değerlendirilmesi sonucunda ortaya çıkar. Denetçiler testler yaparak iç kontrol uygulamalarının ve süreçlerinin etkinliğini değerlendirirler. İç kontrol sisteminin incelenmesi denetçilerin iç kontrol yapısı hakkında görüş sunabilmeleri için gereklidir. İç kontrollerin güvenilirliği toplanan denetim kanıtlarının güvenilirliği açısından da önemlidir. İç kontrollerin içerik, zamanlama ve kapsam açısından yapılan testleri işlemler üzerinde yapılan testlerle eşzamanlı olarak gerçekleştirilir. Kontrollerin testleri yönetimin belirlediği kontrolleri incelemekle başlar. Denetçiler yönetimin kontrollerinin uygun ve yeterli olduğuna karar verdikten sonra işlemlere ilişkin iç kontrolleri incelerler.

Denetim verimliliğini arttırmak için denetim en kısa zamanda en fazla sonuca ulaşılacak şekilde planlanmalıdır. Bu nedenle incelenecek iş süreçleri ve bilgi sistemleri önceliklendirilir.

6.2.2. Sürekli Kontrol ve Risk Değerlendirme İlişkisi

Kontrol ve risk değerlendirmeleri birbirini besleyen iki faaliyettir. Birinin sonucu diğ erinin girdisidir. Risk artışı kontrol zaaflarına bağlı olabilir. Bu durumda kontrol zaaflarını giderici tedbirler alınır. Kontrolleri değerlendirmek de risk seviyelerine göre yapılır. Risk seviyelerine göre alınacak tedbirler değerlendirilir.

6.2.2.1. Sürekli Kontrol Değerlendirmesi

İş süreçlerinin doğruluğu kontrollerin uyumlu, etkin ve verimli olmasına bağlıdır. Kontroller bilginin gizlilik, bütünlük, ulaşılabilirlik ve güvenilirliğini sağlamalıdır.

Sürekli kontrol değerlendirmesi, elektronik ortamda kayıtlar üzerinde önceden tasarlanmış kontrol testleri uygulayarak bağımsız analizler yapmaktır.

Sürekli kontrol değerlendirmesi, kontrollerin limit aşım ları, boş geçilmiş veri alanları gibi standart sorunlardaki tespit yeteneğini ölçebildiği gibi daha karmaşık istatistiksel testler de uygulayarak kontrollerin etkinliğini ölçer. İç kontroller test edilir ve etkinlikleri değerlendirilir. Süreçler, kontrol noktaları, önemli kişiler ve riskler gözden geçirilir.

Aşağıdaki tabloda sürekli denetim için kontrollerin bileşenleri, tanımları, nitelikleri ve kontrol teknikleri özetlenmektedir.

Tablo 2
Gerçek Zamanlı Muhasebe Sistemi ve Sürekli Denetim İçin Kontrol Matrisi

Kontrol bileşenleri	Tanım	Kontrol nitelikleri	Kontrol teknikleri
Kontrol ortamı	Yönetim gerçek zamanlı muhasebe sisteminin var olan kontroller üzerindeki etkilerini değerlendirmelidir. Yönetim yeni riskleri ve muhasebe sistemini iyi yönetmelidir.	Elektronik ortamda iş yapmanın yeni yöntemi Şirketlerarası bağımlılık İş dönemlerindeki değişiklikler Otomasyon seviyesi	Sağlam iş stratejileri ve yönetimin kararlılığı Kurum dışı sistem sağlayıcıların yönetimi Ortaklararası sözleşmelerin el değiştirmesi İnternet üzerinden yapılan ticarete güvenlik kontrolleri Yazılımı geliştirme aşamalarında kontrol etmek
Risk değerlendirmesi	Risk değerlendirmesi elektronik ortamda kayıtların girilmesi ve finansal tabloların hazırlanması sırasında doğabilecek risklerin tespiti, analizi ve yönetimi süreçlerinden oluşur.	Belli bir finansal tablo ve bu tabloyu elektronik olarak hazırlama sırasında meydana gelebilecek risklerin ilişkisi İç ve dış riskler, ilgili olaylar/durumlar Olası yeni risklerin iyi yönetilebilmesi için gerçek zamanlı muhasebenin iç kontrol yapısına etkisinin değerlendirilmesi	Kontrollerin otomasyonu Gürültü seviyesini azaltmak için iyileştirmeler Dijital imza ve tanıma güvenceleri Uyum programı Kontrollerin kendi kendilerini değerlendirme programı
Bilgi ve iletişim	Bilgi sistemi finansal kayıtları, belgeleri ve raporları elektronik olarak oluşturan elektronik muhasebe sistemi ve gerçek zamanlı muhasebe sisteminden oluşmaktadır. İletişim	İşlemlerin doğru, tam ve geçerli olduğunu bütünlük kontrolleri sağlar. İyi bir gerçek zamanlı muhasebe sistemi güvenilir finansal bilgi üretmeli ve finansal tablolarda hata	Bilginin yetkisiz kişilerce görülmesini engellemek için koruma kontrolleri (şifreleme) Yetkili kullanıcıların erişimini sağlamak ve yetkisiz kişilerin erişimini engellemek

	gerçek zamanlı finansal bilgiyi hazırlama ve yaymayı içerir. Kontrol yapısı bilginin tanımlanması, elde edilmesi ve başkasına verilmesi işlerinin zamanlı ve uygun şekilde yapılmasını sağlar.	olmasını önlemelidir. Etkin bir gerçek zamanlı muhasebe sistemi yeterli ve denetlenebilir işlem geçmişi sağlayabilmelidir.	için erişim kontrolleri (güvenlik duvarı-firewall) Denetim veritabanı Yedekleme ve saklama kuralları Sürekli ve uygunluk denetimi
Kontrol faaliyetleri	Kurumsal hedeflere ulaşmak, finansal tabloların güvenilirliğini sağlamak, varlıkları korumak ve kanunlarla uyumun sağlanması için kurallar ve yöntemler geliştirmek. Kontrol faaliyetleri sadece izin verilen işlemlerin yapılmasını, görevler ayrılığının korunmasını, yeterli belge ve kaydın temin edilmesini, varlıkların ve kayıtların korunmasını sağlar.	Kontrol faaliyetleri yazılımın, donanımın, elektronik ortamdaki veri ve kayıtların yetkisiz kişilerce ulaşılmasına ve değiştirilmesine karşı yeterli korumanın sağlanmasını güvence altına alır. Fiziksel erişim kısıtlanmıştır. Etkin ve yeterli gerçek zamanlı muhasebe sistemi kullanılır. Uygun yedekleme, koruma ve beklenmedik durum planları yürürlükte.	Yetkilendirme yöntemleri İşlem belirleme ve tanımlama Şifreleme Donanımsal kontroller Kurumsal kontroller Belgeleme ve kayıtlar Bilgi işleme kontrolleri Görevler ayrılığı Yedekleme ve koruma kuralları
İzleme	Gerçek zamanlı muhasebe sisteminin ve ilgili iç kontrollerin kalitesini, bütünlüğünü ve güvenilirliğini değerlendirme sürecidir. Bu unsur iç kontrol faaliyetlerinin yeterli olduğunu, etkin çalıştığını ve zaman sürecinde güvenilir olduğunu garanti eder.	Devam eden izleme faaliyetleri Dönemsel değerlendirmeleri ayırmak İç denetçilerin yaptığı uygunluk ve sistem denetimleri Dış denetçiler tarafından yapılan sürekli denetim	Sistem denetimleri aracılığıyla Gömülü denetim modülleri Bilgisayar destekli denetim teknikleri Sistem denetiminin otomasyonu Sistem kontrol ve denetim inceleme olanağı Enstantane (snapshot) yaklaşımı*

Kaynak: Zabihollah Rezaee, Rick Elam, Ahmad Sharbatoghlie. “Continuous auditing: the audit of the future”, Managerial Auditing Journal 16. 3 (2001): 154.

* Verinin işlemten önce ve sonra “fotoğrafi” alınır. Uygulamanın doğruluğu ve güvenilirliğini kontrol etmek için kullanılır.

6.2.2.1.1. Kontrol Amaçlarının Tespiti

Ana faaliyetler ve ilgili süreçler saptandıktan sonra kontrol amaçları tespit edilir. Kontrol amaçları COSO başlıkları altında sınıflandırılabilir: yetki, doğruluk, bütünlük, geçerlilik, etkinlik ve verimlilik, görevlerin ayrılığı, düzenleyici kanun ve kurallara uyum.

6.2.2.1.2. Önemli Kontrollerin Tespiti

Sürekli kontrol değerlendirmesi ana faaliyetler üzerindeki kontrollerin tespiti ile başlar. Kontrollerin etkin ve verimli olması için geliştirilmesi gerekir. Hile, hata, israf ve kötü kullanımdan doğan zararları önleme açısından kontroller önemlidir. Ancak, bu kontroller amaçlandığı şekilde çalışmıyor olabilirler veya zaman içinde yetersiz kalabilirler. Yeniden yapılanma, küçülme veya bilgi sisteminde değişiklik yapma kontrolleri zayıflatan unsurlardır.

6.2.2.1.3. Kontrollerin Test Edilmesi

Ana faaliyetler, ilgili süreçler ve bunlara bağlı kontrol amaçları tespit edildikten sonra kontrol noktaları risk seviyelerine göre sınıflandırılır. Her bir kontrol amacına uygun analiz yöntemi geliştirilir. Örneğin, amacı sadece yetkili kişilerin onay vermesi olan bir kontrolü test etmek için hiç onay alınmamış veya yetkisiz kişilerce onaylanmış olan kayıtların tespitine yönelik bir test geliştirilir.

Kontrollerin etkinliğini değerlendirmek için önerilen bilgisayar destekli denetim teknikleri aşağıdaki gibidir:⁹¹

1. Gerçek zamanlı muhasebe sisteminin geçerli ve geçerli olmayan veriyi doğru işlediği, yapılan işlemlerin doğru ve tam olduğuna dair testleri yapmak
2. Uygulama programlarının bir kopyası ile eşzamanlı simülasyon yaparak kontrol faaliyetlerinin etkinliğini değerlendirmek
3. Denetim modüllerini bilgisayar uygulamalarının içine kodlayarak verinin işlenişini sürekli ve eş zamanlı incelemek

⁹¹ Rezaee, Elam, Sharbatoghlie, s. 153.

4. İşlem sırasında denetimi yapılacak bilgiyi seçmek için sürekli ve aralıklı simülasyon yapmak ve anında denetim olanağı sağlamak

Kontrollerin otomasyonunu test etmek için:⁹²

- Kontrol sistemi adım adım ele alınıp tasarımının amaçlara uygunluğu ve dokümantasyonun yeterli olup olmadığı değerlendirilir.
- Kontrollerin etkinliği örnek işlemlerle test edilir.
- Kontrollere ilişkin yazılım kodları incelenir.
- Kontrollere ilişkin kurallar test edilir. (borçlu alacaklı hesaplar, hesap limitleri vb.)
- Uygulamayı başka bir denetim yazılımı ile aynı anda kullanarak aynı sonuca ulaşıp ulaşılmadığı test edilir.

6.2.2.2. Sürekli Risk Değerlendirmesi

Günümüzde kurumlar çok çeşitli risklere maruz kalırlar. Risklerin gerçekleştiği durumda doğacak zararları değerlendirmek için bazı yöntemlere gerek duyarlar. Bu risk yönetim sürecidir. Risk yönetimi belirsizliklerin kuruma etkisini değerlendiren ve alınacak önlemleri belirleyen bir yönetim faaliyetidir.

Risk yönetimine verilen önem her kurumda farklıdır. Bazı kurumlar riskleri düşük, orta ve yüksek diye temel gruplara ayırırken bazı kurumlar daha gelişmiş analizler yaparak risklerin maliyetini ölçmeye çalışırlar.

Kurumun başarısı ve faaliyetlerinin devamı için önem taşıyan risk yönetim süreci denetimin iki ana bileşeninden biridir. Etkin risk yönetimi olan kurumlarda denetçiler sorularına daha kolay cevap bulurlar. Yine de bağımsız bir gözle kurumun karşı karşıya kaldığı riskleri belirlemek, anlamak, maliyetlerini ve etkilerini değerlendirmek, gerçekleşme olasılıklarını hesaplamak denetçilerin görevidir. Denetim bölümünün yapacağı çalışmalar risk tabanlı olup yönetimin riskleri tespit etme ve değerlendirme yeteneğini sorgular.

Etkin bir sürekli risk değerlendirme döngüsü aşağıdaki adımlarla gerçekleşir:

- Riskleri belirlemek

⁹² Coderre, Internal Audit, s. 98.

- Belirlenen risklerin sayısal ve niteliksel değerlendirmesini yapmak
- Riskleri önem derecelerine göre sıralamak
- Gerçekleşmesi durumunda yapılacakları denetlemek
- Riskleri sürekli izlemek, gerekli görüldüğünde düzeltme ve değişiklikler yapmak

6.2.2.2.1. Kurumsal Risk Yönetiminin Değerlendirilmesi

Sürekli risk değerlendirmesinin yapılabilmesi için ilk yapılması gereken yönetimin kurumsal risk yönetimi faaliyetini gerçekleştirip gerçekleştirmediğidir. Eğer kurumsal risk yönetimi yapılıyorsa denetçiler ilgili faaliyetlerin yeterliliğini gözden geçirir. Bu faaliyet yönetim tarafından gerektiği gibi yerine getirilmiyorsa COSO Kurumsal Risk Yönetimi standartları başlangıç noktası kabul edilebilir.

6.2.2.2.1.1. Olası Riskleri Anlamak

Kurumun başarısını etkileyecek tüm riskler belirlenmelidir. Bu tüm kurumu ilgilendiren risklerden sadece bir birimi veya bir projeyi ilgilendiren risklere kadar tüm risklerin tespit edilmesi anlamına gelir.

Denetçilerin olası riskleri belirleyebilmeleri için kurumsal hedefleri ve ilgili faaliyetleri iyi bilmeleri gerekir. Ayrıca, denetçilerin kurumda yapılan işleri ve olağanüstü durumlarda nelerin ters gidebileceği hakkında fikirleri de olması gerekir. Kurum içinde ve dışında yaşanabilecek gelişmelerin kurum faaliyetlerini nasıl etkileyeceği konusu değerlendirilmelidir. Denetçiler riskli alanları tespit ederken bu risklerin kurumu nasıl etkileyeceğini de belirlemelidirler.

Risk belirlemeye detaylı organizasyon şemasından başlanılabilir. Bazı birimler kurum faaliyetleri açısından daha önemlidir. Bu birimlerden başlanarak tüm birimler ve projeler için riskler belirlenmelidir. Risk belirleme faaliyetleri çok iyi anlamayı gerektiren uzun bir süreçtir. Bu süreci kısaltmak için denetçiler önemli gördükleri birimlerdeki bazı kişilerden kendi bölümündeki riskleri belirlemelerini isteyebilirler.

6.2.2.2.1.2. Risk Türleri ve Sonuçları

Sürekli risk değerlendirmesi yapabilmek için risk kategorilerini veya maruz kalınan riskleri belirlemek gerekir. Risk kategorileri riskleri belirleme ve değerlendirmede yardımcı olurken olası sorunların kurumu nasıl etkileyeceğini de anlamamızı sağlar.

Aşağıdaki tabloda bir kurumun karşılaşılabileceği riskler ana hatlarıyla verilmiştir. Risk belirleme aşamasında bu tablodaki riskler temel alınarak bölüm ve proje risklerine kadar inilebilir. Riskler belirlenirken tüm kurumu mu yoksa belli bir bölümü mü etkilediği, içsel mi yoksa çevresel nedenlerden mi kaynaklandığı, başka riskleri tetikleme olasılığı düşünülmelidir.

Tablo 3
Kurumsal Risk Türleri

Stratejik Riskler		
Dış Faktör Riskleri - Sektör riski - Ekonomi riski - Rakip riski - Yasalarda ve düzenlemelerde değişiklik riski - Müşteri ihtiyaçları ve istekleri riski	İç Faktör Riskleri - İtibar riski - Stratejik odaklanma riski - Ana firma destek riski - Patent ve marka koruma riski	
Operasyonel Riskler		
Süreç Riskleri - Tedarik zinciri riski - Müşteri memnuniyeti riski - Döngü süresi riski - Süreç uygulama riski	Uyumluluk Riskleri - Çevresel risk - Yasal risk - Politika ve yönetmelik riski - Dava riski	İnsan Riskleri - İnsan kaynakları riski - Çalışan devir hızı riski - Eğitim riski
Finansman Riskleri		
Hazine Riskleri - Faiz oranı riski - Döviz riski - Sermaye bulma riski	Kredi Riskleri - Kapasite riski - Teminat riski - Yoğunlaşma riski - Ödememe riski - Tasfiye riski	Menkul Kıymet Alım Satım Riskleri - Emtia fiyat riski - Süre (duration) riski - Ölçme riski
Bilgi Riskleri		
Finansal Riskler - Muhasebe standartları riski - Bütçeleme riski - Finansal raporlama riski - Vergilendirme riski - Yasal raporlama riski	Operasyonel Riskler - Fiyatlama riski - Performans ölçme riski - Çalışan güvenliği riski	Teknolojik Riskler - Bilgi erişim riski - İş devamlılığı riski - Kullanılabilirlik riski - Altyapı riski

Kaynak: Robert R. Moeller, Brink's Modern Internal Auditing. 7. Basım. A.B.D.: John Wiley & Sons, Inc., 2009, s.117.

6.2.2.2.1.3. Riske Maruz Kalmanın Sonuçları

Denetim kaynakları sınırsız olmadığı için belirlenen tüm risklerin denetlenmesi mümkün değildir. Bu nedenle başlıca risklere karşı alınan önlemler denetlenmelidir. Bu nedenle kurumsal riskler belirlendikten sonra risklerin etkilerini dikkate alarak önem sıralaması yapılmalıdır. Riskin kuruma verebileceği zararı tespit etmek riskleri önceliklendirmede önem taşır. Risklerin gerçekleşme olasılığı ve gerçekleştiğinde kuruma maliyeti saptanır.

Önem sıralaması yöneticilerin görüşlerini yansıtan anket çalışmasından karmaşık analiz tekniklerine kadar çok çeşitli yöntemlerle yapılabilir. Kurumsal öncelikler hangi risklerin ne ölçüde giderilmesi gerektiği konusunda denetçilere yol gösterir. Örneğin, bir riskin gerçekleşmesi durumunda kurumun para mı, itibar mı yoksa rekabet üstünlüğü mü kaybedeceği riskin kurum açısından önemini ve ayrılması gereken denetim kaynağını da belirler.

6.2.2.2.1.4. Risk Seviyesini Değerlendirmek

Denetçiler aşağıdaki risk faktörlerini değerlendirmelidirler:

- Hesabın büyüklüğü ve niteliği
- İşlem hacmi
- İşlemlerin karmaşıklığı ve değişkenliği
- Hesaba ilişkin yapılan açıklamalar ve verilen bilgiler
- İşlemlerin karmaşıklığı nedeniyle muhasebeleştirme ve raporlamada yaşanan zorluklar
- Üçüncü şahıslara ilişkin işlemlerin varlığı
- Önceki dönemlere göre önemli değişiklikler

Riski değerlendirmenin iki unsuru vardır: olasılık ve önem. Olasılık ilgili riskin gerçekleşme ölçüsünü, önem ise yaşanacak zararın etki derecesini gösterir. Belirlenmiş her risk için önem oranı (riskin gerçekleşmesi durumunda kuruma vereceği zarar) ve riskin gerçekleşme olasılığı tahmin edilir. Oranlar 0,01-0,99 arasında bir sayıdır. Önem oranı ile gerçekleşme olasılığı çarpıldığında risk puanını verir. Risk puanları büyükten küçüğe sıralandığında risk önem sıralaması da yapılmış olur. Risk değerlendirmesi kontrollerin ilgili riskleri ne derece hafiflettiğini de belirlemelidir.

6.2.2.2.1.5. Veri Toplamak ve Analiz Etmek

Risk deęerlendirmesinin son adımı önemli iş süreçleri ve riski yüksek alanlardan veri toplamak ve analiz etmektir. Riski belirlemek, deęerlendirmek ve etkisini azaltacak çalışmaları yapmak için kurumun her seviyesinden veri toplamak gerekir. Bu veriler belirlenen ölçütler karşısında test edilerek deęişen risk seviyeleri tespit edilir.

Sürekli risk deęerlendirmesi aşağıdaki sonuçları doğurur:

- Denetim planı güncellenir. Denetim planında deęişiklikler ve eklemeler yapılabilir.
- Belli bir konuda denetim yapılacaksa amacı ve kapsamı belirlenir.
- Yönetime dikkat edilmesi gereken konularda bilgi verilir.

6.2.3. Sürekli Denetim Modelini Oluşturmak

6.2.3.1. Test Kapsamını Belirlemek

Kontrollerin hangi detayda inceleneceęi belirlenir. Yönetimin yaptığı kontrollerin etkinlięi ve kurumsal yönetimin odaklandığı alanlar göz önüne alınarak denetimin ne derece detaylı yapılacağı saptanır. Yönetim kontrol ve risk deęerlendirmede etkin çalışmalar yapıyorsa bu çalışmaların sonucunda belirlenen seviyeler denetime temel teşkil edebilir. Ancak, yönetim bu konuda etkin deęilse denetçilerin risk ve kontrol seviyelerini belirlemek için daha detaylı bir çalışma yapması gerekir.

6.2.3.2. Bilgi Kaynaklarını Belirlemek

Kurumsal veri ham olarak elimizde bulunan, çoęu zaman yalnız başına bir anlam taşımayan ve işletme faaliyetleri sonucunda ortaya çıkan kayıtlar olarak tanımlanır. Bilgi ise verinin analiz edilip sınıflandırılarak karar verici için anlamlı ve kullanışlı hale gelmesidir. Kurumsal veritabanına yapılan kayıtlar, bu kayıtları kimlerin ne zaman yaptığına ilişkin log bilgisi, kayıt uzunluęu, tipi vb. alan bilgisinin yer aldığı meta data birer veridir. Ham halde bulunan bu verinin nasıl yorumlanacağı ve kullanılacağı denetçiye baęlıdır. Denetçi kurumsal planlama yazılımında bulunan veriyi kendi denetim modelinde nasıl kullanacağını belirler.

Denetimin gerekleşmesi için gerekli bilgi ve bu bilginin kaynakları belirlenir. Denetçi, denetimin nasıl yapılacağını değil denetimin kapsamını düşünerek ihtiyaç duyacağı bilgiyi belirlemelidir.

Denetimin hedefleri ihtiyaç duyulacak veriyi belirleyecektir. Örneğin, kurumun yaptığı anlaşmaların üzerinde yüksek tutarda fatura yazan satıcıları bulmak denetim hedeflerinden biri olsun. Veri kaynaklarını inceledikten sonra konuyla ilgili üç dosyanın tespit edildiğini varsayalım:

- Alım işlemlerinin bulunduğu Satınalma dosyası
- Alım yapılan satıcıların bulunduğu Satıcılar dosyası
- Fiyatlar ve ürünlerin satıcılar bazında listelendiği Ürünler dosyası

Fatura tutarı, olması gerekenden yüksek olan satıcıları saptamak için Satınalma dosyasındaki kayıtlar ile Ürünler dosyasındaki kayıtları karşılaştırmak gerekir. Bu nedenle ilgili kişi veya bölümden bu iki dosya istenmelidir. Satıcılar dosyası fazla ödeme yapılan satıcılar hakkında daha detaylı bilgi almak için istenebilir. Ancak, ele alınan denetim hedefi için gerekli değildir.

Sürekli denetim uygulamalarında bilgi sadece para cinsinden değildir. Her türlü kurumsal faaliyetle ilgili finansal, operasyonel veya uyuma ilişkin bilgi olabilir.

6.2.3.3. Denetim Kanıtlarını Belirlemek

Denetim raporu yayınlayabilmek için denetçi gözlemlerini ve önerilerini denetim kanıtları ile desteklemelidir. Bu nedenle denetime hazırlık aşamasında aşağıdaki konuları belirlemesi gerekir:

1. her bir sav için hangi kanıtlar gereklidir
2. her bir sav için hangi denetim yöntemi yeterli ve inandırıcı kanıtlar toplayabilir
3. ne kadar kanıt yeterlidir
4. yeterli ve inandırıcı kanıtlar toplayabilmek için en güvenilir ve etkin yol nedir

Yeterli denetim kanıtının elde edilebilmesi için aşağıdaki sorulara tatmin edici cevaplar verilebilmelidir:⁹³

1. Kayıtlar elektronik ortamda mevcut mudur?
2. Kayıt saklama yöntemi nedir?
3. Kayıtları koruma faaliyetleri nelerdir?
4. Denetim dönemi için kayıtlara ilişkin detaylı ve özet bilgi var mıdır?
5. Elektronik kayıtlar güvenilir midir?
6. Kayıtların bütünlüğünü sağlamak için şifreleme ve kimlik doğrulama işlemleri var mıdır?
7. Elektronik kanıtların güvenilirliğini sağlayabilecek derecede yeterli ve etkin bir iç kontrol yapısı var mıdır?
8. Finansal tablolardaki sayılar nereden gelmektedir?
9. Elektronik kayıtların başlangıç noktaları nelerdir?
10. İşlemin geçmişi var mıdır ve kapsamı nedir?
11. Elektronik kayıtlar ne zaman, nerede ve nasıl denetlenecek?
12. Denetim kanıtları müşterinin bilgisayar sisteminde denetlenebilir mi?
13. Denetçi elektronik kanıtları denetlemek için yeterli donanım ve yazılım kaynağına sahip midir?
14. Hangi denetim yazılım paketleri kullanılabilir?
15. Elektronik kanıtları denetlemek için hangi bilgisayar teknikleri kullanılabilir?

6.2.3.4. Denetimin Zamanlaması

Denetim uygulamaları çeşitli savları test ederler. Örneğin, belli bir malın veya borcun varlığı, iç kontrollerin güvenilirliği, ilgili kurallara ve düzenlemelere uygunluk gibi belli konuların gerçekleşip gerçekleşmediğini denetçiler incelerler. İncelenen konulara ilişkin kanıtlar sürekli denetim sistemlerinde bilgisayar ortamında elektronik formattadır.

Denetimin zamanlaması elektronik ortamda denetim kanıtlarını bulabilecek şekilde belirlenmelidir. Örneğin, bazı elektronik kanıtlar belli bir dönem sonra yok olabilirler veya değiştirilebilirler. Bu nedenle elektronik kanıtlar geçerliliğini yitirmeden denetimin zamanlaması planlanmalıdır.

⁹³ Rezaee, Elam, Sharbatoghlie, s. 156.

6.2.4. Veri Eriřimi

Veri eriřimi her denetim projesinin kritik bir blmdr. Gerekli veriye etkin bir řekilde ulařmak gerekir. Veri kaynaklarının ve teknolojilerinin ok deęiřik olması, veri eriřim yntemlerini de farklılařtırmaktadır.

Veri eriřimi iin sadece bilgi sistemini genel anlamda bilmek yeterli deęildir. Verinin yapısını, kaynak dosyanın hangi blmlerden oluřtuęu ve hangi bilgiyi barındırdıęının, ilgili dosyaların kimler tarafından yaratıldıęının ve nasıl ulařılabileceęinin deneti tarafından bilinmesi gerekir.

6.2.4.1. Veri Eriřim Yntemleri

Srekli denetim iin veriye elektronik ortamda eriřimin saęlanması gerekir. Eriřim yntemi denetimin amacına baęlı olarak seilir; ancak veri miktarı, bilgisayarlar arası veri trafięi gibi bilgi sisteminin teknik zellikleri de gz nne alınmalıdır.

Srekli denetimde veri eriřimi ařaęıdaki yntemlerin bazılarını birlikte kullanarak saęlanabilir:

- Srekli denetim yazılımı gml denetim modlleri kullanılarak kurumsal bilgi sisteminin iine yerleřtirilir. Denetim yazılımı kurumsal bilgi sisteminin bir parası olarak alıřır. Bylece direkt veri eriřimi saęlanır.
- Kurumsal bilgi sisteminin veri dosyalarına dıřardan eriřim saęlanır, denetimde kullanılacak veriler bu dosyalardan direkt olarak ekilip denetim yazılımının kullanımına hazırlanır. Bu yntemde denetim yazılımı kurumsal bilgi sisteminden baęımsız alıřır ve kurumsal bilgi sisteminin kullandıęı yazılımlar ve veritabanının raporlama ve sorgulama imkanları kullanılmaz.
- Detaylı analiz yapılmak zere kurumsal bilgi sistemi kullanılarak standart raporlar retilir. Bu durumda kurumsal bilgi sistemindeki uygulamalar kullanılarak analizler yapılır. Deneti var olan analiz modllerini kullanır.
- Kurumsal bilgi sisteminin veritabanı kullanılarak eřitli sorgulamalar yapılır. Deneti kurumun veritabanına direkt eriřim saęlar ve ilgili veritabanının sorgulama olanaklarını kullanır.

- Kurumsal bilgi sistemine verileri incelemek için bağlanılır. Bu yöntemde kullanıcı yetkilerine dikkat edilmesi gerekir. “Salt okunur” yetkisiyle bağlanması kayıtların yanlışlıkla değişmesini önleyecektir.

6.2.4.2. Verinin Yerini Belirlemek

Sürekli denetimin kurulabilmesi için doğru verinin elde edilmesi gerekir. İhtiyaç duyulacak veri ve uygulamalar tespit edilir, önem dereceleri belirlenir. Kullanılabilir verinin saptanmasında ilk adım hangi verinin kurumsal kaynak planlama yazılımında var olduğunun ve nerede tutulduğunun bulunmasıdır.

Veri kaynaklarını, dosya formatlarını ve özellikli dosyaların ve alanların içeriklerini gösteren bir doküman hazırlanması faydalı olacaktır. Bu doküman gelecek denetimler için de yararlı bir başvuru kaynağı olacaktır. Bu veri ve uygulamalara erişim hakkının elde edilmesi gerekir. Veriyi sağlayan tarafa bir talepte bulunulacaksa, hangi verilerin denetçiye açık olduğunun ve hangi formatta olduğunun bilinmesi gerekir. Denetçiler elektronik ortamda saklanan verileri bulabilmeli, toplayabilmeli, analiz edebilmeli, yorumlayabilmeli ve raporlayabilmelidirler. Toplanan bilgi somut, doğrulanabilir, amaca uygun ve sonuca ulaşmada faydalı olmalıdır. Elektronik ortamda yer alan bilginin kaynaklarının, kimlerin sahip olduğunun, ilgili programcının belirlenmesi ve iş süreçleri, sistemin kısa özeti gibi ilgili dokümantasyonun sağlanması gerekir. Denetçi verileri bulmak için kurumun ilgili elemanlarına, özellikle bilgi işlem bölümünde çalışanlara ihtiyaç duyar. Bilgi işlem bölümünde çalışanlar ile olumlu çalışma ilişkileri kurmak için, teknoloji dilini öğrenmek ve onları da denetimin gerekleri konusunda eğitmek gerekir. Veri talebinde bulunmadan önce ilgili elemanların ne tür bilgiye ihtiyaç duyacağının düşünülmesi ve sonra bu bilgiyi iletecek bir talep formu geliştirilmesi gerekir.

Denetçilerin kullanacakları bilgiyi elektronik ortama giren ve ilgili uygulamayı programlayan kişilerle iletişim içinde olması diğer bilgi kaynaklarının tespiti veya iş süreçlerini anlama gibi konularda fayda sağlayabilir. Aynı veri için birden fazla kaynak bulunuyorsa, farklı kaynaklardan elde edilen verileri karşılaştırmak riskleri ve kontrol zaaflarını tespit etmek için yararlıdır.

6.2.4.3. Veri Talebinde Bulunmak

Veri istenmesi kritik bir aşamadır. Veri erişimi ile ilgili sorunlar denetimin süresini önemli ölçüde uzatabilir. Bu nedenle hangi veriye ihtiyaç duyulduğunun, verinin kaynağının ve denetçiye nasıl teslim edileceğinin açıklıkla belirtilmesi gerekir. Denetçinin hangi veriye ihtiyacı olduğunu yazıyla bildirmesi veri temini sürecinde hata ve aksaklıkları azaltacaktır.

Talep yazısı ilgili kişinin veya bölümün veriyi temin etmesi için gerekli bütün bilgiyi içermelidir. Talep yazısı aşağıdaki bilgilerden oluşur:

- Talep tarihi.
- Verinin tutulduğu sistemin ismi.
- Dosya ismi, tablo ismi veya rapor ismi.
- Veri için zaman aralığı. Örneğin, başlangıç ve bitiş tarihleri dahil olmak üzere 1 Ocak 2012 ve 31 Aralık 2012 arasındaki veriler istenebilir.
- Bir filtre ölçütü. Örneğin, belli bir alandaki sadece artı değerleri istenebilir.
- Verinin teslim edileceği tarih.
- Verinin teslim edileceği dosya formatı.
- Verinin transfer edilmesi istenilen ortam.

Verinin tümünün alınıp alınmadığını teyit etmek için veriyi temin eden bölümden veriyle ilgili özet bir rapor istenebilir. Özet raporda aşağıdaki bilgiler bulunmalıdır:

- Kayıt düzeni bilgisi (alan isimleri, başlangıç pozisyonları, uzunlukları, veri tipleri ve formatlama ayrıntıları).
- Kontrol toplamları (kayıt sayısı, alan toplamları).
- Kaynak dosyadan yaklaşık 50 kaydın orijinal formatında yazdırılmış örneği. Örnek kayıtlar denetim yazılımına aktarılan kayıtlar ile karşılaştırarak denetimde kullanılacak tabloların düzenlemesinin doğruluğu kontrol edilebilir.

6.2.4.4. Verinin Denetim Yazılımına Aktarılması

Denetçinin kurumsal veriyi kurumsal kaynak planlama yazılımı dışında bir uygulamada analiz etmesi durumunda kaynak veriyi denetim yazılımına aktarması gerekir. Veri aktarımına başlamadan önce hangi verilerden yararlanılabileceği ve bunların hangi

formatta olduđunun tespit edilmesi gerekir. Denetlenecek dosyaların, farklı dosya tiplerinin ve bunlara erişim için gerekli teknolojilerin derinliğine kavranması gerekir.

İncelenen verinin teknik yapısına dikkat edilmesi gerekir. Özellikle farklı veritabanlarından gelen bilginin birleştirilmesi sırasında hatalar oluşabilir. Farklı veritabanlarında kayıtlar farklı formatlarda olabilir. Bu kayıtlar ortak bir formata göre birleştirilmelidir.

6.2.5. Veri Analizi

6.2.5.1. Veri Bütünlüğünü Sağlamak

İncelenen verinin tam ve doğru olması doğru değerlendirme yapabilmek için önemlidir. Denetçiler inceledikleri verinin tam ve doğru olduğuna emin olmalıdır. Bu nedenle analize başlamadan önce veri bütünlüğünün sağlandığından emin olunmalıdır.

Veri alındıktan sonra, bütünlüğünün test edilmesi gerekir. Veri bütünlüğünü test etmeden denetim yapılırsa sonuçlar eksik veya yanlış olabilir. Denetçi aldığı verilere karşı profesyonel bir şüphecilikle yaklaşmalıdır. Verinin bütünlüğünün test edilmesi, analiz sonuçlarının doğruluğuna olan güveni arttıracaktır.

Veri bütünlüğünü sağlamak için üzerinde analiz yapılacak veri dosyasının aşağıdaki özellikleri taşıması gerekir:

- Sadece denetçinin istediğı veriler yer almalıdır.
- Hesaplanmış alanların doğru değerler vermesi gerekir.
- Sayısal alanlarda yalnızca sayısal veriler bulunmalıdır.
- Kayıtlar mükerrer olmamalıdır.
- Sadece geçerli tarihler yer almalıdır.
- Verilerin ilgili alanlarda yer alması gerekir.
- Alan ilişkileri tutarlı ve mantıklı olmalıdır.

Veri dosyası bu standartları karşılamıyorsa, analiz sonuçları ve bu sonuçlara göre yapılan öneriler hatalı olacaktır. Bu nedenle analizlerin doğruluğı test edilmiş veriler üzerinde yapılması gerekir.

Veri bütünlüğü kurumsal verinin yaratılmasından denetçiye ulaşmasına kadar her aşamada farkında olunmadan veya bilerek bozulmuş olabilir. Hata kaynakları aşağıdaki gibidir:

- Veri girişi sırasında hatalar oluşabilir: Veri giren kişi yanlış veri girmiş olabilir, bazı işlemleri kaydetmemiş olabilir, gerekmeyen işlemleri girebilir, hatalı veya mevcut olmayan tarihler gibi geçersiz tarihler girmiş olabilir. Kurumsal kaynak planlama yazılımında bu gibi durumlar için geçerlilik kontrolü yoksa bu hatalar kaynak veride kalacaktır.
- Verinin işlenmesi sırasında hatalar oluşabilir: Kaynak verinin alan tanımlarında veya hesaplanan alanlarda tespit edilemeyen yanlışlar mevcut olabilir. Örneğin, faiz hesaplaması için yanlış bir ifade doğru olmayan faiz harcama değerlerine yol açacaktır. Bu sorunlar eksik, mükerrer veya geçersiz veriye neden olabilir.
- Veriyi denetim yazılımına çekme sürecinde hatalar oluşabilir: Veri talebini karşılayacak olan kişi veya bilgisayar sistemi verinin derlenmesindeki parametreleri yanlış yorumlamış olabilir. Bu ise eksik ya da fazla verilere neden olacaktır. Örneğin, denetçinin 1 Ocak 2012 ve 31 Aralık 2012 arasındaki bütün işlemleri istemiş olduğunu varsayalım. Ancak, veriler başlangıç ve bitiş tarihleri dahil edilmek yerine hariç tutularak derlenmiş olabilir. Bu durumda analiz edilecek dosyada bazı veriler eksik olacaktır.
- Veri dosyasının denetim yazılımının okuyabileceği formata dönüşümü sırasında hatalar oluşabilir: Kurumsal kaynak planlama yazılımı tarafından kullanılan dosya tipi denetçinin kullanacağı denetim yazılımı tarafından tanınmıyor olabilir. Bu durumda kaynak veriyi denetim yazılımının okuyabileceği bir formata dönüştürmek gerekir. Örneğin, IBM'in bazı bilgisayar sistemlerinde tutulan verilerin karakter seti EBCDIC'tir. Birçok yazılım bu karakter setini okuyamadığı için, veriler genellikle çoğu yazılım tarafından okunabilen ASCII'ye dönüştürülür. Dönüşüm süreci bazı veri tiplerinde hatalar oluşturabilir.
- Verinin yaratıldığı bilgi sisteminden başka bir ortama nakli veriyi bozabilir.
- Denetim yazılımına aktarılan veri dosyasında tanımlama hataları olabilir: Denetim yazılımında veriyi almak üzere yaratılan tablo düzeni gerektiği şekilde tanımlanmamış olabilir. Bu da alanlar ve veriler arasında uyumsuzluk yaratacaktır.

Veri bütünlüğünün doğrulanması için yapılabilecekler aşağıda sıralanmıştır:

- Tablo düzeni incelenerek veri tipleri ve alan tanımlamaları kontrol edilir.
- İstenilen bütün kayıtların alınıp alınmadığını, fazla kayıtların bulunup bulunmadığını ve sayısal alan toplamalarının doğru olup olmadığı kontrol edilir.
- Verilerin istenilen sınırlar içinde olup olmadığı kontrol edilir.
- Eksik ve mükerrer kayıtlar, olası diğer yanlışlar için testler yapılır.

6.2.5.2. Dijital Analizler

Veri bütünlüğü sağlandıktan sonra denetim hedeflerine ulaşmak için veri üzerinde dijital analizler yapılır. Testlerin uygulanacağı veri ve yapılacak analizler test kapsamında belirlendiği şekilde olmalıdır.

6.2.6. Sonuçları Değerlendirmek

Sürekli denetim testlerinin zamanlaması ve kapsamı belirlenirken sürekli denetimin amaçları, kurumun risk anlayışı, yönetimin risk izleme uygulamaları göz önüne alınmalıdır. İlk adımda risklerin önem sıralaması yapılır ve sürekli denetim uygulamaları en yüksek risk alanlarından başlayarak hayata geçirilir.

İkinci adım sürekli denetim uygulamalarının hangi sıklıkla çalıştırılacağıdır. Gerçek zamanlı olabildiği gibi belli dönemlerde de sürekli denetim uygulamaları çalıştırılabilir. Zamanlama riskin büyüklüğü ve yönetimin risk izleme görevini ne derece yaptığına bağlı olarak değişir. Kritik süreçlere ilişkin kayıtlar gerçek zamanlı analiz edilmelidir.

Yönetimin izleme görevini ne derece yaptığını tespit etmek için aşağıdaki unsurları değerlendirmek gerekir:

- Ele alınan iç kontrollerin tespiti
- Yönetim izleme sisteminin erişim güvenliği
- Yönetimin kontrollerde tespit edilen anomalileri giderme süresi
- Genel anlamda yapılan düzeltmeler
- Süreçler üzerinde yapılan önceki denetimlerin kayıtları
- Parametre ve seviye testlerinde yapılan değişikliklere ilişkin kayıtlar

Sürekli denetimin sonuçlarını inceleyerek sorunlu alanlar tespit edilir. Kontrol testlerini geçemeyen hareketler kontrol zaaflarının kanıtıdır. Süreçlerin veya hareketlerin birbirleriyle karşılaştırılması ile yapılan karşılaştırmalı analizler artan risk seviyelerini belirler.

Sürekli denetim ilk kurulduğunda hatalı olmayan birçok hareketin sıradışı durum olarak raporlanması normaldir. Zaman içinde test parametreleri düzeltilir.

Her sürecin farklı riskleri ve olağandışı durumları vardır. Tüm risklerin ve olağandışı durumların göz önüne alındığı bir sürekli denetim uygulamasını modellemek neredeyse imkansızdır. Her zaman değerlendirilmemiş bir unsur olacaktır. Bu nedenle bilgi sisteminden gelen her olağandışı durum işlemde hata veya hileye işaret etmez. Bunlardan bir bölümü geçerli işlem olmasına rağmen sürekli denetim uygulamasının “mükemmel” olmayışından kaynaklanan denetim sisteminin hatalarıdır. Yapılan düzeltmelerle denetim modeli geliştirilerek sistem mükemmel yakın bir işleyişe kavuşturulabilir. Ancak, sürecin getirdiği tüm olağandışı durumları denetim modeline koymaya çalışırken hatalı veya hileli işlemlerin sistem tarafından algılanmama durumuna çok dikkat edilmelidir. Sistem parametreleri gerçek olağandışı durumları sistemin fark etmesini engelleyici şekilde ayarlanmamalıdır. Olağandışı durumlar geçerli işlemler olarak kabul edildiğinde denetçiler sürekli denetim uygulamasında düzeltme yapılması gerektiğinin farkına varmayacaklardır. Bu nedenle sürekli denetim uygulamasındaki hata giderilmeyecek ve birçok olağandışı durum gözden kaçacaktır.

Denetim sonuçları önem sırasına göre ele alınmalıdır. Sonuçların detayları aşağıdaki unsurları açıklamalıdır:

- Denetim sonuçları
- Yapılması gerekenler
- Kimin ne zaman bilgilendirildiği
- Beklenen geribildirim tarihi

İlgili kişilerin sorunu gidermek için değişiklik yapmaları durumunda denetimin yeniden yapılması gerekir. Böylece kontrol zaaflarının giderilip giderilmediği veya risk seviyesinin düşürülüp düşürülmediği belirlenir.

Doğru kurgulanmış sürekli denetim uygulaması, yönetimin etkin kontrol yapısı oluşturup oluşturmadığını ve riski ne derece yönetebildiğini gösterir. Ancak, sürekli denetim değişikliklere cevap verebilecek şekilde esnek olmalıdır. Sürekli denetim uygulamaları başlatıldıktan sonra uzun sürelerle kendi başlarına bırakılmaz. Denetçiler sürekli denetim programının etkin ve verimli çalıştığını belli aralıklarla kontrol etmelidirler. Yeni risklerin baş göstermesiyle birlikte yeni kontroller eklenebilir veya bazıları geçerliliğini kaybettiği için kaldırılabilir. Kontrol testlerinde ve parametrelerin verilerinde değişiklik yapılması gerekebilir. Sürekli denetim sonuçları kurumsal risk yönetimi, performans ölçümü ve izleme gibi diğer yönetim faaliyetlerini desteklemelidir.

Sürekli denetim uygulamasından elde edilen sonuçlar sorunların kökenini bulmak ve bu temel sorunları gidermek için kullanılmalıdır. Bu köklü sorunları çözmenin maliyeti vardır. Zaman, emek, para, yönetsel değişiklik, yüzleşme problemi gibi hem maddi hem de psikolojik maliyetler söz konusudur. Sorunun temeline inmek yerine bunların etkilerini gidermeye çalışan bir tutum içine girmek sorunu çözmek değildir. Asıl sorun aynı kaldıkça bu sorundan doğan riskler de devam edecektir. Başka bir gün başka bir olağandışı durumla karşılaşılacaktır. Sürekli denetim uygulamasının sonuçları doğru adımlar atmak için kullanılmalıdır. Denetçiler asıl sorunu çözemeye yönelik görüş bildirmeli ve asıl sorunun çözümüne yönelik yapılan faaliyetleri takip etmelidirler.

6.2.7. Raporlama

Sürekli denetim raporlaması için iki temel seçenek vardır: resmi raporlama ve olağandışı durum notu. Resmi raporlama sürekli denetim uygulamasının faaliyetlerini detaylı anlatan tam denetim raporu yapısındadır. Olağandışı durum notu sürekli denetim faaliyetlerini özetleyen bir çalışma kâğıdını andırır. Sürekli denetim uygulamasında kullanılan rapor tipi bu iki rapor tipinin karması şeklinde düzenlenebilir.

6.2.7.1. Resmi Raporlama

Sürekli denetim uygulaması tarafından tamamlanan faaliyetleri belgelemek için kullanılır. Denetimin amacı, kontrol ortamı, test edilen kontrollerin etkinliği, olağandışı durumlar detaylı şekilde açıklanır. Elektronik ortamda otomatik olarak oluşturulması karmaşık modelleme gerektirir.

Resmi raporlamada en azından aşağıdaki unsurların yer alması gerekir:

- Genel görüş: Test edilen kontrollerin etkinliğinin değerlendirildiği özet açıklamadır. Beklenen denetçi görüşünün sunulduğu bölümdür. En çok okunan bölüm olma özelliğine sahiptir. Bu nedenle raporun başında yer alması uygun olur. Özellikle risk derecelendirmesinde önemli yer tutan konulara ilişkin kontrollerin değerlendirmesi genel görüşte yer almalıdır.
- Denetimin amaçları ve amaçların derecelendirilmesi: Denetimin amacı ilgili denetim faaliyetinin gerçekleşme nedenini açıklar. Denetimin birden fazla amacı olabilir. Denetimin amacı incelenen iş sürecinin hedefine ve risklerine bağlıdır. Süreç hakkında yeterli bilgiye sahip olmadan ilgili denetimin amacını belirlemek ve uygun testleri yapmak olası değildir. Denetimin yapıma amaçları ilgili riskleri ölçüsünde derecelendirilir. Bu derecelendirmenin genel görüşte belirtilen derecelendirme ile uyumlu olması gerekir. Bu bölümde test edilen amaçlar sıralanır. Test sonuçlarına göre iş biriminin başarı derecesi ilgili amacın karşısına yazılır.
- Olağandışı durumlar: Testler sırasında belirlenen olağandışı işlemler ve durumlar detaylı şekilde bu bölümde açıklanır. Olağandışı durumlar denetim amaçları ve kurumsal riskler ile ilişkilendirilmelidir. Olağandışı durumlar ve riskleri konusu raporu okuyan kişilerin yorumuna açık bırakılmadan net bir biçimde irdelenmelidir. Bu durumların nedenleri, kurum üzerindeki etkileri ve denetçilerin gelecekte yapılmasını önerdikleri konular belirtilir.
- İncelenen iş sürecinin tanımlanması: Denetimi yapılan iş süreci ve ilgili iş biriminin faaliyetlerini anlatan bölümdür. Bu bölümde denetim amaçları ile ilgili iş biriminin yaptığı çalışmalara yer verilir.

6.2.7.2. Olağandışı Durum Notu

Olağandışı durum notu sürekli denetim testlerinin sonuçlarını detaylı olarak gösteren bilgilendirme notudur. Resmi raporun olağandışı durumları açıkladığı bölüme göre daha detaylıdır. Kontrol yapısının etkinliğine ilişkin bilgi içermez. Bu notta bir denetim amacı, yapılan testler ve tespit edilen tutarsızlıklar listelenir.

Testler sonucunda kurumsal standartlara uymayan olağandışı durumlar maddeler halinde sıralanır. Bulgular ham haldedir. Farklılıkların nedenleri, etkileri, denetçilerin önerileri yer almaz.

Resmi rapora göre daha hızlı ve kolay hazırlanır. Olağandışı durum notunu hazırlamak için sürekli denetim uygulamasının sonuçlarını almak yeterlidir. Herhangi bir yorum veya neden sonuç ilişkisi yer almadığı için elektronik ortamda otomatik olarak oluşturmak basittir.

6.3. SÜREKLİ DENETİM UYGULAMALARINI GELİŞTİRİRKEN KARŞILAŞILAN ZORLUKLAR

Sürekli denetimin kabul edilen birçok faydasına rağmen sınırlı kullanım alanı bulması üstesinden gelinmesi gereken bazı sorunlar olduğunu göstermektedir. Sürekli denetim modelini geliştirmek uygulamanın yalnızca bir parçasıdır. Sürekli denetim uygulamalarında başarılı olmak için aşağıdaki konulara da eğilmek gerekir.⁹⁴

- Sürekli denetim kavramı ve kurulmasının denetim komitesi ve üst yönetim tarafından benimsenmesi
- Farklı bilgisayar sistemlerindeki verileri almak, üzerinde çalışmak ve analiz etmek için gerekli teknik bilginin öğrenilmesi
- Denetim ekibinde veri analiz tekniklerini uygulayabilecek ve geliştirebilecek kişilerin olması
- Sürekli izleme sisteminin yönetim tarafından kurulmasını desteklemek
- Raporlama ve geribildirim sistemi kurarak denetim sonuçlarının doğru şekilde kullanılmasını sağlamak

İç Denetçiler Enstitüsü (Institute of Internal Auditors-IIA) 2010 yılında yaptığı bir anket çalışmasında sürekli denetim modelinin kullanılmama nedenlerini araştırmıştır. Ankete 127 kişi katılmıştır. Bu çalışmanın sonuçları aşağıdaki tabloda açıklanmıştır.

⁹⁴ David Coderre, “Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment”, Global Technology Audit Guide, s. 2.

Tablo 4
Sürekli Denetim Modelinin Uygulanmama Nedenleri

Cevap	Oran (%)	Kişi Sayısı
Yetersiz kaynaklar	48.8	62
Teknik beceri yetersizliği	21.3	27
Yönetimin ilgisizliği	20.5	26
Çok karmaşık olması	5.5	7
Yüksek ön maliyet	14.2	18
Değer yaratmaması	2.4	3
Süreci kurmak için çok zamana ihtiyaç olması	27.6	35
Veri ve sistemlere erişim güçlüğü	24.4	31
Bilgi sistem altyapısının karmaşıklığı	16.5	21
Bağımsızlık ve tarafsızlıktan ödün vermek	3.1	4
Diğer	25.2	32

Kaynak: Tammy Whitehouse. “Whatever Happened to Continuous Auditing?”, Compliance Week. 30 Kasım 2010. www.complianceweek.com (Ocak 2011).

6.3.1. Karşılaşılan Sorunlar

Sürekli denetim uygulamalarını kurabilmek için aşağıda açıklanan zorlukların üstesinden gelinmesi gerekir.

6.3.1.1. Güvenli Sistem

Denetlenecek bilginin güvenli bir sistemde oluşmuş olması gerekir. Sürekli denetim sistemi manipülasyona açık olmamalı ve sonuçları farklı kişilerce farklı yorumlanmayacak şekilde çıkmalıdır. Sistem güvenliği önemlidir.

Sürekli denetim ile ilgili güvenlik sorunları:

- Gizlilik
- Denetim veya izleme sonuçlarına erişim
- Test parametrelerinin değerleri ve yapılan değişikliklerin takibi
- Sürekli denetim sonucunda hile de ortaya çıkartılabileceği için test parametreleri ve denetim sonuçlarına yetkilendirilmemiş kişilerin erişiminin engellenmesi gerekir.

6.3.1.2. Zamanlama

Zaman kavramının denetçiler açısından önemli bir yeri vardır. Belli bir an tekrar yaratılamaz, o ana geri gidilemez veya o an durdurulamaz. Zaman insanın kontrol edemediği ve değiştiremediği bir şey olduğu için zamanla ilgili testler güvenilir kabul edilmektedir.⁹⁵ Sürekli denetim ortamında kullanılan veri dijital ortamda yaratılmış ve saklanmıştır. Günümüz teknolojisinde veriyi başka bir zamanda yaratılmış, değiştirilmiş veya okunmuş göstermek mümkündür. Bu nedenle denetimde yapılacak testlerde tarih önem taşıyorsa ilgili tarihin değiştirilmediğinden emin olunması gerekmektedir.

6.3.1.3. Verinin Saklanması

Elektronik ortamda verinin değiştirilmesi kolay olduğundan denetimi yapılacak kayıtların değiştirilmediğinden emin olunması başlı başına bir sorundur. Kurumlar elektronik ortamda verinin saklanmasına ilişkin bazı kurallar uygulamaktadırlar. Sisteme yazmayı engelleme veya silmeyi engelleme gibi önlemler yaygın olarak uygulanan çözümlerdir. Sistemin tuttuğu verinin ilk kayıt tarihi ve sonraki değişikliklere ilişkin bilgiler genelde kayıtlar üzerinde oynanmadığını ispat etmek için kullanılırlar. Ancak, sistemin kayıtlarla ilgili tuttuğu bu bilgi yeterli güvenceyi vermemektedir. Sistem kullanıcılarının değiştiremeyecekleri unsurlar sistem sahibi tarafından bizzat değiştirilebilir veya yok edilebilirler. Örneğin, kurum çalışanları sistem kayıtları üzerinde oynama yapamayabilir, ancak üst düzey yöneticilerin isteğiyle sistem yöneticileri değişiklikler yapabilirler.

Bazı veri saklama sistemleri silme ve değişiklik yapma işlemlerine ait dijital denetim kanıtları bırakmaktadırlar. Bu tür sistemlerin kullanılması durumunda denetçiler kayıtlarda değişiklik olmadığına dair tam güvence verebilirler.

Elektronik veride değişiklik yapılmadığına dair tam güvence sağlamak için bazı teknolojiler kullanılabilir. Aşağıda bu teknolojilerin bazıları yer almaktadır:⁹⁶

- Güvenli Dijital Denetim Kanıtları: Verinin değiştirilmediğini doğrular. Kayıtların değiştirilmesi, silinmesi veya eklenmesi durumunda denetim başarısız olur, ancak

⁹⁵ Steven W. Teppler. "Digital Data And The Meaning Of Audit", The CPA Journal. (Şubat 2003).

⁹⁶ Randal Burns ve Zachary Peterson. "Security Constructs for Regulatory-Compliant Storage", Communications Of The ACM 53. 1 (Ocak 2010): 126-130.

orijinal içerik belirlenemez. Bu teknolojiyi uygulamak için verinin bir parçasının şifrelenmiş kimlik kanıtlama kodundan oluşması gerekir. Bu kod yardımı ile verinin tam ve sağlam olduğu anlaşılır. Ancak, veride bir değişiklik yapıldıysa yine bu kod ile değişiklik yapıldığı ve bu değişikliği yapan kullanıcının bilgilerine ulaşılır.

- **Güvenli Silme:** Bir kayıt ilk defa sisteme girildiğinde birbirine bitişik veri blokları olarak sabit sürücüde yerini alır. Değişiklik yapıldığında değişen veri bloğu sabit sürücüde farklı bir yere kaydedilir ve diğer ilişkide olduğu veri blokları ile yan yana durmaz. Bir şifreleme ile bir veri bloğu silindiği anda ilişkide olduğu tüm veri bloklarını silmek ve topluca başka bir yere kopyalamak mümkündür. Buna güvenli silme denir. Ancak, yeniden yazma sırasında tüm veri bloklarının sürümü değişeceği ve eski sürüme ulaşılma imkanı kalmayacağı için kayıtların değişikliğe uğradığı anlaşılabacaktır.
- **Kimlik Doğrulama Şifrelemesi:** Kişisel veya hassas bilginin yetkisiz kişilerce erişimine engel olunması gerekir. Genel uygulama bu bilginin şifrelenerek saklanmasıdır. Ancak, günümüz teknolojisinde şifrenin kırılması veya bilginin bir bölümünün değiştirilmesi mümkündür. Bu nedenle yalnız şifreleme bilginin tam ve doğru olduğunu göstermez. Her okuma işleminde kimlik bilgisi üretilmeli ve her yazma işleminde kimlik bilgisi doğrulanmalıdır. Bunu sağlamak için kimlik doğrulama şifrelemesi kullanılabilir. Bu teknolojiye her veri bloğu özgün kimlik bilgisine sahiptir ve kendi kimlik bilgisi ile birlikte şifrelenir. Bir veri bloğunda değişiklik yapılması durumunda kimlik bilgisi değişecek ve ilişkide bulunduğu diğer veri bloklarındaki kimlik bilgileri ile uyumlayacaktır. Böylece veri bloğunun değişikliğe uğradığı tespit edilir.

6.3.1.4. Sistem Verimliliği

Kullanılmakta olan bilgi sistemine sürekli denetime ilişkin kontroller eklemek bilgisayar sistemini yavaşlatacaktır. Kullanıcı hangi amaçla bu bilgisayarı kullanıyor olursa olsa bilgisayarın yanıt süresi uzayacaktır. Yanıt süreleri uzadıkça verim düşecektir. Uzun yanıt süreleri sistemi tamamıyla kullanım dışı bırakabilir.

Murthy bir e-ticaret uygulamasına üç tip kontrol ekleyerek sistem verimliliğini ölçmüş. İlgili uygulamada sistem verimliliğini aşağıdaki gibi tespit etmiştir:⁹⁷

- Yapılmakta olan işlem bilgisi ve bir veritabanından alınan bilginin karşılaştırması: katlanılabilir bir sistem yükü getiriyor.
- Yapılmakta olan işlem bilgisi ile birçok veritabanından elde edilen bilginin karşılaştırması: sadece sistemin yoğun olduğu dönemlerde sisteme zarar verecek ölçüde yavaşlatıyor.
- Yapılmakta olan işleme ilişkin bilginin veritabanındaki ilgili bilgiye ait ortalama, toplam, minimum ve maksimum değerlerle karşılaştırılması: her zaman sistemin çok yavaşlamasına neden oluyor ve sistem verimliliğini olumsuz etkiliyor.

6.3.1.5. Veri Standardizasyonu

Bilgi sistemine girilen veri standart olmalıdır. Standart olmayan verinin test edilmeden önce denetçi tarafından temizlenmesi gerekir. Bu işlem otomasyondan elde edilecek verimin düşmesine yol açar.

6.3.1.6. Otomasyon

Sürekli denetim süreci yüksek otomasyona sahip olmalı ve denetlenen ile denetçinin sistemi arasında etkin bir bağ kurulmalıdır. Denetim sistemimi Siemens uygulamasında olduğu gibi kurumsal kaynak planlama sisteminin üzerine inşa edilebilir. Ancak birçok kurum bilgi teknolojilerinde homojen bir yapıya sahip değildir. ACL 2006 anketi, ankete katılan 858 kurumun %58'inde bölünmüş veri yapısının çok önemli sorunlar yarattığını tespit etmiştir.⁹⁸

6.3.1.7. Raporlama

Sürekli denetim raporlarının doğru ve anlaşılabilir olması, belli aralıklarla ve zamanında hazır olması gerekir.

⁹⁷ Baksa ve Turoff, s.6.

⁹⁸ Baksa ve Turoff, s.3.

6.3.1.8. Bilgi Yklenmesi

Srekli denetim sistemleri incelenmesi gereken bilgiyi arttırabilir. Belli bir zaman diliminde denetilerin inceleyebileceğinden fazla bilginin deęerlendirilmesi gerektiğinde buna bilgi yklenmesi denir. Bilgi yklenmesini azaltacak teknikler kullanılabilir. Karar destek sistemleri, olasılıkları sınırlandırmak iin dijital ajanlar, veri grselleřtirme programları, bilgi kalitesini lme programları, veriyi filtreleme, birleřtirme ve kategorilere ayırmak, olaęandışı olayların raporlanmasına iliřkin teknikler bilgi yklemesini azaltmak iin kullanılabilir.

6.3.1.9. Teknolojik Bilgi

Denetilerin kullanılan teknolojik altyapı konusunda yeterli bilgiye sahip olmalıdır.

6.3.1.10. Sistemin Benimsenmesi

Srekli denetim sistemlerinin benimsenmesi beklenenden daha yavaş olmaktadır. Bu sistemlerin kullanıcılar tarafından kabul grmesi o kurumda bu konudaki alıřmaların devam etmesi, kalıcı ve etkin olması aısından nemlidir.

Venkatesh'in Teknolojinin Kabul ve Kullanımı Teorisi (Unified Theory of Acceptance and Use of Technology, UTAUT) srekli denetim sistemlerinin kabul grme potansiyelini belirlemede kullanılabilir.⁹⁹ Bu teoride kullanıcı davranıřlarını belirleyen drt ana unsur vardır:

- Verim beklentisi (performance expectancy): sistemi kullanmanın kiřinin iřinde verimi arttıracığına olan inancı.
- aba sarf etme beklentisi (effort expectancy): kiřinin sistemi ğrenmek ve kullanmak iin ne kadar aba sarf etmesi gerektiğine dair beklentisi.
- Sosyal etki (social influence): kiřinin nemli veya gl kiřilerin sistemin kullanılmasına verdikleri nemi deęerlendirme derecesi.
- Kolaylařtırıcı unsurlar (facilitating conditions): kiřinin kurumsal ve teknik altyapının sistemin kullanımını destekleyip desteklemediğini dřnmesi.

Cinsiyet, yař, istek ve tecrbenin bu drt unsur zerinde direk etkisi vardır.

⁹⁹ Baksa ve Turoff, s.5.

Venkatesh ve arkadaşlarının 2003 yılında yayınladığı çalışmada Teknolojinin Kabulü ve Kullanımı Teorisi'ne göre yeni bir sürekli denetim sisteminin kullanımına karşı duyulacak istek kullanıcının sürekli denetim sisteminin üst yönetim tarafından desteklendiği, kullanımının kolay olduğu, kurumsal ve teknik altyapının kullanımı desteklediği, işinde verimi arttıracığına inandığı durumda en üst düzeye ulaşacağı belirtilmiştir.

Curtis'in 2009 yılında yayınladığı çalışma Venkatesh'in Teknolojinin Kabulü ve Kullanımı Teorisi'ni destekler niteliktedir. Muhasebeciler üzerinde yapılan bu çalışmada kullanımı kolay, karmaşık olmayan modeller ile kurulmuş ve işlerinde somut fayda sağlayan sürekli denetim sistemlerini kullanmaya istekli olduklarını göstermiştir. 1996 yılında Fischer'in muhasebe firmaları üzerinde yaptığı araştırma bu firmalarda çalışan muhasebecilerin daha etkin ancak daha karmaşık denetim uygulamaları kendilerine sunulursa eskiden beri uygulamakta oldukları denetim süreçlerini kullanmayı tercih edeceklerini tespit etmiştir. Hall ve Khan'ın 2003 yılında yaptığı çalışma ise kullanıcıların yeni bilgi ve beceri öğrenmesini gerektiren buluşların uygulanmasının daha fazla zaman aldığını göstermektedir.

Bailey James 1983 yılında bir bilgi sisteminden sağlanacak tatmini beş sistem özelliği ile açıklar:¹⁰⁰

- Doğruluk (accuracy): sistem çıktılarının doğruluğu
- Güvenilirlik (reliability): sistem çıktılarının tutarlılığı ve güvenilirliği
- Zamanlılık (timeliness): sistem çıktılarından sağlanan bilginin kullanıcıya doğru zamanda ulaşması
- Uygunluk (relevance): kullanıcının beklentilerini sistemin karşılaması
- Sisteme duyulan güven (confidence in the system): kullanıcının sisteme karşı duyduğu güven

Bu çalışma sürekli denetim sisteminin yukarıdaki özelliklere ne ölçüde sahipse o derece benimseneceğini ortaya koymaktadır.

¹⁰⁰ Baksa ve Turoff, s.5.

6.3.1.11. Maliyet

Maliyet algısı sürekli denetim sistemlerinin kurulmasına yönelik yönetici desteğini azaltmaktadır. Economist dergisinin Eylül 2008 sayısında yayınladığı üst düzey yöneticiler arasında yaptığı ankette yöneticilerin sürekli denetim sisteminin kurulmasında en büyük engelin %48 ile maliyet olduğuna inandıkları tespit edilmiştir. Karmaşık iş süreçlerinin modellenmesini engel olarak gören yöneticilerin oranı maliyeti ön plana çıkartanların yarısından daha azdır.¹⁰¹

Denetim süreçlerinin otomasyonu ile olabilecek kayıpların önlenmesi, denetim maliyeti gibi bazı unsurlar ölçülebilir. Ancak, sürekli denetimden kurumun sağlayacağı tüm faydayı ölçmek mümkün değildir. Risk yönetimine sağladığı yarar, daha iyi karar verme olanağı, daha az uygunluk sorunlarının yaşanması, hile riskini azaltması gibi ölçülemeyen faydaları da vardır. Bu nedenle sürekli denetimin fayda maliyet analizini yapmak kolay değildir.

Fayda maliyet analizi ile sürekli denetim sisteminin kurulmasına karar verecek yöneticiler için bir çözüm sürekli denetim uygulamasının kapsamını sınırlı tutmaktır. Örneğin, Alles (2006) kolaylıkla otomasyonu yapılabilecek denetim süreçlerinin modellenmesi ve bunlar için sürekli denetim sisteminin geliştirilmesi, maliyeti yüksek veya modellenmesi mümkün olmayan denetim süreçlerinin ise denetçiler tarafından geleneksel yöntemle yapılmasını önermiştir. Sürekli denetimin olağandışı durumları tespit aşamasının otomasyonu için geliştirilecek algoritmalar, olağandışı durumlarda atılması gereken durumlara ilişkin karar sisteminin otomasyonundan daha kolay ve daha az maliyetli görülmektedir.

6.3.1.12. İşlemlerin Tamamı Üzerinde Denetim Yapılamaması

Sürekli denetim tanımı gereği işlemlerin gerçek zamanlı veya gerçekleşme anına mümkün olduğunca yakın bir sürede denetiminin yapılmasını gerektirir. Ancak, bazı kurumlarda henüz tüm işlemlerin gerçek zamanlı denetimi teknik imkansızlıklar veya maliyetin çok yüksek olması nedeniyle yapılamamaktadır.

¹⁰¹ Baksa ve Turoff, s.4.

Bu kurumlarda sürekli denetim sistemlerinin kurulabilmesi için tüm işlemlerin değil belli sayıda işlemin denetlenmesi fikri ortaya çıkmıştır. Bu amaçla üç strateji geliştirilmiştir: sayma stratejisi, dönemli strateji ve karma strateji.¹⁰²

- Sayma stratejisi (counting strategy): Her n sayıdaki işlemten sonraki işlemin denetlenmesidir. Buradaki kritik karar n sayısını bulmaktır. N büyük olduğunda hatalı işlemlerin fark edilmeme olasılığı artar. N küçüldükçe denetim maliyeti yükselir.
- Dönemli strateji (periodic strategy): Bu stratejide işlem sayısı değil zaman esas alınır. Denetim başladıktan bir süre sonra ara verilir ve belli bir süre gerçekleştikten sonra tekrar başlar. Denetim dönemleri arasında bir denetim yapılmayan süre vardır. Denetim yapılmayan sürenin uzun olması hatalı işlemlerin fark edilmeme riskinin artmasına, kısa olması da maliyetlerin artmasına yol açar.
- Karma strateji (hybrid strategy): Sayma ve dönemli stratejilerin birlikte kullanılmasıdır.

Bu stratejilerin hangisinin maliyetine oranla daha etkin olduğu üzerinde araştırmalar devam etmektedir. Ancak, hangi strateji seçilirse seçilsin işlemlerin tamamı üzerinde denetim yapılmaması hata payını arttıracak ve finansal raporların güvenilirliğini azaltacaktır.

6.3.2. Karşılaşılan Sorunları Gidermek İçin Yapılması Gerekenler

Sürekli denetim uygulamalarını geliştirirken karşılaşılan sorunları gidermek için denetçilerin yapmaları gerekenler:

- İlgili verilere zamanında ulaşmak.
- Kurum içinde kullanılan farklı bilgi sistemleri varsa verileri bu sistemlerden toplayıp kullanılabilir duruma getirmek.
- Sistem performansını düşürmeden büyük miktarda veriyi analiz edebilmek.
- Uygun analizler geliştirmek, riskleri ve önemli kontrol noktalarını belirlemek için iş süreçlerini anlamak.
- Sürekli denetim testlerini ve analizlerini yapmak için en etkin veriyi ve kontrol noktalarını belirlemek.
- Önemli kontrol noktalarını ve riskleri kapsamlı biçimde test ve analiz etmek, sonuçları zamanında raporlamak.

¹⁰² Jagdish Pathak, Ben Chaouch ve Ram S. Sriram. “Minimizing cost of continuous audit: Counting and time dependent strategies”, Journal of Accounting and Public Policy. 24 (2005): 65.

- Olağandışı kayıtları veya süreci araştırırken yapılan testleri ve analizleri anlamak.
- Riskleri sayısal veri halinde toplamak.
- Sürekli denetimde kullanılan değişkenleri izlemek ve düzeltmek, sürekli denetim sistemini yönetilebilir sonuçlar verecek şekilde ayarlamak.
- Yapılan çalışmanın maliyeti ve harcanan çaba ile çalışmadan sağlanan faydayı dengelemek.
- Yapılacak işleri önceliklendirmek.
- Sistemin ikaz ettiği konulara eğilmek.
- Sürekli denetim sisteminin güvenliğini sağlayarak yapılan analizlerin veya değişkenlerin yetkisiz kişilerce değiştirilmesini önlemek.

7. SÜREKLİ DENETİMDE KULLANILAN DİJİTAL ANALİZ TEKNİKLERİ

Denetçi tarafsız görüş bildirmek için denetime konu olan veriyi çeşitli analiz teknikleri ile incelemek zorundadır. Analiz teknikleri genellikle denetimin üç aşamasında kullanılır:¹⁰³

- Planlama aşaması: Planlama aşamasında yapılan analizler denetçiye yol gösteren analizlerdir. Denetim sırasında yapılacak testler, denetimin zamanlaması, dikkat edilmesi gereken konular bu aşamada yapılan analizler sonucunda belirlenir.
- Test aşaması: Bu aşamada yapılan analizler hesap toplamaları veya bazı tür işlemlerin maddi doğruluk testleridir.
- Sonuç veya gözden geçirme aşaması: Denetçi görüşünü bildirmeden son kez kanıtları yeniden değerlendirir. Bu aşamada analiz tekniklerini kullanarak savlarını gözden geçirir.

Dijital analiz tekniklerinin sürekli denetimde kullanılması ile işlemleri gerçekleştikleri anda denetlemek, olağandışı durumlarda ilgili kişileri uyarmak, birçok farklı işlemi aynı anda değerlendirerek karar vermek ve düşük maliyetle testleri tekrarlayabilmek mümkün olmaktadır.

Gerçek zamanlı muhasebe sisteminin güvenilir ve doğru finansal bilgi ürettiğini onaylayabilmek için, işlemlerin maddi doğruluk testlerinin ve kontrollerin testlerinin eşzamanlı yapılması gerekir. Dijital ortamda işlemler ve kontrolleri inceleyen çeşitli araç ve teknikler vardır. Bunlar paket program olarak satın alınabilir veya denetçi tarafından geliştirilebilir. Bu araç ve tekniklere topluca Bilgisayar Destekli Denetim Araç ve Teknikleri (Computer Aided Audit Tools and Techniques, CAATT's) adı verilir.

1987 yılında kurulan ACL Services Ltd. denetçiler için ACL (Audit Command Language) adlı bir program geliştirir. Bu programın modülleri sürekli denetimde kullanılan ilk dijital analiz teknikleri olarak kabul edilir. Bu teknikler Bilgisayar Destekli Denetim Araç ve Teknikleri (Computer Aided Audit Tools and Techniques, CAATT's) diye anılmaya başlanır.

¹⁰³ Nick A. Dauber ve diğerleri. The Complete Guide To Auditing Standards And Other Professional Standards For Accountants. A.B.D.: John Wiley & Sons, Inc., 2008:141.

Ancak, günümüzde akademisyenler bu program dışında kalan dijital analiz tekniklerini de CAATT's kavramı içine almaktadırlar.

Sürekli denetimde Bilgisayar Destekli Denetim Araç ve Teknikleri (Computer Aided Audit Tools and Techniques, CAATT's) gerçek zamanlı sistemlerde denetçi olmadan veri üzerinde inceleme yapmak amacıyla kullanılan analiz yöntemleri ve diğer denetim testlerini tanımlamak için kullanılır.¹⁰⁴

Sürekli denetimde analizler bilgisayar tarafından otomatik olarak yapılır. Bu analizler işlem detaylarını (fatura tarihi, satıcı adı vs.) veya hesap toplamalarını (her satıcıya yapılan toplam ödeme) veri olarak alır.

Sürekli denetimde kullanılan analiz teknikleri istatistik, makine öğrenimi¹⁰⁵ (machine learning) ve veri madenciliği¹⁰⁶ (data mining) alanlarından gelir. Temel veri analiz teknikleri regresyon, sınıflama (classification), ilişkilendirme (association) ve kümelemedir (clustering).¹⁰⁷ Bu analizlerde geçmiş verinin gelecekteki veriye benzeyeceği varsayımı vardır.

Veri analizleri genellikle işlemlere uygulanır; iç kontrollerin izlenmesi için kullanılmaz. Kontrollerin izlenmesi “uygun” veya “uygun değil” şeklinde bir önermeye dayanır. Ancak, analizler iç kontrol ihlal olasılığı yüksek olağandışı durumların tespitinde kullanılabilir. Veri analizleri işlemlere uygulandığında ilgili işlemin nitelikleri (fatura tarihi, satıcı, sipariş kalemleri vs.) dikkate alınır. Bu nitelikler ele alınarak işlemin “normal” olup olmadığı değerlendirilir.

Dijital analiz tekniklerinin uygulama alanları aşağıdaki gibidir:

1. İşlemlerin analizinde kullanılan araç ve teknikler (tools and techniques for analysing transactions): Hile ve hataları ortaya çıkartmak ve denetim koşulunu yerine getirmek için işlemlerin doğru olduğunun araştırılması gerekir. Bu nedenle işlemler üzerinde maddi doğruluk testlerinin yapılması gerekir.

¹⁰⁴ Ryan A. Teeter, Michael G. Alles, Miklos A. Vasarhelyi. “Remote Audit: A Research Framework”. Eylül 2010. <http://www.raw.rutgers.edu> (18 Şubat 2011).

¹⁰⁵ Makine öğrenimi yapay zekanın bir koludur. Bilgisayarların veritabanından veya sensörler aracılığıyla edindiği bilgiyi değerlendirip kendi kendine öğrenmesi ve karar alabilmesi için algoritmalar geliştiren bir bilim dalıdır.

¹⁰⁶ Veri madenciliği büyük miktarda verinin bilgisayar programı kullanılarak analiz edilmesi ve gelecekte ilgili tahminde bulunabilmemizi sağlayabilecek içsel ilişkilerin tespit edilmesidir.

¹⁰⁷ Chan ve Vasarhelyi, s.6.

İki türlü maddi doğruluk testi uygulanabilir:

a. Analiz yöntemleri (analytical procedures)

Analitik yöntemler finansal veriler arasında karşılaştırma ve ilişki kurmaya dayanır. Rasyoların hesaplanması ve bunların geçmiş yılların rasyoları ile karşılaştırılması tipik bir analitik yöntemdir. Bu yöntem sadece hataları tespit etmekle kalmaz ilgili kurum ve sektör performansı hakkında da bilgi verir. Denetimin planlama aşamasında işi ve sektörü tanımak için analitik yöntemler kullanılmalıdır. Kanıt toplama aşamasında da hatalı finansal bilgileri tespit etmek için kullanılabilir. Denetimin raporlama aşamasında kullanılan analitik yöntemler denetim hakkında genel sonuçlar, işlemler ve toplamaların ne derece makul olduğu ve kurumun kar eden bir kuruluş olarak faaliyetlerine ne derecede devam edebileceği bilgisini verir.

b. İşlemlerin testleri (tests of transactions)

Hataları ve olağandışı durumları anında tespit etmek için işlemler sürekli test edilirler. İşlemlerin sürekli test edilmesi dönem sonlarında bakiyeler üzerinde yapılan testlerin miktarını ve zorluk derecesini azaltır. Ancak, işlemler üzerine uygulanan testler sonucu toplanan kanıtlar işlemlerde önemli hatalar ve kuraldışı uygulamalar yapıldığını gösterirse hesap toplamalarına ilişkin yapılacak testlerin kapsamı genişletilmelidir. İşlemlerin testi ile kontrollerin testi genellikle aynı anda yapılır.

c. Bakiyelerin testleri (tests of balances)

Denetçiler finansal tablolarda yer alan bakiyelerin doğruluğu hakkında görüş bildirmek için bakiyeler üzerinde maddi doğruluk testleri yaparak kanıt toplarlar. Cari hesap bakiyelerinin doğrulanması, borçların tekrar hesaplanması, amortismanların tekrar hesaplanması bu tür testlere örnektir. Toplamlar üzerinde yapılacak testlerin kapsamı kontroller ve işlemler üzerinde yapılan testlerin sonuçlarına bağlıdır.

2. İç kontrollerin testi ve risk değerlendirmesinde kullanılan araçlar (tools used in testing of internal controls and assessing risk)

Denetim planlaması yapabilmek için denetçiler öncelikle hangi alanların risk taşıdığı ve incelemenin nerede yoğunlaşacağını tespit eder. Bu nedenle denetçiler iç kontrollerin ne derece yeterli ve etkin olduğunu araştırırlar.

Kontrollerin testleri de eşzamanlı yürütülmelidir. Böylelikle denetçiler iç kontrol sisteminin güvenilirliği konusunda görüş bildirebilirler. İç kontrol sistemine ne

derecede güvenilebileceğini bilmek denetim planlama aşamasında önemlidir. Maddi doğruluk testinin türü, zamanlaması ve kapsamı buna göre tespit edilir.

Sürekli denetim ortamında izleme denetlenmemiş verinin “normal” kabul edilen başka bir veri ile karşılaştırmalı değerlendirmesi ile yapılır. Bu karşılaştırma sonrasında “normal” sınırlar içinde olmayan veri aykırı değer veya anomali kabul edilir, olağandışı durum olarak denetçinin daha detaylı incelemesi için raporlanır.

7.1. VERİ İLE İLGİLİ ANALİZLER

7.1.1. Veri Bütünlüğüne Yönelik Analizler

7.1.1.1. Filtreleme (*filter or display criteria*)

Filtreleme, belirlenen ölçütlerdeki verilerin seçilmesine ve diğer kayıtlardan ayırarak raporlanmasına olanak veren bir yöntemdir. İncelenmek istenen ölçütler tespit edildikten sonra tüm kayıtların yer aldığı veritabanı sadece ilgili ölçütleri sağlayan kayıtları bulmak için taranır. İlgili ölçütleri sağlayan kayıtlar raporlanır. Raporlanan bu kayıtlar üzerinde inceleme yoğunlaştırılır.

Örneğin, hatalı bir işlemin belli bir tarih aralığında yapıldığından şüphe ediliyorsa ilgili tarih aralığındaki kayıtları filtreleyerek sadece o kayıtlar üzerinde inceleme yapılabilir. Hatalı işlemin yapılan ödemelere ilişkin olduğu biliniyorsa iki tarih arasındaki kayıtlar üzerinde ikinci bir filtreleme kullanılarak sadece ödemelere ilişkin kayıtlar ayrıştırılabilir. Belli bir satıcıya ilişkin ödemenin hatalı olduğu düşünülüyorsa üçüncü bir filtreleme yapıp sadece ilgili satıcıya ilişkin iki tarih arasındaki ödemeler tespit edilebilir.

Uygulaması kolay olmasına rağmen çok etkin bir yöntemdir. İncelenecek verilere ait ölçütlerin belirlenmesi inceleme odağını daraltarak inceleme süresini kısaltır. Filtreleme yönteminin asıl güçlüğü doğru ölçütlerin belirlenmesindedir. İncelemek için ayrılan veri setinde gereksiz kayıtların olması denetim süresini arttıracaktır. Ancak, ölçütleri belirlerken inceleme kapsamının gereğinden fazla daraltılarak hatalı kayıtların ortaya çıkmasının engellenmemesi gerekir.

7.1.1.2. Tanımlama ve Denklem (expression/equation)

İncelenecek verilerin eksiksiz ve doğru olduğunu teyit etmek için ilgili verilerin tekrardan hesap edilmesi gerekir. Hesaplamaları yapabilmek için yeni denklemler kurulur ve yeni tanımlamalar yapılır.

Örneğin, faturalarda yer alan miktar ve birim fiyat haneleri çarpılarak fatura toplamının doğruluğu kontrol edilebilir. Bu işlem kayıtlardaki tüm faturalar için yapıp fatura toplamı ile hesaplanan tutar arasında fark olan faturalar raporlanabilir.

Kayıtlar üzerinde hesap yapabilme yeteneği yönetim raporlarında yer alan verilerin doğruluğunun teyidi için de kullanılabilir. Örneğin, yönetim raporlarındaki ara toplam ve toplamların tekrar hesaplanması sonuçları vahim olabilecek durumları önleyebilir.

Örnek: Kayıp stoklar¹⁰⁸

Bir fabrikanın denetimi sırasında ilk altı aylık ve son altı aylık satış ve üretimde kullanılan stokların maliyeti hesaplanmıştır. Satılan malın maliyetinin % 15.61 artarken satışların sadece % 8.74 arttığı tespit edilmiştir. Bu fark karlılık oranına da yansımış, ikinci altı ayda % 2.31 düşüş görülmüştür. Bu bulguların ışığında denetçiler stoklara odaklanmaya karar vermişler ve dönem sonu stoklarını tekrardan hesaplamışlardır.

Yapılan hesaplamalar:

Dönem başı stoklar = $\sum[\text{dönem başı stok miktarları} \times \text{fiyat}]$

Dönem içi işlemler = $\sum[(\text{alınan miktarlar} - \text{üretimde kullanılan miktarlar}) \times \text{fiyat}]$

Dönem sonu stoklar = $\sum[\text{dönem başı stoklar} + \text{dönem içi işlemler}]$

Yapılan karşılaştırmada hesaplanan dönem sonu stokların kayıtlarda yer alan stoklardan daha az olduğu bulunmuştur.

Sonuç: Denetçiler stoklar üzerinde yaptıkları hesaplamalar ile bazı stokların kayıp olduğunu tespit etmişlerdir.

¹⁰⁸ David Coderre. Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide. A.B.D.: John Wiley & Sons, Inc., 2009: 86.

7.1.1.3. Boşlukların Tespiti (gaps)

Belli bir sırayı takip eden kayıtlar içinde eksik kayıtları arama yöntemidir. İşlemler bir sıra takip ediyorsa ve kayıtlar ardışık ise bu yöntemle işlenmemiş veya silinmiş kayıtları kolaylıkla tespit etmek mümkündür. Kayıtların tamamı taranır, içlerinden eksik olan kayıtlar raporlanır.

Örneğin, fatura numaraları ardışıktır. Kesilen fatura numaraları kontrol edildiğinde sayılar birbirini takip etmiyorsa, yani dizin içinde boşluklar varsa, bazı faturaların kayıtlara hiç girilmediği veya silindiği sonucuna varılabilir.

Denetimin sağlıklı yapılabilmesi için kayıtların eksiksiz olması önemlidir. Bazı kayıtların girilmesi unutulmuş veya bazı haneler boş bırakılmış olabilir. Bu yöntem sayesinde kayıtlardaki eksiklikler bulunup denetim öncesi tamamlanabilir.

Olmayan kayıtların tespiti hileyi de işaret edebilir. “Hileyi araştırırken olmayanları belirlemek çoğu kez olanları belirlemek kadar önemlidir.”¹⁰⁹ Eksik kayıtlar farklı hileleri işaret edebilir. Bunlardan bazıları:

- Eksik yapılmış ödemeler
- Eksik çekler veya faturalar
- Kayıtlara girilmemiş sipariş emirleri
- Satışları ve diğer gelirleri bildirmeyen şubeler
- Belli bir güne ait dekontların kaybolmuş olması
- Yazar kasa kayıtlarının olmayışı
- Su veya elektrik sayaçlarının okunmamış olması

7.1.1.4. İstatistiksel Analiz (statistical analysis)

Kayıtlar üzerinde yapılacak istatistiksel analizler detaylı incelemeye girmeden önce genel bir fikir vermesi açısından kullanılabilir. Ortalama değer, standart sapma, en düşük ve en yüksek değeri bulmak en çok kullanılan istatistiksel analiz teknikleridir. İstatistiksel

¹⁰⁹ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s. 93.

analizler sayısal ve tarih alanlarındaki anomalileri tespit ederek riskli alanların belirlenmesini sağlar.

Örneğin, ödeme emirleri üzerinde yapılacak istatistiksel analiz sonucunda her satıcıya yapılan ortalama ödemeler bulunarak, tespit edilen limitlerin dışında olan ödeme emirleri üzerinde detaylı inceleme yapılabilir.

İstatistiksel analiz diğer analizleri yapabilmek için çeşitli verileri de sağlayabilir. Örneğin, örnekleme için denetimi yapılacak işlemlerin tam miktarı “kayıt sayıları” istatistiksel analizi ile belirlenebilir.

Örnek¹¹⁰: Stoklardaki eksiklikler

Perakende zincirine bağlı mağazalardan birinde geçen yıl yapılan denetimde çeşitli malların kaybolduğu tespit edilmiştir. Bu nedenle bu mağazanın yöneticisi yılsonu primini alamamıştır. Yönetici, iş yoğunluğu nedeniyle kayıpların nedenini araştırmaya vakit bulamadan bir yıl daha geçmiştir. Yıllık denetim başlamak üzeredir. Bu yıl da stoklarda eksiklikler vardır. Ancak, bu yıl primini tehlikeye atmamak için eksik malları rapor etmek yerine kayıtlarda bazı girişleri eksi olarak yazmıştır.

Mağazada çok sayıda mal vardır. Ayrıca, bunların bir bölümü ya yolda ya da satışta bulunmaktadır. Tamamını saymak imkansız olduğu için belli örnekler alınarak inceleme yapılabilecektir. Denetçi, denetime başlamadan önce, mağazayı daha yakından tanımak için bazı istatistiksel analizler yapar. Stoklar üzerinde yapılan analizlerden bazıları en düşük ve en yüksek girişlere bakmaktır. Bu analizin sonucunda bazı negatif sayılı giriş olduğu tespit edilir. Bu kayıtlar incelendiğinde girişlerin aynı kişi tarafından yapıldığı ortaya çıkar.

Normal dağılım ve log-normal dağılım tablolarını kullanarak belli bir kaydın normal değerler içine düşüp düşmediği karşılaştırılır. Örneğin: Bir fatura ele alınır. Bu faturanın satıcısının daha önceki faturalarının toplamaları üzerinden normal dağılım tespit edilir. İlgili faturanın toplamı bu tablo ile kıyaslanır, toplam miktarın normal sınırlar içine düşüp düşmediği belirlenir.¹¹¹

¹¹⁰ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s. 98.

¹¹¹ Pamela Jersey. “Using Analytical Procedures For Continuous Auditing And Fraud Detection”, 1998. Boston College. <http://www.auditnet.org/contaudit.htm> (13 Aralık 2008).

7.1.1.5. Eş Kayıtların Tespiti (duplicates)

Aynı işlemin birden fazla kaydedilmemiş olması gerekir. Kopyalanmış kayıtların elektronik olarak tespit edilebilmesi için kayıtlardaki bazı hanelerin içindeki verilerin ilgili kayda özel olması ve bir eşinin daha olmaması gerekmektedir. Sistem tüm kayıtları anahtar hanelere göre kontrol eder, eşleşen haneler varsa ilgili kayıtları raporlar.

Örneğin: Her çek yaprağının üzerindeki seri numarası birbirinden farklıdır. İnceleme sonucunda farklı ödemelerin aynı seri numaralı çekle yapıldığı tespit edilirse kayıtlarda hata veya hileden şüphe edilebilir. Aynı satıcı için birden fazla kayıt açılması cari hesabın takibini zorlaştıran, genelde kurumlar tarafından istenmeyen bir unsurdur. Çeşitli kısaltmalar kullanılarak aynı satıcıya birden fazla kayıt açıldığının tespit edilmesi her zaman hile olduğunu göstermese de düzeltilmesi gereken bir hatadır.

İşlem sayısının fazla olduğu yerlerde denetimi yapılan örnek kayıt setinde eş kayıtların bulunma olasılığı çok düşüktür. Kopyalanmış kayıtların parasal değeri önemli bir miktar tutsa da incelen kayıtlar içinde yer almıyorlarsa denetim sırasında tespit edilemezler. Ancak, eş kayıtların tespiti elektronik ortamda kayıtların tamamı üzerinde yapıldığı için etkinliği yüksek bir analizdir.

Hangi hanenin kayda özel olduğunu tespit etmek için denetlenen sistemin işleyişini iyi bilmek gerekir. Örneğin, kısmi ödemeler yapıldığında birden fazla kaydın ilgili fatura hanesinde aynı fatura numarası olacaktır. Ödemelere ilişkin analiz fatura numarasına göre yapıldığı takdirde kısmi ödemelerin kayıtları doğru olsa bile birden fazla giriş yapılmış gibi raporlanacaktır.

7.1.1.6. Sınıflama ve Sıralama (sorting and indexing)

Kayıtlar belli bir alan temel alınarak artan veya azalan değerlere göre sıraya koyulur. Örneğin, işlemleri tarihlerine göre sıralamak. Uygulaması çabuk ve kolay bir yöntemdir. Fazla sayıda işlemin olduğu yerlerde olağandışı durumların saptanmasını kolaylaştırır. Verilerin tam olup olmadığını kontrol etmek için kullanılan analizlerden biridir.

Örneğin, müşteri talepleri seri numarası ardışık basılı evraka alınıyorsa ve sisteme bu evraka göre kaydediliyorsa seri numarasına göre yapılacak sıralama sonucunda listenin başına ve sonuna bakıldığında olağandışı seri numaralarını tespit etmek kolay olacaktır. Ayrıca, serinin belli yerlerinde boşluklar varsa bu da eksik kayıtları işaret edecektir.

Sıralama tüm kayıtlar üzerinde çabuk ve kolayca yapılabildiği için etkin bir analiz türüdür. Listenin başına ve sonuna bakarak olağandışı durumların tespit edilebileceği bazı durumlar aşağıdaki gibidir:

- Çok eski veya gelecek tarihli kayıtlar
- Belirlenen değer aralığından daha yüksek bir değer girilmiş veriler
- Alıcı ve satıcı isimlerinin başında boşluk bırakılması veya olağandışı harflerin olması
- Kayıtların bazı hanelerine veri girilmemiş olması
- Sadece sayısal verilerin olması gereken hanelerde harflerin olması
- Sadece harflerin olması gereken hanelerde sayıların olması

Örnek: Hayali hesaplar¹¹²

Sigorta poliçeleri üzerinde denetim yapılacaktır. Daha önceki denetimler örnek olarak seçilen bazı poliçeler üzerinde yapılmıştır. Önemli bir sorunla karşılaşmamıştır. Bu sene elektronik ortamda denetim yapılmasına karar verilmiştir. İlk adım olarak denetçiler poliçeleri numaralarına göre sıralarlar. Sigorta poliçelerinin seri numaralarının ilk dört hanesi ilk yapıldıkları yılı göstermektedir. Oysa alınan rapora göre DC koduyla başlayan bazı poliçeler bulunmaktadır. Yönetici bu konuyla ilgili sorgulandığında bu poliçelerin kendi özel dosyaları içinde durduğunu söyler. Böylece bu poliçelerin daha önceki yıllardaki denetimlerde hiç ortaya çıkmadıkları anlaşılır. Yönetici yıllık hedefini tutturup prim almaya hak kazanmak için iki yıl önce on yedi hayali hesaba poliçe düzenlemiştir. Bir sonraki yıl hedefini yakalayabileceğini düşünmüştür. Ancak bir sonraki yıl da hedeflerini tutturamamış ve hayali hesaplara satılan poliçelerin sayısı yirmi altıya çıkmıştır. Bu sene ise bu sayı elli dokuzdur. Yönetici satış rakamlarını şişirmenin bir sakınca yaratmadığını düşünmektedir. Hedeflerin çok yüksek olduğunu düşünüp davranışını rasyonalize etmiştir.

¹¹² Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s.109.

7.1.2. Veri Hakkında Bilgi Verici Analizler

7.1.2.1. Özetleme (summarization)

Her kategoriye ilişkin kaç adet kayıt girildiğini ve/veya belli alanlardaki sayıların toplamının bulunduğu bir yöntemdir. Özetleme, belli bir alana giren kayıtların tespit edilmesi ve toplam değerinin bulunması için kullanılır. Hileli kayıtların tutulduğu geçersiz hesapları bulmak için iyi bir yöntemdir. Örneğin, her hesaba ait gelirlerin ve harcamaların toplamı kolaylıkla tespit edilebilir.

Özetlemenin kullanım nedenlerinden biri de sisteme kaydedilen verilerin kontrolünü yapmaktır. Belli hanelere yanlış giriş olduğunda veya veri girilmesi gereken yerlerin boş geçilmesi durumunda sistemin kullanıcıyı uyarması beklenir. Ancak sistem kontrolündeki yetersizlikler nedeniyle kullanıcılar hatalı giriş yapsalar da sistem bu kayıtları kabul edebilir. Bu analiz tekniği sistem kontrol eksikliklerini de ortaya çıkartmaktadır.

Örnek¹¹³: Sağlık sigortası poliçeleri kapsamında yapılan ödemeleri inceleyen denetçi özetleme tekniğini kullanarak yapılan sağlık girişimlerini cinsiyete göre özetler. Bulgular aşağıdaki gibidir:

<u>İşlem</u>	<u>Cinsiyet</u>	<u>Adet</u>
Histerektomi	Kadın	127
Histerektomi	Erkek	3
Histerektomi		12

Histerektomi, rahmin alınması girişimidir. Bu girişimin erkeklere yapılması imkansızdır. Ancak kayıtlara göre üç erkek histerektomi olmuştur. Ayrıca, cinsiyeti belli olmayan on iki hastaya daha histerektomi yapılmıştır. Cinsiyet girilmeden poliçelerin kabul edilmesi bir sistem kontrol zaafıdır.

¹¹³ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s. 77.

7.1.2.2. Katmanlara Ayırmak (stratification)

Sayısal alanları alt bölümlere ayırarak inceleme yöntemidir. Her alt bölümde yer alan kayıtların adedi ve/veya toplam değeri bulunarak anomaliler araştırılır. Verilerin profiline ilişkin genel bilgi edinmek için kullanılır.

Örnek¹¹⁴: Bir firmanın iş sözleşmelerini değer aralıklarına (0-4999, 5000-9999, 10000-24999, vb.) göre ayırdığımızda aşağıdaki tablo çıkmaktadır:

<u>Sözleşme Miktarı</u>	<u>Adet</u>	<u>Toplam Sözleşme Miktarı</u>
0-4999	0	0
5000-9999	3	28,394
10000-24999	176	3,350,984
25000-49999	444	16,674,390
50000-99999	342	21,985,213
100000-500000	1	404,182
Toplam:	966	42,443,163

Bu yöntem yüksek değerdeki sözleşmelere odaklanmamızı sağlasa da firmanın limit üstü ve limit altı sözleşmelerini de ortaya koymaktadır.

7.1.2.3. Tablolama (cross tabulation/pivot tables)

Bu yöntemde veriler iki boyutlu tablo haline getirilir. Denetçilerin verileri daha iyi anlayabilmesi için verilerin yeniden düzenlenmesidir. Veriler tablo formatında düzenlendiğinde daha anlaşılır bir hale gelirler. Olağandışı kombinasyonları tabloda rahatça görebildiğimizden anomalileri tespit etmek için etkin bir yöntemdir.

Kayıtların tablo haline getirilebilmesi için en az iki haneden oluşması gerekmektedir. Bir hanedeki değerler tablonun satırlarını (x eksen) oluştururken diğer hanedeki değerler kolonları oluşturur (y eksen).

Örneğin, çalışan bazında fazla mesai ödemelerinin hangi amaçlarla yapıldığını tablolarsak, fazla mesai ücretlerinin ödenmemesi gereken durumları rahatlıkla tespit edebiliriz.

¹¹⁴ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s. 77.

7.1.2.4. Yaşlandırma (aging)

İki tarih arasında kaç günlük bir fark olduğunun tespitine yaşlandırma denir. Birbirini takip eden işlemlerin gerçekleşme süreleri denetçiler için önemli bilgilerdir. Verilerin doğruluğundan ve uygunluğundan emin olmak için kullanılan bir analiz türüdür. Tarihleri birbirleriyle kıyaslamak önemli sonuçlar doğurabilir. Örneğin, ihale başvurusunun tarihi ihalenin kapanış tarihinden sonraki bir günü gösteriyorsa veya satış faturası ilgili malın depoya giriş tarihinden önceki bir tarihte kesilmişse, yapılan kayıtların doğru olmadığı veya uygulamaların hatalı olduğu sonucuna varılır.

Yaşlandırma, çalışmaların verimliliği konusunda da yol göstericidir. Örneğin, satışın gerçekleşmesi ile ödemenin yapılması arasında geçen süre, stokların ne kadar süre depoda kaldığı gibi bilgiler uygulamalardaki verimsizlikleri ve düzensizlikleri gösterir.

Elektronik ortamda tüm kayıtlar üzerinde yapılacak yaşlandırma anomalilerin tespitinde çok yararlı olacaktır.¹¹⁵ Aşağıdaki işlemlerin yaşlandırma analizi verileri anlamamız açısından büyük fayda sağlayacaktır:

- Süreleri dolduğu halde ödemeleri yapılmamış hesaplar
- Alacak düzeltmesi yapılmış hesaplar
- Stok devir hızı
- İşlem görmeyen hesaplar
- Gelecek tarihli, tarih hanesi boş geçilmiş veya geçersiz tarih girilmiş kayıtlar
- Son günden sonraki bir tarihte yapılmış işlemler
- İhalelerin kapanış gününden önce yapılmış ilgili ihalelere ait sözleşmeler
- İhale kapanış tarihinden sonra verilen fiyat teklifleri
- Ekipmanların bozulma ortalamaları
- Çeşitli işlerin yapılma süreleri

¹¹⁵ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s.133.

7.1.2.5. Birleştirme ve İlişkilendirme (join/relate)

Bu yöntem fiziksel olarak veya bir rapor şeklinde iki veya daha fazla veritabanındaki kayıtların birleştirilmesini öngörür. Dikkat edilmesi gereken farklı veritabanlarında olan bu kayıtların hangi alanlarının ilişkilendirileceğidir. Her alan tek bir alanla ilişkilendirilebileceği gibi birçok alanın tek bir alanla da ilişkilendirilmesi mümkündür. Farklı veri dosyalarını birleştirme ve ilişkilendirme olağandışı işlemlerin tespit edilmesini sağlayabilir.

Örnek ¹¹⁶: Çalışanların maaş ödemelerinin yer aldığı dosya çalışanların kişisel dosyaları ile birleştirildiğinde, bazı çalışanların kişisel dosyalarında yer almayan ancak onlara yapılmış gibi görünen ödemeler tespit edilmiştir. Bu kayıtlarda hata veya hile olduğu kolayca görülmektedir.

7.1.3. Veride Trendleri Tespit Etmeye Yönelik Analizler

7.1.3.1. Trend Analizi (trend analysis)

Trend analizi farklı zaman dilimleri veya farklı yerlerdeki değişimleri gösteren bir yöntemdir. Verilerdeki anomalilerin tespitinde kullanılır.

Her yıl aynı dönemlerde aynı bölge için yapılan denetimler trend analizi yapabilmek için en ideal koşulu sağlar. Farklı bölgelerdeki çalışma yöntemlerini karşılaştırmak ve bölgeler arası farklılıkları tespit etmek takip edilmesi gereken bölgelerin belirlenmesinde faydalı olur.¹¹⁷

Örnek: Bayi bazında kusurlu mal iadesine ilişkin kayıtlar üzerinde trend analizi yapılmıştır. Analiz sonucunda dönemler itibariyle hep aynı bayiinin diğerlerinden daha yüksek oranda kusurlu mal iade ettiği ortaya çıkmıştır. Kusurlu mallarda mal değişiminin yanı sıra bir komisyon da ödenmektedir. İlgili bayiinin komisyon alabilmek için bilerek kusurlu malı satın alması söz konusu olabilir.

¹¹⁶ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s. 79.

¹¹⁷ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s. 79.

7.1.3.2. Regresyon Analizi (regression analysis)

Regresyon analizi, verilerin deęerlerini tahmin etmek veya tahmini deęerlerle gerekleřen deęerleri karřılařtırmak iin kullanılır. Veriler arasındaki iliřkileri tespit eder. İřlemlerin beklenildięi řekilde gerekleřiř gerekleřmedięi de regresyon analizi ile anlařılabilir. Verilerdeki anomalilerin tespitinde kullanılır.

Örnek¹¹⁸: Bina yneticisi bazı boř daireleri kiralar ve kiraları toplar. Ancak, bina sahibine bildirmez. Apartmanın elektrik ve su tketimi zerinde regresyon analizi yapılırsa aslında tketilmesi gereken su ve elektrik miktarının gerekleřenden daha az olması gerektięi ortaya ıkacaktır. Fark incelendięinde ise dairelerin kiralandıęı anlařılacaktır.

Regresyon analizi doęrusal olmayan iliřkileri de ortaya koyabilmektedir. İlk bakıřta ilgili gibi grnmeyen verilerin birbirlerini nasıl etkiledięini anlamak ve doęrusal olmayan iliřkilerde deęer tahmin etmek iin kullanılan gl bir analiz teknięidir.

7.1.3.3. Paralel Simlasyon (parallel simulation)

Bilgisayar programlarının mantıęını doęrulamak iin kullanılır. Benzer bir mantık eřitli iřlemlere uygulanır. Sonra bilgisayar programından da aynı sonu alınıp alınmadıęına bakılır.

Örnek¹¹⁹: Bilgisayar programcısı ek deme iřlemlerinde bazı deęiřiklikler yaparak arkadaşlarına fazla deme yapılmasını saęlamıřtır. Denetiler, veriler zerinde tekrar hesaplama yaparak olması gereken ek deme miktarlarını tespit ederler. Denetilerin bulguları ile bordro programından alınan deme listeleri karřılařtırılır. Aralarında fark olduęu ortaya ıkar, bordro programı daha detaylı incelemeye alınır.

¹¹⁸ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s. 81.

¹¹⁹ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s. 80.

7.1.4. Gelişmiş Analiz Teknikleri

7.1.4.1. Veri Profilleme (data profiling)

Bu analiz belli bir verinin profilini çıkartır. Verinin oluştuğu ortam da dikkate alınır. Veriler bir dizi analiz tekniği ile incelenir ve standartlar tespit edilir. Bu standartların dışındaki veriler raporlanır. Olağandışı kabul edilen verileri ilgilendiren işlemlere odaklanılır. Örneğin, ödemeler incelendiğinde sadece yüksek değerler değil tüm ödeme işlemlerindeki satıcılar incelenir. Bu satıcılardan kurum için olağandışı biri tespit edilirse anomali olarak raporlanır.

Genelde analiz teknikleri verilerin belli bir özelliğini dikkate alarak farklı olanları tespit eder. Veri profillemeye ise normal şartlarda gözden kaçabilecek, küçük değerlerdeki veya göze batmayacak işlemlerdeki hata ve hilelerin ortaya çıkarılmasında faydalanan ileri analiz tekniğidir.

Ayrı bir bilgisayar programı yazılması gerekebilir. Yüksek risk söz konusu ise bu program sık sık çalıştırılarak hilenin erken tespit edilmesi ve kayıpların en aza indirilmesi için kullanılabilir.

Örnek¹²⁰: Bir kurumdaki ödeme kartlarına ait işlemleri inceleyen denetçiler ödeme miktarlarının profilini çıkartmak istemektedirler. Aşağıdaki analizleri uygularlar:

- En düşük, en yüksek ve ortalama on işlem
- Ödeme miktarlarına göre sınıflandırma (0-99, 100-299, 300-500, vb.)
- En sık yapılan ödeme miktarı
- Tam rakamlı işlemler (2000, 7000, vb.)
- En çok ve en az işlem gören satıcılar veya kart numaraları

Veri profillemeye kullanılan bazı teknikler aşağıdaki gibidir:

- İstatistiksel analiz: ortalama değer, mutlak değer, en yüksek ve en düşük değerler, eksi, artı ve sıfır değerler gibi temel istatistik analizleridir.
- Alt bölümlere ayırmak

¹²⁰ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s. 194.

- En sık kullanılan değer: Aynı değerın çok sayıda tekrarlanması bir anomaliyi işaret edebilir. Örneğin, aynı miktarda yapılmış ödemeler bir faturanın birçok kez ödendiğinin işareti olabilir. En sık kullanılan üç değer veya en az kullanılan değerler için de incelemeler yapılabilir.
- Yuvarlama: Bir tam sayıyı gösteren veya yuvarlama yapılmış rakamlar incelenir. Örneğin, bir kurum için seyahat harcamalarının günlük limiti 200 TL'dir; bir satış elemanı seyahate gittiğinde günlük harcamalarını sürekli 200 TL'ye yuvarlıyorsa olağandışı bir durum var demektir.
- En az ve en çok kullanılan kategori: Örneğin en az ve en çok kullanılan satıcı hesaplarını belirlemek masrafların profili çıkartmak için kullanılabilir.
- Oran analizi: hile için kullanılan oranlar da finansal oranlar gibi verilerdeki ani değişikliklerin tespiti için kullanılır. En sık kullanılan oranlar aşağıdaki gibidir:
 - en yüksek değer/en düşük değer
Örnek: bir ürün için uygulanan en yüksek satış fiyatı en düşük satış fiyatına bölündüğünde bulunan oran 1'e yakınsa, satış fiyatının varyansının düşük olduğunu anlaşılır; ancak 1'den çok yüksekse ürünün bazı müşterilere gereğinden daha fazla fiyata satıldığını işaret eder.
 - en yüksek değer/ikinci en yüksek değer
 - cari yıl/bir önceki yıl
Oran analizi uzun yıllar belli dönemler için tekrarlanırsa çok etkilidir. Tarihsel veriler trendleri ve olağandışı işlemleri ortaya çıkarmak açısından önemlidir.
 - bir faaliyet/diğer bir faaliyet
- Zaman serisi analizleri: geçmiş dönemlere ait verinin geleceği tahmin yeteneğinin yüksek olduğu durumlarda kullanılır. Örneğin, insanlar sosyal ve iş yaşamları içinde her gün belli rutin davranışları tekrarladıkları için zaman serisi analizleri davranış profillerini çıkartmak için etkin bir analiz yöntemidir.

7.1.4.2. Benford Kanunu (Benford's Law)

Benford Kanunu, verilerdeki hanelerin gerçekleşme sıklığı ile teorik tekrarlanma olasılığını karşılaştırır. Amerikalı astronom ve matematikçi Simon Newcomb 1881 yılında yayınladığı bir makalede logaritma kitaplarında 1 ile başlayan sayılara 2'den daha fazla, 2 ile

başlayan sayılara 3'den daha fazla bakıldığına ve en az 9 ile başlayan sayılara bakıldığına dair gözlemlerini dile getirmiştir. O dönemde bu gözlem önemsenmemiş ve uzun süre bu makale unutulmuştur. General Electric'in New York'taki laboratuvarında fizikçi olarak çalışan Frank Benford, 20.229 adet farklı sayısal veri üzerinde yaptığı çalışmasını 1938 yılında tamamlar. Nehir uzunlukları, beysbol istatistikleri, elementlerin atom ağırlıkları, şehirlerin nüfusları gibi farklı alanlarda sayısal değerleri inceleyerek ilk, ilk iki ve ilk üç hanede belli sayıların tekrarlanma olasılıklarını tespit etmiştir. Benford'un incelediği verilerin %30,6'sı 1 rakamı ile başlarken, %8,0'i 5 ile ve %4,7'si de 9 ile başlamıştır. Bir veri kümesindeki sayıların ilk rakamının 1 olma olasılığı 0,111 (1/9) değil, 0,306'dır. Homojen bir dağılım göstereceği sanılan sayılar aslında logaritmik bir dağılım göstermektedir. Örneğin, bir sayının 314 ile başlama olasılığı $\log_{10}(1+(314)-1)$ olarak belirlenmiştir.

Tablo 5
Benford Kanunu'na Göre Bir Sayının İlk Dört Basamağındaki
Rakamların Ortaya Çıkış Frekansları

RAKAMLAR	BASAMAKLAR			
	BİRİNCİ	İKİNCİ	ÜÇÜNCÜ	DÖRDÜNCÜ
0		11,9680%	10,1780%	10,0180%
1	30,1030%	11,3890%	10,1380%	10,0140%
2	17,6090%	10,8820%	10,0970%	10,0100%
3	12,4940%	10,4330%	10,0570%	10,0060%
4	9,6910%	10,0310%	10,0180%	10,0020%
5	7,9180%	9,6680%	9,9790%	9,9980%
6	6,6950%	9,3370%	9,9400%	9,9940%
7	5,7990%	9,0350%	9,9020%	9,9900%
8	5,1150%	8,7570%	9,8640%	9,9860%
9	4,5760%	8,5000%	9,8270%	9,9820%

Kaynak: Mustafa Türkyener. “Benford Yasası ve Mali Denetimde Kullanımı”. Sayıştay Dergisi 64 (2007): 115.

1990'ların başlarında Benford Kanunu'nun denetimde kullanılması fikri gelişir ve bir sayısal analiz tekniği olarak literatüre geçer. Dijital analiz tekniği olarak kullanıldığında belli rakamlar ve rakam kombinasyonlarının normalin dışında tekrarlanması durumunda bu anomalileri tespit eder.¹²¹ Bu da verilerin doğal akışını bozan hata veya hilenin habercisi olarak yorumlanabilir. Bu varsayım Benford Kanunu'nun muhasebe hilelerini tespit etmek için kullanılmasına yol açmıştır.

¹²¹ Jerskey, s.1.

Özellikle hile tespitinde önemli yer tutan bu istatistik modelinin denetim yazılımlarında yer alması ile uygulanması kolaylaşmış ve yaygınlaşmıştır. Örneğin, ACL yazılımı kullanıcıları için ilgili dosya ve ilgili veri alanlarını belirlemek işlemleri Benford Kanunu'na göre değerlendirmek için yeterlidir.

Benford analizi sonuçlarını değerlendirirken doğru bir işlemi yanlış, yanlış bir işlemi de doğru olarak değerlendirme olasılığı yüksektir. “Benford analizleri, verilerin hileli olduğunu %68 oranında, hilesiz olduğunu ise %67 oranında ortaya çıkarmaktadır.”¹²² Benford Kanunu olasılık dağılımına uymayan bir veri alanı varsa sıradışı işlem olarak raporlamadan önce başka analizler de yapılmalıdır. ACL gibi denetim yazılımları hane hane analiz yaparlar. Bu analiz şekli hatalı olmayan bir işlemin olağandışı olarak değerlendirilme olasılığını arttırmakta ve yanlış alarmların doğmasına yol açmaktadır. Önce ilk haneyi, sonra ilk iki haneyi birden kullanarak yapılan Benford analizlerinin daha doğru sonuç verdiği saptanmıştır.¹²³

Benford Kanunu birçok veri alanının denetimi için uygundur. Ancak bazı durumlarda hatalı sonuç verir:

- Birbirine yakın büyüklükteki veri: Sayı setindeki değerlerin birbirine yakın olmaması gerekir. Örneğin, yetişkin kişilerin boylarına ilişkin bir sayı seti üzerinde Benford analizi yapılırsa sayılar arasında çok fark olmayacağı için bu modelin önerdiği olasılıklar doğru olmayacaktır.
- Müdahale edilmiş veya alt-üst limit konmuş veri: Örneğin, kontrata bağlanmış kira ödemeleri gibi müdahale edilmiş veya harcırak gibi alt ve üst limiti olan ödemelere ilişkin veri Benford dağılımında olmayabilir.
- Kodlanmış ve atanmış veri: Rastgele sayıların kullanılmaması durumunda yanlış sonuçlar çıkacaktır. Örneğin, telefon numaraları, posta kodları, kimlik numaraları, çek numaraları, loto ve piyango bileti numaraları.
- Küçük veri setleri: Gözlem sayısı az ise istatistiksel olarak geçerli olsa da Benford modeline uygun bir dağılım gerçekleşmeyebilir. Bu kanunun geçerli olabilmesi için geniş bir veri seti tercih edilmelidir.

¹²² Türkyener, s. 111.

¹²³ Richard Cleary ve Jay C. Thibodeau. “Applying Digital Analysis Using Benford’s Law to Detect Fraud: The Dangers of Type I Errors”, A Journal Of Practice & Theory 24. 1 (Mayıs 2005): 80.

- İnsan düşüncesinden etkilenmiş sayı grupları: Örneğin, 10 TL yerine 9.90 TL olarak psikolojik eşiğe göre saptanan fiyatlar Benford olasılık dağılımını olumsuz etkileyecektir.

7.1.4.3. Rakam Analizi (Digital Analysis)

Nigrini ve Mittermaier 1997 yılında sayılar içinde yer alan rakamları analiz ederek olağandışı durumları ortaya çıkartan yeni bir yöntem bulmuşlardır. Bu yöntem sayılar içindeki rakamların diziliş sırası ve kaç defa tekrarlandıkları gibi biçim düzenlerini araştırır ve modelleme yapar. Denetlenen işlemlerle ilgili sayıların modele uygun olmaması olağandışı durumu gösterir.

Nigrini ve Mittermaier bu yöntemi Benford Kanunu'na alternatif olarak geliştirdiklerini belirtmişlerdir.¹²⁴ Rakam analizinin Benford Kanunu'na göre bazı üstünlükleri vardır. Bu yöntem Benford Kanunu ile analiz edilmeye uygun olmayan sayı kümeleri için de kullanılabilir. Benford Kanunu'nun kullanılabilmesi için sayıların rasgele olması gerekir. Oysa muhasebe verisi genellikle bir ortalama çevresinde toplanmıştır ve çoğunlukla alt ve üst limitleri vardır.

Rakam analizi altı testten oluşur:

- İlk rakam: Benford Kanunu'nu ile uyumludur.
- İkinci rakam: Benford Kanunu ile uyumludur.
- İlk iki rakam: Denetlenmiş eski veride ilk iki basamaktaki rakamlara eş rakamlar aranır. Herhangi ilk iki rakam denetlenmiş veride olduğundan daha fazla tekrarlanmışsa hile, hata, yanlış tanımlama veya süreçlerdeki verimsizliklerden kaynaklanabilir. Bu sayıların detaylı incelenmesi gerekir.
- Rakam tekrarı: Aynı rakamların sayılar içinde tekrarlanma sıklıkları belirlenir. Tekrarlanma sıklıklarına göre sayılar sıralanır. Örneğin, 50, 500,5000 ve 505 sayılarında 50 rakamı tekrarlanmıştır. İlk iki rakam testi yapıldıktan sonra belli bir sayı etrafında yoğunlaşma varsa rakam tekrarı testinin yapılması önerilmektedir.
- Yuvarlama: Uydurma veya tahmini sayıları belirlemek için kullanılır. Anomali veya hataları bulması beklenmez.

¹²⁴ Mark J. Nigrini, “Continuous Auditing”. 2000.
http://aaahq.org/audit/midyear/01midyear/papers/nigrini_continuous_audit.pdf (14 Aralık 2011).

- Son iki rakam: Uydurma veya tahmini sayıları belirlemek için kullanılır. Anomali veya hataları bulması beklenmez.

Sürekli denetimde rakam analizinin kullanımı kolaydır. Aşağıdaki adımları atarak bir uygulama gerçekleştirilebilir:

1. Testlerden uygun olanları seçilir.
2. Denetlenmiş veri üzerinde bu testler uygulanır.
3. Sayıların biçim düzenlerinin modeli oluşturulur.
4. Denetlenecek yeni veri test edilir.
5. Bulgular model ile karşılaştırılır.
6. Modele uymayan veri anomali olarak kabul edilir.

7.1.4.4. Devamlılık Denklemi (continuity equations)

Finansal veriyi iş süreçleri ile ilişkilendirerek yönetim kararlarının finansal veriyi nasıl etkilediğini açıklayan bir model yaratmaktır.

Devamlılık denklemi ilk defa 1990'ların başında Bell Laboratuvarları'nda (şimdiki AT&T) müşteri faturalandırma sürecinin bir parçası olarak kullanılmaya başlanmıştır.

Bu modellerin amacı hem finansal hem de finansal olmayan verinin birbirleri ile olan ilişkisini araştırmak ve standart kurum faaliyetlerine uymayan kayıtları tespit etmektir. Kurum için önemli iş süreçlerine odaklanır. Tek başına bir işlemi incelemek yerine farklı iş süreçleri ile ilgili rutin işlemler izlenir. Kayıtları tek tek incelemekten farkı her verinin bir kayıt altkütmesine göre değerlendirilmesidir.

Devamlılık denklemleri iş süreçlerindeki düzensizliklerin tespiti için de kullanılır. Belli bir kuralı çiğnemediği için doğruluğu onaylanan işlemler, sürecin bütününe ve geçmiş örneklere bakıldığında anomali olarak tespit edilebilir.

Devamlılık denklemi modelinin aşamaları:¹²⁵

¹²⁵ Alexander Kogan ve diğerleri. "Analytical Procedures for Continuous Data Level Auditing: Continuity Equations". Temmuz 2010. <http://www.raw.rutgers.edu> (18 Şubat 2011).

1. Örnek veri altkütmesi oluşturmak: Kurum faaliyetlerinin normal seyrinde gitmesi durumunda gerçekleşmesi beklenen veriye ilişkin örnek oluşturulur. Bu veri genellikle standart uygulamaların sonucunda elde edilmiş, doğruluğu ve bütünlüğünden emin olunan, belli bir döneme ait veri altkütmesidir. Bu örnek veri altkütmesi modeli belirlemek için kullanılır.
2. Olasılık modeli kurmak: Bir istatistik kuramı ele alınıp örnek veri altkütmesi kullanılarak bir model geliştirilir. İlgili faaliyeti etkileyen önemli unsurlar (zaman, bölge, ürün, müşteri, vs.) modelin değişkenleridir. Bu model, ilgili kurumsal faaliyetlerin sonuçlarını tahmin etmek için kullanılacaktır.
3. Varyansı aralığını belirlemek: Bu bir olasılık modeli olduğu için veri kümesinin varyansı olacaktır. Bu varyans hesaplanır. Gerçekleşen veri belirlenen varyans aralığı dışında ise o veride bir anomali olduğu varsayılır.
4. Olağandışı durum raporlaması: Varyans aralığının dışında kalan veri olağandışı durum olarak ilgili kişilere raporlanır. Her anomali bir problemin göstergesi olmayabilir. Sadece istatistiksel dalgalanmalardan kaynaklanan bir durum da olabilir. Denetçilerin zamanının etkin kullanılması için olağandışı durumlar oluşturacağı risk açısından değerlendirilebilir ve derecelendirilebilir.
5. Modelin Kendi Kendine Öğrenme Protokolü (Online Model Learning Protocol): Modelin kendini yenilemesidir. En eski veri örnek veri altkütmesinden çıkar ve en yeni veri onun yerini alır. Parametrelerin tahmini için kullanılan örnek veri altkütmesinin büyüklüğü aynı kalır. Parametreler ve varyans aralığı yeniden belirlenir. Yeni veri girişi yapıldıkça model de yeni şartlara uyum sağlar.

Devamlılık denklemi kuramı çerçevesinde yaratılan model ile kurumun tüm kayıtları belli süreç kurallarına göre test edilir. Ancak, yaratılan modelin tüm olasılıkları göz önüne almış olması imkansızdır. Bu nedenle devamlılık denklemleri sürekli denetimde veri doğrulama işleminden sonra ikinci savunma seviyesi olarak kullanılmalıdır.

Devamlılık denklemini kurmak için kullanılan olasılık modelleri:

- Doğrusal Bağlanım Modeli (Linear Regression Model, LRM): Doğrusal bağlanım modeli sadece bir ilişkiyi modelleyebilir.
- Eşanlı Denklemler Modeli (Simultaneous Equation Model, SEM): İş süreçlerinin birbirleriyle olan ilişkilerini eşzamanlı modeller. Model, kurumda yer alan tüm iş süreçlerinin birbirleriyle olan ilişkisini gösteren formüllerden oluşur.

- Vektör Otoregresyon Modeli (Vector Autoregressive Model, VAR): Dzeng 1994 yılında yaptığı bir çalışmada VAR'ın tahmin yeteneğinin üstünlüğünü tespit etmiştir.
- Otoregresif Koşullu Değişen Varyans Modeli (Generalized Autoregressive Conditional Heteroscedasticity Model, GARCH): Tarihsel verinin varyansını hesaplayarak gelecekteki verinin varyansını tahmin etmek için kullanılan bir zaman serisi modelidir. Tarihsel verinin varyansı anomalilerin tespiti için kullanılabilir.

7.1.4.5. Kümeleme Analizi (cluster analysis)

Kümeleme analizi verinin nitelikleri veya birbirleri ile olan ilişkisine bakarak verinin gruplara ayrılmasıdır. Grup içindeki veri ne kadar benzeşirse ve gruplar arası fark ne kadar fazla ise kümeleme analiz sonuçları daha sağlıklı olur. Bu analiz veriyi bir bütün olarak ele alır, sonra belli değişkenleri dikkate alarak alt kümeler ayırır.

Alt kümeler ayırma işlemi hem verinin yapısını anlamak hem de veriyi incelemek açısından faydalıdır. Örneğin, pazar araştırmalarında müşterileri sınıflaması demografik yapıya göredir. Müşteriler demografik özelliklerine göre kümelendir ve her küme için farklı pazar stratejileri geliştirilir. Benzer bir çalışma muhasebe kayıtları üzerinde yapılabilir.

Muhasebe kayıtları üzerinde kümeleme analizi aşağıdaki adımlardan oluşur:¹²⁶

1. Veri kümesini oluşturan kayıtların benzeştiği ve ayrıldığı yönler araştırılır.
2. Benzerlikler ve farklılıkları ortaya koyacak değişkenler tespit edilir.
3. Veri benzerlikleri ölçülür, yani iki verinin sayısal değeri arasındaki fark tespit edilir.
4. Kümeleri oluşturacak yöntem, yani algoritma seçilir.
5. Veri benzerliklerine göre alt gruplara ayrılır.
6. Bu alt gruplar analizi yapılacak kümeleri oluşturur. Kümeleri oluştururken küme içindeki varyansın minimum, kümeler arası varyansın ise maksimum olmasına dikkat edilir.
7. Kümeler birbirleri ile karşılaştırılır. Kümeler arası farklar, küme ortalamaları gibi kümeyi oluşturan veri değerlerindeki farklılardan anlaşılır.
8. Az veri olan kümeler hile veya anomali olma olasılığı yüksek kayıtları içerir. Sadece bu kümeler üzerinde detaylı inceleme yapılır.

¹²⁶ Sutapat Thiprungsri, "Cluster Analysis for Anomaly Detection in Accounting Data". Temmuz 2010. <http://www.raw.rutgers.edu> (18 Şubat 2011).

Bir istatistik analiz türü olduğu için formüle edilmesi ve programlanması kolaydır. Bu nedenle küme analizi sürekli denetimde muhasebe kayıtlarında hile ve anomali tespitinde kullanılabilecek bir analiz türüdür.

7.1.4.6. Kayıt Günlüklerinin İşlem Madenciliği (process mining of event logs)

İşlem madenciliği bir bilgisayar sisteminin kayıt günlüklerinden bilgi sağlama işlemidir. Bilgisayar sistemleri girilen kayıtların hangi kullanıcı tarafından, hangi terminalden, ne zaman girildiğine dair tanımlayıcı bilgileri kayıt günlükleri adı verilen bir dosyada tutar. Bazı işletim sistemleri kayıtlar üzerinde yapılan değişikliklere ait bilgileri de saklar. Bu dosyalar sistem tarafından otomatik olarak yaratılır.

Kayıt günlüklerindeki verinin kişilerden bağımsız sistem tarafından otomatik olarak kaydedilmesi buradan elde edilecek bilgiyi önemli bir denetim kanıtı yapar. Kayıt günlüklerinde yer alan bilginin doğruluğunun ve bütünlüğünün kabul edilmesi sistem tarafından yaratılmış olmasından kaynaklanır. Ayrıca, bu bilgi adli incelemeler için de kanıt niteliği taşır.

Kayıt günlüklerinde işlemlerin kimin tarafından ve ne zaman kaydedildiği bilgisine ulaşılır. Buradan “görevler ayrılığı” ilkesinin ihlal edilip edilmediği, kaydı giren kişinin ilgili işlemi yapmaya yetkili olup olmadığı saptanabilir.

Kayıt günlüklerinde yer alan diğer bir bilgi de kayıtlar üzerinde yapılan değişikliklere ait olanlardır. Ne tür değişiklikler yapıldığı, ilk kaydedilen bilginin ne olduğu, değişikliklerin kimin tarafından ve ne zaman yapıldığı bilgisine ulaşılır. Bu bilgiden yararlanılarak veritabanında yer alan bilginin doğruluğuna onay vermek mümkün olur.

İşlem madenciliği denetçinin “nasıl”, “kim” ve “neden” sorularına cevap arar. Bu sorular farklı kategorilerdeki yöntemlerle cevaplanır. Denetimde işlem madenciliği yöntemleri:

- İşlem kategorisi: İşlemin yapıldığı zaman ve yer kaydından “Bu işlem nasıl yapılmıştır?” sorusuna cevap aranır. İşlemin gerçekleştiği yer ve zaman iş sürecinde belirlenen, yani olması gerekenle karşılaştırılarak kontrol zaafaları tespit edilir.

- Organizasyonel yapı kategorisi: Kaydın kimin tarafından girildiğine ve/veya değiştirildiğine ilişkin bilginin incelendiği kategoridir. “Bu işlem kimleri kapsar?” sorusuna cevap aranır. Yetkili kişilerin ilgili kayıt üzerinde işlem yapıp yapmadığı incelenir. Görevler ayrılığı ilkesi ve yetkilendirme süreçleri denetlenir.
- Olay kategorisi: “İlgili işlemde ne oldu?” sorusuna cevap aranır. Bir işleme, yani olaya odaklanılır. Bu işlemin geçmişi ve ilgili kişileri arasındaki ilişkiler araştırılır. Bir işlemle ilgili farklı nitelikleri analiz etmek için kullanılır. Örneğin, sipariş miktarı ve ilgili siparişin satıcısı.

İşlem madenciliğinin denetimde kullanım alanları:

- İşlemi ortaya çıkartmak: Sistemdeki kayıtlara bakarak gerçekleşen işlemin özellikleri belirlenir, yani modeli ortaya konur. İşlem modeli öncelik sırasının belirlenmesi, paralellik oluşturma, eşzamanlı işlemlerin belirlenmesi, ayrıcalıklı seçimlerin ve döngülerin tespiti gibi yöntemlerle oluşturulur. Bu model işlemle ilgili belirlenmiş iş süreçleri ile karşılaştırılır. Yapılmaması gereken işlemler tespit edilir. Örneğin, onay alınmadan gerçekleşen satın almaların tespit edilmesi onay işleminin sistemde kayıtlı zamanı ile sipariş işleminin yapıldığı zamanı kontrol ederek yapılabilir. Yapılmaması gereken işlemler raporlanır. Ve/veya ilgili işlemin nasıl yapıldığına dair tespit edilen modeller kullanılma sıklığına göre tablolandır. Az sıklıkla tekrarlanan modellere ilişkin işlemlerde hata veya hile olduğu varsayımı ile denetçi bilgilendirilir.
- Uygunluk kontrolü: Uygunluk kontrolü önceden belirlenmiş iş süreçlerine ilişkin işlemler için yapılabilir. İşlemler tek tek ele alınarak önceden belirlenen modele uygun olup olmadığı tespit edilir. Uygunluk kontrolü üç analiz tekniği ile yapılır: durum uzayı analizi (state space analysis), yapısal analiz (structural analysis), günlüğü tekrarlama analizi (log replay analysis). Ayrıca, nadir görülen olaylar da bireysel bazda ele alınarak bu yöntemlerle iş süreçlerine uygunluğu kontrol edilebilir.
- Performans analizi: Performans analiz teknikleri kurumun iş süreçlerinin performansını ölçer. Süreçler ve önemli performans ölçütleri hakkında bilgi verir. Örneğin, belli bir sürecin tamamlanma süresi önemli bir performans ölçütü olabilir. Kayıt günlüklerinde yer alan zamanlardan yararlanılarak ilgili sürecin maksimum, minimum ve ortalama süreleri tespit edilerek o sürecin performansı ölçülür. Süreçlerin hızlı veya yavaş seyri yolsuzluk, hata veya kontrol zaaflarını işaret edebilir.

- Sosyal ağ analizi: Bu analiz bilgisayar sistemini kullanan kişiler üzerine yoğunlaşır. Çalışanlar bazında hangi işin kimden kaynaklandığı ve kaç defa yapıldığı raporlanır. Ayrıca, çalışanların oluşturdukları sosyal ağ denetlenir ve iş akışı yönetimi ile ilgili bilgi verir.
- Karar madenciliği ve doğrulama: Kayıt günlükleri işlemlerin tekrarlanma sıklıklarına göre incelenir. Tüm varsayımlar ve işlem özellikleri işlem bazında test edilir. Karar madenciliği ve doğrulama işlevi kayıt günlüklerindeki zaman ve kaydı giren kişi bilgilerinin dışındaki bilgileri de kullanır. Süreçlerdeki karar noktalarına odaklanır. Örneğin, sipariş fişi yaratma sürecinde “imza” veya “imzalamadan diğer işleme geçme” kararının hangi şartlarda verildiğini inceler. Makine öğrenimi (machine learning) algoritmalarını kullanarak bu karar noktalarının özelliklerini tespit eder. Karar madenciliği ve doğrulama bir tür uygunluk kontrolüdür. Ancak uygunluk kontrolünde olduğu gibi modelin tamamı ele alınmaz; sadece işlemin belli koşullara uygunluğu kontrol edilir. Algoritma işlemin koşula uygunluğunu kontrol eder. Bu tür analizin sonucu yoruma açık değildir. Sonuç ya “doğru” veya “hatalı” şeklindedir. Bu nedenle, doğrulama işlemi kesin sonuç barındırır. İşlemler ve ilgili süreçlere ilişkin iç kontrollerin doğru işleyip işlemediği kanıtlanmış olur.

7.2. FAALİYETLER VE SEKTÖR HAKKINDA BİLGİ VERİCİ ANALİZLER

7.2.1. Oran Analizi (ratio analysis)

Kurumun finansal tablolarında yer alan iki hesabın birbirleriyle oransal ilişkisini gösterir. Kurumun faaliyetleri ve performansı hakkında bilgi verir. Bu oranlarla bir denetim modeli geliştirilebilir.

Green ve arkadaşları 1997’de oran analizi ile bir denetim modeli geliştirmişlerdir. Bu modelde beş oran ve üç hesap kullanılmıştır.

Kullanılan oranlar:

şüpheli alacaklar karşılığı/net satışlar

şüpheli alacaklar karşılığı/alıcılar

brüt kar/net satışlar

alıcılar/toplam aktifler

Kullanılan hesaplar

net satışlar

alıcılar

şüpheli alacaklar karşılığı

Modelin performansının ve doğru tahmin yeteneğinin %32-%62 arasında değiştiğini tespit etmişlerdir.

7.3. ÇEŞİTLİ KONULAR İÇİN DİJİTAL TEKNİKLER

7.3.1. Otomatik Doğrulama (Automatic Confirmation)

Bilgilerini doğrulamak için kullanılan mektupla teyit alma şekli bilgisayar sistemleri kullanılarak da yapılabilir. Denetim programları hesap bakiyeleri gibi bazı bilgileri veritabanından alarak üçüncü şahıslara doğrulanması amacıyla elektronik ortamda gönderebilir. Gelen cevaplar sistemdeki verilerle karşılaştırılır. Farklılıklar detaylı incelemeye tabi tutulur.¹²⁷

Bazı araştırmacılar otomatik doğrulamanın gelecekte en önemli denetim kanıtı olacağını düşünmektedir.¹²⁸

7.3.2. Dijital Analizde Kullanılan Örneklem Yöntemleri

Üzerinde inceleme yapılacak örnek kayıtların seçimidir. Denetim programları çeşitli istatistiksel örneklem yöntemlerini kullanarak veya denetçinin vereceği ölçütleri değerlendirerek kayıtlar içinden örnek set oluştururlar. Bilgisayar tarafından yapılan bu seçim çoğunlukla hatalı veya hileli kayıtlara odaklanmayı sağlar, denetim zamanını kısaltır.¹²⁹

¹²⁷ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s. 81.

¹²⁸ Vasarhelyi, Alles ve Kogan, “Principles of Analytic Monitoring for Continuous Assurance”, s. 18.

¹²⁹ Coderre, Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide, s. 81.

8. SÜREKLİ DENETİM VE BİLGİ SİSTEMLERİ

8.1. SÜREKLİ DENETİMDE ÖNE ÇIKAN TEKNOLOJİK GELİŞMELER

Sürekli denetimin yapılabilmesi bilgi teknolojilerine bağlıdır. Bilgi teknolojilerini ilgilendiren her türlü gelişme sürekli denetim uygulamalarının gelişmesi ve yaygınlaşması yararına olacaktır. Bilgi teknolojilerindeki bazı unsurlar sürekli denetim için özellikle önem taşımaktadır.

8.1.1. Bilgi Girişi

Bilgisayar sistemlerine bilgi girişi en yaygın şekliyle klavye kullanılarak yapılır. Ancak, bazı durumlarda bilgi bir aygıt aracılığı ile bilgisayar sistemine direkt kaydedilir. Barkod okuyucuları, algılayıcılar, elektronik aygıtların çıktılarını bilgisayara kaydeden program ve ekipmanlar bilgi girişinde kullanılan donanımlardan bazılarıdır. Otomatik bilgi girişi hem hataları hem de zaman kaybını önler.

8.1.2. Veri Formatında Standardizasyon

Sürekli denetim sistemleri bilgiyi veritabanlarından alır. Kullanılan denetim programlarının denetim faaliyetini yerine getirebilmesi için ilgili veritabanının veri formatını tanınması gerekir. Denetim sisteminin veri formatı bilgi sisteminden farklı ise denetlenecek veriyi kendi formatına dönüştürmesi gerekir. Bu da bellek ve işlemci gibi sistem kaynaklarının daha çok kullanılması anlamına gelir. Veri formatının standardizasyonu farklı veritabanlarından gelen bilginin analiz edilmesini kolaylaştırır.

Son yıllarda XML (extensible markup language) veri formatı yaygınlaşmakta olup neredeyse bir standart halini almıştır. XML bir metin formatıdır. Hem insanlar hem de bilgisayarlar tarafından anlaşılabilir biçimde belgeleri kodlama kurallarını tanımlar. Metin belli işaretlerle etiketlenir. Bu etiketler metnin biçimini tanımlar. Yapısı basit, açık ve Internet kullanımına uygundur.

8.1.3. Veri Saklama

Sürekli denetim uygulamalarında saklanması gereken veri miktarı çoktur. Bunun nedenleri sürekli denetimde hedeflenen verinin tamamı üzerinde denetim yapılması ve bazı analizlerin geçmiş dönem verisine ihtiyaç duymasıdır. Denetimin başarısı incelenen veri miktarı ile doğru orantılı olarak artar. Sabit sürücü, bellek, CD, DVD, yedekleme üniteleri veri saklama aygıtlarıdır. Bu aygıtlara kaydedilebilecek veri miktarı teknoloji ile sınırlıdır. Teknoloji geliştikçe saklayabilecekleri veri miktarı da artmaktadır. Veri saklama teknolojilerindeki gelişme sürekli denetimin gelişmesi ve yaygınlaşmasını olumlu etkilemektedir.

8.1.4. Veri Ambarı (Data Warehouse)

Kurumsal veritabanından ilgili bilgi çekilerek yeni bir veritabanı yaratılır. Buna veri ambarı denir. Burada sadece denetimi yapılacak bilgi ve ilgili işlemler bulunur.

Veri ambarı yaratmanın amacı:

- Denetçiler ilgilendikleri veriye kolaylıkla ulaşabilirler. Gereksiz bilgi içinde zaman kaybetmezler.
- Denetçiler istedikleri formatta veriyi saklayabilirler.
- Denetçiler analizlerini kurumsal veriye zarar verme endişesi olmadan yapabilirler.
- Zaman serisi analizleri için eski dönemlere ait bilgiyi kolay ulaşılabilecek şekilde tutabilirler.
- Veri madenciliğini kolaylaştırır.

Veri ambarı yaratmak için aşağıdaki adımlar atılmalıdır:¹³⁰

1. Veri modeli: İhtiyaç duyulacak bilginin ne olacağı belirlenir.
2. Veri kaynakları: İlgili bilginin kullanıldığı kurumsal uygulamaların hangileri olduğu belirlenir.
3. Fiziki veritabanı: Bilginin bulunacağı veritabanının türü ve yapısı belirlenir.
4. Çekme ve dönüştürme: İlgili bilgiyi kurumsal uygulamalardan çekmek ve veritabanının yapısına uygun bir formata dönüştürmek için yazılım geliştirilir.

¹³⁰ Coderre, Internal Audit, s.52.

5. Veri ambarını doldurmak: Çekme ve dönüştürme işlemi yaparak veri ambarına veri yüklenir.
6. Kullanıcı araçları ve eğitim: Kullanıcıların kolayca işlem yapabilmeleri için kullanıcı araçları (sorgulama vb.) geliştirilir. Kullanıcılara ihtiyaç duyacakları eğitim verilir.

8.1.5. Bilgisayar Ağ Teknolojileri

Bilgisayar ağı (network) en az iki bilgisayar arasında bilgi paylaşımı yapabilen yazılım ve donanım topluluğudur. Bilgisayar ağı bilgisayarlar (sunucular, terminaller), çeşitli aygıtlar (modem, router vb.), ilgili yazılımlar (ağ işletim sistemi, paylaşımlı uygulama yazılımları, firewall vb.) ve bilgiyi aktarma ortamından (elektrik kablosu, fiber optik kablo, radyo sinyali, mikrodalga, kızılötesi) oluşur.

Aktarma ortamının kapasitesi, yani bir saniyede aktarabildiği bilgi miktarı bit olarak ölçülür. Her ortamın saniyede aktarabildiği bilgi miktarı birbirinden farklıdır ve bu alandaki teknolojik gelişmeyle doğru orantılı olarak bu miktar artmaktadır. Saniyede aktarılabilen en yüksek bit miktarı ağın bant genişliğini belirler.

Terminallerdeki kullanıcılar tarafından çalıştırılan tüm uygulama yazılımları ağ üzerindeki sunucular ve diğer terminaller arasındaki veri aktarımı için aynı bant genişliğini kullanırlar. Aynı zaman diliminde ne kadar çok uygulama çalıştırılırsa o kadar çok veri aktarımına ihtiyaç duyulur. Uygulamalar görevlerini tamamlayabilmek için diğer yazılımların daha önce vermiş oldukları komutların tamamlanmasını beklemek zorundadırlar. Bu nedenle ağ üzerindeki bilgisayarlar arasındaki her türlü veri aktarımı sistem üzerinde bir yükür ve çalışmasını yavaşlatır.

Gerçek zamanlı denetim uygulamaları sürekli veri aktarımını gerektirdiği için ağların bant genişliği çok önemlidir. Özellikle mesai saatleri içinde kurumsal uygulamalar yoğun olarak kullanılırken gerçek zamanlı denetim uygulamaları çalıştırmak ağa çok yük getirmektedir. Bant genişliğinin yeterli olmayışı birçok kurumda sürekli denetim faaliyetlerini aksatmaktadır. Bu alandaki teknolojik gelişmeler yönetimin sürekli denetime bakışını olumlu etkileyecektir.

8.1.6. Şifreleme

Bilginin bütünlüğünü korumak, yetkisiz kişilerce görülmesini ve değiştirilmesini önlemek için kullanılan teknolojilerden biri şifrelemedir. Şifreleme teknolojisindeki gelişmeler bilgi güvenliği açısından önemlidir.

İki tür şifreleme vardır:

- Yetkisiz kişilerce verinin görülmesini ve üzerinde herhangi bir değişiklik yapılmasını önlemek için veri bir anahtar ve bir algoritma kullanılarak şifrelenir. Örneğin, anahtar 128 bitten oluşan bir sayı olabilir. Şifrelenen veri orijinal metninden çok farklı harf ve sayılar haline gelir. Yeni biçimi insanlar tarafından anlaşılamayacağı için yetkisiz kişilerin eline geçmesi durumunda verinin kullanılması mümkün olmayacaktır. Verinin orijinal formuna dönmesi yalnız onu şifreleyen anahtar ve algoritma ile yapılabilir. Bu nedenle bazı kurumlar hassas bilginin şifrelenerek saklanmasını öngörürler. Yeterli zaman, teknik bilgi ve ekipman ile şifre kırılabilir. İlgili anahtarın kaç bitlik bir sayı olduğuna ve algoritmanın karmaşıklığına bağlı olarak şifrenin kırılması güçleşir.
- Kullanıcıların bilgisayar ağına bağlanabilmeleri için kullanıcı adı ve şifreye ihtiyaçları vardır. Şifre kişiye özeldir; ilgili kişiden başkasının şifreyi bilmemesi ve kullanmaması gerekir. Kullanıcı şifreleri kullanıcının kurumdaki görevini yerine getirebilmesi için gerekli bilgiyi görebileceği ve kullanabileceği kadar yetkiyi kapsar. Kullanıcı yetki sınırları içindeki bilgi üzerinde işlem yapabilir. Kullanıcı şifrelerinin ne zaman, hangi terminalden kullanıldığı ve yapılan işlemler sistem tarafından bir log dosyasında tutulur. Sürekli denetim sistemlerinin denetim kanıtları bulmak için incelediği log dosyaları bunlardır.

8.1.7. Yapay Zeka

Yapay zeka uygulamaları bilgisayarın insan gibi düşünme, mantık yürütme ve kendi kendine öğrenebilme yeteneği örnek alınarak geliştirilmiş yazılımlardır. Çok farklı türleri ve uygulama alanları vardır.

Yapay zeka uygulamaları denetçinin izleme ve analiz etme faaliyetini tanımlayabileceği ve kendi kendine karar verebilen, gerekli denetim modüllerini çalıştırabilen

programlardır. Sürekli denetim sistemlerinde denetim kanıtları toplarken ve yorumlarken sonuca ulaşmak için yapay zeka uygulamalarından özellikle aşağıdaki durumlarda yararlanır:

- Eldeki veri yeterli değilse ve boşlukları doldurmak için mantık yürütmek gerekiyorsa
- Sistemin veriyi değerlendirip kendi yaptığı değerlendirmeye göre otonom davranışlar sergilemesi bekleniyorsa

8.1.8. Karar Destek Sistemleri

Karar destek sistemleri (decision support systems) “karar verme” faaliyetinde kullanılan bilgisayar yazılımlarıdır. Kullanım alanları geniştir. Sağlıktan yönetime her konuda kullanım alanları vardır. Özellikle, karmaşık veri analizi gerektiren ve karar verirken belli bir konuda uzmanlık isteyen konularda kullanılır. Yazılım kullanıcının bilgisayarla iletişim kurduğu bir arayüz, veri havuzu, verinin ilgili konuyla ilişkisini gösteren modellerin yer aldığı “uzmanlık”, sistemin konu hakkındaki kararını sunduğu sonuç bölümlerinden oluşur. Karar destek sistemleri ‘akıllı’ seçimler yapsa da bir yapay zeka uygulaması değildir. Veri havuzu ve bu verinin kullanımına ilişkin kurallar çerçevesinde çalışır. Özgün düşünme yeteneği yoktur.¹³¹

Karar destek sistemleri doğru karar almayı kolaylaştıran ve çabuklaştıran yazılımlardır. Konu hakkında fazla bilgisi olmayan kullanıcıların bile bir uzman gibi etkin kararlar alabileceği bilgi kaynaklarıdır. Bu sistemlerin kullanımı daha hatasız, daha tutarlı ve daha tarafsız kararların alınmasını sağlamaktadır. Özellikle karar verme sürecinde yüksek hacimli veri kümelerinin analizi gerekiyorsa karar destek sistemleri etkin bir yardımcıdır.

Denetimde karar destek sistemlerinin kullanımı yaygınlaşmaktadır. Denetçiler birçok konuda karar destek sistemlerini kullanırlar. Riskleri tanımlamak, denetim stratejilerini geliştirmek, denetimi planlamak, kontrolleri değerlendirmek, kırmızı bayrakları incelemek için testler uygulamak, çalışma kağıtlarını düzenlemek, örnekleme kümesini belirlemek, analitik işlemler yapmak, beyin fırtınası, veride hile aramak ve belli bir konuda eğitim almak denetçilerin karar destek sistemleri kullanarak yaptıkları işlerden bazılarıdır.

¹³¹ Jagdish Pathak. Information Technology Auditing. Almanya: Springer, 2005:34.

Ekonomik, sosyal ve politik gelişmeler kurumsal riskleri de değişime uğratar. Belli bir zaman dilimindeki kurumsal riskler ele alınarak planlanan bir denetimde seçilen denetim testleri başka bir zaman diliminde geçersiz veya yetersiz kalabilir. Karar destek sistemleri değişen riskleri değerlendirip denetim testlerini yeni şartlara göre uyarlayabilir.

Karar destek sistemlerinin sürekli denetimde kullanılması denetime değer katacaktır. Sürekli denetim sistemleri gerçek zamanlı sistemler olduğu için karar destek sistemlerinin değişen risk türü ve seviyelerine denetim testlerini uyarlayabilme özelliği denetimin etkinliğini arttıracaktır.

8.1.8.1. Karar Destek Sistemleri İle Veri Madenciliği (Data Mining)

Veri madenciliği “veri yığınları içerisinde karar alabilmek için potansiyel olarak faydalı olabilecek, uygulanabilir ve anlamlı bilgilerin çıkartılması işlemidir”.¹³²

Veri madenciliği süreci:

- Sorunun tanımlanması: Veri madenciliği belli bir soruna cevap bulmak için kullanılır. Belli bir konuya odaklanılmış ve sorun açık bir dille ifade edilmiş olmalıdır. Sorunun iyi tanımlanmış olması araştırılan verinin özelliklerinin tam olarak tespit edilmesini sağlar.
- Modelin kurulması: Amaca uygun bir model tanımlanır. Model genellikle matematiksel bir fonksiyondur. Modelin etkinliği gerçek dünyadaki olayları açıklama yeteneği ve yanlış pozitif veya negatiflerin miktarı ile ölçülür. İdeal modele ulaşıncaya kadar veri hazırlama ve model kurma aşamaları tekrarlanır. Model ne kadar başarılı olursa olsun gerçek dünyadaki işlemlerin tamamını kapsayamaz. Bu nedenle işlemleri açıklayıcı özelliği belli sınırlar içindedir. Yanlış pozitifler gerçekte normal bir işlemi modelin olağandışı olarak tespit etmesidir. Yanlış negatifler ise modelin tespit edemediği anomalilerdir. Yanlış pozitiflerin veya negatiflerin fazla oluşu veri bütünlüğünün sağlanamamış olmasına veya modelin veriyi açıklamada başarısız olmasına bağlıdır. Kurumsal iş süreçlerine ve çeşitli dış etkenlere bağlı olarak verinin özellikleri veya kaynağı değişebilir. Bu durumda modelin doğru sonuç

¹³² Davut Pehlivanlı. Hile Denetimi Metodoloji ve Raporlama. İstanbul: Beta Basım, Ekim 2011:77.

vermesi için güncellenmesi gerekebilir. Zaman içinde kurulan modellerin izlenmesi ve değerlendirilmesi gerekir.

- Verinin hazırlanması: İstenen verinin veritabanında bulunması ve analiz edilmek üzere denetim yazılımına aktarılması işlemidir. Kaynak veritabanından çekilen ve analiz edilmek üzere başka bir yazılıma aktarılan verinin transfer sırasında tam ve doğru olarak aktarıldığından emin olmak gerekir. Farklı kaynaklardan alınan verinin uyumlu olmasına dikkat edilmelidir. Farklı veritabanlarından çekilen verinin uyumsuzluğu meta datasından, kodlamasından, kullanılan ölçü biriminden veya güncelleme hatalarından kaynaklanabilir. Analizlerin doğruluğu açısından veri bütünlüğünün sağlanması önemlidir. Analiz öncesi verideki uyumsuzluklar giderilmeli ve tek bir veritabanında birleştirilmelidir.
- Analiz: Yapılan analizler verinin model ile uyum derecesini belirler. Modele uymayan veri olağandışı olarak tanımlanır, hata veya hile unsurları aranır. Denetimde veri madenciliği birçok farklı dijital teknikler kullanılarak yapılabilir. Benford Kanunu bu tekniklerden en bilinenidir. Bazı hanelerin diğer hanelere göre daha fazla görülmesi veride tekrarlanan bir benzerliktir. Veri kümeleri içindeki şablonlar çoğunlukla iş kolu, ekonomik durum, kurum büyüklüğü gibi birçok nedenle kurumlar arasında farklılık gösterir. Ancak, Benford Kanunu'nun herhangi bir veri kümesine uygulanabilmesi denetçiler için büyük bir kolaylık yaratmıştır. İş kolu, kurum ve veri kümesi ne olursa olsun ilgili veri kümesindeki sayıların 1 ile başlama oranının %31, 9 ile başlama oranının %5 olduğu istatistiki olarak kabul görmektedir. Bu durumun kolaylıkla programlanabilir ve her tür veriye uygulanabilir olması ACL gibi denetimde kullanılan paket programlarda yer almasını sağlamıştır.

Veri madenciliği genellikle büyük hacimli veri yığınları için kullanılır. Veri miktarı büyüdükçe ilgili veriyi bulmak daha karmaşık hale gelmektedir. Karar destek sistemlerinin büyük ve karmaşık veri kümeleri içinde birbirine benzeyen veri, işlem ve süreçlerini ortaya çıkarma yeteneği denetçilerin en büyük yardımcısıdır.

8.1.8.2. Karar Destek Sistemleri İle Metin Madenciliği (Text Mining)

Metin madenciliği (text mining) veri madenciliğinin bir türüdür. Sadece sayı yerine metin içinde benzer şablonlar aranır. Bu teknik Internet'e, e-postalara, söyleşi grupları, finansal forumlara, bloglara, gazete ve dergi gibi basında yer alan metinlere uygulanabilir.

Denetimde metin madenciliğinin kullanımına ilişkin bazı örnekleri şöyle sıralayabiliriz:¹³³

- ATHENS anahtar kelimelerin tanımlanması ile Internet'te metin madenciliği yapan bir sistemdir. Kullanım alanı daha ziyade denetlenen kurumun müşterileri hakkında bilgi toplamaktır. Sistem Internet ve basında yer alan haberleri tarayarak müşteriler hakkında çıkmış haberleri derler.
- Keila ve Skillicorn 2005 yılında Enron'un e-postaları üzerinde metin madenciliği yapmışlardır. Yöneticilerin kelime seçimlerinin kurumsal değişimi gösterdiğini tespit etmişlerdir. Çalışanların kuruma bağlılıklarındaki azalmayı, yöneticilerin rollerindeki değişimi, risklere karşı alınan önlemlerdeki farklılaşmayı e-postalardaki kullanılan kelimeleri inceleyerek ortaya çıkarmışlardır. Kullanılan algoritmalar insan psikolojisi üzerine yapılan araştırmalara dayanır. Çalışmalar aldatıcı mesajlar yazan kişilerin olumsuz duyguları daha fazla dile getirdiğini, daha az birinci tekil şahıs ve daha fazla eylem ifade eden fiilleri kullandığını saptamıştır. İletişimde kullanılan yanıltıcı ifadeler hilenin göstergesi olarak kabul edilirse metin madenciliği hile tespiti için bir araç olarak görülebilir. Ayrıca, e-postalar üzerinde yapılan metin madenciliği ilgili kişinin belli bir konu veya hesaba ilişkin neler hissettiğini de açıklayabilir.
- Metin madenciliği sosyal ağların değerlendirilmesi için de kullanılmaktadır. Örneğin, Culotta ve arkadaşları 2004 yılında bir firmada çalışanların kimlere e-posta gönderdiklerini belirleyip Internet taraması ile bu kişilerin uzmanlık alanlarını bulan bir sistem geliştirmişlerdir. Bu sistem kurum içindeki e-posta kullanıcılarının her birinin oluşturdukları kendi sosyal ağ haritalarını çizmekte ve ilişkide oldukları kişilerin uzmanlık alanlarını göstermektedir. Araştırmalara göre sosyal ağlar kurumsal stratejiler ve karar süreçleri hakkında tahmin yapmamızı sağlamaktadır. Kişinin sosyal bağlantıları onun risk algılamasını şekillendirdiği için sosyal ağındaki değişim kişinin kararlarını da önceki dönemlere göre farklılaştıracaktır.

¹³³ James E. Hunton ve Jacob M. Rose. "21st Century Auditing: Advancing Decision Support Systems to Achieve Continuous Auditing", Accounting Horizons 24, 2 (2010):301-302.

8.1.8.3. Karar Destek Sistemlerinde Veri Profilleme Analiz Tekniğinin Kullanılarak Bilgi Sistemlerine İzinsiz Girişlerin Önlenmesi

Bilgi sistemlerine yetkisiz erişim gizliliğin ihlali ve veri bütünlüğünün kaybı ile sonuçlanabilir. Bu nedenle kurumlar çalışanlarına yetkileri sınırlandırılmış kullanıcı adı ve şifresi vererek bilgi sistemlerinin güvenliğini sağlamaya çalışırlar. Bu yetkiler çalışanların görevlerini yapmalarına yetecek ölçüde belli dosyalar ve alanlar üzerinde işlem yapmalarına olanak verir. Ancak, bazen çeşitli nedenlerle kullanıcılar görevleri dışında kalan işlemleri yapmak veya dosyalara erişmek isteyebilirler. Bilgi güvenliğini tehdit eden bu durumların gerçekleştiği sırada fark edilmesi ve önleminin alınması gerekir. Karar destek sistemleri ile izinsiz girişleri takip edebilecek sürekli denetim uygulamaları geliştirilebilir.

Bilgi sistemlerine izinsiz giriş yapmak olarak kabul edilen durumları aşağıdaki gibi sıralayabiliriz:

- Şifre tahmini (password guessing): Hedef alınan kişinin şifresini bulmak için sayısız denemeler yapılarak şifresi tahmin edilmeye çalışılır. Bu yöntemi kullanabilmek için kullanıcı adının bilinmesi gerekir. Şifre tahmini için sayısız karakter bileşimlerini deneyen yazılımlar vardır. Sistem belli sayıda hatalı giriş yapıldıktan sonra iletişimi kesse bile bu yazılımlar otomatik olarak sisteme yeniden bağlanıp denemelere devam edebilirler. Aynı kullanıcı için anormal sayıda birbirini ardına hatalı giriş yapılıyor olması o sırada şifre tahmini yapıldığını gösterir. Başarılı şifre yönetimi olan kurumlarda şifre kırmak daha zordur, ancak müdahale edilmezse imkansız değildir.
- Olduğundan başka kişi gibi görünmek (masquerading): Hedef alınan kişinin kullanıcı adı ve şifresi kullanılarak sisteme giriş yapılır veya kullanıcının sisteme bağlı olduğu hatta girilir. Böylece farklı bir kişi olarak sisteme kendini tanıtmış ve o kişiymiş gibi işlem yapmış olur. Burada amaç o kişinin dosyalarına girmek olabileceği gibi kişinin yetkilerini kullanarak sistemin başka taraflarına geçmek de olabilir. Kişinin her zaman kullandığı terminalden bağlanmaması, aynı anda farklı terminallerden aynı kullanıcının sisteme bağlanmış olması, sistemin normalden çok kullanılması, olağandışı saatlerde erişimin olması ilgili kullanıcıdan başka kişilerin aynı kullanıcı adı ve şifresiyle sistemi kullandıklarının göstergesidir.
- Göz atma (browsing): Kullanıcı yetki sınırlarını zorlar veya izinsiz işlemler yapar. Örneğin, görmemesi gereken bilgiye erişim sağlamak, kullanıcı yetkilerini arttırmak,

vs. Kullanıcı kendisiyle ilgisi olmayan dosyalara erişim sağlamaya çalışarak yetki sınırlarının ne olduğunu anlamaya çalışır. Erişim girişimleri tamamen deneyseeldir. Kullanıcının davranış profiline uymayan dosya ve komutları kullanması, çok sayıda engellenen dosya erişim istekleri ve çok sayıda yerine getirilmeyen komut ilgili kullanıcının göz atma faaliyeti içinde olduğunu gösterir.

Tablo 6

Bilgi Sistemine Yetkisiz Erişim Sağlamak İsteyen Kişilerin Yaptıkları Eylemler

Eylem (çok sayıda)	Şifre Tahmini	Olduğundan Başka Kişi Gibi Görünmek	Göz Atma
Sisteme girişler		X	
Geç girişler		X	X
Başarısız girişler	X		
Başarısız eylemler		X	X
Terminal kullanımı	X	X	
Dosya kullanımı		X	X
Başarısız dosya erişimi		X	X
Komut kullanımı		X	X
Başarısız komut kullanımı		X	X

Kaynak: Peter J. Best, George Mohay ve Alison Anderson. “Machine-Independent Audit Trail Analysis – A Tool For Continuous Audit Assurance”, *Intelligent Systems In Accounting, Finance and Management*. 12 (2004):92.

İzinsiz girişleri belirlemek için sistem faaliyetlerini denetlemek gerekir. İlgili denetim kanıtları alt seviye sistem faaliyetlerinden oluşur ve olay tabanlıdır. Örneğin, belli bir günde şifre tahmini yapılarak sisteme erişim sağlanmaya çalışıldığına dair denetim kanıtı o günkü hatalı şifre girişlerinin tümünü inceleyerek elde edilebilir. Bilgisayar sistemleri hatalı giriş yapan kullanıcıları raporlayabilir. Ancak, birçok kullanıcı çeşitli nedenlerle şifrelerini yanlış yazarlar. Giriş yapılan terminalin klavyesine alışık olmamak, yanlışlıkla bir harfe basmak, başka bir şifre ile karıştırmak gibi birçok nedenle hatalı girişler yapılır. Bu girişlerin çok azı şifre tahmini için yapılan rastgele girişlerdir. Her bir kullanıcının yaptığı hatalı girişin nedenini aramak çok zaman alır. Bu kadar alt seviye inceleme yapmak çok fazla denetçi zamanına ihtiyaç duyan ve etkin olmayan bir faaliyettir.

Bu tür işlemleri araştırmak için karar destek sistemleri geliştirilebilir. Her kullanıcının faaliyetleri ve bu faaliyetlerin sıklığı ile ilgili bilgi sistemde tutulur. Kullanıcı genel

kullanımına göre olağandışı işlemler yapmaya, normalde incelemediği kayıtlara bakmaya başlarsa sistem başka bir kişinin giriş yapmış olabileceği uyarısı verir.

Sisteme izinsiz girişlere ait denetim kanıtlarının bilgisayar tarafından otomatik olarak bulunmasına ilişkin ilk önemli çalışma 1987 yılında Denning tarafından yapılmıştır. Denning'in izinsiz giriş modeli altı bölümden oluşmaktadır:¹³⁴

1. Kullanıcılar
2. Sistem tarafından yönetilen kaynaklar (dosyalar, komutlar, aygıtlar, vb.)
3. Denetim kayıtları (sisteme giriş, bir dosyaya erişim gibi kullanıcıların yaptıkları işlemler, yani denetlenecek veri)
4. Profiller (kullanıcıların sistemi kullanırken yaptıkları işlemlerin özelliklerinin belirlendiği istatistiksel modeller)
5. Olağandışı işlemler (kullanıcının belirlenmiş davranış profiline uymayan işlemler)
6. Faaliyet kuralları (anomali tespiti, rapor hazırlama gibi belli bir durum oluştuğunda yapılacaklar)

İzinsiz girişlerin sistem tarafından tespit edilebilmesi için sistem tarafından tutulması gereken kayıtlar şöyle sıralanabilir: eylem tarihi ve saati, kullanıcı adı, terminal kodu, eylemin cinsi, eylemin başarılı veya başarısız olduğuna dair bilgi.

Denetim için veri olacak eylemler ise şöyle sıralanabilir: sisteme giriş, dosya yaratmak, dosya silmek, dosyanın adını değiştirmek, dosya okuma, dosya yazma, komut yerine getirme. Bilgisayar bu eylemleri analiz ederek o sırada izinsiz erişim faaliyeti olup olmadığını araştırır.

Kullanıcı davranışları genellikle istikrarlıdır. Kullanıcılar iş tanımları gereği çalıştıkları kurumlarda belli görevleri yerine getirirler. Bu nedenle günlük faaliyetleri çoğunlukla bir şablona uyar. Hafta sonu, ay sonu ve yılsonu bazı ek işler gerektirse de bunlar günlük iş programından küçük sapmalardır. Ayrıca, çalışanların tercihleri de belli davranış kalıplarını oluşturur - aynı bilgisayar terminalini kullanmak, benzer saatlerde e-posta okumak gibi.

¹³⁴ Best, Mohay ve Anderson, s. 89.

Çalışanların geçmiş davranışlarının gelecekte yapacaklarını büyük ölçüde açıklayabildiğini varsayarsak ilgili eylemlerde olağandışı bir durum olup olmadığının analizi için denetim verisini zaman serileri yöntemi ile değerlendirmek etkin bir istatistik tahmin yöntemidir. Geçmiş faaliyetlere bakarak kullanıcının her eylem için güven aralığı oluşturulabilir. Güven aralığının dışında kalan sayıdaki eylemler olağandışı durumları belirler.

Olağandışı durumlarda sistemin kime ve nasıl bilgi vereceğine ait kurallar önceden belirlenmiştir. Karar destek sistemi veritabanında faaliyet kurallarına ait bilgileri tutar. Olağandışı bir durum oluştuğunda önceden belirlendiği şekilde rapor düzenleyerek ilgili kişilere gönderir. Rapor formatı sadece bir uyarı mesajı olabileceği gibi resmi bir rapor formatında da olabilir. Bilgilendirme e-posta, cep telefonuna mesaj gönderme vb. şekillerde yapılabilir.

8.1.9. Uzman Sistemler

Uzman sistem (expert system) önceden programlanmış bir dizi kurallar sayesinde belli bir konuda karar alması için o konunun uzmanı olmayan kullanıcıya rehberlik eden bir bilgisayar yazılımıdır. Bu yazılımlar karmaşık ve uzmanlık isteyen sorunların çözümünde danışmanlık görevi görür. İlgi alanı bellidir ve sınırları çizilmiştir.

Uzman sistemler üç ayrı bölümden oluşur:

1. Bilgi tabanı (knowledge base): Özellikli bir veritabanı yapısına sahiptir. İlgili konuya ait tüm veri ve bu veriyi birbiriyle ilişkilendiren kural, mantık ve bağlantılardan oluşur. Bilgi tabanı örneği:

eğer yaşıyorsa öyleyse ölümlüdür

eğer yaşı biliniyorsa öyleyse doğum yılı = şu anki yıl - yaşı

2. Sonuç çıkarma motoru (inference engine): Bir bilgisayar yazılımıdır. Kurallar üzerinde mantık yürütür. Bilgi tabanından aldığı veri ve kurallar üzerinde mantık yürüterek yeni bilgi yaratır. Kendi veritabanında olmayan bilgiye ulaşması nedeniyle bir yapay zeka uygulamasıdır ve karar destek sistemlerinden bu yönüyle farklılaşır. Sonuç çıkarma motoru iki şekilde çalışır. Kullanıcı tüm bilgileri baştan verir veya sistem sonuca ulaşma sürecinde çeşitli sorular sorarak kullanıcının kendisini yönlendirmesini ister.

3. Konuşma motoru (dialog interface): Kullanıcının sistem ile iletişimini sağlayan arayüzdür. Kullanıcı bu arayüz ile sorularını sorar ve sonuç çıkarma motorundan gelen yeni bilgiyi görür.

Uzman sistemlerin kullanımı aşağıdaki adımlardan oluşur:

1. Kullanıcı bir konuşma motoru yardımıyla sorular sorar.
2. Sonuç çıkarma motoru bilgi tabanından ilgili veri ve kuralları çeker ve kendisine yüklenmiş mantık kurallarını uygulayarak bir sonuca ulaşır.
3. Sistem konuşma motoru aracılığı ile sonucu kullanıcıya iletir.

Uzman sistemlerin kullanılabilmesi için:¹³⁵

- tanımlanabilen bir sorunun olması,
- sorunun analitik yöntemlerle çözülebilmesi,
- sorunun sınırlı bir etki alanının olması,
- sorunun göreceli olarak sabit olması gerekir.

8.2. SÜREKLİ DENETİMDE KULLANILAN DENETİM YAZILIMLARI

Denetim yazılımları denetçilerin varsayımlarını modelleyebildikleri ve test edebildikleri uygulamalardır. Bu yazılımlar veri erişimini kolaylaştırır, birçok analiz tekniğini içinde barındırır, belirlendiği şekilde işlemleri tekrarlar ve istenen şekilde raporlama yapar.

Denetim yazılımlarının kullanıldığı alanlar:¹³⁶

- Dosyaları analiz etmek ve karşılaştırmak
- Belirli kayıtları seçmek ve inceleme yapmak
- İncelenecek örnek veri seti oluşturmak
- Hesaplamaları doğrulamak
- Doğrulama mektuplarını hazırlamak

¹³⁵ Coderre, Internal Audit, s.67.

¹³⁶ Frederick Gallegos ve diğerleri. Information Technology Control And Audit. 2. Basım. A.B.D.: CRC Press LLC, 2004:99.

Denetim yazılımları birkaç kategoriye ayrılır:¹³⁷

- Genel amaçlı denetim yazılımları: Bu tür yazılımlar programcıya ihtiyaç duymadan denetçinin kurumsal veritabanından bilgi çekebildiği ve temel denetim analizlerini yapabildiği uygulamalardır.
- Rapor üreten diller: Bu tür yazılımlar belli bir veritabanında sorgulama yapmak için kullanılırlar. Sorgulama dilleri de denir.
- Test verisi teknikleri: Yeni uygulanacak olan denetim modellerini test etmek için sisteme test verisi gönderilir. Test verisi analizlerin doğru çalışıp çalışmadığını kontrol eder.
- Özel amaçlı test ve analiz yazılımları: İşletim sistemi, log dosyaları gibi bilgisayar sistemine ait dosyaları denetlemek için kullanılır.
- Uzman sistemler
- Gömülü denetim uygulamaları: Kurumsal kaynak planlama yazılımının kodları içinde yer alan denetim modülleridir.

8.2.1. ACL

ACL yazılımı veri çekme ve bilgisayar destekli analiz tekniklerini içinde barındıran genel amaçlı bir denetim programıdır. Kanada kökenli bir yazılım şirketi olan ACL Services Ltd. tarafından geliştirilmiştir.

ACL denetim yazılımının birçok özelliği olmakla birlikte odaklandığı işlev veri analizini hızlı, etkin ve kapsamlı bir şekilde gerçekleştirmektir. Veri analizi planlama aşamasında konulan hedeflere ulaşmak ve tanımlanmış sorulara cevap bulmak için denetlenen veri üzerinde yapılan testlerdir.

ACL bir sürekli denetim yazılımı olmamakla birlikte kurumsal kaynak planlama yazılımı ile birlikte çalışabilir ve otomatize edilmiş denetim analizlerini belli süreçlerin bitiminde belli aralıklarla kendisi başlatabilir. ACL'in bu özelliği onu sürekli denetimde kullanılabilecek yazılımlar arasına sokmaktadır.

¹³⁷ Moeller, s. 487.

ACL denetim yazılımının öne çıkan özellikleri aşağıdaki gibidir:

Güçlü veri analizi yeteneği vardır:

Denetçi ACL'in güçlü veri analiz yeteneği ile aradığı cevapları bulabilir. ACL bir yapay zeka uygulaması değildir. Bir karar destek sistemi yapısında da değildir. Ancak, yazılımın parçası olan fonksiyonlar ve komutları kullanarak matematiksel formüller bilgisayara kolaylıkla tanıtılabilir.

ACL'in veri analiz yeteneği yazılımın parçası olan fonksiyonlar, komutlar ve komut satırlarından (scripts) sağlanır. Komut satırları (scripts) tekrar tekrar çalıştırılabilen komut dizileridir. Denetçi bu araçları birlikte kullanarak kurgulayabileceği tüm matematiksel modelleri veri analizinde kullanabilir. Denetçi sorularına cevap bulabileceği bir matematiksel model yaratabilirse bu araçları arka arkaya çalıştırarak denetim modelini yazılıma tanımlayabilir. Bir başka deyişle denetçi yalnızca kendi hayal gücü ve matematik bilgisi ile sınırlıdır.

Farklı veri tiplerini işleme yeteneği güçlüdür:

Denetçinin ihtiyacı olan bilgi farklı kurumlarda veya farklı veri tabanlarında olabilir. Bu da birçok sistem ve farklı veri tiplerinin kullanılması demektir. ACL yazılımı farklı veri tiplerini veri bütünlüğünü bozmadan kendi işleyebileceği fil uzantılı dosyalara kolaylıkla çevirebilir. ACL Microsoft Excel çalışma sayfaları ve Access tablolarından, eski düz dosyalara ve delimited dosyalara kadar hemen her dosya tipine erişebilir. ACL'in bu özelliği denetçinin denetlediği kurumdan ve onun bilgi işlem bölümünden destek alma ihtiyacını azaltmaktadır. Ayrıca, denetim süresini kısaltmakta ve denetçinin kullanacağı veri kaynakları konusunda esnek olmasını sağlamaktadır.

ACL'in kullanabileceği veri formatları aşağıdaki gibidir:

- Microsoft Excel, Microsoft Access, ve XML dosyaları: ACL Excel, Access ve XML dosyalarına doğrudan erişim için ActiveX Data Objects (ADO) adı verilen bir Microsoft teknolojisi kullanır. ACL ile bu dosyalara erişim için kullanıcı katkısına çok az gerek vardır.
- ODBC uyumlu kaynaklar: ACL birçok veri formatından kullanıcının çeşitli düzeydeki katkılarıyla tablolar yaratır. Veriyi özgün formatında kullanmak en ideal yöntemdir. ACL'in en az müdahale ile tanıyabildiği veri ODBC (Open DataBase Connectivity-Açık Veritabanı Bağlantısı) uyumlu kaynaklardan gelen veridir. ODBC bir başka Microsoft

teknolojisi. Günümüz veritabanı sistemlerinin çoğu ODBC uyumludur. dBASE dosyalar ODBC uyumlu veri kaynaklarıdır. dBASE ACL'in en hızlı ve kolay okuduğu formattır. Modern sistemlerin pek azı veriyi dBase dosyalarında tutmaktadır. Ancak, sistemlerin çoğu bu formata veri ihraç edebilmektedir.

- Flat (Düz) dosyalar: Bunlara tekst dosyaları da denilir. Düz bir dosyada sadece veri bulunur. Excel ve dBASE formatlarından farklı olarak düz dosyalarda alan tanımı bilgisi yoktur. ACL'in tablo düzeni yaratması için, ya dosyayı kullanıcının tanımlaması ya da dışsal bir tanım dosyası kullanması gerekir.
- Rapor (print-image) dosyaları: Kaynak veri dosyalarına doğrudan erişim imkanının olmadığı durumlarda ilgili veriye ilişkin bir rapor dosyasının elektronik kopyası da veri kaynağı olarak kullanılabilir. ACL rapor dosyalarını okuyabilir, ama tablo düzenini kullanıcının tanımlaması gerekir. Rapor dosyalarında genelde çoklu kayıt tipleri bulunur; bu kayıtlar kimi zaman bir satırı aşabilir. En yaygın tipleri detay, üst ve alt bilgi kayıtlarıdır. Her kayıt tipinde yaratılacak tabloya dahil edilmek istenilen bilgiler bulunabilir. Bu durumda, bu kayıt tiplerinin ACL'e tanıtılması gerekir.
- Delimited dosyalar: Delimited dosyalar genellikle metin satırında değişir uzunlukta bir kayıt olan dosyalardır. Bir kayıttaki alanları birbirinden ayırmak için virgül veya tab gibi özel karakterler kullanılır. Delimited dosyaların en yaygın kullanılan tipi CSV (virgülle ayrılmış değerler) dosyalarıdır.

ACL'in veri yapısı dosyalardan oluşur. Dosya tek başına saklanan ve işlenen veri bütünüdür. Kurumsal kaynak planlama yazılımından çekilen veri anlam bütünlüğünü koruyacak şekilde dosyalar halinde saklanır. Örneğin, cari hesaplara ait kayıtlar cari adı verilen dosyada, yevmiye dökümleri yevmiye adı verilen dosyada saklanabilir. Böylece denetçinin ilgili veriyi bulması kolay olur.

Kurumsal verinin bütünlüğü korunur:

ACL, kaynak veritabanından veriyi sadece okuma özelliği olan bir yazılımdır. Kaynak veriyi değiştirmez, silmez veya ekleme yapmaz. Bu nedenle bu yazılımın kullanımı kaynak verinin bütünlüğünü bozmaz.

Büyük dosyaların analizi çok hızlı tamamlanır:

Denetim binlerce kayıttan oluşan dosyalar üzerinde yapılıyor olabilir. Bir kurumun bir veya birkaç yıllık üretim bilgileri, muhasebe kayıtları, muhasebe işlemlerinin log dosyaları gibi veri kaynakları çok sayıda kayıt içeren dosyalardır. Büyük miktarlarda kaydın incelenmesini gerektiren durumlarda ACL denetim yazılımının analizleri hızlı yapması birkaç yönden önemlidir. Hızlı analiz yeteneği öncelikle denetim süresini kısaltır. Denetçi kısa sürede farklı sorgulamalar yaparak kararını oluşturacak analiz sayısını arttırır. Ayrıca, bu sayede denetçi örnekleme yöntemiyle çalışmak yerine dosyanın tümü üzerinde analizlerini yapabilir. Bu da analiz sonuçlarının doğru ve tamam olduğu konusunda güvenilirliği arttırır.

Analizler otomatikleştirilebilir:

ACL komutlarının etkileşimli veya sürekli çalışması sağlanabilir. Analizlerin otomatikleştirilmesi aynı denetim modelinin birden fazla kullanılması durumunda denetim süresini kısaltır, daha az emek harcanmasını sağlar. Analizlerin otomatikleştirilebilme özelliği ACL'in sürekli denetim uygulamaları geliştirmek için kullanılabilmesine olanak tanır.

Çalışmaların kaydı tutulur:

ACL'in kullanımı sırasında yapılan her işlem, analiz ve sonucu log dosyalarında tutulur. Log dosyası yazılımın otomatik olarak yarattığı bir kayıt izleme sistemidir. Denetçi gerçekleştirdiği işlemleri ve yapmış olduğu analizleri bu log dosyaları sayesinde kolaylıkla gözden geçirebilir. Analizlerin üzerinden geçerek denetim modelinde iyileştirmeler yapabilir. Sonuçları değerlendirerek yönetim kararlarına faydalı olabilecek yeni öneriler getirebilir. Log dosyaları denetimin dokümantasyonu sürecinde de yararlanılabilecek değerli bir kaynaktır. Atılan her adım tüm detayıyla bu dosyalarda yer aldığı için dokümantasyon sürecinde unutulmuş veya hatalı kaydedilen bir işlem olmayacaktır.

Denetçi önceki denetimlerde bulunan sorunları daha detaylı incelemek ve bu sorunların yönetim tarafından giderildiğine emin olmak isteyebilir. Başkaları tarafından yapılmış önceki denetimler hakkında bilgi almak için log dosyalarına başvurulabilir. Log dosyaları yapılan tüm işlemleri gösterdiği için önceki denetimlerde yapılan analizleri ve sonuçlarını izlemek kolaydır. Bu dosyalardan sorunlu alanları tespit edebilir ve denetimini planlayabilir.

Verinin analiz edilmek üzere ACL'e transfer edilmesi aşağıdaki şekillerde yapılabilir:

- Verinin bir kopyası alınır ve ACL'in okuyabileceği bir sürücüye koyulur. İlgili kişi veya bölümden kullanılacak verinin ACL'in okuyabileceği bir dosya yapısına transfer edilmesi istenebilir. Kaynak verinin bir kopyası ACL'in okuyabileceği bir formatta denetçiye verilir. Bazı dosya tiplerinde ACL'in veriyi yapılandırmak için kullandığı meta data vardır. Diğer dosya tipleri kullanıcı düzenlemesi gerektirir. Dosyanın büyüklüğü temin edileceği ortamı da belirler. Genelde dosyalar CD, DVD, Zip disk veya network sürücüsü yardımıyla okunabilir.
- Kaynak veriye erişim hakkı denetçiye tanınır. Ana makineye erişim için denetçiye kullanıcı adı ve şifre verilir. Doğrudan erişim yönteminde ACL veriyi ODBC veya ADO gibi veri erişim teknolojilerini kullanarak orijinal formatı içinde kaynağından okur ve verileri içeren yeni bir tablo yaratır.

ACL'in veri analiz yeteneği diğer denetim yazılımları arasında öne çıkmasını sağlamıştır. ACL'in analiz araçları ile olağandışı işlemleri tespit etmek, çift veya fazla ödemeleri belirlemek kolaydır.

Veri analizinin unsurları:

ACL'de veri analizi komutlar, ifadeler, fonksiyonlar ve değişkenler kullanılarak yapılır.

- Komutlar: İstatistikler, tabakalandırma, yaşlandırma gibi temel analizler komutlar kullanılarak yapılır. Sonuçlar bir dosyaya, ekrana, yazıcıya veya grafiğe gönderilebilir.
- İfadeler (expressions): İfadeler komutlar kullanılırken filtre ve/veya hesaplanmış alanlar yaratmak amacıyla kullanılır. ACL'de mantıksal, sayısal, tarih ve karakter olmak üzere dört tip ifade bulunur. İfadeler kullanılarak mantık koşulları belirlenebilir ve çeşitli hesaplamalar yapılarak veri dosyasında olmayan değerler yaratılabilir. İfadeler belli bir komut için tanımlanabilir veya daha sonra çeşitli komutlarla kullanılmak üzere bir isim verilerek saklanabilir.
 - Filtreler: Filtre analiz edilecek veriyi seçmek için kullanılan mantıksal bir ifadedir. Örneğin, belli bir zaman aralığındaki veriler incelenmek istenildiğinde tüm kayıtların taranıp sadece tarih alanı ilgili zaman aralığında olan kayıtların amacıyla seçilmesi gerekir. Bu işlem filtreler aracılığıyla gerçekleşir.

Üç tip filtre vardır:

Global: Global filtre görünüşteki veya analiz edilen kayıtları sınırlar. Bir kez oluşturulduğunda, silinene kadar aktif olarak kalır.

Komut: Komut filtresi tek bir komuta uygulanır. Böylece komut, bu filtre kriterini karşılayan kayıtlar için çalıştırılır. Komut bir kez çalıştırıldıktan sonra filtre etkisiz hale gelir.

Hızlı filtre: Hızlı filtre global filtreye işlevini görür. Bu seçenek ile filtrede kullanılacak mantıksal işlem türü hızlıca tanımlanır.

- Hesaplanmış alanlar: Hesaplanmış alanlar kaynak veri ve ifadeler kullanılarak yaratılan sanal alanlardır. Hesaplanmış alanlar ek veri oluşturmak amacıyla yaratılır. Bu alanlar sadece denetim yazılımının tablosunda mevcuttur ve kaynak verinin bir parçası değildir. Orijinal verileri değiştirmeden veri dosyasındaki bilgiler üzerinde hesaplar yapılmasına olanak veren bir alanlardır. Fiziksel olarak verinin içinde bulunmazlar. Örneğin, iki farklı alandaki verinin toplanarak yeni bir alan yaratılması hesaplanmış alandır. Hesaplanmış bir alan gerçek fiziksel alan gibi kullanılabilir. Hesaplanmış alanlar karakter, sayısal, tarih veya mantıksal değerler alabilir, koşullu ya da koşulsuz olabilirler.

Hesaplanmış alanların dört ana kullanımı vardır:

- Matematiksel hesaplamalar yapmak
- İlgili alanı bir veri tipinden bir başka veri tipine dönüştürmek
- Kelime ikamesi yapmak
- Doğru/yanlış testleri yapmak (filtreler)
- Fonksiyonlar: Fonksiyon veri üzerinde hesaplama yapan önceden tanımlı matematiksel ifadelerin yer aldığı bir rutindir. Fonksiyonlar değişkenler sayesinde kaynak veriyi girdi (input) olarak kabul eder.
 - Değişkenler: Değişkenler farklı veri veya değeri alabilen saklama birimleridir. Belirleyici isimleri vardır. Genellikle alacakları değer ile ilgili isimler verilir. Yazılımın çalışması sürecinde farklı değerler alır. Bu farklar girdi olan kaynak verinin değerinden kaynaklanabileceği gibi hesaplanan veri nedeniyle de olabilir. Değişkenler komutlar, ifadeler ve fonksiyonlarda kullanılır.

Sonuçların raporlanması:

ACL veri analizinden elde edilen sonuçların raporlanması ve destekleyici belgelerin yaratılması için raporlama özelliğine sahiptir. Rapor yapısı esnektir. Rapor düzeni istenildiği gibi formatlanabilir, rapor içeriği özet veya detaylı olabilir.

Raporlamada kullanılabilecek unsurlar aşağıdaki gibidir:

- Görüntüler: Bir tablo istenildiği gibi düzenlendikten sonra yazdırılabilir veya diğer uygulamalara ihraç edebilir.
- Grafikler: Bulguların görsel sunumu için analiz sonuçlarından grafikler yaratılabilir ve bu grafikler istenildiği gibi formatlanabilir, rapora eklenebilir.
- Sonuç tab'ı (Results tab): Sonuç tabındaki sonuçlar başka uygulamalara kolaylıkla kopyalayıp yapıştırılabilir.
- Log: Log veri analizi sürecinde yapılan tüm işlemleri, yani uygulanan komutları, kullanılan tabloları ve elde edilen sonuçları kaydeden ve gösteren bir ACL özelliğidir. Log bir raporlama aracı olarak kullanılabilir. Log öğeleri diğer uygulamalara kolayca kopyalanabilir. Uzun ve karmaşık analizlerde bazı komutların ya da sonuçların detayları log'dan takip edilebilir.

8.2.2. XBRL

XBRL (Extensible Business Reporting Language) farklı sistemlerden bilgi çekebilen, birbiriyle ilişkilendiren, standart formatta sunan bir raporlama yazılımıdır. 2000 yılında XBRL International Inc. çatısı altında toplanan bir konsorsiyum tarafından geliştirilmektedir. Bu konsorsiyumda muhasebeciler, denetçiler, iş hayatından kişiler, programcılar ve kanun koyucular gibi çok farklı mesleklerden ve kuruluşlardan kişiler bulunmaktadır.¹³⁸

İnternet tabanlı teknoloji standartları ile raporlama standartlarının birleşiminden oluşmuştur. Ana amaç finansal tabloların kolaylıkla üretilebilen, bilgisayarların da kullanabileceği standart formatta olmasını sağlamaktır. Elektronik raporlama formatları olan Web sayfaları veya PDF dosyalarından farklıdır. PDF dosyaları ve Web sayfaları insanların okuyabilmesi için tasarlanmışlardır. Ancak, XBRL bilgisayarların anlayabileceği bir rapor formatıdır. XBRL formatındaki veri kurum içi bilgisayarlar veya diğer kurumların

¹³⁸ XBRL ile ilgili bilgiye www.xbrl.org İnternet sitesinden ulaşılabilir.

bilgisayarları arasında anlam farklılığı olmadan ve bütünlüğü bozulmadan transfer olabilir, analiz edilebilir ve istenen formatta raporlanabilir.

XML (Extensible Markup Language) veri formatını temel olarak alır. XBRL XML formatındaki veriyi standart finansal raporlar halinde düzenler. XBRL ile hazırlanmış dosyalar diğer uygulamalar tarafından tekrar kullanılabilir. XBRL bilgiyi standart hale getirerek ilgili tarafların bilgi sistemlerinde kolayca tekrar analiz edilebilir hale getirmektedir. Örneğin, kurumsal bilgi XBRL'e dönüştüğü andan sonra bu bilginin tekrar sisteme girilmesi gerekmeden başka kuruluşlar tarafından analiz edilebilir. Böylece vergi beyannameleri, yasal raporlar ve denetim raporları ilgili kuruluşlar tarafından kolaylıkla değerlendirilebilir.

Taksonomi:

XBRL diğer yazılımlardan farklı olarak kendine özgü bir taksonomi kullanır. Raporlamada kullanılan bilgi kümeleri (finansal tabloları oluşturan hesaplar, dip notlar ve denetçi raporlarının içindeki öğeler) özelliklerine göre sınıflandırılmış ve bu yazılıma özgü isimlerle adlandırılmıştır.

XBRL'in taksonomisi ana hatlarıyla aşağıdaki gibidir:

- Temel özellikler: İlgili verinin temel özellikleri belirlenir. Sayı, tarih, metin veya başka bir cins mi olduğu, bilanço hesapları gibi belli bir tarihe mi yoksa gelir tablosu hesapları gibi bir döneme mi ait olduğu, genellikle borç hesabı mı yoksa alacak hesabı mı olduğu belirlenir.
- Etiketler (labels): Her farklı madde ayrı ayrı tanımlanır, yani etiketlenir. Örneğin, sıfır, artı ve eksi sayılar birbirinden farklı etiketler alır.
- Karşılaştırmalar (cross-references): Bir maddenin anlamını bulmak için çeşitli kurumlardaki kullanım alanları ile karşılaştırmalar yapmaktır.
- Hesaplamalar ve formüller (calculations and formulas): Farklı olayların birbirleriyle olan matematiksel ilişkilerini gösterir. Raporlanan öğelerin soyut ilişkileri tanımlanmış olur. Bu ilişkilerin geçerliliği çeşitli uygulamalar ile test edilebilir.
- Sunumlar (presentations): Sunumlar taksonomi içinde olmasa da XBRL farklı formatlarda sunumlar yapmayı desteklemektedir. Kullanıcıların ihtiyacı olabilecek temel sunum formatları yazılımın içinde bulunmaktadır.

Kurumsal veri XBRL'in taksonomisi ile eşleştirilerek yeniden tanımlanır ve kullanıma hazır hale getirilir. XBRL'in hazır olan taksonomisi bu yazılımı kullanacak kurum için yeterli

değilse veya bazı öğeleri yeterince ifade edemiyorsa, kurum kendi kullanımına göre taksonomiye ekler yapabilir.

XBRL'in özellikleri:

- Standart format: Standart taksonomi sayesinde finansal raporlama ile ilgili tüm işlemler standart normlarda sınıflandırılır. İşlemlerin ve süreçlerin tanımları standarttır ve bir kurumdan diğerine değişmez. Böylece kurumsal veriyi farklı insanlar farklı değerlendirmez. Bu da kurumsal verinin kolaylıkla anlaşılmasını ve analiz edilebilmesini sağlar. Finansal raporlamaya bir standart getirilmiş olur.
- Zamanlama: XBRL veriyi XML formatında ve XBRL taksonomisi ile sınıflandırılmış bir şekilde saklar. Bu bilgisayar sistemlerinin anında kullanabileceği bir format olduğu için verinin transferi, analizi, raporlaması ve denetimi çok kısa sürede yapılabilir. Bu özelliği XBRL'i sürekli denetimde kullanılabilecek bir yazılım haline getirmiştir.
- İçerik: Günümüz ticari yaşamında finansal raporlardan çok şey beklenmektedir. Gerçeğin doğru ve anlaşılır biçimde raporlanması esastır. Ancak bunu yaparken günümüz koşullarında açıklanan bilgi miktarı çoğalmış, konular ve detaylar artmıştır. Yüz sayfayı bulan finansal raporlar ve ilgili notlar içinden istenilen bilgiye kolayca ulaşmak mümkün değildir. XBRL yazılımında finansal tabloları araştırıp istenilen bilgiyi bulan bir araç vardır. Bu sayede kullanıcı istediği bilgiye hızlı bir biçimde ulaşp istediği formatta görüntüleyebilir.

XBRL'in faydaları:

- Finansal raporlarda bir standart sağladığı için ilgili kişi ve kurumlar tarafından kolayca ve doğru bir şekilde anlaşılmasını sağlar.
- Kurumsal veri hızlı, ucuz ve kolay bir şekilde kurum içinde veya başka kurumlar tarafından farklı uygulamalar veya analizler için kullanılabilir.
- Denetimi kolaylaştırır, hızlandırır. Denetçiler daha fazla kurumu aynı sürede denetleyebilirler.
- Raporlama ile ilgili görevler ve süreçler kısa sürede tamamlanır. XBRL kullanılan sistemlerde finansal raporlama hızlı ve etkin bir süreçtir.¹³⁹
- Verinin değiştirilmesini ve amacından farklı biçimde yorumlanmasını engeller.
- Elektronik ortamda raporlamayı kolaylaştırır.

¹³⁹ Nigel Matthews. "How Continuous Auditing and XBRL-GL Work Together to Provide Improved Business Value". (19 Mayıs 2008).

- Kurumun içinde bulunduğu sektörde standart uygulamalar gelişmesine yardımcı olur.
- Birçok önde gelen yazılım şirketleri tarafından desteklendiği için diğer kurumsal yazılımlarla birlikte kullanılabilir ve yeni işlevler eklenerek etkinliği arttırılabilir.

Standart format devlet kuruluşları için denetimde büyük kolaylık sağlamaktadır. Bu nedenle XBRL'in yaygınlaşmasını devlet kuruluşları da desteklemektedir. Amerika Birleşik Devletleri'nde başta Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü (The American Institute of Certified Public Accountants, AICPA) ve Sermaye Piyasası Kurulu (Securities and Exchange Commission-SEC) XBRL'in geliştirilmesi için çalışmaktadırlar. SEC XBRL raporlarını resmi raporlama olarak kabul etmekte ve XBRL kullanıcıları için standart raporlama ile içeriği aynı olan ayrı bir raporlama sistemi kullanmaktadır.

XBRL sadece Amerika Birleşik Devletleri'nde değil tüm dünyada uygulama alanı bulan bir yazılımdır. XBRL International Inc.'in birçok ülkede şubesi vardır. Bölgesel ofisler ilgili kişi ve kuruluşlarla bir araya gelip o bölgedeki kanun koyucuların da desteği ile bölgesel taksonomiye geliştirir, ülkenin kanun ve ihtiyaçlarına uygun rapor formatları hazırlarlar. Avrupa Birliği 2003 yılında XBRL'in Avrupa Topluluğu'nda kullanılması için Avrupa XBRL Projesi'ne 6. Çerçeve Programı'ndan bir milyon Avro fon sağlamıştır. İngiltere, İspanya, Almanya, Hollanda, Danimarka, İtalya, Belçika, İrlanda XBRL raporlamayı resmi kurumların desteğiyle kendi ülkelerinde yaygınlaştırma konusunda önemli çalışmalar yapmakta olan ülkelerdir.

8.2.3. R

R açık kaynak kodlu bir istatistik yazılımıdır. R bir programlama dili olmakla birlikte veri analizi için de kullanılmaktadır.

R çok geniş istatistiki (doğrusal ve doğrusal olmayan modelleme, klasik istatistik testleri, zaman serileri analizi, sınıflandırma, kümeleme vb.) ve grafik çizim teknikleri sunmaktadır. R bir programlama dili olarak tasarlanmış ve kullanıcıya yeni fonksiyonlar tanımlama olanağı vererek kullanıcının ilave özellikler geliştirmesine, veri analizi yapmasına ve ilgili grafikleri düzenlemesine olanak tanımıştır. R diğer birçok istatistiki hesaplama dilinden daha kuvvetli bir nesneye yönelik programlama kabiliyetine sahiptir.

R C, C++ ve Fortran programlama dillerini de otomatik olarak tanıyabilmektedir. Bu dillerle geliştirilen program modülleri R’da çalışabilmektedir. R’ın sağladığı bu esneklik yoğun hesaplama gerektiren ileri seviye kullanımlar için tercih nedenidir. Weka gibi bazı veri madenciliği yazılımlarında istatistiksel analizlerin R ile yapılmasını sağlayan bir arayüz bulunmaktadır.

R’ın açık kaynak kodlu oluşu bu yazılımın denetim faaliyetlerinde kullanımını arttırmaktadır. Yazılımın yaptığı hesaplamalar açık kaynak kodlarında kolayca takip edilebilir. Fonksiyon tanımlamadaki esnekliği, diğer yazılımlarla birlikte çalışabilmesi ve grafik sunum yeteneği de bu yazılımın kullanımını daha popüler hale getirmektedir.

9. LİTERATÜRDE SÜREKLİ DENETİM UYGULAMALARI

Sürekli denetim uygulamalarındaki zorluklara rağmen literatürde yer alan bazı başarılı örnekler vardır.

9.1. AT&T FATURALAMA SİSTEMİ

AT&T Bell Laboratuvarı'nın kullandığı faturalama sisteminin gerçek zamanlı denetlenmesi konusunu Vasarhelyi ve Halper 1991 yılında yayınladığı bir makalede incelemiştir. Kurulan sürekli denetim sistemine Sürekli İşlem Sistemi (Continuous Process System - CPAS) adını vermişlerdir. CPAS faturalama sisteminden veri alıp bu veriyi belli standartlarla karşılaştırdıktan sonra standartlara uymayan işlemlerde denetçileri uyaran ve denetim raporu hazırlayan bir sistemdir.¹⁴⁰

Sistemin gönderdiği uyarı mesajları dört çeşittir:

Tip 1: çok önemli olmayan, ama sistemin çalışmasına ilişkin anomalilerde gönderilir.

Tip 2: düşük seviye işletme yönetimine ilişkin anomalilerde gönderilir.

Tip 3: direkt olarak denetçilerin bilgilendirildiği önemli olağandışı işlemler olduğunda gönderilir.

Tip 4: denetçilerin ve üst yönetimin bilgilendirildiği kriz olarak kabul edilebilecek önemli sorunlar olduğunda gönderilir.

Ayrıca, CPAS'da denetçilerin sistemin faaliyetine ilişkin raporları inceleyebilecekleri, denetim uygulamalarını tekrarlayabilecekleri ve olağandışı işlemlere ilişkin tanımlamalar yapabilecekleri bir de arayüz programı bulunmaktadır.

¹⁴⁰ Baksa ve Turoff, s.6.

9.2. KANADA KRALİYET ATLI POLİSİ ÖDEMELER DEPARTMANLARI

Kanada Kraliyet Atlı Polisi 2004-2005 mali yılında yaptıkları ödemelere ilişkin finansal işlemlerin denetlenmesi için bir sürekli denetim sistemi geliştirmiştir.¹⁴¹

Kanada Kraliyet Atlı Polisi beş idari bölgeye ayrılmıştır. Polis teşkilatının satın aldığı mal ve hizmetlerin sayısı yılda 500.000 adet civarındadır. Bu mal ve hizmetlerin tutarı yaklaşık 1,5 milyar Kanada Doları'dır. Satın alınan mal ve hizmetlerin bedelleri bir merkezden yönetilen yedi ofis ve Kanada'ya dağılmış birçok ödeme noktasından oluşmaktadır.

Amaç:

Denetçilerin amacı tüm ödeme noktalarında yapılan finansal işlemlerin merkez ofisin belirlediği kurallarla ve yasalarla uyumlu olduğuna ve ödeme işlemlerine ilişkin kontrollerin etkin olduğuna dair güvence vermektir.

Kanada Kraliyet Atlı Polisi için geliştirilen sürekli denetim sisteminin riskleri ve kontrol zaaflarını tespit etmesi, performans ve etkinlik açısından trendleri incelemesi, anomali ve hileleri araştırması hedeflenmiştir.

Kapsam:

Ödeme ofislerinde ve noktalarında çalışan kişiler ödeme faaliyetine ilişkin birçok işlemde sorumludurlar. Alınan mal ve hizmet bedeli olan faturaların ve makbuzların ödenmesi, nakit kartların bedellerinin ödenmesi, bölümler arası hesaplaşma, personele yapılan ani ödemeler, seyahat masraflarına ait ödemeler yapılan işlerden bazılarıdır. Ayrıca, satıcılar ve polis teşkilatı içindeki diğer ilgili kişilerin sorularını yanıtlamak, ödemelere ilişkin sorunları çözmek, masrafları ilgili kebir hesaplarına göre sınıflandırmak, satıcı bilgilerini güncel tutmak ödeme noktalarında çalışan personelin sorumluluğundadır.

İş süreçlerinin tasarımının kalitesi ve personelin bu süreçleri uygulamadaki etkinlikleri satıcı ilişkileri ve nakit yönetimi üzerinde etkilidir. Kontroller, riskleri maliyeti kabul edilebilir bir seviyeye indirmeyi amaçlar. Bu nedenle kontrollerin tasarım kalitesi ödeme faaliyetinin maliyeti ile ilişkilidir.

¹⁴¹ David Coderre. "A Continuous View of Accounts". Internal Auditor. (Nisan 2006): 25-31.

Veri kaynağı:

Denetçiler ilk önce ödemelere ilişkin finansal kayıtların bulunduğu veritabanlarından ve insan kaynaklarına ait kayıtların tutulduğu veritabanlarından ilgili bilgiyi ayrı bir veritabanına çekerler. Böylece denetimin yapılacağı veritabanı oluşturulur.

Risklerin belirlenmesi:

Denetçiler kurumsal politikaları, çalışanlarla yapılan görüşmeleri, önceki dönemlere ait denetim sonuçlarını, Internet araştırmalarını da değerlendirerek yeni risk unsurlarını başlangıçtaki risk değerlendirmelerine eklerler. Ödeme noktalarını maliyet, kalite ve zaman tabanlı performans ölçütleri gibi çeşitli performans ölçütlerine göre birbirleriyle kıyaslarlar. Ödeme noktalarının personel maliyetini maliyet tabanlı performans ölçütü olarak alırlar. Fatura bazında yapılan ortalama hata sayısı verilen hizmetin kalitesini gösterdiği için kalite tabanlı performans ölçütü olarak kullanılır. Ödeme noktalarında uygulanan iş süreçlerinin etkinliğini değerlendirmek için fatura ödemelerinin ortalama kaç günde ödendiği gibi zaman bazlı ölçütler ele alınır.

Denetçiler yapılan işlemleri cinslerine göre gruplayarak analiz ettiğinde işlem tipine göre ödeme noktalarındaki operasyonel süreçler daha iyi anlaşılmıştır. Bu analiz denetçilerin çok sayıdaki işlem cinsi, işlem sayısı ve ödeme noktasından kaynaklanan karmaşık yapıyı anlamalarını ve risk değerlendirmesini yapabilmelerini sağlamıştır. Ayrıca, denetimde kayıtlara yapılan düzeltmelerle elle kesilen çekler kıyaslamıştır. Bu hem iş yükünü hem de riski arttıran bir faaliyettir.

İnsan kaynakları veritabanından elde edilen bilgilerle ödeme noktalarının organizasyon yapısı karşılaştırılmıştır. Raporlama yapısı, personel sayısı ve sınıflandırması, personelin ilgili işte çalışma yılı, personele verilen eğitim süreleri kıyaslanan ölçütlerden bazılarıdır. İnsan kaynakları veritabanından alınan bilgi ile yapılan işlem cinsleri ve miktarları risklerin belirlenmesinde kullanılmıştır. Örneğin, az sayıda ve yeterli eğitimi olmayan personel ile karmaşık ödeme işlemlerini gerçekleştirmeye çalışmak bir risk oluşturmaktadır.

Denetçiler yapılan işlemleri cinsleri, miktarları ve parasal değerleri açısından inceleyerek hangi işlem tiplerinin denetime dahil edileceğini tespit etmişlerdir. Ayrıca, genel

risk deęerlendirmesi ile hangi ödeme noktalarına gidilip yerinde inceleme yapılacağı tespit edilmiştir.

Kontrol deęerlendirmesi:

Kontrol zaafları risk seviyelerini yükselttięi için denetçiler kontrol zaaflarını tespit etmek istemişlerdir. Denetçiler ilk olarak ilgili yazılımı inceleyerek ödemeler modülündeki önemli kontrolleri tespit etmişlerdir. Daha sonra denetim yazılımını kullanarak bu kontrollerin tasarlandığı şekilde çalıştığını test etmişlerdir. Örneęin, denetim yazılımı kullanılarak ödeme görevinde çalışanların yaptıkları işlemler cinslerine göre incelenmiş ve görevler ayrılığı ilkesine ne derece uyulduğu belirlenmiştir. Yapılan dięer analizlerden bazıları: 5.000 Kanada doları üzerindeki faturalarda sipariş formu olması; satıcı bilgilerine ilişkin kayıtların sadece yetkili kişilerce deęiştirilebilmesi; teslim alınan, faturada yazan ve sipariş edilen miktarların aynı olması. Bu testlerin istendięi zaman tekrarlanabilmesi için denetçiler yazılım modülleri geliştirmişlerdir.

Performans deęerlendirmesi:

Performans ve etkinliğe ilişkin incelemeler için trend analizleri yapılmıştır. Örneęin, çalışanların işlem miktarları ve türleri ile operasyonel etkinlikleri ele alınarak ödeme noktalarının etkinlikleri kıyas edilmiştir. Denetim yazılımı etkinlik derecelerini hesaplamak için kullanılmıştır. Çalışanların işleme koydukları fatura sayısı, bir ödemeyi yapmanın ortalama maliyeti, ge ödenen faturaların oranı, erken ödenen faturaların oranı, tekrarlanan ödemeler, elle yazılan çeklerin oranı, 500 Kanada dolarının altında kalan ödemeler hesaplanan etkinlik ölçütlerinden bazılarıdır. Yılları kapsayan trend analizi sorunlu alanları ve yapılan iyileştirmeleri göstermiştir.

Anomaliler ve hile:

Bu uygulamada sürekli denetim sistemine ilave olarak beyin fırtınası teknięi ile anomaliler ve hile olasılığı olan işlemler tespit edilmiştir. Örneęin, denetçiler görevler ayrılığı ilkesine göre hareket edilmeyen ödeme noktalarında çalışanların bilgisayarda satıcı kaydı yaratabileceęi, sipariş fişi girebileceęi, fatura kesebileceęi ve ödeme yapabileceęi fikrini öngörmüşlerdir. Dięer bir deęerlendirme de ödeme noktalarının aynı faturaya çift ödeme yapabilecekleridir. Denetçiler beyin fırtınası sırasında ortaya atılan olasılıklara karşı otomatikleşmiş testler geliştirmişlerdir. Çift ödemelere, eski tarihli sipariş formları kaydedilmesine, limit politikasından kurtulmak için siparişleri bölmeye, kaydı ve ödemeleri

sadece bir çalışan tarafından satıcılara, kaydı ve onaylaması ve/veya ödemesi aynı kişi tarafından yapılmış işlemlere, aynı satıcının birden fazla kaydedilmesine ve bilgilerinin eksik olmasına karşı testler geliştirilmiştir. Gelişmeyi izleyebilmek için önceki dönemlerle karşılaştırmalar yapılmıştır.

Sonuç:

Denetçiler hileli işlemler tespit etmemişlerdir. Ancak, bazı kontrol zaafıları ve kurumsal politikalara uymayan uygulamalar tespit etmişlerdir. Satıcı kayıtlarında ve fatura girişlerinde hatalar tespit edilmiş, 100.000 Kanada Doları tutarında fazla ödeme iade alınmıştır. Satıcı tablolarının düzeltilmesi sayesinde çift ödemeler azalmıştır.

Sürekli denetim sisteminin faydalı bir yönü de denetçilerin yönetime yaptıkları önerilerin ne kadarının yerine getirildiğinin tespitidir. Örneğin, denetçiler 500 Kadana Doları altındaki satın alımların nakit kartları ile yapılmasının işlem maliyetini düşüreceğini öngörmüşlerdir. Altı ay sonra yapılan kontrolde küçük alımlarda nakit kartları kullanımının arttığını ve önerilerinin etkin biçimde uygulandığını görmüşlerdir.

Sürekli denetimin sonucu olarak ödeme noktalarında yapılan finansal hatalar, hile ve ziyan olasılığı azalmıştır. Ayrıca, ödeme noktalarının nasıl çalıştıkları daha iyi anlaşılmış ve farklı işlem cinsleri olduğu tespit edilmiştir. Bazı ödeme noktalarının etkinliği ve verimliliği yeterli bulunmamıştır.

Denetçiler veri analiz teknikleri kullanarak kontrol zaafıları ve merkez ofisinin belirlediği uygulamalarla uyumlu olmayan finansal işlemler tespit ettiler.

Çok sayıda ödeme noktasının olması denetimi zorlaştırmaktadır. Ancak, tüm finansal işlemlerin elektronik ortamda yapılması bilgi teknolojilerinin kullanılmasına imkan sağlamıştır. Böylece denetçiler riskleri değerlendirmek, önemli kontrolleri test etmek, hile zarar ve kötü kullanımı belirlemek için bir sürekli denetim sistemi kurabilmişlerdir.

9.3. SIEMENS'İN SAP GÜVENLİK AYARLARI

Siemens kurumsal kaynak programı olarak SAP kullanmaktadır. SAP sisteminin önemli güvenlik parametrelerini denetlemek için sürekli denetim sistemi geliştirilir.¹⁴² Bu sistem olağandışı durum tespit ettiğinde ilgili kişileri e-posta yolu ile uyaracak şekilde programlanmıştır. Sistem olağandışı durumları hiyerarşik bir yapıda tespit eder ve aynı konu ile ilgili yeni bir uyarı göndermeden önce denetçilere inceleme yapmak ve olağandışı durumu düzeltmek için belli bir süre tanımaktadır. Böylece denetçilerin uyarılara boğularak artık onları dikkate almayacakları bir duruma gelmeleri önlenmiş olmaktadır.

9.4. HCA INC. SÜREKLİ DENETİM UYGULAMASI

HCA Inc. sağlık sektöründe faaliyet gösteren, Amerika Birleşik Devletleri ve Avrupa'da 190'ın üzerinde hastane işleten bir kuruluştur. Denetim bölümü HCA bünyesinde yer alan çok sayıda ve farklı coğrafi bölgelerde faaliyet gösteren hastaneleri denetlemede yetersiz kalmıştır. Bazı hastanelere 3-4 yıllık aralarla denetim yapılabilmektedir. Denetim etkinliğini arttırmak için 2002 yılında iç denetim bölümü sürekli denetim uygulaması geliştirmiştir.¹⁴³

Etkin bir sürekli denetim uygulaması geliştirebilmek için yedi adımda çalışmalar yapılmıştır:

1. Yapılacak testleri belirlemek
2. Test yöntemlerini belirlemek
3. Test ölçütlerini belirlemek
4. Testleri otomatize etmek
5. Test sonuçlarının açıklanması
6. Geribildirim almak
7. Sürekli denetim sisteminden kazanımları takip etmek

Yapılacak testleri belirlemek:

Denetçiler, sürekli denetim sisteminin yapması gereken testleri iki ana kategoriye ayırmışlardır. Birinci test kategorisi direkt raporlama, ikinci test kategorisi ise dolaylı

¹⁴² Baksa ve Turoff, s.7.

¹⁴³ Lee Nelson. "Stepping Into Continuous Audit". Internal Auditor. (Nisan 2004): 27-29.

raporlamadır. Direkt raporlama sınıfına giren testler kesin olarak belli bir standardın ihlal edilmiş olduğunu gösteren olağandışı işlemlere ait olup ilgili kişi direkt olarak durumdan haberdar edilir. Örneğin, bir hesap bakiyesinin ay sonunda çıkartılan kebir hesaplarından farklı olması. Dolaylı raporlama kategorisindeki testler ise sürekli denetim sistemi tarafından tespit edilen olağandışı işlemlere ait analizin ilgili kişiler tarafından bitirilmesini gerektiren konulardadır. Örneğin, bir hastane bir varlığı satın alıp ondan hiçbir gelir elde edememişse bu olağandışı bir durumdur. Ancak, bu durum raporlanmadan önce gerçekten olağandışı bir durum olup olmadığının kararını ilgili kişinin vermesi beklenmektedir. Yani, bu durumda analizin bitirilmesi ilgili kişiye bırakılmaktadır. Bilgisayar sistemi raporlamayı ilgili kişi analizi bitirdikten sonra yapmaktadır.

Test yöntemlerini belirlemek:

İlk önce var olan sistemin içine denetim modüllerinin yerleştirilmesi düşünülmüştür. Ancak olağandışı durumları önlemek için sistemin içinde gerekli kontroller olması gerektiğinden bundan vaz geçilmiştir. Ayrıca, denetim modüllerinin kurumsal yazılımın içine konulması işinin bilgi işlemcilerin önceliği olmayacağı için yeterli desteğin alınamayacağı düşünülmüştür. Çeşitli önemli finansal göstergelerdeki trendlerin takip edilmesinin bir test yöntemi olacağı düşünülmüş, ancak HCA’de bu zaten yapılmakta olduğu için böyle bir çalışmanın tekrardan ibaret olacağı anlaşılmıştır.

Araştırmalar sonucunda kurumsal veritabanlarından çekilen veri üzerinde ilgili analizlerin yapılmasına karar verilmiştir. İşlemlerin izlenmesi, yapılan değişiklikler ve hesap bakiyeleri denetim yazılımı kullanılarak analiz edilmiştir.

Test ölçütlerini belirlemek:

Testlerin iki önemli ölçütü yerine getirmesi beklenmiştir. Testlerin belli bir denetim amacını gerçekleştirmeye yönelik olması ve yönetime net sonuçlar sunması gerekmektedir. Bu iki ölçütü yerine getiren testlerin sürekli yapılması denetim değerini ve etkinliğini arttıracığı öngörülmüştür.

Testleri otomatize etmek:

Hangi testlerin sürekli denetim sistemine uygun olduklarını tespit ettikten sonra test etme sürecinin otomatize edilmesi gerekmektedir. HCA denetçileri hazır paket programları inceledikten sonra onlardan birinin kullanımının yazılım geliştirmeye göre daha az maliyetli

olacağına karar vermişlerdir. İnceledikleri programların çoğunu hem işlevsel hem de \$100'ın altında fiyatlara satıldıkları için düşük maliyetli bulmuşlardır. Bu yazılımlar belli bir tarih ve saatte veya belli bir dosyanın varlığını tespit ettiği anda denetim testlerini başlatabilmektedirler.

Test sonuçlarının açıklanması:

Sürekli denetimin faydalı olabilmesi için olağandışı olarak belirlenen işlemler hakkında ilgili kişilerin bilgilendirilmesi gerekmektedir. Denetim sisteminin ilgili olağandışı durumu kime ve nasıl raporlanacağı tespit edilmelidir. Ayrıca, bu raporların gecikmeden ilgili kişiye ulaştırılması gerekmektedir. İlk önce e-posta yoluyla bilgilendirme yapılması düşünülmüştür. HCA yüzlerce hastane ve binlerce çalışandan oluşmaktadır. İşten ayrılma, transfer veya terfi gibi nedenlerle birçok çalışan yer değiştirmektedir. Denetçiler e-posta adreslerini güncel tutmak için çok zaman harcayacakları anlamış ve bu yöntemin uygulanabilir olmadığına karar vermişlerdir.

Denetçiler olağandışı işlemleri ilgili kişilere raporlamak için HCA'nın merkezi güvenlik yazılımını kullanmışlardır. Bu yazılım HCA'ya bağlı hastanelerin bilgisayarlarında bulunan uygulamaların güvenlik yönetiminden sorumludur. Her hastanenin kendi bünyesinde bulunan güvenlik koordinatörleri ile işbirliği yapılarak anabilgisayar kullanıcı adının hastanenin PC networkündeki kullanıcı adı ile eşleştirilmesi sağlanmakta ve e-posta adresi tespit edilmektedir. Denetim raporları bir Web sunucusunda tutulmaktadır. İlgili kişiye bu Web sunucusuna ulaşım mesajını okumasını bildiren bir e-posta gönderilmektedir. Kişi bu Web sunucusundan denetim raporuna erişebilmektedir. Denetim raporu Excel formatında olup istenirse kullanıcı tarafından kendi bilgisayarına indirilebilmektedir.

Raporlama yapılan kişiler iş tanımlarına göre tespit edilmiştir. Olağandışı durum hastaları ilgilendiren bir işlemde kaynaklanıyorsa hastaların kimlikleri ve/veya özel durumlarına ilişkin bilgilerin gizliliğine önem verilerek raporlama yapılmaktadır.

Geribildirim almak:

Rapor gönderilen kişiden geribildirim istenmişse, ilgili kişi Excel formatındaki denetim raporunun içine görüşlerini yazıp denetçilere e-posta yoluyla göndermektedir. Bu görüşler elektronik çalışma kağıtlarının içinde dosyalanmaktadır. Ayrıca, takibi gerektiren bir konu ise gelecekte de takip edilmek üzere dosyalanmaktadır.

Geribildirimler iki türlü olmaktadır. Ya alınacak önlemler veya olağandışı işlemin gerçekleşmesinin geçerli nedenleri konusunda bilgi verilmektedir.

Sürekli denetim sisteminden kazanımları takip etmek:

HCA sürekli denetim sistemi olağandışı işlemlerin raporlanması üzerine kurulmuştur. Olağandışı durumların zaman içinde azalmış olması sistemin faydalı olduğunun kanıtı olmuştur. Ayrıca, potansiyel uygunluk sorunlarına karşı yapılan analizlerde sürekli denetim sisteminin etkinliği ölçülmektedir.

Yöneticilerden gelen istek üzerine sürekli denetim sisteminde yer alan testleri kendi bölümlerini ilgilendiren işlemler üzerinde uygulayabilmeleri için bir link verilmiştir. Bu linkten giren yöneticiler istedikleri parametreleri seçerek kendi denetimlerini yapabilmektedirler. İstenen testler günde beş kez tekrarlanmakta ve test sonuçları Web sunucusuna gönderilmektedir. Sistem denetim yapıldıkça ilgili kişiyi e-posta yolu ile bilgilendirmektedir. Bu sistem yöneticilerin sorunları daha hızlı çözmelerini sağlamıştır.

Tablo 7
Sürekli Denetim Uygulamalarının Karşılaştırılması

	AT&T	Kanada Kraliyet Atlı Polisi	Siemens
Amaç	Büyük kağıtsız faturalama sisteminin denetlenmesi	Yapılan ödemelerin kontrollerinin değerlendirilmesi	Kurumsal kaynak planlama yazılımının güvenlik parametrelerinin izlenmesi
Onaylama motoru	Önceden belirlenmiş sistem kuralları	Ödeme noktalarındaki maliyet, kalite ve zaman temelli performans ölçütlerinin karşılaştırılması	Siemens'in bilgisayar güvenlik politikaları
Veri	Faturalama sisteminden çekilir	Finans ve insan kaynakları sistemlerinden çekilir.	Kurumsal kaynak planlama yazılımının güvenlik tablolarından çekilir.
Alarm	Tip 1: ikincil sistem sorunları Tip 2: operasyon yönetimi Tip 3: yüksek seviye olağandışı durumlar denetçilere bildirilir Tip 4: çok önemli krizler, denetçilere ve üst yönetime bildirilir	Yok.	E-posta yoluyla gönderilir, hiyerarşik yapıya sahiptir.

Kaynak: Robert Baksa ve Murray Turoff. "The Current State of Continuous Auditing and Emergency Management's Valuable Contribution", 7th International ISCRAM Conference. Seattle, ABD: Mayıs 2010.

9.5. T.C. SAYIŞTAY BAŞKANLIĞI BİLGİSAYAR DESTEKLİ DENETİM SİSTEMİ YAZILIMI PROJESİ

2010 Haziran’ında başlayan ve yazılım çalışmaları devam eden Sayıştay Başkanlığı Bilgisayar Destekli Denetim Sistemi Yazılımı Projesi sürekli denetim yolunda Türkiye’nin kat ettiği yolu göstermesi açısından önemli bir projedir. Gerek etki alanının büyüklüğü gerekse Sayıştay’ın yapacağı denetimlere getireceği yenilikler açısından bakıldığında Türkiye’nin en büyük denetim projesi olarak kabul edilebilir. TÜBİTAK UEKAE, Marmara Üniversitesi ve Komtaş Bilgi Yönetimi tarafından üstlenilen bu çalışma aynı zamanda bir Ar-Ge projesidir.

Amaç:

Sayıştay TBMM adına kamu dış denetimini anayasa ve kanunlarla kendisine verilen inceleme, denetleme ve raporlama görevlerini yerine getiren bir kamu kurumudur. Sayıştay merkezi yönetim bütçesi kapsamındaki kamu idarelerini, sosyal güvenlik kuruluşlarını, mahalli idareleri, kuruluş kanunları veya diğer özel kanun hükümleri gereğince Sayıştay denetimine tabi kurumları, döner sermayeleri ve fonları denetler. Bu projenin amacı Sayıştay Başkanlığı’nın denetim faaliyetlerini destekleyen bir yazılım geliştirmektir.

Kapsam:

Yazılımın kullanılacağı alanlar Sayıştay Başkanlığı’nın denetim faaliyetlerinin tümünü kapsamaktadır. Denetlenen kuruluşların çeşitliliği ve sayıları göz önüne alınacak olursa geliştirilmekte olan yazılımın binlerce kişinin yapacağı birçok farklı konudaki milyonlarca işlemi denetleyeceği açıktır. Dolayısıyla geliştirilen yazılımın farklı tipteki ve yüksek miktarda işlemleri analiz edebilmesi gerekmektedir.

Veri kaynağı:

Yazılımın veri kaynağı Sayıştay Başkanlığı’nın denetlediği kurum ve kuruluşlardan ilgili kanunun öngördüğü tarihlerde gönderilen ve denetlenecek işlemlerin yer aldığı dijital dosyalardır. Birçok işlemin bilgisayar ortamında gerçekleşmiş olmasından dolayı denetlenecek veri dijital formatta yer almaktadır. Kurumlar tarafından gönderilecek dosya tipinin XML veya metin (text) olması kararlaştırılmıştır. Yazılım sadece bu formatlardaki veri dosyalarını okuyabilecek şekilde tasarlanmıştır.

Kurumların hangi tarihlerde denetime konu olan veriyi Sayıştay Başkanlığı'na gönderecekleri ilgili yasa ve yönetmeliklerle belirlenmiştir. Dolayısıyla veri akışı sürekli değildir. Yazılım tarafından analiz edilecek veri belli bir dönemi kapsayan işlemlerden oluşmaktadır. Şu anki mevzuat işlemlerin gerçekleştiği anda denetiminin yapılmasına uygun değildir. Bu nedenle sürekli denetimin tanımında yer alan “gerçek zamanlı denetim” kavramının bu projede uygulanması kanunlar değişmediği sürece mümkün değildir.

Denetim sisteminin aşamaları:

Veri erişim süreci: Denetlenecek kurumlardan denetimi yapılacak işlemleri içeren kaynak veri dosyaları alınır. Bu dosyalar belli bir dosya tipinde (XML veya metin) ve daha önce belirlenmiş bir şablona uygun olarak düzenlenmiş olmalıdır. Kaynak veri sisteme yüklenir. Bu süreçte veri bütünlüğü kontrol edilerek denetime hazır hale getirilir.

Denetim yönetim sisteminin belirlenmesi: Bu aşama, Sayıştay Başkanlığı'nda görevli denetçilerin görev yetki ve sorumluluklarına uygun şekilde yazılımın erişim ve yetkilendirmeye ilişkin yapısının düzenlenmesini içerir. Sisteme kimin tarafından hangi görevlerin yerine getirileceği bir zaman planı çerçevesinde tanımlanır. Denetçiler yapmaları gereken işlemleri sistemden takip ederler.

Denetim süreci: Denetçi sisteme girdiğinde kendine atanan işleri görür ve tercih ettiği analizleri yapar. Konuların çeşitliliğini göz önüne alarak şu aşamada dijital analizlerin seçimi denetçiye bırakılmıştır.

Raporlama: Denetçilerin analizler sırasında tespit ettikleri olağandışı işlemler ilk amirleri olan ekip şeflerine raporlanır. Rapor formatları Sayıştay Başkanlığı'nın standartları göz önüne alınarak hazırlanmıştır. Nihai denetim raporunun sistem tarafından otomatik olarak hazırlanması planlanmamıştır. Raporlama analiz bulgularının bildirimi amaçlıdır.

Projede kullanılan dijital analiz teknikleri:

Sayıştay Başkanlığı ile yapılan görüşmeler sonucunda ihtiyaç duyulan dijital analiz teknikleri belirlenmiştir. Karşılıklı hesapların kontrolü, tarih ve limitlere ilişkin geçerlilik kontrolü, birlikte çalışması gereken ve birlikte kullanılmaması gereken hesapların kontrolü gibi konular ve veri bütünlüğünü değerlendiren analizler projeden beklenen incelemelerin temelini oluşturmaktadır.

Projenin sürekli denetim boyutu:

Yazılım daha ziyade bilgisayar destekli denetim tekniklerini kullanan bir denetim sistemini andırsa da özellikle SGK'nın sağlık harcamalarının (ilaç harcamaları gibi) denetimi için düşünülen analizler sürekli denetime yakın bir sistemin geliştirildiğini göstermektedir. Veri kaynağına erişimin büyük ölçüde dönemsel oluşu denetimin gerçek zamanlı yapılması önünde bir engeldir. Ancak, geliştirilen sistemin üzerinde çalıştığı verinin ontolojik yapısı denetlenen işlemle ilgili iş süreçlerini, kişileri ve olayları da incelemeye almaya olanak tanımaktadır. Sistem sadece işlemi değil, işlemle bağlantısı olan diğer işlemleri, kişileri, kurumları ve durumları da veri olarak alır ve ileri istatistik uygulamaları ile hata ve hile olasılığını inceler. İhtiyaç duyduğu veriyi otomatik olarak farklı bilgi kümelerinden alıp analiz etme yeteneği bir akıllı teknoloji uygulamasıdır. Bu bağlamda projenin bir bölümünün sürekli denetim uygulaması olduğu kabul edilebilir.

10. UYGULAMA

10.1. GENEL BİLGİLER

10.1.1. Konu: Araç Takip Sistemlerinin Üretimine İlişkin Satın Alma Döngüsünün Sürekli Denetimi

Bu bölümde yer alan Türkiye uygulamasının konusu bir kurumun bir bölümünü ilgilendiren satın alma döngüsünün sürekli denetimidir. Verisi incelenen bölüm araç takip sistemleri üretmektedir.

Sürekli denetim uygulaması ACL yazılımı kullanılarak geliştirilecektir.

10.1.2. İlgili Kurumun Tanıtımı

Bu bölümde verisi incelenen kurum bir anonim şirkettir. 1978 yılında Ankara’da kurulan bu anonim şirket 1987 yılında şirket merkezini İstanbul’a taşımıştır.

Kurum iki ana konuda faaliyet göstermektedir. Bunlardan birincisi yangın söndürme, kurtarma, güvenlik araç ve gereçleri imalatı, diğeri ise bilişim alanındadır. Kurumun bilişim alanındaki faaliyetleri temsilcisi olduğu bilgisayarların ithalatı ve satışı ile teknoloji projelerine özel amaçlı yazılım ve donanım üretmektir.

Kurum müşterilerine anahtar teslim çözümler sunmaktadır. Projelendirme, modelleme, simülasyon, montaj ve satış sonrası servis bünye içinde yapılmaktadır. Kurum konusu ile ilgili bazı yabancı firmaların Türkiye temsilcisidir. Ayrıca, çeşitli yerli ve yabancı firmalarla çözüm ortaklığı yaparak uluslararası bir hizmet ağı üzerinden faaliyet göstermektedir.

Müşteri profili ağırlıklı olarak kamu sektörü, askeri birimler ve belediyelerdir. Özel sektörde de önde gelen firmalara projeler yapılmıştır.

Faaliyet alanlarında öncü konumda olan kurum her yıl büyüme kaydetmiştir. Kurumun başarısı satış rakamlarından görülmektedir.

Kurumun 2011 yılı satışları:

yurt içi:	15.691.000 TL
yurt dışı:	432.000 TL
toplam:	16.123.000 TL

Kurumun 2012 yılı satışları:

yurt içi:	26.446.000 TL
yurt dışı:	1.655.000 TL
toplam:	28.101.000 TL

Kurum faaliyetlerini toplamda 92 kişinin çalıştığı Ankara ve İstanbul'da bulunan ofis, üretim, servis ve depo amaçlı kullanılan on mekanda sürdürmektedir.

10.1.3. Araç Takip Sistemleri Hakkında Genel Bilgiler

Kurum birkaç yıl önce teknoloji projelerine yeni bir çalışma alanı eklemiş, araç takip sistemleri konusunda anahtar teslim proje çözümleri sunmaya başlamıştır.

Araç takip sistemlerinin çalışma mantığı küresel yer belirleme uydularından alınan gerçek zamanlı konum, hız, yön gibi verileri GSM şebekeleri üzerinden GPRS aracılığı ile kontrol merkezine gönderilmesi esasına dayanır. Kontrol merkezi özel bir yazılım ile gelen verileri işler, haritalar üzerinde kullanıcının anlayacağı şekilde görüntülenmesini sağlar. Takip edilen araçtan gelen veriler çeşitlendirilebilir. Kullanılan cihazın özelliklerine bağlı olarak konum, hız, yön gibi verilerin yanı sıra eklenen algılayıcılarla yüzlerce verinin kullanıcıya ulaşması sağlanabilir.

10.1.4. Araç Takip Projeleri Hakkında Genel Bilgiler

Kurum, araç takip sistemleri projelerini üç bölüme ayırmaktadır: cihazın üretimi, yazılım, montaj. Teknolojisi tamamen kuruma ait olan cihaz çeşitli mekanik ve elektronik parçalardan oluşmaktadır. Bu parçalar tedarikçilerden satın alınıp kuruma ait bir atölyede birleştirilmektedir. Yazılım kuruma bağlı çalışan uzmanlar tarafından geliştirilmiştir. Temel işlevi GPRS aracılığı ile gelen bilgiyi Google'dan satın alınan haritalar üzerine yerleştirmektir.

İstenirse araç ve taşıdığı mala ilişkin bilgiler de görülebilmektedir. İmalat süreci tamamlanan cihazlar atölyenin deposundan alıcı kuruluşun belirteceği adreste bulunan araca gönderilir ve monte edilir. Yazılım alıcı kuruluşun kontrol merkezine yüklenir. Cihazlar ve ilgili yazılım çalışır durumda teslim edildiğinde proje tamamlanmış kabul edilir.

10.2. SATIN ALMA DÖNGÜSÜ VE DİJİTAL ORTAMDA DENETİMİ

10.2.1. Satın Alma Döngüsünün Tanımı

Satın alma süreci çeşitli mal ve hizmetlerin işletme dışındaki üçüncü kişilerden satın alınmasına yönelik işlemlerin bütünüdür. Bu mal ve hizmetlerin karşılığı olarak yapılan işlemler de ödeme sürecini meydana getirir. Satın alma süreci mal ve hizmet alımı ile başlar ve ödeme ile sona erer. Bu nedenle bu süreç çoğu zaman satın alma ve ödeme süreci olarak anılır.

Üçüncü şahıslardan satın alınan mal ve hizmetlerin başlıcaları aşağıda sıralanmıştır.¹⁴⁴

- Ticari mal
- İlk madde ve malzeme
- Yardımcı malzemeler ve işletme malzemeleri
- Maddi Duran Varlıklar
- Maddi Olmayan Duran Varlıklar
- Pazarlama ve satış ile ilgili alınan mal ve hizmetler
- Yönetim faaliyetleri ile ilgili alınan mal ve hizmetler
- Araştırma ve geliştirme ile ilgili alınan mal ve hizmetler

10.2.2. Satın Alma Süreci

10.2.2.1. Satın Alma Sürecinin İşleyişi

Tipik bir satın alma süreci aşağıdaki gibidir:

1. Satın alma talebi: Üretim gibi ilgili bir bölüm mal veya hizmetin satın alınmasını talep eder. Satın alma işlemleri bir merkezden yapılıyorsa satın alma talebi Satın Alma

¹⁴⁴ Nejat Bozkurt, Muhasebe Denetimi. 3. Basım. Türkiye: Alfa Basım Yayın Dağıtım Ltd. Şti., 2000, s. 279.

Bölümü gibi ilgili bölüme gönderilir. Bazı kurumlarda veya özellikli mal ve hizmetler için satın alma işlemlerini her bölüm kendi yerine getirir. Bu durumda satın alma talebi bölüm içindeki ilgili kişiye gönderilir. Satın alma taleplerinin direkt olarak onaylayacak kişiye/bölüme gönderildiği kurumsal süreçler de olabilir.

2. Onay: Satın alma talebi ilgili kişi veya bölüm tarafından onaylanmalıdır. Onay süreci alınacak malın/hizmetin özelliklerine ve bedeline göre değişebilir. Örneğin, bazı alımları bölüm müdürünün onaylaması yeterli olurken yüksek bedelli olanları genel müdürün onaylaması kurumsal tercih olabilir.
3. Satın alma emri: Satın alma talebi onaylandığında satın alma işlemini yapacak kişi veya bölüme satın alma emri gönderilir.
4. Satıcı tercihi: İlgili kişi/bölüm alınacak malın/hizmetin niteliğine ve bedeline göre kimden satın alma işlemini gerçekleştireceğini belirler. Satıcılar genellikle kalite ve fiyat avantajlarına göre tercih edilir. Kurumun önceden yapmış olduğu anlaşmalar ve almış olduğu temsilcilikler satıcı tercihinde rol oynayabilir.
5. Satın alma yöntemi: Malın/hizmetin özellikleri gereği belli bir satıcıdan temin edilmesi gerekiyorsa o satıcı ile direkt temasa geçilir. İlgili malın/hizmetin birden fazla satıcısı olması durumunda teklif toplama veya ihale açma gibi yöntemler kullanılır. Bedeli yüksek olmayan mal/hizmetler için veya yüksek seviyede güvenilirlik gerektiren durumlarda daha önceden çalışılmış satıcılar tercih edilebilir.
6. Sipariş: Satıcıya ilgili mal/hizmetin özellikleri, miktarı, teslim tarihi, teslim yeri, ödeme bilgileri gibi konular bildirilir. Satıcı tüm konularda mutabık ise kuruma onayını bildirir.
7. Teslim: Satıcı ilgili malı sipariş sırasında belirlenen yere teslim eder veya ilgili hizmeti gerçekleştirir.
8. Ödeme: Mal/hizmet fatura edildiği anda satıcı alacaklı duruma geçer. Faturanın kesilmesi genellikle teslimde veya teslimden sonraki kanuni süre içinde yapılır. Sipariş verildiğinde, teslimde veya vadeli olarak ödeme yapılabilir. Ödeme siparişte belirlenen şekilde gerçekleşir.

10.2.2.2. Satın Alma Sürecinde Hata ve Hilenin İşleyişi

Satın alma sürecinde çalışanlardan kaynaklanabilecek hata ve hileler aşağıda belirtilmiştir.

Sürecin Anlaşılması:

Hile ve hata riskini azaltmak için satın alma sürecinin detaylı planlanması ve çalışanlar tarafından anlaşılması gerekir. Tam olarak belirlenmemiş veya çalışanların bilgi sahibi olmadığı süreçler yoruma açıktır. Çalışanlar uygulamada aynı süreç için farklı uygulamalarda bulunabilirler. Bu da denetimi zorlaştıracı, hata ve hileyi arttırıcı bir durumdur.

Operasyonel Risk:

İş yoğunluğu, dikkatsizlik, bölümler arası iletişim eksikliği, ilgili belgelerin kaydını yapacak görevliye ulaşmaması, vb. sorunlar nedeniyle çalışan hatalarından kaynaklanan operasyonel riskler vardır. Bu hataları aşağıdaki gibi sıralayabiliriz:

- Belgenin kurumsal kaynak planlama yazılımına kaydedilmemesi: Bazı belgeler iş yoğunluğu nedeniyle daha sonra girilmek üzere bir yere konulabilir ve orada unutulabilir. Faaliyeti gerçekleştiren, belgeleri onaylayan ve/veya bilgi sistemine giren görevliler farklı mekanlarda bulunuyorlarsa ve/veya farklı bölümlerde çalışıyorlarsa ilgili belgenin kurumsal kaynak planlama yazılımına giren kişiye ulaşmama olasılığı vardır.
- Belgenin bir bölümünün kaydedilmesi: Çok sayıda kalemde oluşan belgeler girilirken bazı kalemlerin kayıt edilmesi gözden kaçabilir. Örneğin, aynı fatura ile birçok farklı mal alınması ve bu mallardan birinin kayıt edilmesinin atlanması.
- Belgelerin bir bölümünün muhasebeleştirilmemesi: Kurumsal kaynak planlama yazılımının çeşitli bölümlerinden girilen kayıtların genel muhasebe sistemine, yani muhasebe hesaplarına yansımaları için ‘entegrasyon’ işleminin yapılması gerekir. Bu kayıtların muhasebe hesaplarına yansımadan sorumlu kişi tarafından bir kez daha onaylanmasını gerektiren bir tür kontrol mekanizmasıdır. Entegrasyon modülü belli aralıklarla çalıştırılıyorsa birçok belgenin aynı anda bu işleme tabi tutulması gerekir. Bu sırada bazı belgelerin muhasebeleştirilmesi gözden kaçırılabilir.
- Eksik bilgi girilmesi: Kurumsal kaynak planlama yazılımlarının kendi içlerinde kontrol mekanizmaları vardır. Genellikle önemli alanların boş geçilmesine izin

vermezler. Örneğin, tarihi yazmadan fatura kaydının yapılmasına birçok yazılım izin vermez. Ancak, bu tüm kurumsal kaynak planlama yazılımları için geçerli değildir. Bazı yazılımlar kullanıcıya tüm hakları tanımaktadırlar. Kurumsal kaynak planlama yazılımında yer alan fişlerdeki bazı alanlar kullanıcının isteğine bağlı olarak kullanılan alanlardır. Bu alanlar belge numarası, özel kod, açıklama vb. adı altında yer alırlar. Kurumsal bilgi sisteminden alınacak raporlar göz önüne alınarak bu alanlar ya boş bırakılır ya da belli bir kod veya bilgi girilir. Raporlama sisteminin kullandığı alanlara planlanan şekilde girişlerin yapılması gerekir. Bunun aksi durumunda ilgili kayıt raporlarda yer almayacaktır.

- Hatalı bilgi girilmesi: İlgili kişinin kaydı girerken yapacağı bir hata belgenin muhasebe hesaplarına yansımaması, yanlış hesaplara aktarılması, raporlarda hiç yer almaması, raporların hatalı bilgi vermesi, denetim sırasında denetlenecek veri örneği içinde yer almaması gibi birçok istenmeyen sonuçlar doğurabilir.

Hile Riski:

Stoklar çalışanlar tarafından aşağıdaki şekillerde çalınabilir:¹⁴⁵

- Gizlenmemiş hırsızlıklar: Malların transfer sırasında veya depodan çalınmasıdır. Kişi gizlemeye gerek görmeden malı almıştır.
- Gizlenmiş hırsızlıklar: Evrak üzerinde oynama yaparak malların yok oluşu gizlenmeye çalışılır. Örneğin, sahte yükleme belgesi yaratmak, envanter rakamlarıyla oynamak vb. Hırsızlıklar iki şekilde gizlenebilir:

- Hileli talepler ve transferler: Hileli satın alma ve sipariş formları düzenlenir veya mal transferi sırasında çalınır. Bu tür hileyi gerçekleştirmek için sahte talep belgesi yaratılır veya transferi planlanan malın miktarını fazla gösterip aradaki fark çalınır. Örneğin, depodan üretim birimine transferi sırasında fazla gösterilen malın çalınması.
- Sahte alış raporları: Bu hile türünde teslim edilen mal eksik veya kusurlu gibi gösterilir. Daha sonra bu mallar fire olarak kayıtlardan düşer veya kusurlu olduğu için alış değerinden çok ucuza satılır.

¹⁴⁵ Nejat Bozkurt. İşletmelerin Kara Deliği: Hile – Çalışan Hileleri. 2. Basım. İstanbul: Alfa Yayınları, Ekim 2011:312.

Stokların çalınmasını önlemek için alınabilecek önlemlerin başında görevler ayrılığının sağlanması, fiziki sayımın yapılması, belgelendirme ve onaylama süreçlerinin etkin çalışmasının sağlanması ve eksik mallara ilişkin müşteri şikayetlerinin dikkate alınması gelmektedir.

Satın alınan malların bedellerinin ödenmesi sırasında da hileli işlemler yapılabilir. Bunlardan başlıcaları aşağıda sıralanmıştır:

- Şişirilmiş faturalar: Malın değeri fazla gösterilerek fazla ödeme yapılması sağlanır.¹⁴⁶
- Sahte belge düzenlenmesi: Sahte fatura düzenlenir veya satıcı adı değiştirilerek farklı birine ödeme yapılması sağlanır. Bu durumda miktar, satıcı veya ödemenin yapıldığı kişi sahte olsa da ödeme yöntemi meşrudur.¹⁴⁷
- İptal veya iadeler: Sipariş iptal edilmiş veya gelen mallar iade edilmiş gibi gösterilir.
- Sahte kişilere ödeme yapılması: Ödeme malın satıcısından farklı bir kişiye veya kuruma yapılır.
- Çifte ödemeler: Onaylanan ödemelerin farklı zamanlarda birden fazla kez yapılmasıdır.

Nakit işlemleri olabildiğince azaltmak, ödemeleri tercihan bankadan yapmak, satın alma işlemlerini kaydeden ile ödemeyi yapan kişilerin farklı olmasını sağlamak, belgeleme ve onaylama süreçlerinin etkin çalışmasını sağlamak, satıcılar ve bankalarla sıkça mutabakat yapmak ödemelerde hileli işlem olasılığını düşürmek için alınabilecek önlemlerdir.

10.2.3. Denetim Kanıtı Olarak Kullanılabilecek Belge ve Raporlar

Satın alma sürecinde yapılan işlemlere ilişkin denetim kanıtı olarak kullanılabilecek temel belge ve raporlar aşağıdaki gibidir:

1. Satın alma talep formu: Satın alma talebi “satın alma talep formu” düzenlenerek ilgili kişiye/bölüme iletilir. Bu form en azından malın/hizmetin özelliklerini, biliniyorsa marka model cins vb. önemli bilgileri, miktarı ve kimin veya hangi bölümün bu talebi yaptığı bilgilerini içerir. Bazı kurumlar satın alma talep formlarını daha detaylı bilgiler içerecek şekilde düzenlerler. Satın alınan ile talep edilenin uyumluluğunun denetimi açısından en ideali kurumun standart bir satın alma talep formu kullanmasıdır. Sözel

¹⁴⁶ Peter Goldmann. Anti-Fraud Risk And Control Workbook. A.B.D.: John Wiley & Sons, Inc., 2009:33.

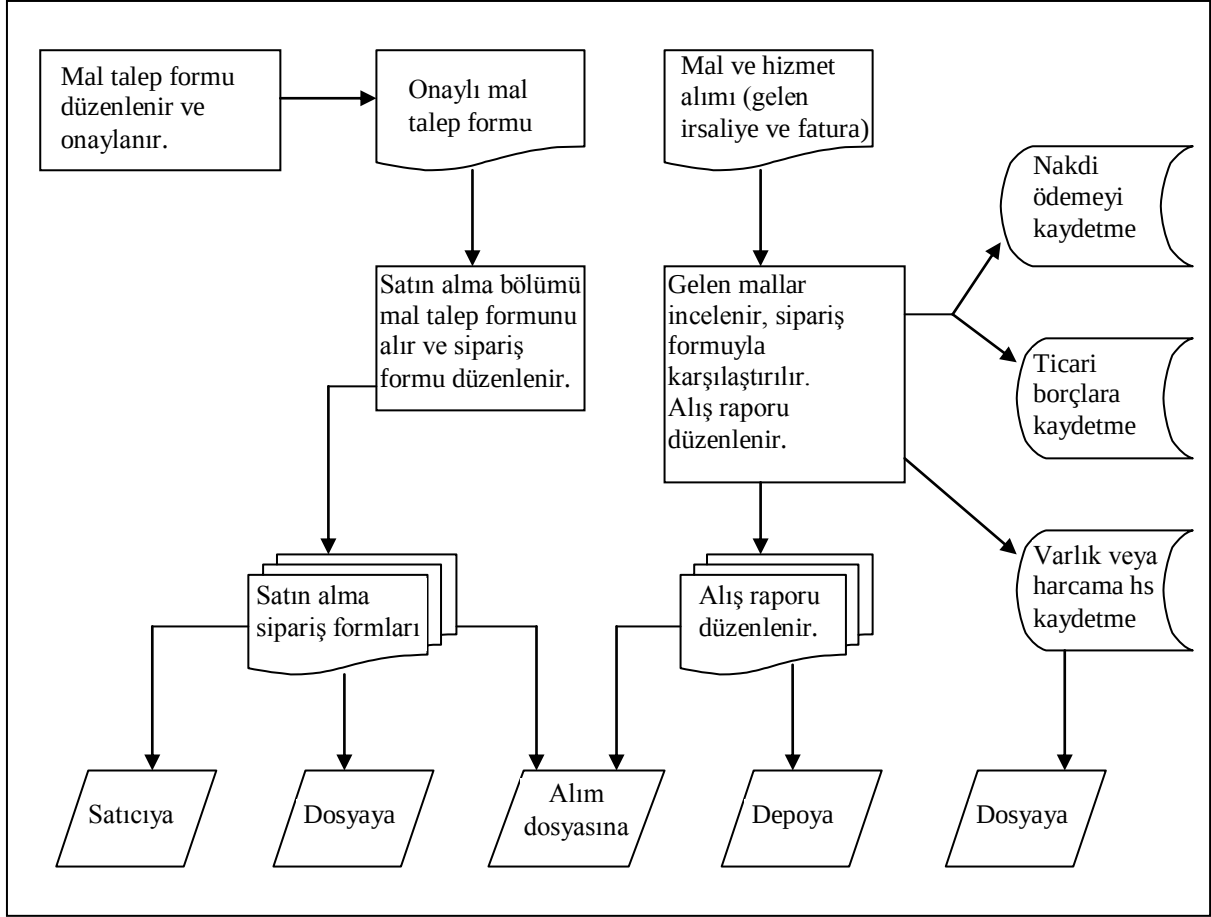
¹⁴⁷ Association of Certified Fraud Examiners. Fraud Examiners Manual. A.B.D.: Association of Certified Fraud Examiners, Inc., 2007:1501.

bildirimler, ofis içi yazışmalar, standart olmayan formlar ve bazen bunların hepsinin birden kullanımı denetimi zorlaştırmaktadır.

2. Onaylama işlemi sırasında düzenlenen belge veya girilen kayıt: Onaylama çoğunlukla satın alma talep formunun ilgili kişi tarafından imzalanması ile gerçekleşir. Dijital ortamdaki talep formlarında dijital imza, onaylayacak kişinin sadece kendi şifresiyle ilgili dosyaya ulaşım koyabileceği bir ibare vb. şekillerde onay verilebilir.
3. Satın alma emri: Onaylama işleminden sonra ayrıca bir “satın alma emri” düzenlenir veya onaylı satın alma talep formu satın alma emri yerine kullanılır. Satın alma emirlerinin standart bir formatta düzenlenmesi onaylanan mal/hizmet ile satın alınan mal/hizmetin uyumluluğunun denetimini kolaylaştırır.
4. Satın alma sipariş formu: Alınacak mal/hizmet ile ilgili tüm bilgileri içeren belgedir. Marka, model, cins, renk vb. özellikler ile miktar, tutar, teslim şartları, ödeme koşulları gibi bilgileri içerir. Yapılacak alıma ilişkin en detaylı bilgi bu formda bulunur. Bu nedenle başta cari hesaplar, stoklar ve ödemelere ilişkin incelemeler olmak üzere denetimde kullanılabilecek önemli bir belgedir. Satın alma sipariş formu kurum tarafından düzenlenir ve satıcıya gönderilir. Satıcıdan sipariş formunda yazan bilgiler çerçevesinde hareket edeceğine dair onay alınmalıdır.
5. Sevk irsaliyesi: Mal tesliminde satıcının düzenlediği bir belgedir. Bu belgede malın cinsi, miktarı, tutarı gibi teslim edilen mala ilişkin bilgiler, teslim tarihi ve satıcı bilgileri yer alır. İrsaliye üzerinde yer alan kodlar satıcı firma tarafından kullanılan kodlardır.
6. Teslim fişi: Mal tesliminde kurumun düzenlediği bir belgedir. Malın kurumun stoklarına girdiğini gösterir. Depo giriş fişi vb. adlarla da anılır. Teslim fişinde giren malın kodu, ismi, miktarı gibi mala ait temel bilgiler ile malı kontrol edip teslim alan kişinin adı bulunur. Sipariş bilgileri, talep eden kişi veya bölüm, satıcı bilgileri, fiyat ve ödeme bilgileri de yer alabilir. Formatı ve içerdiği bilgi detayı kurumun ihtiyaçlarına göre değişir. Bu belgede kodlar ve ibareler kurumun kaynak planlama yazılımında yer aldığı şekliyle kullanılır. Satıcının mal ile birlikte gönderdiği irsaliyede yazan kodlardan farklı olabilir.
7. Hak ediş raporu: Hizmet alımları için kullanılır. Alınan hizmetin ödemesi çeşitli aşamaların tamamlanmasına veya zamana bağlı ise kurum hak ediş raporu hazırlar. Burada tamamlanan hizmete veya geçen süreye bağlı olarak satıcıya yapılacak ödemenin detayları yer alır.

8. Alış faturası: Mal/hizmet alımını belgeleyen ve ödemeye esas olan bir belgedir. Satıcı tarafından doldurulur. Cins, marka, açıklama, miktar, birim fiyat, toplam tutar, ilgili vergiler gibi alınan mala/hizmete ilişkin bilgiler ile ad, adres, vergi dairesi gibi satıcıyı tanımlayıcı bilgiler bulunur.
9. Ödemeye ilişkin belgeler: Kurumun satıcıya alınan mal/hizmetin ödemesini hangi yolla, ne zaman yaptığını ve ödenen tutarı gösteren belgelerdir. Çek veya senet ile yapılan ödemelerde çek/senet bordrosu, nakit yapılan ödemelerde kasa tediye fişleri kurum tarafından düzenlenir. Ödeme banka kanalıyla yapıldıysa ilgili banka dekontu düzenler.
10. Yevmiye kayıtlarının dökümü: Satın alma ve ödeme sürecinde yapılan işlemlere ilişkin düzenlenen yevmiye maddelerinin dökümüdür.
11. Büyük defter kayıtlarının dökümü: Satın alma ve ödeme sürecinde yapılan işlemlerin ilgili ana hesaplar bazında dökümüdür.
12. Hesap dökümleri: Belli bir masraf, stok veya satıcıya ait hesaplara yapılan kayıtların detaylarının listelendiği dökümlerdir.

Yapılan işlemlere ilişkin girilen kayıtlar ve ilgili belgelerin sürekli denetimde kanıt olarak kullanılabilmesi için dijital ortamda bulunması gerekir. Kurum satın alma sürecinde yukarıda adı geçen belgeleri kullansa bile bu belgeler ve yapılan işlemler kurumsal bilgi sistemi içinde değilse sürekli denetim planlaması içinde yer alamaz. Bu nedenle sürekli denetimde denetim kanıtları için kullanılabilecek belge ve dökümler yapılabilecek analizleri ve bu analizlerin etkinliğini belirler.

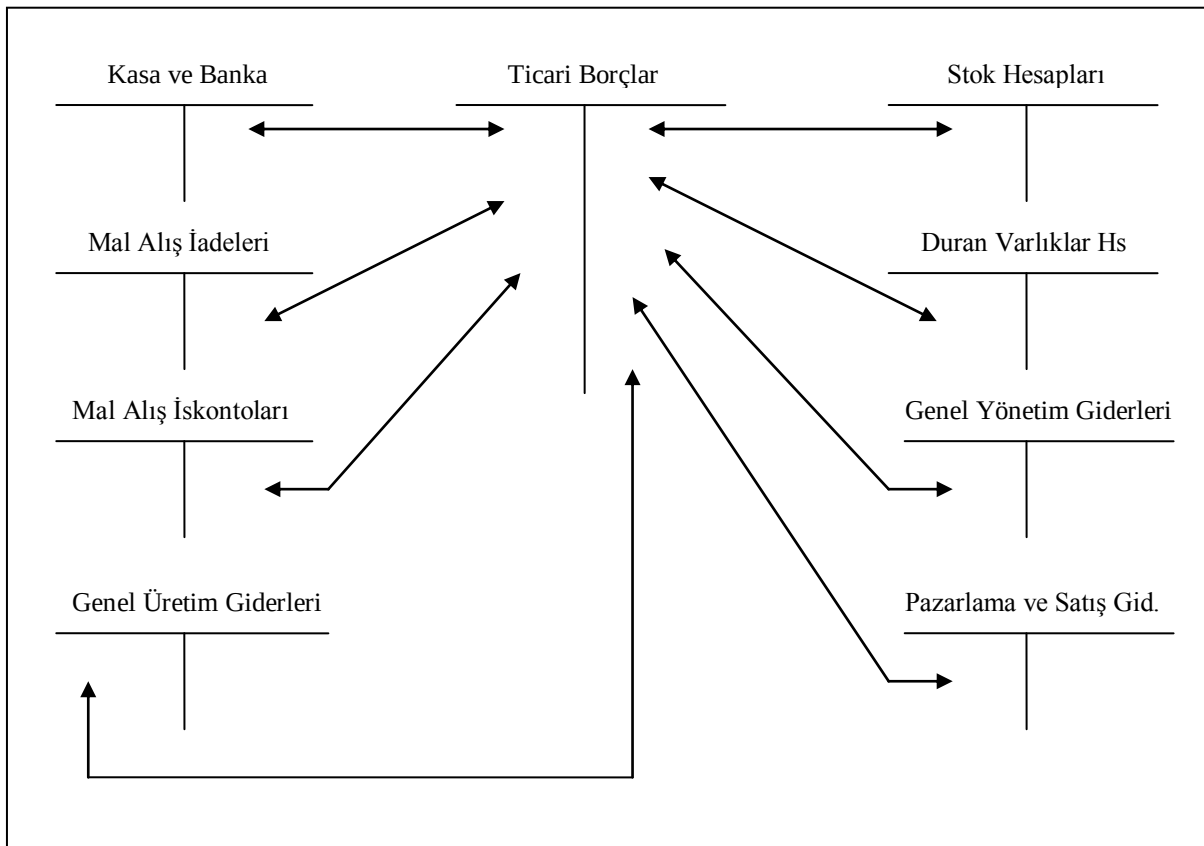


Şekil 15: Satın Alma Sürecindeki İşlemlerin Akışı

Kaynak: Cemal Elitaş ve Murat Kiracı. “Satın Alma Sürecinde Kontrol Testi ve Bir Nitelik Örnekleme Uygulaması”, Mali Çözüm Dergisi. (Temmuz-Ağustos 2010): 52.

10.2.4. Satın Alma Döngüsünde Hesapların İşleyişi

Mal ve hizmet alımları ve bunlara ilişkin ödemelere ait işlemlerde hareket gören ana hesap ticari borçlar hesabıdır. Stoklar, çeşitli varlık hesapları, çeşitli gider hesapları, kasa ve banka hesapları da diğer işlem gören hesaplardır. Satın alma sürecini denetlemek amacıyla kurulan bir sürekli denetim sistemi bu süreçte işlem gören hesapları denetlemelidir.



Şekil 16: Satın Alma ve Ödeme Döngüsündeki Hesapların İşleyişi

Kaynak: Bozkurt, Muhasebe Denetimi, s. 280.

10.2.5. Satın Alma İşlemlerinde Kontrol Testleri

10.2.5.1. Geçerlilik

Satın alma sürecinde kurumsal kaynak planlama sistemine girilmiş olan kayıtların kurum ile ilgili alınan mal ve hizmetlere ait olduğunu kontrol eden testlerdir. Denetimin hedefi belli bir projeye yönelik satın alma süreci ve kayıtlarının incelenmesi ise kayıtların proje ile ilgili olduğu test edilmelidir.

Satın alınan mal veya hizmet aşağıdaki durumlarda geçerli değildir:

- Ortak, yönetici veya çalışanların şahsi kullanımları için satın aldıkları
- Denetlenen proje ile ilgili olmayan satın almalar için girilen kayıtlar

Geçerlilik kontrol testleri:

- Süreç kontrolü: Her satın alınan mal ve hizmet için satın alma sürecinde belirlenen işlemlerin yapılması, gerekli onayların alınması ve gerekli belgelerin doldurulması gerekir.
- Satın alma talebi kontrolü: Satın almayı talep eden bölüm ilgili mal veya hizmetin nerede kullanılacağını ve hangi proje ile ilgili olduğunu talep formunda belirtir. Bu formda belirtilen proje ile satın alma sonrası girilen kaydın ilişkilendirildiği proje aynı olmalıdır.
- Alış faturalarının işlenmesi: İlgili projeye ait alış faturaları incelenerek hesaplara ve mizana doğru tutarların yansıdığı kontrol edilir.
- Ödemenin kontrolü: Satın alınan mal ve hizmetlerin ödemeleri incelenir. Yapılan ödemelerin projeye ilişkin alımlara ait olduğu tespit edilir.

10.2.5.2. Tamlık - Bütünlük

Gerçekleşmiş satın alma işlemlerinin kayıt edilmiş olduğunu kontrol eden testlerdir. Satın alınan mal veya hizmete ilişkin bir işlem bilerek veya yanlışlıkla kayıt altına alınmamış olabilir. Örneğin, alınan mala ait alış faturası kaydedilmemiş olabilir. Yapılan işlemlere ilişkin kayıtların tamamının kurumsal kaynak planlama yazılımına girilmesi gerekir. Kayıtların tamlığı çeşitli kontrol testleriyle doğrulanabilir.

Tamlık kontrol testleri:

- Sıra numarası kontrolü: Genellikle muhasebede kullanılan belgeler numaralıdır. Bu sıra numaraları birbirini takip eden sayılardan oluşur. Belgelerin numaraları kontrol edilerek atlanan sıra numarası olup olmadığı aranır. Sıra numaralarında atlama olması kayıt edilmemiş belgeler olduğunun işaretidir.
- Etkilenen hesapların kontrolü: Satın almaya ilişkin işlemler kayıt edildiğinde birden fazla hesap etkilenir. Bu nedenle kurumsal kaynak planlama yazılımının birçok modülü yapılan bir işlemde etkilenir. Örneğin, mal alımında en azından cari, stok, fatura ve muhasebe modülleri etkilenecektir. Bilgi sisteminin yapısına göre farklı modüllerden alınan raporların ve/veya kayıtlar karşılaştırılarak kayıtların bütünlüğünü kontrol edilir.

10.2.5.3. Doğruluk

Satın alma işlemlerinin doğru bir şekilde kayıt edildiğini kontrol eden testlerdir. Bu testler olması gereken, gerçekleşen ve kayıt edilen işlemlerin tutarlılığını tespit eder.

Doğruluk kontrol testleri:

- İşlemlerin doğru kaydedildiğinin kontrolü: İşlemlerin mekanik doğruluğu kontrol edilir. Kurumsal kaynak planlama yazılımında modüllere yapılan girişler, etkilenen hesaplar ve mizan toplamaları ile kontrol edilir.
- Hesaplanan tutarların kontrolü: Kayıtlarda hesaplanan alanlar varsa bu alanların matematiksel kontrolünün yapılması gerekir. Örneğin, alış faturasında birim fiyat ve miktarın çarpımının fatura tutarına eşit olduğunun kontrol edilmesi. Hesaplamalar tekrar yapılarak kayıtlardaki hesaplanan tutarlara eşit olduğu tespit edilir.
- Satın almanın planlanan şekilde gerçekleştiğinin kontrolü: Satın almaya ilişkin işlemlerin onaylanan şekliyle gerçekleştirilmesi beklenir. Bu nedenle kurumsal kaynak planlama yazılımına girilen kayıtların planlanan satın alma işlemleri ile aynı olması gerekir. Örneğin, satın alınan malın talep edilen mal olması, alış faturasında yer alan birim fiyatın sipariş sırasında satıcı ile anlaşılan fiyat olması.

10.2.5.4. Sınıflandırma

Satın alma işlemlerinin doğru hesaplara kaydedildiğini kontrol eden testlerdir. Satın alma sürecinde gerçekleşen işlemlerin doğru bir şekilde sınıflanması, yani doğru hesapları etkilemesi gerekir.

Sınıflandırma kontrol testleri:

- Muhasebe hesap planı ve kurumsal kaynak planlama yazılımının ilgili modüllerindeki kodlamanın yeterliliği kontrol edilir. Açılan alt hesapların, üretim reçetelerinin, cari ve stok kartlarının kodlamasının yapılan işi doğru, tam ve açıklayıcı bir biçimde yansıtan raporlar üretecek şekilde olması gerekir. Bilgi sisteminden beklenen yönetim kararlarına yardımcı raporlar üretmesidir. Bu raporlar kurum yönetimine günlük işlemlerde olduğu kadar taktik ve stratejik kararlarında da yol göstermelidir. Vizyoner bir bakış açısıyla yapılacak detaylı ve tutarlı bir kodlama işlemlerin kurumsal faaliyetlere uygun sınıflandırılmasının ilk adımıdır. Kodlama kurumsal kaynak planlama yazılımının özellikleri ve ihtiyaç duyulan raporlar göz önüne alınarak yapılır.
- Kurumsal kaynak planlama yazılımına yapılan girişlerin gerçekleşen işleme uygun hesaplara kaydedildiği kontrol edilir. Örneğin, alış faturasındaki satıcı adı ile kurumsal kaynak planlama yazılımında işlem gören satıcı cari kartı aynı olmalıdır. Aksi durumda yapılan satın alma sonucunda ilgisiz bir satıcı alacaklanmış olur. İlgili cari karttaki muhasebe kodu muhasebe hesap planında ilgili satıcı için açılmış alt hesabın kodu ile aynı olmalıdır. Aksi halde cari hesaplar modülünün ürettiği raporlar ile muhasebe modülünden elde edilen raporlar birbirini tutmaz ve farklı cariler alacaklı görünür.
- Borçlanan cari hesapların ödemelerinin makul süreler çerçevesinde gerçekleştiği kontrol edilir. Ödemelerin yapılmamış olması ilgili işlemin doğru hesaba kaydedilmediğinin göstergesi olabilir.

10.2.5.5. Zamanlılık

Satın alma işlemlerinin doğru tarihlere kaydedildiğini kontrol eden testlerdir. Yapılan işlemler hem zamanlı bir şekilde bilgi sistemine kaydedilmeli hem de belgeler üzerinde yazan tarih ile sistemdeki belge tarihi birbirini tutmalıdır.

Zamanlılık kontrol testleri:

- Bilgi sistemine kayıt: İşlemin gerçekleşmesi ile kurumsal kaynak planlama yazılımına kaydı arasında bir süre geçer. Bu zamanın kurum yönetiminin belirlediği süreyi aşmaması gerekir. Bilgi sisteminden alınan raporlar yönetsel kararlarda önemli rol oynar. Bu raporların güncelliğine gölge düşmesi ya hatalı karar almaya ya da yönetsel kararlarda bilgi sisteminden gelen raporların kullanılmamasına yol açar. Örneğin, kurum yönetimi alış faturalarının kuruma tesliminden bir saat içinde bilgisayara girilmesini öngörüyorsa yapılan bir satın almanın faturasının bir gün sonra sisteme girilmesi bilgi sisteminin ürettiği yönetim raporlarının geçerliliğini azaltır. Yöneticiler işlemlerin kaydedilmesindeki sürenin değişken olduğundan haberdar ise bilgi sisteminden gelecek raporlara güvenmeyeceklerdir. Bu da bilgi sisteminin kuruma faydasını azaltacaktır. Yöneticilerin kurumsal politikalara uygun olarak girişlerin bir saat içinde yapıldığını düşünmesi de hatalı kararlara yol açabilir. Güncel olmayan bilgilere farkında olmadan güvenilerek verilen kararlar kurumun zararına olabilir. Günümüzde kurumlar arası elektronik veri transferinin artması bu sürenin kısılmasına yardımcı olacak bir gelişmedir. Kayıtların kurumsal kaynak planlama yazılımına giriş süresine ilişkin bir kurumsal politikanın olması, çalışanların bundan haberdar olması ve uyması gerekir.
- Belge tarihi: Kurumsal kaynak planlama yazılımına yapılan kayıtların tarihi ile belgelerin tarihi aynı olmalıdır. Örneğin, alış faturasının tarihi ile bilgi sistemine yapılan girişte fatura tarihi olarak girilen tarihin aynı olması gerekir. Belge tarihleri ile kayıtlı işlemlerin tarihleri karşılaştırılır.

10.2.5.6. Yetkilendirme

Satın alma işlemlerine ilişkin yetkilendirmenin yönetim tarafından düzenlendiğini ve çalışanların kurumsal politikalar çerçevesinde işlem yaptığını doğrulayan kontrol testleridir. Satın alma sürecinde ilgili kurumsal faaliyeti yapan, kurumsal kaynak planlama yazılımına ilgili belgeleri kaydeden, yapılan işlemlere ilişkin onay veren kişiler ve bu kişilerin çalışma prensipleri belirlenmiştir. Satın alma faaliyetlerinin yetkilendirilmiş kişiler tarafından belirlenen sınırlar içinde gerçekleştirilmesi gerekir.

Yetkilendirme kontrol testleri:

- Kurumsal yönetim açısından: Yönetimin satın alma sürecinde hangi faaliyetlerin kimler tarafından yapılacağını ve bu kişilerin hangi prensipler çerçevesinde çalışacağını belirlemesi ve çalışanlara duyurması gerekir. Örneğin, bir mal alımı söz konusu olduğunda sipariş vermeye yetkili kişi belirlenmelidir. Herhangi bir çalışanın bu faaliyeti gerçekleştirmesi hata ve hile riskini doğuracağı gibi israf olasılığını da arttıracaktır. İlgili kişinin sipariş verebileceği maksimum miktar ve/veya tutar da belirlenmelidir. Sınırsız yetkiler büyük riskler doğurur. İhtiyacın veya kurumun ödeme gücünün üstünde alımlar gerçekleşebilir. Kişilerin yetkileri kuruma verebilecekleri zararın önemi göz önüne alınarak sınırlandırılır. Onaylama ve yetkilendirme süreci gözden geçirilir.
- Çalışanlar açısından: Çalışanların kurumsal faaliyetleri yetkileri çerçevesinde sürdürmeleri gerekir. Çalışanın yetkisi olmadığı işlemleri gerçekleştirmesi veya belirlenen limitleri aşması kurumsal riskleri arttırır. İşlemin yetkisiz bir kişi tarafından yapılması kişinin konu hakkında tam bilgisinin olmadığı durumda hata yapma, kötü niyetli olması durumunda hile yapma olasılığını arttırır. Yetkili bir kişinin kendisine belirlenen limitlerin üzerine çıkması yönetimin kurumsal ödeme planını önemli ölçüde etkileyebilir ve ödeme gücüne sokabilir. Kurumsal itibarın zedelenmesi ve mali durumun bozulması dikkat edilmesi gereken risklerdir. Satın alma işlemlerini gerçekleştiren kişilerin ilgili konuda yetkilendirilmiş kişiler olduğu doğrulanmalıdır. Ayrıca, kişilere belirlenen limitlerin gerçekleşen işlemlerle karşılaştırılması gerekir. Yönetim tarafından yayınlanmış işlem limitleri ve/veya onaylanan sipariş emri ile gerçekleşen satın almalar karşılaştırılır.

10.2.5.7. Görev Ayrımları

Görev ayrımı belirli işlemlerin belirli kişiler tarafından yapılmasını öngören bir kontroldür. Hata ve hile riskini azaltmak için iş süreçlerindeki çeşitli fonksiyonlar farklı kişiler tarafından gerçekleştirilir.

Satın alma sürecinde görev ayrımı yapılırken aşağıdaki konular dikkate alınmalıdır:

1. Sipariş eden ile teslim alan ayrımı: Sipariş işlemini yapan kişi ile teslim alan kişinin aynı olması durumunda hayali ve/veya yetkisiz alımların yapılmasına fırsat verilmiş olur. Malların çalınma veya olmayan mallara ödeme yapılma riskini doğurur. Ayrıca,

satın alınan mal veya hizmetin miktarı, fiyatı, özellikleri veya satıcısının onaylanandan farklı olma riskini arttırır.

2. Fatura ve cari hesap işlemlerinde görev ayrımı: Alış faturasını kaydeden ile ödemeyi yapan birbirinden farklı kişiler olmalıdır. Alış faturalarını işleyen ile satıcı faturasını destekleyici belgelerle karşılaştırıp satıcı cari hesaplarının güncellenmesinde sorumlu olan kişinin aynı olması durumunda satın alma işlemlerinin onaylanandan farklı fiyat ve koşullarda gerçekleşmesi, alınmayan mallar veya hizmetler için ödeme yapılması olasıdır.
3. Cari hesap ve ödeme işlemlerinde görev ayrımı: Satıcı cari hesaplarının güncellenmesinden sorumlu olan ile ödemeyi yapan birbirinden farklı kişiler olmalıdır. Ödeme yapan kişinin borç kayıtlarına ulaşması durumunda hayali belgelere dayalı yetkisiz işlemlerin yapılma riski doğacaktır.
4. Cari hesap ve büyük defter işlemlerinde görev ayrımı: Satıcı cari hesaplarına işlem yapabilen kişinin büyük defter hesaplarına da işlem yapma yetkisinin olması sakıncalıdır. Kötü niyetli bir çalışanın cari hesap ve büyük defter kayıtlarında değişiklik yaparak yakalanmadan zimmetine para geçirme olasılığı artar.

10.2.5.8. Özetleme

Satın alma işlemlerinin ilk kaydının yapıldığı hesaplar ile işlemlerin toplam tutarının aktarıldığı hesapların uyumlu olduğunu kontrol eden testlerdir. Örneğin, bir malın satın alma işlemi sırasında ilgili stok kartı hareket görür. Stok kartı ile ilgili işlemler belli aralıklarla muhasebe modülüne entegre ediliyorsa, entegrasyon sırasında ilgili işlemler özetlenip toplam tutar tek kalem halinde muhasebe modülüne aktarılıyor olabilir. Entegrasyon öncesi ve sonrası karşılaştırılarak yapılan özetlemenin doğruluğu kontrol edilebilir. Özetleme kurumsal kaynak planlama yazılımının yapısına göre değişir. Günümüzde bilgisayar teknolojilerinin gelişimine bağlı olarak modüller arası aktarılan bilginin özetlenmesine ihtiyaç azalmıştır. Her işlemin ilgili hesaplarda bire bir takip edilebilmesi denetimi kolaylaştırmaktadır. Kurumsal kaynak planlama yazılımı özetleme yaparak hesaplar ile ilgili raporlar üretir. Yazılımın yapısında hata olmadığı sürece sistemden alınan değişik türde özet raporlarda da hata olmayacaktır.

Özetleme kontrol testleri:

- Stok ve cari kartlardaki işlemler muhasebede ilgili hesaplara aktarılmış olduğu kontrol edilir.
- Satın alma, borçlar hesabı gibi yardımcı defterlerin tutulması ve kurumsal kaynak planlama yazılımına toplam tutarların işlenmesi durumunda yardımcı defterlerin toplamalarının sağlanması yapılır.

10.3. SÜREKLİ DENETİM UYGULAMASINI GELİŞTİRMEK İÇİN ÖN HAZIRLIK

10.3.1. Denetim Amacı

Araç takip sistemlerinin maliyetinin büyük bir bölümü cihazları üretmek için satın alınan mallardan oluşmaktadır. Her projede kullanılan malların sayısı yüzü geçmektedir. Bu mallar farklı tedarikçilerden temin edilmektedir. Bir projede ihtiyaç duyulan bir girdi her zaman tek seferde değil bazen de birkaç parti halinde kuruma teslim edilmektedir. İmalatı tamamlanan cihaz araca monte edilmek üzere sevk edilene kadar üretim biriminin deposunda saklanmaktadır. Üretim ve depolama birden fazla fiziki mekanda gerçekleşebilir. Bir projeye ilişkin cihazların çıkışı parti parti gerçekleşmektedir. Alıcı aracın bulunduğu adresi bildirdikçe cihazlar montaj ekibine çıkış yapılmaktadır.

İşlemlerin karmaşıklığı ve çok sayıda fiziki mekanın kullanılması hata ve hile ihtimalini arttırmaktadır. Bu nedenle araç takip sistemlerinin üretiminde kullanılacak hammadde, yardımcı madde, mal ve malzemelere ilişkin satın alma döngüsünün denetimine yönelik bir sürekli denetim uygulaması geliştirilmesi hedeflenmiştir.

10.3.2. Yönetimin Desteği

Kurum yönetimi, araç takip sistemlerinin üretimine ait satın alma süreci ve ilgili kayıtların denetlenmesinin önemli ve öncelikli bir konu olduğunu belirtmiştir.

Çalışma sürecinde hem kurum yönetimi hem de bilgi paylaşımında bulunan çalışanlar bu uygulamanın gerçekleşmesine tam destek vermişlerdir.

10.3.3. Teknik Bilgi

Bu uygulamayı gerçekleştirmek için aşağıdaki konularda teknik bilgiye sahip olmak gerekir:

1. ACL denetim yazılımı: Veri analizi ACL denetim yazılımında yapılacağı için ACL'e veri aktarımı ve analizi konularında en azından temel bilgiye sahip olunması gerekir.
2. Kurumsal kaynak planlama yazılımı: Mikro kurumsal kaynak planlama yazılımından alınacak veri analizde kaynak veri olarak kullanılacaktır. Bu nedenle bu yazılımdan alınabilecek işlem hareket dökümleri ve raporlar konusunda bilgi sahibi olunması gerekir.
3. Excel: ACL denetim yazılımına aktarılacak kaynak veri Excel dosyaları formatındadır. Bu nedenle Excel yazılımını temel düzeyde bilmek gerekir.

10.3.4. Denetim Yazılımı

Bu uygulamada ACL denetim yazılımının kullanılması öngörülmüştür. Bu yazılımın seçilmesinde üç temel neden vardır:

1. ACL yazılımı birçok farklı formatı otomatik olarak okuyabilmektedir. Kurumdan alınacak verinin ayrıca bir düzenlemeye gerek duyulmadan denetim yazılımına aktarılması oluşabilecek hataları ve bilgi kaybını önlemesi açısından önemlidir. Bu uygulamada kaynak veri kurumsal kaynak planlama yazılımından denetim programına aktarılarak analiz edilecektir. Bu nedenle aktarım sırasında veri bütünlüğünün korunması önemli bir konudur.
2. ACL denetim yazılımının dijital analiz olanakları çok gelişmiştir. Birçok dijital analiz tekniği yazılıma tanımlanmış durumdadır. Ayrıca, yazılım komut satırları (scripts) denilen bir uygulaması sayesinde denetçinin istediği matematiksel formülleri tanımlamasına da olanak vermektedir.
3. Analizleri otomatikleştirme özelliği ACL'in sürekli denetim uygulamalarında kullanılmasını kolaylaştırmaktadır. ACL'in komut satırları (scripts) sayesinde veri üzerinde yapılacak işlemler ve analizler belirlenen sıra içinde gerçekleştirilebilir, sonuçlar raporlanabilir ve ilgili kişilere e-posta ile gönderilebilir.

10.3.5. İş Süreçleri

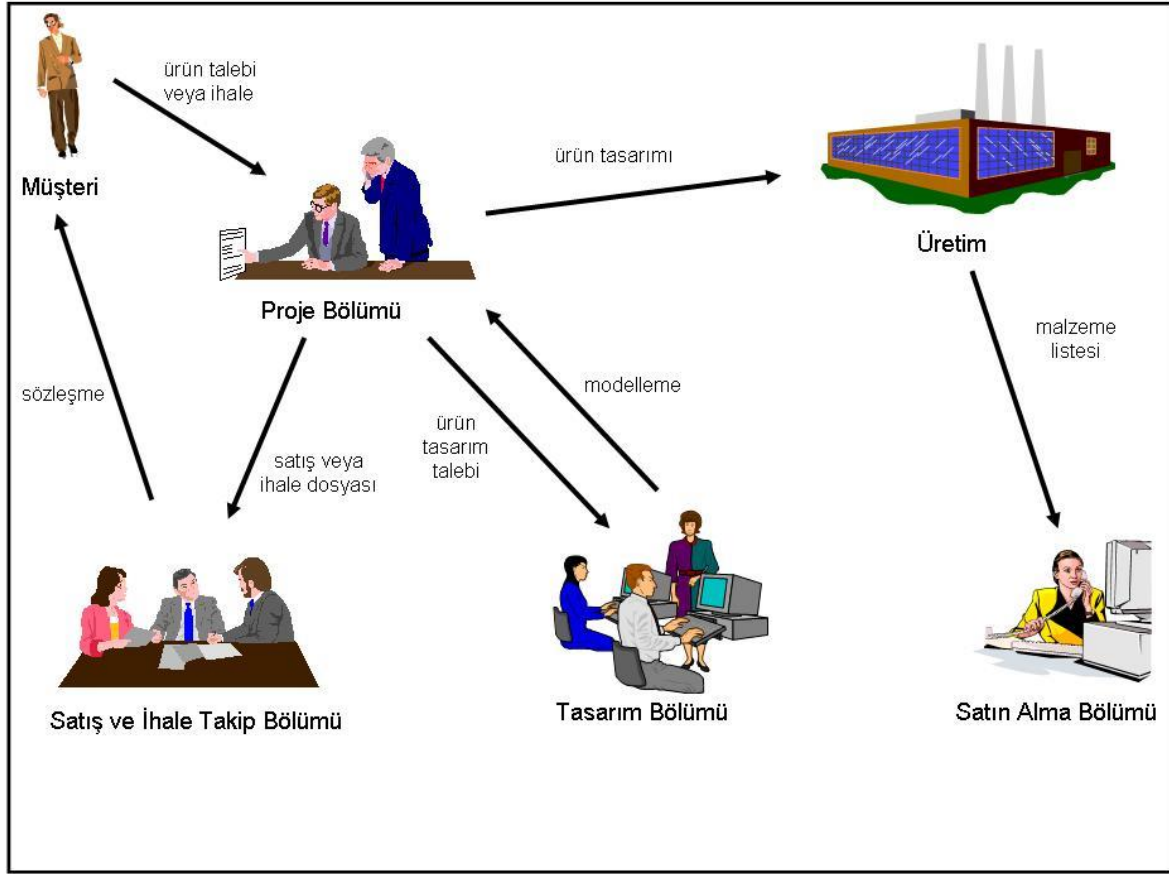
Üretime ilişkin satın almaya neden olan işlemler ve iş süreçleri aşağıda açıklanmıştır.

Araç takip sistemi talebi kuruma iki şekilde gelir. Müşteri direkt olarak talep eder veya kurum açılmış bir ihaleye başvurur. Her talep bir proje olarak kabul edilir. Projenin ilk değerlendirilmesi Proje Bölümü tarafından yapılır. Proje Bölümü ürünün teslim süresini, sipariş hacmini, kurumun teknolojik altyapısını ve mali imkanlarını göz önüne alarak projenin kuruma uygunluğunu ve yapılabilirliğini değerlendirir.

Proje Bölümü tarafından uygun bulunan proje genel koordinatörün onayına sunulur. Onaylanan proje Tasarım Bölümü'ne gönderilir. Bu bölüm Proje Bölümü tarafından bildirilen teknik özelliklere göre ürünü bilgisayar ortamında tasarlar, çizer, parçaları birleştirir ve çalışma simülasyonunu yapar, kısaca ürünün modellemesini yapar. Tasarım Bölümü tarafından kullanılan yazılım ürüne ilişkin teknik çizimleri ve üretime ilişkin diğer bilgileri dijital ortamda sağlar. Ürünün parça listesi de bu yazılımdan sağlanabilir. Ancak yazılım üretim sırasında kullanılan diğer malzemeler konusunda bilgi vermemektedir.

Tasarım Bölümü teknik çizimleri ve ilgili bilgiyi Proje Bölümü'ne gönderir. Proje Bölümü Satın Alma Bölümü'nden bilgi alarak maliyet hesabını yapar, satış/ihale dosyasını hazırlar.

Bu dosya Satış ve İhale Takip Bölümü tarafından müşteriye/ihaleye gönderilir, kabul süreci takip edilir. Müşterinin projeyi kabul etmesi durumunda Proje Bölümü projeye ilişkin teknik çizimleri ve diğer bilgiyi üretim müdürüne gönderir.



Şekil 17: Araç Takip Sistemi Projelerinin Üretim Öncesi Hazırlık Dönemini Gösteren İş Akışı

Araç takip sistemi birçok parçadan ve bir yazılımdan oluşmaktadır. Sistemi oluşturan parçalardan bazıları ve yazılım kurum içinde üretilirken bazı parçaların üretimi taşaron firmalara yaptırılmaktadır.

Üretim müdürü projenin imalatında kullanılacak hammadde, yardımcı madde, mal ve malzemelerin listesini çıkartır. İhtiyaç listesi Satın Alma Bölümü'ne gönderilir. Bu liste Excel formatındadır.

Satın Alma Bölümü ihtiyaç listesindeki ürünleri yurtiçi ve yurtdışından satın alır. İlgili tedarikçilere ve taşaronlara faks veya e-posta yoluyla fiyat isteme formu gönderir. Bu formda istenen malın teknik özellikleri yer alır. Tedarikçiler ve taşaronlar birim fiyat, ödeme şekli ve teslim şartlarını bildirirler. Bu bilgi faks veya e-posta yoluyla kuruma ulaşır. Kabul edilen teklifler gelen belge üzerine kaşe ve imza ile onaylandıktan sonra karşı firmaya fakslanır. Böylece sipariş verilmiş olur.

Tedarikçiler ve taşaronlar bilgilendirme için kurumun onlara gönderdiği formu veya kendi formlarını kullanırlar. Faks ile gönderilen doküman ve standardizasyonun olmayışı bu belgelerde dijital analizi imkansız kılmaktadır. Ancak, onaylanan formlar temel alınarak Satın Alma Bölümü tarafından Excel formatında sipariş dosyası hazırlanır. Sipariş dosyasında stok kodu, birim fiyatı, tedarikçi bilgileri, ödeme şekli, teslim tarihi gibi bilgiler yer alır. Bu dosya dijital analize uygundur.

Kurum politikası olarak her ürün ilgili tedarikçi veya taşarondan alınır. Dolayısıyla ürünler farklı firmalardan temin edilir. Aynı ürün farklı projelerde farklı firmalardan temin edilebilir. Ancak, bir proje içindeki bir ürünün tedarikçisi tektir.

Satın alınan ürünlerin teslimi genellikle üretim yerinin deposuna irsaliye ile yapılır. Depo sorumlusu siparişi kontrol eder ve üretim müdürünün onayı ile ürünleri teslim alır. Birden fazla proje aynı üretim yerinde yapılabilir. Bu nedenle depo sorumlusu irsaliyenin arkasına ilgili projenin kodunu yazar ve teslim alan olarak imza atar.

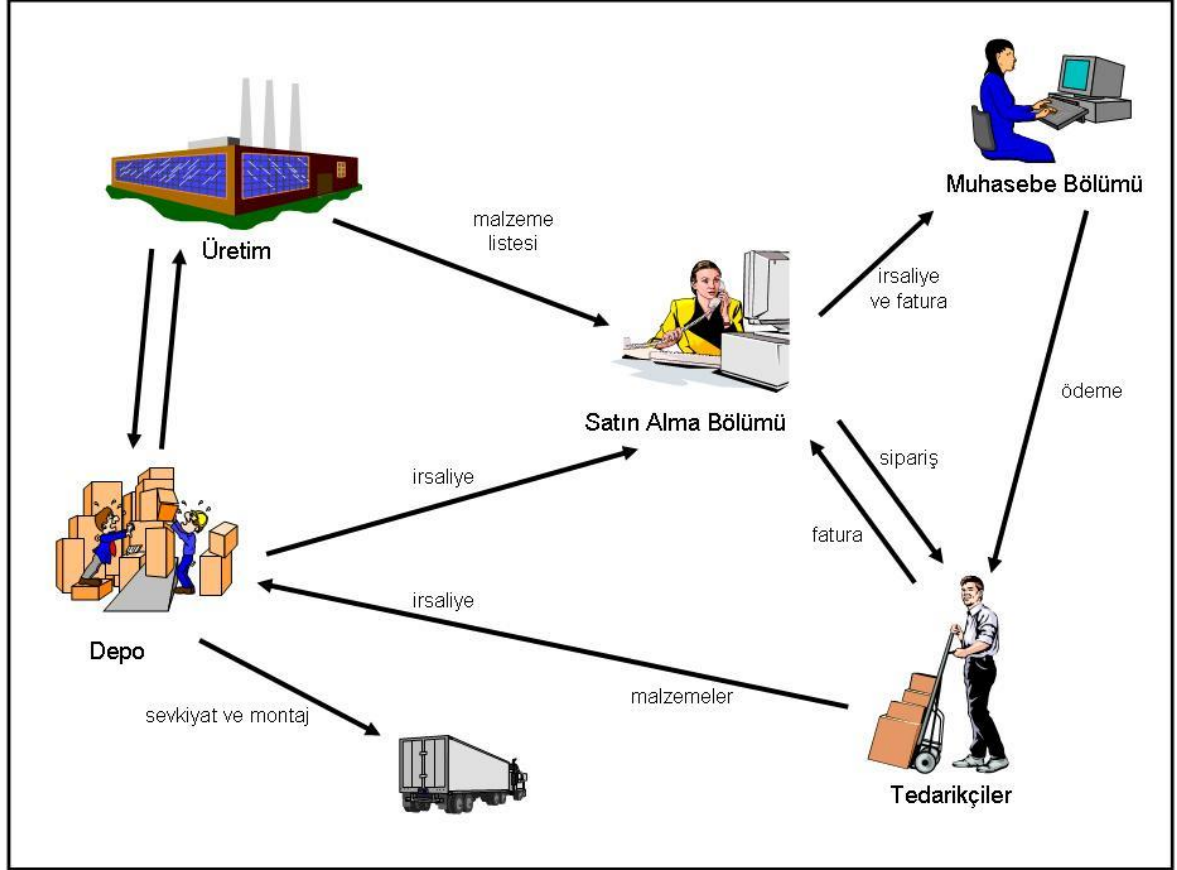
Depo sorumlusu irsaliyeyi ve ürün ile birlikte gönderilmesi durumunda faturayı Satın Alma Bölümü'ne gönderir. Tedarikçi faturayı direkt olarak Satın Alma Bölümü'ne de gönderebilir. Satın Alma Bölümü yetkilisi irsaliye ve fatura bilgilerini sipariş dosyası ile kontrol eder. Faturanın arkasına proje kodunu yazar, bilgilerin doğru olduğunu belirtmek için imzasını atar. Ayrıca, fatura numarasını sipariş dosyasına “evrak no” olarak kaydeder.

Satın Alma Bölümü tarafından kontrol edilen ve onaylanan irsaliye ve faturalar Muhasebe Bölümü'ne gönderilir. Muhasebe Bölümü irsaliye ve faturaları kurumsal kaynak planlama yazılımına kaydeder. İlgili fişler proje kodu belirtilerek kesilir.

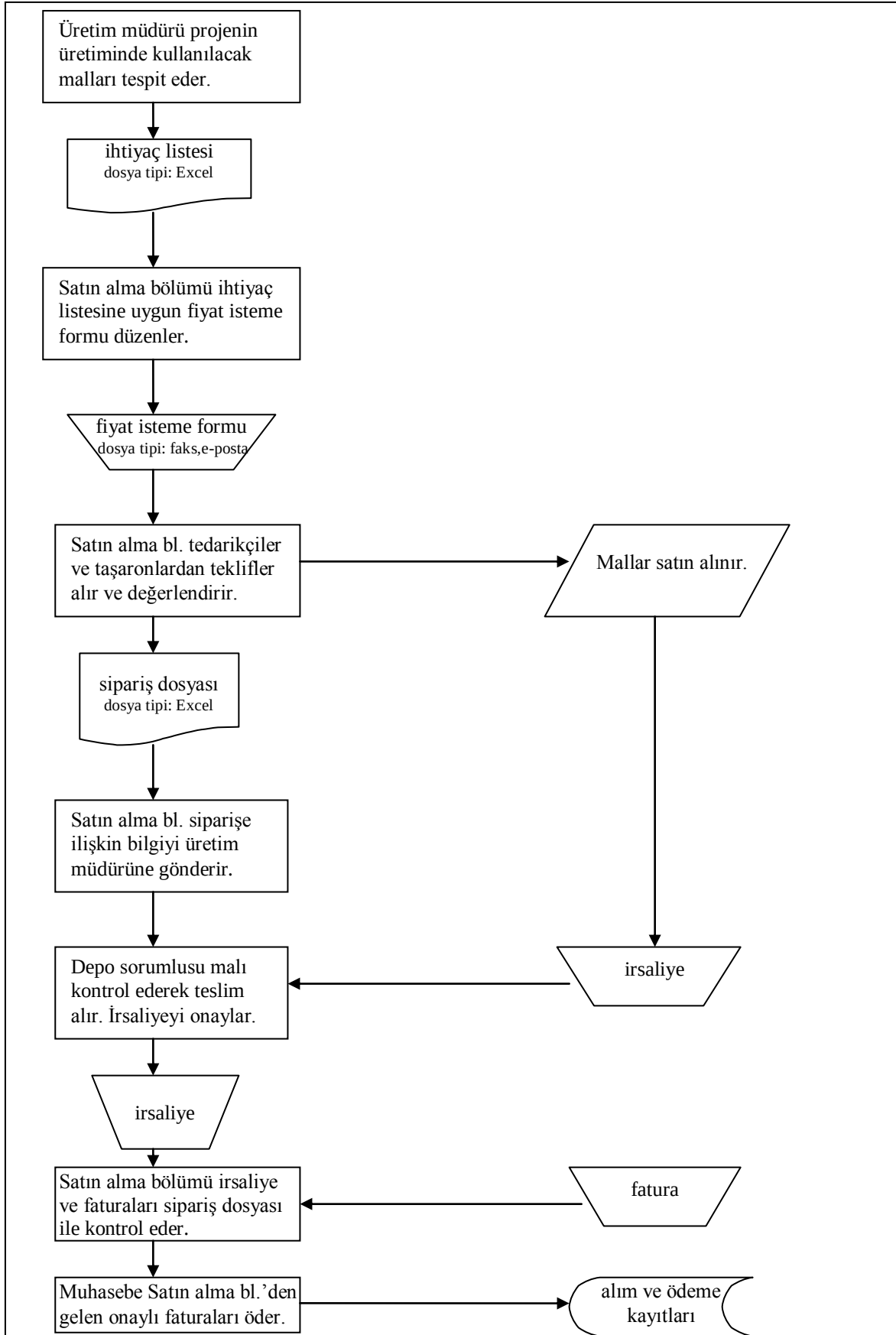
Kurum ayrıca bir depo giriş fişi düzenlememektedir. Kurum, satıcılardan gelen irsaliyelerin onaylanması işlemini depo giriş fişinin kesilmesi işlemine eşdeğer olarak kabul etmektedir. Muhasebe Bölümü'nün gelen irsaliyelere kestiği fişler depo kayıtları için esas teşkil etmektedir. Depoda periyodik olarak yapılan fiziki sayımlar bu kayıtlar ile karşılaştırılmaktadır.

Muhasebe Bölümü sipariş dosyasında belirtilen ödeme şartlarını esas alarak gelen faturaları öder. Ödeme aracı çoğunlukla banka havalesidir. Çek, senet ve kasadan nakit ödeme

de yapılabilmektedir. Ödemelere ilişkin kayıtlar kurumsal kaynak planlama yazılımına Muhasebe Bölümü yetkilileri tarafından girilmektedir. Nakdin sayılması ve banka mutabakatları gibi kontroller de Muhasebe Bölümü yetkilileri tarafından gerçekleştirilmektedir. Dijital ortamda bir mutabakat yapılmamaktadır.



Şekil 18: Üretim Sürecinde Yapılan Satın Alma ve Stok Hareketleri



Şekil 19: Kurumun Satın Alma Döngüsü

10.3.6. Önemli Kontrol ve Riskleri Belirlemek

Yapılan incelemeler sonucunda kurumsal kontroller ve ilgili riskler aşağıda belirlenmiştir:

1. Kurum faaliyetlerinin kaydı ve görevler ayrılığı:

Kurumda yapılan incelemede görevler ayrılığının başarılı bir şekilde planlandığı görülmüştür. Karmaşık işlemleri olan ve çoklu fiziki ortamda gerçekleşen üretime ilişkin bilgi ve belge akışı etkindir. Çalışanlar arası iletişim üst düzeydedir.

Kurum yönetimi belge kaydındaki operasyonel risklere karşı görev ayrımı yöntemi ile bir kontrol sistemi geliştirmiştir. Uygulamada çalışanların olağandışı durumlarda iletişim içinde olup kayıtları kendilerinin düzeltmesi beklenmektedir. Örneğin, depo sorumlusu satın alınan malzemeyi ve irsaliyesini kontrol ettikten sonra irsaliyenin arkasına malzemenin kullanılacağı birimi ve proje kodunu yazıyor, imzalıyor. Böylece irsaliye depo giriş fişi görevini görüyor. İrsaliye başka bir mekandaki satın alma bölümüne geldiğinde depo sorumlusunun imzasına bakılıyor. İmza malzemenin tam ve doğru geldiğini, üretimde kullanılmak üzere depoya girdiğini gösteriyor. İmzanın olmayışı malzemenin girişi veya belgeleme sürecindeki bir hataya işaret ettiği için satın alma bölümü çalışanları konuyu araştırıyor. Satın alma tarafından onaylanan irsaliyeler muhasebe bölümüne gönderiliyor. Hem depo sorumlusunun hem de satın alma sorumlusunun onayı aranıyor. Hata olması durumunda muhasebe bölümü çalışanları inceleme yapıyor.

Görüldüğü üzere belge akışında kademeli kontroller bulunmaktadır. Bu kademeli kontroller operasyonel risklerin giderilmesinde etkindir. Ancak, bu kontroller ve belgelerin bir bölümü dijital ortamda değildir. Bu nedenle dijital ortamda tüm kontrollerin denetimini yapmak olanaksızdır. Kurumsal kaynak planlama yazılımına yapılan girişler sipariş dosyası ile karşılaştırılarak ilgili kayıtların denetimi yapılmıştır.

2. Kurum faaliyetlerinin farklı mekanlarda olması:

Kurum faaliyetlerini Ankara’da bir ofis, İstanbul’da biri merkez olmak üzere dört ofis, bir fabrika, bir montaj atölyesi, tamir bakım onarım faaliyetlerinde bulunan bir servis ve iki depo olmak üzere on farklı fiziki alanda gerçekleştirmektedir. Kayıtların girildiği ve belgelendirilen işlemlerin kaynaklandığı fiziki ortamların çok değişik

yerlerde olması ve kayıt sürecine çok sayıda çalışanın katılması hile riskini azaltırken hata riskini çoğaltmaktadır.

3. Yapılan satın almanın miktar ve çeşitlilik açısından karmaşık olması:

Araç takip sistemi birçok parçadan oluşmaktadır. Bu nedenle her proje için yapılacak satın alma sayısı çoktur.

Alımlar her zaman tek seferde yapılmamaktadır. Bu da sipariş ile teslim edilen malın miktarının kontrolünü zorlaştırmaktadır.

Her projenin birbirine benzeyen ve ayrılan yanları vardır. Her talep müşterinin belirlediği özel istekleri karşılayacak şekilde projelendirilmekte ve üretilmektedir. Bir projeye ait satın almalarda bazı mallar benzer olsa da bazıları farklılık gösterecektir. Yapılan satın almanın hangi projeye ait olduğunu takip etmek ilgili çalışanlar arasında üst düzey iletişim ve dikkat gerektirmektedir.

Bazı parçalar kurum içinde üretilirken bazı parçalar taşaron firmalar tarafından üretilmektedir. Bu nedenle alımlar hammadde, yardımcı madde, yarı mamul, mamul ve malzeme kategorilerinden olabilir.

Bir malın tedarikçisi farklı projelerde farklı firmalar olabilmektedir. Ancak, aynı projede bir malı tek bir firma sağlamaktadır. Bu da satıcıların denetimi açısından kolaylık sağlamaktadır.

4. Sipariş sürecindeki denetim riskleri:

Sipariş süreciyle ilgili denetim kanıtı olarak kullanılabilecek tek dosya Satın Alma Bölümü'nün tuttuğu sipariş dosyasıdır. Sipariş sürecinde üretilen fiyat isteme formları aşağıdaki nedenlerden dolayı sürekli denetim uygulamasında denetim kanıtı olarak kullanılamamaktadır:

- Kurumun teklif alırken kullanabileceği bir fiyat isteme formu bulunmaktadır. Ancak, bu form her zaman kullanılmamaktadır. Satıcılardan gönderilen formlar veya kurumdan giden mesajlar da fiyat isteme formu olarak kabul edilmektedir.
- Teklif alma aşaması faks veya e-posta yoluyla yapılmaktadır. Faks ile gönderilen formlar ayrıca bilgisayara girilmediği için bu teklifler dijital ortamda bulunmamaktadır. Bu da kurumsal kaynak kullanım yazılımının sipariş modülünü ve bu modülden elde edilebilecek tüm denetim kanıtlarını etkisiz kılmaktadır.

10.4. SÜREKLİ DENETİM MODELİNİ OLUŞTURMAK

10.4.1. Test Kapsamı

Denetimin kapsamı kurumun araç takip sistemleri üreten biriminin satın alma sürecinde etkilenen hesaplar ve ilgili kayıtlardır.

10.4.2. Bilgi Kaynakları

Satın alma döngüsünün denetimi için ilgili işlemlerden etkilenen hesapların dökümlerini incelemek gerekir. Bu uygulamada Satın Alma ve Muhasebe bölümlerinin yaptığı kayıtların dökümleri bilgi kaynakları olarak kullanılmıştır.

Uygulamada kullanılan bilgi kaynakları:

1. Kurumsal Kaynak Planlama Yazılımı: Kurumsal kaynak planlama yazılımının finans yönetimi, stok yönetimi ve genel muhasebe modüllerinden elde edilen cari hesaplar, stok ve muhasebe işlemleriyle ilgili hareket dökümleri kaynak veri olarak kullanılmaktadır. Bu modüllere girişler Muhasebe Bölümü çalışanları tarafından yapılmaktadır.
2. Sipariş Dosyası: Satın Alma Bölümü tarafından Excel formatında tutulan dosya ilgili projeye ait satın alınması planlanan tüm malların satıcı ve ödeme bilgilerini içermektedir. Her proje için ayrı bir sipariş dosyası tutulmaktadır. Bu dosya kurumsal kaynak planlama yazılımına yapılan girişleri kontrol etmek amacıyla kullanılan en önemli kaynaktır.

10.4.3. Denetim Kanıtları

Satın alma süreci ve ilgili stok kayıtlarının denetiminde kullanılabilecek denetim kanıtları ve bu belge ve raporların sürekli denetim uygulamasındaki yeri aşağıda incelenmiştir:

1. Satın alma talep formu:
Üretim müdürü araç takip sistemini üretmek için ihtiyaç duyacağı hammadde, yardımcı madde, malzeme ve elinde olmayan demirbaşların listesini üretim

başlamadan önce Satın Alma Bölümü'ne gönderir. İlgili proje için satın alınacak mallar büyük ölçüde üretim başlamadan önce belirlenir. Bu ihtiyaç listesi satın alma talep formu işlevini görür.

Üretime ilişkin satın alma büyük ölçüde Satın Alma Bölümü tarafından gerçekleştirilir. Üretim sürecinde zaman zaman öngörülemeyen bazı malzemelere ihtiyaç duyulabilir. Çivi, conta vb. maddi değeri az olan bu malzemeler Üretim Bölümü tarafından direkt olarak tedarik edilir.

2. Satın alma talep formunun onaylanmasına ilişkin belge:

Üretim müdürü tarafından Satın Alma Bölümü'ne gönderilen bu liste Excel formatında bir dosyadır ve kurum için satın alma talep formudur. Üretim müdürünün e-postasından gönderilmiş olması onun onay verdiği anlamına gelir.

3. Satın alma emri:

Satın alma talep formu Satın Alma Bölümü'ne ulaştığında ilgili form satın alma emri olarak kabul edilir.

4. Satın alma sipariş formu:

Satın Alma Bölümü satın alma talebinde yer alan malların dökümünü ve satın alma sürecinde ihtiyaç duyulacak bilgileri (bilinen teknik özellikleri, adetleri, tedarikçiler vb.) bir dosyaya girer. Bu dosyanın ismi sipariş dosyasıdır. Sipariş dosyasının hazırlanma sürecinde Proje Bölümü ve Üretim Bölümü'nden bilgi ve onay alınır. Bu dosya Excel formatındadır.

Sipariş dosyasında yer alan bilgilere göre ilgili tedarikçilere faks veya e-posta yoluyla ulaşılır. Tedarikçilerden fiyat, teslim süresi, teslim yeri, ödeme koşulları gibi satın almaya yönelik bilgiler istenir. Kurumun kullandığı belli bir sipariş formu bulunmamaktadır. Tedarikçiler de ilgili bilgileri faks veya e-posta yoluyla kuruma ulaştırır. Bazı tedarikçiler kendi firmalarına ait standart sipariş formu ile cevap verirken bazıları kurum tarafından gönderilen formu veya e-postayı yanıtlayarak cevap verirler.

Yazıcıdan çıktısı alınan e-postalar ve gönderilen fakslar ilgili kişiler tarafından incelenir ve imzalanır. Bu belgeler kurum açısından satın alma sipariş formu, arkasındaki imza da onay olarak kabul edilir. Satın Alma Bölümü sipariş takibi yapabilmek için bu formları kullanarak sipariş dosyasını hazırlar.

Satın alma sipariş formları standart formatta ve elektronik ortamda olmadığı için sürekli denetimde kullanılamazlar. Ancak, Satın Alma Bölümü tarafından hazırlanan sipariş dosyası bilgisayar ortamında olup Excel formatındadır. Kurumsal kaynak planlama yazılımının dışında üretilen bu dosya önemli bir denetim kanıtıdır ve bu uygulamada kullanılan belgelerden biridir.

5. Sevk irsaliyesi:

Tedarikçiler kuruma sevk irsaliyelerini elektronik ortamda göndermemektedirler. Ancak, sevk irsaliyeleri Muhasebe Bölümü tarafından kurumsal kaynak planlama yazılımına girilmektedir. Stok hareketleri raporunda sevk irsaliyelerine ait kayıtlar izlenebilmektedir.

6. Teslim fişi:

Tedarikçiler depoya malları sevk irsaliyeleri ile teslim ederler. Depo sorumlusu gelen malları inceler, sipariş edilenlerle karşılaştırır ve hata olmaması durumunda teslim alır. Teslim alırken sevk irsaliyesinin arkasını imzalar ve ilgili projenin kodunu yazar. Onaylanan sevk irsaliyesi kurum için teslim fişi olarak kabul edilmektedir. Ancak, bu durum teslim fişlerinin elektronik ortamda yer almadığı için sürekli denetimde kullanılamayacağı anlamına gelir.

7. Alış faturası:

Alış faturaları tedarikçiler tarafından ya Satın Alma Bölümü'ne gönderilir ya da malla birlikte depoya bırakılır. Depoya bırakılan alış faturaları Satın Alma Bölümü'ne gönderilir. Alış faturaları Satın Alma Bölümü tarafından sipariş dosyası ile karşılaştırılır. Faturadaki bilgiler sipariş dosyası ile tutuyorsa satın alma sorumlusu tarafından onaylandığını belirtmek için arkası imzalanır. Faturayı proje ile ilişkilendirmek için ilgili projenin kodu yazılır.

Sevk irsaliyesinde olduğu gibi alış faturaları da elektronik ortamda yer almazlar. Onaylı alış faturaları Muhasebe Bölümü'ne gönderilir ve muhasebe sorumlusu tarafından kurumsal kaynak planlama yazılımına kaydedilirler. Yevmiye dökümlerinde, cari ve stok hareketleri raporunda bulunan alış faturası kayıtları uygulamada kullanılmıştır.

8. Ödemeye ilişkin kayıtlar:

Ödemeler ilgili muhasebe sorumlusu tarafından yapılır. Ödemelerin belgesi olan çek/senet bordroları, banka dekontları ve kasa tediye fişlerine ilişkin kayıtlar ilgili muhasebe sorumlusu tarafından kurumsal kaynak planlama yazılımına girilir. Yevmiye dökümlerinde ve cari hesap hareketleri raporunda ödemelere ilişkin kayıtlar izlenebilmektedir. Ödemeler satıcının kurum ile ilişkisine ve daha önceki mal alımlarından kaynaklanan alacak tutarına bağlı olarak yönetimin onayıyla yapılmaktadır. Bu nedenle satıcılara yapılan ödemelerin belli bir proje ile ilişkilendirilmesi mümkün görülmemektedir.

9. Yevmiye kayıtları:

Kurumsal kaynak planlama yazılımı değişik modüllerden oluşmaktadır. Bu uygulamada yararlanılan genel muhasebe, finans yönetimi ve stok yönetimi modüllerinden yapılan tüm girişler birer yevmiye kaydı oluşturur. Tüm finansal işlemlerin yansıdığı yevmiye kayıtları dökümü önemli bir denetim kanıtıdır.

10. Hesap dökümleri:

Kurumsal kaynak planlama yazılımına girişler farklı modüllerden yapılır. Her modülden ayrı ayrı girişlerin dökümünü almak mümkündür. Hesap dökümleri elektronik ortamda bulunduğu için sürekli denetim uygulamalarında kullanılabilir. Genel muhasebe, finans yönetimi ve stok yönetimi modüllerinden yapılan girişlere ait dökümler bu uygulamada denetim kanıtı olarak kullanılmıştır.

10.4.4. Denetimin Zamanlaması

Satın almanın ve stok kayıtlarına yapılan giriş ve çıkışların yoğunluğu dikkate alınarak denetim modüllerinin ayda bir çalıştırılmasının yeterli olacağına karar verilmiştir. Ayda bir yapılan denetimin hile veya hatadan kaynaklanan riskleri kabul edilebilir bir seviyede tutacağı öngörülmüştür.

Her ayın onuncu günü bir önceki aya ait ilgili kayıtlar denetim yazılımına aktarılır ve denetim modülleri çalıştırılır. Her ayın onuncu gününe kadar bir önceki aya ait belgelerin sisteme girilmiş olduğu varsayımı yapılmaktadır.

Bu uygulamanın konusu olan araç takip sistemi projesine ilişkin sözleşme 17 Kasım 2011 tarihinde imzalanmış. Projeye ilişkin testler 2012 başında bitmiş ve üretime Nisan 2012’de geçilmiştir. Projeye ilişkin satın alma büyük ölçüde Mart 2012’de başlamıştır. Bu nedenle denetim testlerinin başlangıç tarihi 1 Nisan 2012 olarak tespit edilmiştir.

10.5. VERİ ERİŞİMİ

Proje ile ilgili tüm bölümlerle (Proje, Tasarım, Satış ve İhale Takip, Üretim, Satın Alma, Muhasebe Bölümleri) görüşülüp kullanılan belgeler ve yapılan kayıtlar konusunda bilgi alınmıştır. Kurum yönetimi Satın Alma ve Muhasebe Bölümlerinden veri alınmasına izin vermiştir.

10.5.1. Veri Erişim Yöntemi

İlgili kişilerin belirlenen zamanlarda ihtiyaç duyulan veriyi istenilen formatta denetçiye göndermelerine karar verilmiştir. Bu veri dosyalarını denetçi kendi denetim yazılımına aktararak kurumdan bağımsız bir şekilde denetimi gerçekleştirecektir.

10.5.2. Verinin Yeri

Kurum kayıtlarını Mikro yazılım şirketinin kurumsal kaynak planlama programında tutmaktadır. Bu yazılım Excel formatına veri aktarabilmektedir. Uygulama için kullanılan ACL denetim yazılımı da Excel formatında veri okuyabilmektedir. Veri formatını değiştirmek için Excel’in kullanımının hataya veya kayba yol açmadığı tespit edilmiştir. Bu nedenle kurumsal kaynak planlama yazılımından alınacak verinin Excel’e dönüştürülmesi ve bu Excel dosyalarının ACL yazılımı tarafından okunması öngörülmüştür.

Satın alma ve üretim sürecinde bazı çalışanların Excel formatında bilgi kaydettiği ve bu bilgiyi iş süreçlerinin bir parçası olarak görevlerini yerine getirmek için kullandıkları tespit edilmiştir. Bu dosyalar kurumsal kaynak planlama yazılımının dışında tutulmaktadır. Bu dosyalardan Satın Alma Bölümü’nün sipariş ve mal alımlarını takip ettiği Excel formatındaki sipariş dosyası denetim sürecine bağımsız kaynak olarak dahil edilmiştir.

Kaynak veri olarak kullanılan dosyalar:

- Sipariş dosyası: Satın Alma Bölümü tarafından tutulan ve alınacak malları gösteren tablodur.
- Yevmiye dökümü: Mikro kurumsal kaynak planlama yazılımı genel muhasebe modülünden alınan bir rapordur. Bu rapor Mikro yazılımında genel muhasebe – raporlar - genel hareket raporları seçilerek elde edilir.
- Cari hesap hareketleri raporu: Mikro kurumsal kaynak planlama yazılımı finans yönetimi modülünden alınan bir rapordur. Bu rapor Mikro yazılımında finans yönetimi – raporlar – cari hesaplar - cari hareket raporu seçilerek elde edilir.
- Cari hesap ekstresi: Mikro kurumsal kaynak planlama yazılımı finans yönetimi modülünden alınan bir dökümdür. Bu döküm Mikro yazılımında finans yönetimi – raporlar – cari hesaplar - cari hesap ekstresi seçilerek elde edilir.
- Stok hareketleri raporu: Mikro kurumsal kaynak planlama yazılımı stok yönetimi modülünden alınan bir rapordur. Bu rapor Mikro yazılımında stok yönetimi – raporlar - stok hareket raporları – detaylı stok hareket raporu seçilerek elde edilir.

Kurumsal kaynak planlama yazılımındaki ilgili kayıtların belirlenen sürelerde muhasebe sorumlusu tarafından Excel formatında denetçiye direkt gönderilmesi, diğer Excel dosyalarının da dosyayı tutan kişi tarafından direkt olarak denetçiye gönderilmesine karar verilmiştir. Böylece farklı kaynaklardan tarafsız bilgi akışı sağlanmıştır.

10.5.3. Veri Talebi

Hataları önlemek için veri talebi kuruma yazılı olarak e-posta yoluyla iletilmektedir.

Aşağıda örnek talep yazısı görülmektedir:

Kime: Muhasebe Bölümü

Kimden: Hülya Hazar

Konu: veri talebi

Talep tarihi: 2 Ocak 2013

Aşağıda belirtilen verinin bir kopyasının tarafıma gönderilmesini rica ederim:

Verinin tutulduğu sistem: Mikro kurumsal kaynak planlama yazılımı

Dosya/rapor ismi: cari hareket raporu

Zaman aralığı: 1-31 Aralık 2012 (dahil)

Filtre ölçütleri:	yok (kayıtların tümü dahil edilecek)
Teslim tarihi:	en geç 10 Ocak 2013
Veri formatı:	Excel dosyası
Veri gönderme aracı:	e-postam

Ayrıca, ilgili dosya/raporların kontrol toplamalarını bildirmenizi rica ederim.

Uygulamanın ilk planlama aşamasında ilgili dosya/raporlara ilişkin meta data bilgisi ve 50 adet kayıt örneği alındığı için aylık veri talebi sırasında bu bilgileri tekrar almaya ihtiyaç duyulmamıştır.

10.5.4. Verinin ACL Denetim Yazılımına Aktarılması

Kurumdan gelen Excel dosyaları ACL'in "data definition wizard" modülü ile ACL tabloları haline dönüştürülür. Bu tablolar ACL dosyası olarak saklanır. ACL tablolarının bulunduğu dosyalar fil uzantılıdır.

Excel dosyaları birer birer ACL tablolarına dönüştürülebilmektedir. Kurumdan gelen dosyaların tamamını birden ACL tablolarına dönüştüren bir komut bu uygulamada kullanılan ACL sürümünde yoktur.

10.6. VERİ ANALİZİ

Veri analizinde kullanılan dosyalar:

- Sipariş dosyası
- Yevmiye dökümü
- Cari hesap hareketleri raporu
- Cari hesap ekstresi
- Stok hareketleri raporu

10.6.1. Veri Bütünlüğü

Denetime başlamadan önce denetim yazılımına aktarılan dosyaların veri bütünlüğü sağlanmalıdır. Bazı kayıtların hiç olmaması veya bazı alanların boş olması kayıtların girişinde veya denetim yazılımına aktarımı sırasında oluşabilir.

Veri genellikle iki şekilde geçersiz kabul edilir:

- Kayıtlardaki bazı alanların boş olması
- Veri tanımlarındaki uyumsuzluklar

Geçersiz veri aşağıdaki nedenlerden oluşur:

- Veri girişinde yapılan hatalar: Örneğin, fatura kaydı giren kişinin yanlışlıkla tarih alanına carinin adını yazması veri alanlarında tanım uyumsuzluğuna yol açar.
- Verinin tanımlamasında yapılan hatalar: Örneğin, metin girilmesi gereken bir alan tarih olarak tanımlanmış olabilir.
- Veri aktarımı sırasında oluşan hatalar: Örneğin, kaynak veriyi denetim yazılımına aktarma sırasında kurumsal kaynak planlama yazılımının veritabanı ile denetim yazılımının veritabanı arasındaki iletişimin kesilmesi verinin bir bölümünün aktarılamamasına yol açabilir.
- Veri yapılarının korunması ile ilgili hatalar: Kaynak verini aktarılması veya tabloların birleştirilmesi sırasında ilgili alanların farklı tanımlanmış olması veri yapılarında hataya neden olacaktır. Örneğin, cari kod alanı bir tabloda sayısal diğer bir tabloda metin olarak tanımlanmış olabilir. Bu iki tablonun birleştirilmesi sırasında yeni yaratılan alan ya geçersiz karakterlerden oluşacak veya boş çıkacaktır.

Geçerlilik kontrolü:

Veri bütünlüğünü doğrulamak için tablonun geçerliliği kontrol edilmelidir. Tablodaki veriler doğruysa ve tablonun alan tanımları veriyle uyuyorsa ilgili tablonun geçerli olduğu kabul edilir. Analize başlamadan önce geçerlilik hatalarının çözülmesi gerekir.

Verify komutu

Verify komutu kaynak veriyi, bu verinin denetim yazılımına transferi sırasında oluşabilecek sorunları ve tablodaki tanımlama hatalarını aşağıdaki şekilde kontrol eder:

- Karakter alanlarında sadece geçerli yazdırılabilir karakterlerin (harfler, rakamlar, semboller ve uluslararası karakterler) varlığı kontrol edilir. Veride görünmeyen, yazdırılamaz nitelikte karakterlerin olması durumunda yazılım geçerlilik hatası bildirecektir.
- Sayısal alanlarda sadece geçerli sayısal karakterlerin (rakamlar, ondalık haneler ve para birimleri) yer aldığını kontrol eder.
- Tarih alanlarında sadece geçerli tarihlerin yer aldığını kontrol eder. Tarih alanlarında hata oluştuğunda tarih formatı ve tarihlerin geçerli takvim tarihleri olduğu kontrol edilmelidir.

Kontrol toplamalarının teyit edilmesi:

Veri ile ilgili kurumdan alınan bilgi ile denetim yazılımında oluşturulan tabloların tutarlı olması gerekir. Kontrol toplamalarının teyidi denetim yazılımına aktarılan verinin bozuk olup olmadığını, aktarılan kayıtların sayısının kaynak dosyadaki kayıt sayısı ile aynı olup olmadığını belirlemek için yapılır. Denetim yazılımında aktarılan kayıt sayısı kaynak dosyadaki kayıt sayısına eşit olmalıdır. Kontrol toplamaları kurumdan alınan toplamalarla uyuşmuyorsa ACL’de oluşturulan tabloların kaynak verilerden doğru olarak derlenmediğini, aktarılan kayıt sayısının az veya fazla olduğunu gösterir.

ACL’de Count, Total ve Statistics komutları kontrol toplamalarının teyidi için yapılan analizde kullanılır.

Count: Kayıt sayısını gösterir.

Total: Sayısal alanların toplamalarını gösterir. Tarih alanları ile kullanılmaz.

Statistics: Kontrol toplamalarını oluşturur. Tarih alanları ile de kullanılabilir.

Sınır değerleri:

Tabloların alt ve üst sınır değerlerinin istenilen doğrultuda olduğuna emin olmak gerekir. Örneğin, cari borçların yer aldığı bir alanın alt sınır değerinin sıfıra eşit veya büyük olması, üst sınır değerinin de pozitif bir sayı olması beklenir. 2012 yılı için yapılacak analizlerde kayıt tarihinin alt sınırının 1 Ocak 2012, üst sınırının 31 Aralık 2012 olması gerekir. Tabloda sınırlar dışında kalan kayıtlar varsa geçerli kayıtlar filtrelenerek yeni bir tablo oluşturulur. Kayıtlar yetersizse kaynak veri kurumdan tekrar istenir.

ACL’de Statistics komutu ve Between() fonksiyonu verilerin beklenen değerlerin sınırları içinde olup olmadığını kontrol etmek için kullanılır.

Statistics: Kontrol toplamlarının ek olarak bir alanın sayısal ve tarih tipindeki verileri için sınır değerlerini de gösterir. Bu değerler verinin doğruluğunu kesinleştirmek için bilinen değerlerle karşılaştırılır.

Between(): Sayısal, tarih veya karakter verileri belirtilen sınırlar arasında kalan kayıtların elde edilmesi için kullanılan bir filtreleme fonksiyonudur.

Eksik kayıtların saptanması:

Kontrol toplamları kurumdan alınan özet raporla aynı olsa bile kayıtların tam olduğu anlamına gelmez. Kayıtlarda eksik değerler olabilir.

ACL'de Gaps komutu ve Isblank() fonksiyonu kullanılarak kayıtların tamam olup olmadığı kontrol edilir.

Gaps: Sıralı rakamlardan oluşan bir listede eksik değer aralıklarını ve eksik değerleri ortaya çıkarır.

Isblank(): Değer girilmemiş alanı olan kayıtları çıkartır. Hiçbir zaman boş kalmaması gereken alanlar için kullanılır. Örneğin, kayıt tarihi, müşteri numarası vb. kritik alanlarda eksiklik olmamalıdır.

Mükerrer kayıtların saptanması:

Bir tabloda bazı alanlarda mükerrer değerler olabilir. Örneğin, aynı satıcıdan birçok kez mal alınmış olabilir. Bu nedenle fatura dökümü incelendiğinde ilgili satıcıya ait birçok kayıt bulunacaktır. Ancak, bazı değerler sadece bir kez yer almalıdır. Örneğin, satıcıların listelendiği bir tabloda bir satıcı birden fazla aynı veya benzer adlarla yer alıyorsa aynı cari için birden fazla hesap açılmış demektir. Mükerrer kayıtların geçerlilikleri kendi kapsamları çerçevesinde incelenir.

ACL'de Duplicates komutu aynı değeri taşıyan kayıtları belirler.

Duplicates: Bu komut tümüyle mükerrer olan kayıtları veya sadece belli alanlarında mükerrer değer taşıyan kayıtları bulmak için kullanılır.

Güvenilirlik testi:

Kaynak veride bazı alanlar başka alanlar kullanılarak hesaplanmış olabilir. Hesaplanan değerlerin doğru olup olmadığı kontrol edilmelidir. Örneğin, bir mal kaleminin toplam satış fiyatı birim fiyatı ile satış miktarının çarpımına eşittir. Bu hesaplama tekrar yapılarak toplam değerler kontrol edilir.

Makullük derecesinin test edilmesi:

Bir tabloda hangi verilerinin bulunması gerektiğiyle ilgili olarak kimi zaman sağduyulu varsayımlara ihtiyaç olabilir. Bu varsayımları test etmek için, çeşitli komutlar kullanılır.

İlişkilerin test edilmesi:

İlişkilerin test edilmesi iki alandaki verilerin tutarlı olup olmadığının teyididir. İki alan karşılaştırılarak ilişkiler test edilir. Bu karşılaştırma filtreler kullanılarak veya alanlar arasındaki farkı hesaplayarak yapılabilir.

Tablo 8
Veri Bütünlüğünün Analizi İçin Uygulanan Testler

Kontrol	Amaç	ACL Komutu
Geçerlilik	Veri tipleri ve alan tanımlarının uygunluğu	Verify
Kontrol Toplamları	Kayıt sayısının kontrolü	Count
	Sayısal alan toplamlarının kontrol toplamlarına uygunluğu	Total
	Kayıt ve alan toplamlarının kontrol toplamlarına uygunluğu	Statistics
Sınır Değerleri	Verilerin doğru sınırlar içinde olması	Statistics
	Verilerin doğru sınırlar içinde olması	Between ()
Eksik Kayıtlar	Sıralama dışında kalan değerlerin olmaması	Gaps
	Alanlarda olmaması gereken boşlukların kontrolü	Isblank ()
Mükerrer Kayıtlar	Tablolarda mükerrer kayıtların veya mükerrer değerlerin olmaması	Duplicates
Güvenilirlik	Kaynak verilerdeki hesaplamaların doğruluğu	Hesaplanmış alanlar
Makullük	Verilerin beklentileri karşılaması	Çeşitli komutlar
İlişkiler	Verilerin alanlar arasında tutarlı olması	Çeşitli komutlar

Tablo 9

Veri Bütünlüğü Testlerinin Uygulandığı Tablo Alanları

	Sipariş Dosyası	Yevmiye Dökümü	Stok Hareketleri Raporu	Cari Hesap Hareketleri Raporu	Cari Hesap Ekstresi
Verify	tüm alanlar	tüm alanlar	tüm alanlar	tüm alanlar	tüm alanlar
Count	tüm tablo (alan seçilmesi gerekmiyor)	tüm tablo (alan seçilmesi gerekmiyor)	tüm tablo (alan seçilmesi gerekmiyor)	tüm tablo (alan seçilmesi gerekmiyor)	tüm tablo (alan seçilmesi gerekmiyor)
Total	Adet Giren net tutar	Borç Alacak	Giren net tutar Çıkan net tutar	Cari hesap borç Cari hesap alacak	TL borç TL alacak
Statistics	Tarih Birim fiyat Adet Giren net tutar	Tarih Borç Alacak	Tarih Giren net tutar Çıkan net tutar Muhasebe fiş tarihi	Tarih Cari hesap borç Cari hesap alacak Muhasebe fiş tarihi	Tarih TL borç TL alacak
Between()	Tarih	Tarih	Tarih	Tarih	Tarih
Isblank()	Stok kodu Tarih Cari kodu Birim fiyat Adet Giren net tutar	Yevmiye no Tarih Sıra no Hesap kodu Borç Alacak	Stok kodu Muhasebe kodu Tarih Cari adı Evrak tipi Evrak no Muhasebe fiş tarihi Muhasebe fiş no	Tarih Evrak no Evrak cinsi Vade Cari hesap kodu Muhasebe fiş tarihi Muhasebe fiş sıra no	Tarih Evrak no Evrak cinsi Vade Cari hesap kodu
Duplicates	Stok kodu				
Hesaplanmış Alanlar	Birim fiyat x adet = giren net tutar				Giriş miktarı x stok net birim fiyat (ana) = stok net tutar (ana)

10.6.2. Dijital Analizler

Buradaki sürekli denetim uygulaması üretim müdürünün ilgili proje için satın alma talebinde bulunması ile başlayan ve alınan mallar için ödemenin yapılması ile son bulan süreçteki finansal işlemleri kapsamaktadır.

Dijital analizler kaynak veriden denetim yazılımına aktararak oluşturulan tabloların veri bütünlüğü kontrolü yapıldıktan sonra uygulanmalıdır. Veri bütünlüğü sağlanmamış tablolar üzerinde yapılacak dijital analizler yanlış sonuçlara varılmasına yol açabilir.

10.6.2.1. Geçerlilik Kontrol Testleri

Süreç kontrolü:

Satın alma talebi için uygulanacak kontrol testleri bölümler arasında süreçte belirtilen bilgi ve belge akışının da değerlendirilmesine yardımcı olur. Alınan ve ödemesi yapılan mallar satın alma talebi ile uyuyorsa Üretim müdürü – Satın Alma Bölümü, Depo – Satın Alma Bölümü ve Satın Alma Bölümü – Muhasebe Bölümü arasındaki bilgi ve belge akışının zımnen belirlendiği gibi olduğunu düşünebiliriz.

Onaylama satın alma işlemlerine ilişkin belgelerin arkasına yetkili kişinin imza atması ile yapılmaktadır. Onaylama sürecinin kanıtları dijital ortamda olmadığı için bu sürecin geçerlilik kontrol testleri yapılamamaktadır.

Satın alma talebi kontrolü:

Mal alımında faturalar stok yönetimi modülü kullanılarak kurumsal kaynak planlama yazılımına kaydedilmektedir. Bu nedenle sipariş dosyasındaki satıcı ve stok isimleri ile stok hareketleri raporundaki cari hesap ve stok isimleri karşılaştırılır. İlgili projeye ait yapılmış kayıtlardaki cari hesap ve stok isimlerinin sipariş dosyasındaki isimlerle uyuşması gerekir. İsimlerde farklılık aşağıdaki durumlarda ortaya çıkar:

- Sipariş dosyası ile kurumsal kaynak planlama yazılımına cari hesap ve stok isimlerinin aynı şekilde girilmesi gerekir. Aynı olmaması durumunda denetim yazılımı karşılaştırma yaparken onları eşleştiremeyecektir. Kısaltmalar, noktalama işaretleri, büyük ve küçük harflerin kullanımı yazımda farklılık oluşturur. Bir insanın iki dosyadaki ismi karşılaştırırken aynı olduğunu kabul edebileceği durumlarda bilgisayar karşılaştırma işlemini yaparken hatalı olarak kabul edebilir. Bu hataları önlemek için

karşılaştırmaları yaparken cari hesapların ve stokların kodlarının kullanılması daha uygun olacaktır. Her cari hesap ve stok için kodlar özgündür. Bu nedenle bu uygulamada isimler yerine kodlar karşılaştırılmıştır.

- Mal Satın Alma Bölümü'nün onayladığı satıcıdan alınmamıştır.
- Talep edilenden farklı mallar satın alınmıştır.
- Satın Alma Bölümü'nün onayı istenmeden Üretim Bölümü direkt olarak malı satın almıştır. Bu durum satın alma sürecinde hata olduğunu gösterir.
- Proje kodu hatalı girilmiştir. Sevk irsaliyesi ve faturanın arkasına ilgili proje kodu yazılır. Girişler yapılırken bu kod esas alınır. Depo sorumlusunun proje kodunu yanlış girmesi ve daha sonra onaylayan kişilerin bunu fark etmemeleri veya kurumsal kaynak planlama yazılımına başka bir projeye ait işlemin kaydı yapılırken ilgili projenin kodunun yazılması bu duruma neden olur.

	Sipariş Dosyası	Stok Hareketleri Raporu
Filtre	Proje kodu = 455	Proje kodu = 455
		Evrak tipi = giriş faturası
		Hareket cinsi = toptan
Karşılaştırma	Stok kodu	Stok kodu
	Cari kod	Cari kodu

Alış faturalarının işlenmesi:

Alış faturalarının mizana doğru yansıdığını denetlemek için alış faturalarının yevmiye dökümünde yer alıp almadığı kontrol edilir. Alış faturalarının kurumsal kaynak planlama yazılımına kaydı ile cari hesaplar etkilenir ve ilgili satıcının hesabı alacaklanır. Mizan ve finansal tabloların temeli ise yevmiye kayıtlarıdır. Bu nedenle cari hesap hareketleri raporundaki alış faturaları yevmiye dökümündeki alış faturaları ile karşılaştırılır. İki dosyadaki değerler birbirini tutuyorsa alış faturaları hesaplara ve mizana doğru işlenmiştir.

	Cari Hesap Hareketleri Raporu	Yevmiye Dökümü
Filtre	Proje kodu = 455	Proje kodu = 455
	Evrak cinsi = alış faturası	Fiş tipi = mahsup
	Hareket cinsi = toptan fatura	
İlişkilendirme	Evrak no	Açıklama = Al.fat.:<evrak no>
	Muhasebe fiş tarihi	Tarih
	Muhasebe fişi yevmiye no	Yevmiye no
	Muhasebe fiş sıra no	Sıra no
Karşılaştırma	Cari hesap ismi	Hesap adı
	Cari hesap alacak	Alacak

Cari hesap hareketleri raporunda muhasebe kodu yer almadığı için hesap isimleri karşılaştırılmıştır. Cari hesap hareketleri raporu finans modülünden alınmakta olup yine bu modüldeki cari hesap kartlarında yer alan isimleri esas alır. Yevmiye dökümü ise genel muhasebe modülünden alınan bir rapordur ve hesap adlarını hesap planından alır. Satıcılar için cari hesap kartları açılırken girilen isimler muhasebe hesap planına birebir girilmemiş, çeşitli kısaltmalar yapılmıştır. Örneğin, cari hesap kartında “Burç Makina Ticaret Limited Şirketi” yazılmış olan satıcı hesap planına “Burç Makina Ltd.Şti.” olarak girilmiştir. Bu nedenle bu uygulamada cari hesapların isimleri ilk beş harflerine göre karşılaştırılmıştır.

Ödemenin kontrolü:

Ödemelerin denetimine ilişkin uygulama geliştirirken iki önemli sorun karşımıza çıkmaktadır:

- Ödemelerin cari hesap modülüne yansımaması: Muhasebe bölümü yapılan ödemeleri kurumsal kaynak planlama yazılımına iki farklı modül kullanarak işlemektedir. Satıcılara çek ve senet ile yapılan ödemeler kurumsal kaynak planlama yazılımına finans yönetimi modülündeki çek senet bölümü kullanılarak kaydedilmektedir. Bu modül kullanıldığı zaman ilgili ödeme finans yönetimi modülündeki cari hesaplara yansır. İlgili kayıtları da cari hesap hareketleri raporunda görmemize olanak verir. Muhasebe entegrasyonu ile bu kayıtlar ilgili muhasebe hesaplarına yansır. Muhasebe entegrasyonu sonrasında bu işlemleri yevmiye dökümünde izlemek mümkündür. Satıcılara bankadan ve kasadan yapılan ödemeler kurumsal kaynak planlama yazılımına genel muhasebe modülü ile kaydedilmektedir. Muhasebe entegrasyonu tek yönlü işleyen bir sistemdir. Genel muhasebe modülünden yapılan işlemleri diğer modüllere yansıtan bir entegrasyon olanağı bulunmamaktadır. Genel muhasebe modülü ile kaydedilen işlemler finans yönetimi modülündeki cari hesaplara yansımadığı için nakit ve bankadan yapılan ödemeleri cari hesap hareketleri raporunda görmek mümkün değildir. Bu işlemlerin izlenebileceği raporlar sadece genel muhasebe modülünden elde edilen raporlardır. Satıcılara yapılan ödeme işlemlerine ait kayıtların tamamı yevmiye dökümünde yer almaktadır. Bu nedenle bu uygulamada ödeme işlemlerine ilişkin denetim yevmiye dökümü kullanılarak gerçekleştirilmiştir.
- Ödemelere ilişkin kayıtlarda proje kodunun kullanılmaması: Aynı satıcıdan birden fazla projeye ilişkin mal alınabildiği için satıcının toplam alacağı farklı projelerden kaynaklanabilmektedir. Satıcıya avans ödemesi yapılabildiği gibi ödeme birden fazla

havale ile gerçekleştirilebilmektedir. Muhasebe bölümü ödemeleri yaparken proje bazında ayırım yapmamakta ve ilgili kaydı girerken proje kodu koymamaktadır. Bu nedenle kurumsal kaynak planlama yazılımından alınan raporlarda ödemeler ile projeleri birebir karşılaştırmak mümkün değildir.

Ödemelerin onaylanan mallar ve ilgili satıcılara yapıldığını denetlemek için sipariş dosyası ile yevmiye dökümü karşılaştırılır. Yukarıda belirtilen zorluklar nedeniyle bu uygulamada sipariş dosyası ve yevmiye dökümü kullanılarak alınan mallarla ilgili herhangi bir ödemenin gerçekleşip gerçekleşmediği kontrol edilmiştir. Ödeme ile ilgili fişlerde proje kodu bulunmadığı için bu analizde yevmiye dökümü proje kodu ile filtrelenmemelidir. Bu kontrol sipariş dosyasında adı geçen satıcılara yapılan ödemelerin projeye ilgili olma olasılığının yüksek olmasına dayanmaktadır.

Satın alınması planlanan ancak alımı henüz gerçekleşmemiş stoklar varsa sipariş dosyasında kaydı olduğu halde yevmiye dökümünde yer almayacaktır. Alımı gerçekleşen stokların mal alım faturalarının numaraları sipariş dosyasının “evrak no” alanına yazılmaktadır. Sipariş dosyasında evrak numarası olan kayıtlar yevmiye dökümünde aranmalıdır.

	Sipariş Dosyası	Yevmiye Dökümü
Filtre	Proje kodu = 455	
	Evrak no > 0	
		Hesap kodu = 12 veya 32 (başlayanlar)
		Fiş tipi = tediye, mahsup
		Borç > 0
Karşılaştırma	Muhasebe cari kodu	Hesap kodu

10.6.2.2. Tamlik – Bütünlük Kontrol Testleri

Gerçekleşmiş işlemlerin kurumsal kaynak planlama yazılımına kaydedilmiş olduğu sıra numaraları ve etkilenen hesapların kontrolü ile denetlenir.

Sıra numarası kontrolü:

Mikro kurumsal kaynak planlama yazılımında yer alan modüllere kayıt girerken kullanılan tüm fişlerde fişin tarihi ve sıra numarasını gösteren alanlar vardır. Her yeni kayıt

girildiğinde fiş tarihi olarak günün tarihi, sıra numarası olarak da bilgisayar tarafından otomatik olarak verilen ardışık fiş numaraları ekrana yansır. Fiş numarası sadece bir kez kullanılan bir sayıdır. Ayrıca, evrak veya belge numarası ve tarihi adı altında iki alan daha bulunmaktadır. Bu alanların amacı fatura, irsaliye, çek senet bordrosu, banka dekontu gibi kurumun aldığı ve verdiği belgelerin üzerinde yer alan tarih ve seri/sıra numaralarını kaydetmektir. Mikro yazılımı kullanıcının bu alanlara müdahale etmesine, kullanıcının istediği tarihi ve fiş numarasını girmesine olanak vermektedir. Tarih alanlarına sadece tarih formatında bilgi yazılabilirken sıra veya belge numarasını gösteren alanlara hem harf hem de sayı yazılmasına olanak vermektedir. Kurum çalışanları Mikro yazılımına veri girişi sırasında fişin tarih ve sıra numarasını gösteren alana belgenin tarih ve numarasını kaydetmektedirler. Bu nedenle fiş tarih/sıra numarası ile belge tarih/sıra numarası aynı olmaktadır. Bu uygulama nedeniyle Mikro yazılımına yapılan kayıtlar ardışık sıra numarası takip etmemekte ve sıra numarası kontrolü yapılamamaktadır. Tamlik bütünlük testlerinin daha sağlıklı olabilmesi için fiş tarih ve sıra numaralarına kullanıcıların müdahale etmemesi önerilir. Belgelerin orijinal tarih ve sıra numaralarını kaydetmek için ilgili alanlar vardır. Aynı tarih ve numarayı iki yere kaydetmek alınan raporların değerini arttırmamaktadır.

Sıra numarası kontrolü yapılabilecek tek tablo sipariş dosyasıdır. Sipariş dosyası üretim müdüründen gelen talep doğrultusunda projenin üretimine başlanmadan hazırlanan ve projenin tamamlanması için alınacak malları gösteren bir tablodur. Bu tabloda her satır alınacak bir stok için ilgili bilgiyi içerir. Her satıra sıra numarası olarak 1 ile başlayan ardışık sayılar verilmiştir. ACL'in Gaps komutu kullanılarak sıra numaraları kontrol edilir. Gaps komutu sıralı bir sayı listesinde eksik kalemleri gösterir. Sipariş dosyasında sıra numaralarının birbirini takip etmemesi onaylama sürecinden sonra eklenen veya çıkartılan bir satın almayı işaret edebilir.

	Sipariş Dosyası
Komut = Gaps	Sıra no

Etkilenen hesapların kontrolü:

Mal satın alındığında fatura numarası sipariş dosyasında “evrak no” başlıklı alana kaydedilir. “evrak no” alanı dolu ise ilgili malın kaydı kurumsal kaynak planlama yazılımında aranır. Satın alınan malın fatura girişi kurumsal kaynak planlama yazılımına stok yönetimi modülündeki fatura bölümünden yapılır. Fatura kaydı yapıldığı anda ilgili cari hesap ve stok

hesapları etkilenecektir. Muhasebe entegrasyonu sonrasında da bu fatura girişi muhasebe hesaplarına yansıyacaktır. Kurumsal kaynak planlama yazılımına ilgili fatura işlenmişse stok hareketleri raporunda izlenebilir. Sipariş dosyasında evrak numarası olan kayıtlar stok hareketlerinde izlenebilmelidir.

	Sipariş Dosyası	Stok Hareketleri Raporu
Filtre	Proje kodu=455	Proje kodu = 455
	Evrak no > 0	
		Evrak tipi = giriş faturası
		Hareket cinsi = toptan
İlişkilendirme	Stok kodu	Stok kodu
	Cari kod	Cari kodu

10.6.2.3. Doğruluk Kontrol Testleri

Doğruluk kontrol testleri olması gereken ve kayıt edilen işlemlerin tutarlılığını kontrol eder.

İşlemlerin doğru kaydedildiğinin kontrolü:

Kurumsal kaynak planlama yazılımının farklı modüllerinden alınan rapor ve dökümlerdeki kayıtlar birbirleriyle eşleştirilir. Bu eşleştirme farklı modüllere yapılan girişlerin ve etkilenen hesapların birbirleriyle tutarlılığını gösterir. Yapılan eşleşmede kayıtlar uyuşuyorsa işlemlerin kurumsal kaynak planlama yazılımının tüm modüllerine doğru girildiği sonucuna varılır. Böylece işlemlerin mekanik doğruluğu kontrol edilmiş olur. Aşağıdaki tablolar belirtilen şekilde filtrelendir ve eşleştirilir:

	Cari Hesap Ekstresi	Stok Hareketleri Raporu
Filtre	Proje kodu = 455	Proje kodu = 455
	Evrak cinsi = alış faturası	Evrak tipi = giriş faturası
	Hareket cinsi = toptan fatura	Hareket cinsi = toptan
İlişkilendirme	Evrak no	Evrak no
	Cari hesap kodu	Cari kodu
	Stok/... kodu	Stok kodu
Karşılaştırma	Stok net tutar (ana)	Giren net tutar

	Cari Hesap Hareketleri Raporu	Yevmiye Dökümü
Filtre	Proje kodu = 455	Proje kodu = 455
	Evrak cinsi = alış faturası	Fiş tipi = mahsup
	Hareket cinsi = toptan fatura	
İlişkilendirme	Evrak no	(Açıklama)
	Muhasebe fiş tarihi	Tarih
Karşılaştırma	Cari hesap alacak	Alacak

Hesaplanan tutarlarının kontrolü:

İlgili dosyalardaki hesaplanan tutarların kontrolü aşağıdaki gibidir:

	Sipariş Dosyası
İşlem yapılacak alanlar	Birim fiyat
	Adet
Karşılaştırma yapılacak alan	Giren net tutar
İşlem	Birim fiyat x Adet
Karşılaştırma	Birim fiyat x Adet = Giren net tutar

	Cari Hesap Ekstresi
İşlem yapılacak alanlar	Stok net birim fiyat (ana)
	Giriş miktarı
Karşılaştırma yapılacak alan	Stok net tutar (ana)
İşlem	Stok net birim fiyat (ana) x Giriş miktarı
Karşılaştırma	Stok net birim fiyat (ana) x Giriş miktarı = Stok net tutar (ana)

Satın almanın planlanan şekilde gerçekleştiğinin kontrolü:

Sipariş dosyasında yer alan satıcı, alınacak mal, malın miktarı ve fiyatı onaylanan satın alma talebidir. Bu nedenle sipariş dosyasındaki bilgiler kurumsal kaynak planlama yazılımına yapılan kayıtlar ile karşılaştırılarak satın almanın planlanan şekilde gerçekleştiği kontrol edilebilir. Yapılan karşılaştırmada kayıtlar uyuşuyorsa işlemlerin doğru olduğu sonucuna varılır. Kurumsal kaynak planlama yazılımından alınan cari hesap ekstresi alınan mala ilişkin bilgilerin kontrolü için sipariş dosyası ile karşılaştırılır. Proje ile ilgili mallar değişik tarihlerde alınabileceği için denetim yapılan güne kadar proje ile ilgili alımlar toplanır ve sipariş dosyasında yer alan adet ve tutarlarla karşılaştırılır.

	Sipariş Dosyası	Cari Hesap Ekstresi
Filtre	Proje kodu = 455	Proje kodu = 455
		Evrak cinsi = alış faturası
		Hareket cinsi = toptan fatura
İlişkilendirme	Stok kodu	Stok/... kodu
Karşılaştırma	Cari kod	Cari hesap kodu
	Adet	Giriş miktarı
	Birim fiyat	Stok net birim fiyat (ana)
	Giren net tutar	Stok net tutar (ana)

Cari hesap ekstresinden elde edilen miktar ve tutar toplamalarının en fazla sipariş dosyasında yer alan miktar ve tutarlar kadar olması beklenir. Giriş miktarı sipariş dosyasında yer alan adetlerin üzerindeyse planlanandan fazla alım yapılmış, “stok net birim fiyat (ana)” “birim fiyat”tan daha yüksekse onaylanandan daha pahalıya alınmış demektir. Cari kodların uyuşmaması ise malın onaylanan satıcıdan alınmamış olduğunu gösterir.

10.6.2.4. Sınıflandırma Kontrol Testleri

Mal alım faturalarını işlerken ilgili muhasebe stok kodu “15” ile başlamalıdır. Cari hesapların muhasebe kodları ise alıcılar için “12” veya satıcılar için “32” ile başlamalıdır. Bazı satıcılar aynı zamanda alıcı oldukları için firma yetkilileri ilgili cari hesapları “120 Alıcılar” altında sınıflama yapmışlardır. İşlemlerin doğru ana hesaplara kaydedildiğini kontrol etmek için kurumsal kaynak planlama yazılımından alınan yevmiye dökümü aşağıda belirtilen şekilde filtrelenir ve olması gereken muhasebe kodları ile karşılaştırılır. Yapılan karşılaştırmada muhasebe hesap kodları uyuşuyorsa işlemlerin doğru sınıflandırıldığı sonucuna varılır.

	Yevmiye Dökümü
Filtre	Proje kodu = 455
	Fiş tipi = mahsup
	(Açıklama) = Al.fat.
	Hesap kodu <> 7**
Karşılaştırma	Alacak > 0 ise, Hesap kodu = 12 veya 32 (başlayanlar)
	Borç >0 ise, Hesap kodu = 15 (başlayanlar) veya 191*

* Yevmiye dökümünde alış faturaları için borçlu hesap stok hesabı veya 191 İndirilecek KDV hesabı olabilir.

** 7 Maliyet hesaplarına ilişkin kayıtlar analiz kapsamına alınmamıştır.

10.6.2.5. Zamanlılık Kontrol Testleri

Bilgi sistemine kayıt:

Kurumsal kaynak planlama yazılımına işlemler kaydedilirken fiş tarihi alanına belge tarihi girilmektedir. Bu nedenle fişlerin sisteme kaydediliş tarihleri denetim yapılmak üzere alınan raporlarda ve dökümlerde yer almamaktadır. Bu da ilgili raporlara ve dökümlere dayanarak belgelerin kurumsal kaynak planlama yazılımına kaydı için geçen sürenin tespitini olanaksız kılmaktadır.

Belge tarihi:

Mal alım faturaları kurumsal kaynak planlama yazılımına stok yönetimi modülü kullanılarak işlenir. Stok yönetimi modülünden girilen fişler kanuni süre olan on gün içinde topluca genel muhasebe modülüne aktarılmaktadır. Bu nedenle yevmiye maddelerinin tarihleri ile ilgili fişlerin tarihleri birbirinden farklıdır. Fişin tarihi aynı zamanda faturanın da tarihidir. Stok yönetimi modülünden kaydedilen mal alım faturalarına ilişkin fiş tarihlerinin ilgili kaydın muhasebe fiş tarihi ile karşılaştırarak belgelerin kanuni süresi içinde muhasebeleştirildiğini kontrol edebiliriz.

	Stok Hareketleri Raporu
Filtre	Proje kodu = 455
	Evrak tipi = giriş faturası
	Hareket cinsi = toptan
Doğrulama	(Muhasebe fiş tarihi) =< (Tarih + 10)

10.6.2.6. Yetkilendirme Kontrol Testleri

Kurumda tüm satın alma işlemleri Satın Alma Bölümü'nün yetki ve sorumluluğundadır. Projeye ait satın alımlar büyük ölçüde Satın Alma Bölümü çalışanları tarafından gerçekleştirilmektedir. Üretim sırasında acil ihtiyaç duyulan malzemeler Satın Alma Bölümü'nün bilgisi dahilinde Üretim Bölümü tarafından alınmaktadır.

Satın Alma Bölümü projeyle ilgili yapılması gereken tüm alımları sipariş dosyasına kaydetmektedir. Gerçekleşen alımlar ise stok yönetimi modülündeki mal alım faturası ile kurumsal kaynak planlama yazılımına kaydedilmektedir.

Gerçekleşen alımların sipariş dosyasında olması yapılan alımların Satın Alma Bölümü'nün bilgisi dahilinde olduğunun işaretidir. Stok hareketleri raporunda ilgili projeye ait mal alım faturaları sipariş dosyasında yer alıyorsa mal alımlarının yetkili kişiler tarafından yapıldığı sonucuna ulaşılır.

	Sipariş Dosyası	Stok Hareketleri Raporu
Filtre	Proje kodu = 455	Proje kodu = 455
		Evrak tipi = giriş faturası
		Hareket cinsi = toptan
Karşılaştırma	Stok kodu	Stok kodu

10.6.2.7. Görev Ayrımları Kontrol Testleri

Kurumun bilgi sisteminden alınan raporlarda kayıtların kimler tarafından girildiğine dair bilgi bulunmamaktadır. Bu nedenle bu konuda dijital analiz yapılamamıştır. Ancak, aşağıdaki nedenlerden dolayı kurumda görev ayrımları olduğu ve etkin olarak işlediği düşünülebilir:

1. Sipariş eden ile teslim alan ayrımı: Satın Alma Bölümü tarafından sipariş edilen mallar üretim yerinin depo sorumlusu tarafından teslim alınmaktadır. Kurum faaliyetleri birçok fiziki mekana dağılmış bulunmaktadır. Satın Alma Bölümü İstanbul Kozyatağı'ndaki merkez büroda çalışırken bu uygulamada yer alan projenin üretim yeri ve deposu İstanbul Tarabya'da bulunmaktadır. Bu nedenle sipariş eden ile malı teslim alan kişinin aynı kişi olması mümkün değildir.
2. Sipariş eden ile ödeme yapan görev ayrımı: Sipariş işlemleri Satın Alma Bölümü tarafından yürütülmekte ve satıcılarla tüm iletişim bu bölümün yetkilileri tarafından yürütülmektedir. Ödemeyi yapan kişiler Muhasebe Bölümü yetkilileridir. Bu nedenle sipariş veren ile ödemeyi yapan kişiler birbirinden farklıdır.
3. Fatura, cari hesap, ödeme ve büyük defter işlemlerinde görev ayrımı: Görev ayrımları konusunda tek risk ödemenin, fatura girişinin ve muhasebe hesaplarına kayıtları aktarma işlemlerinin Muhasebe Bölümü tarafından yapılmasıdır. Ayrıca, Muhasebe Bölümü çalışanları kurumsal kaynak planlama yazılımının tüm modüllerine giriş yapma, güncelleme ve silme yetkisine de sahiptir. Ancak, satıcı ilişkileri Satın Alma tarafından sağlandığı için satıcılara yapılan ödemeler ve satıcı hesapları sürekli Satın

Alma Bölümü çalışanları tarafından kontrol edilmektedir. Bu da hata ve hile riskini azaltmaktadır.

10.6.2.8. Özetleme Kontrol Testleri

Kurum tarafından kullanılmakta olan Mikro kurumsal kaynak planlama yazılımında stok işlemleri stok yönetimi modülünden yapılmaktadır. Girilen mal alım faturaları ilgili stok hesaplarını borçlandırırken ilgili cari hesapları da alacaklandırmaktadır. Kayıtlar ilgili muhasebe hesaplarına entegrasyon yoluyla aktarılmaktadır. Bu modüllerden yapılan kayıtların doğru muhasebe hesaplarına gittiğini kontrol etmek için stok hareketleri raporunda yer alan işlemlerin muhasebe hesap kodları yevmiye dökümünde yer alan hesap kodlarıyla karşılaştırılır. Stok hareketleri raporundaki muhasebe hesap kodu yevmiye dökümündeki ilgili kaydın muhasebe kodu ile uyuşuyorsa mal alımda hareket gören hesaplar doğru muhasebe hesaplarına kaydedilmiş kabul edilebilir.

	Stok Hareketleri Raporu	Yevmiye Dökümü
Filtre	Proje kodu=455	Proje kodu=455
	Evrak tipi = giriş faturası	Fiş tipi = mahsup
	Hareket cinsi = toptan	
	Giren net tutar > 0	Borç > 0
İlişkilendirme	Evrak no	(Açıklama)
	Muhasebe fiş tarihi	Tarih
	Muhasebe fiş no	Sıra no
	Giren net tutar	Borç
Karşılaştırma	Muhasebe kodu	Hesap kodu

10.6.2.9. Benford Analizi

Alış faturalarının belge numaraları üzerinde yapılacak Benford Analizi kurumsal kaynak planlama yazılımına kaydedilen faturalarda hile tespiti için kullanılabilir. Fatura numaralarındaki hanelerin tekrarlanma yüzdesi teorik tekrarlanma olasılığı ile karşılaştırılır.

Benford Kanunu'na göre fatura numaralarının ilk hanesinin istatistiki dağılımı aşağıdaki gibi olmalıdır:

1 = % 30,1 2 = % 17,6 3 = % 12,5 4 = % 9,7 5 = % 7,9
6 = % 6,7 7 = % 5,8 8 = % 5,1 9 = % 4,6

Gerçekleşen dağılımın bu teorik dağılımdan farklı olması durumunda gerçek olmayan faturaların kurumsal kaynak planlama yazılımına kaydedilmiş olma ihtimalinden söz edilebilir.

Benford Kanunu'nun hileyi ortaya çıkartma oranı %68'dir. Bu durumda Benford analizine dayanarak gerçek bir faturayı olağandışı olarak raporlama ihtimali çok yüksektir.

Bu uygulamada kullanılan kaynak veride fatura numaraları rapor ve dökümlerde “evrak no” başlığı altında yer almaktadır. Ancak faturalarda seri numarası olması durumunda fatura numarası başında seri numarası ile girilmiştir. Bu nedenle bu analiz fatura numaralarından seri numaraları kaldırılarak yapılmıştır.

10.7. VERİ ANALİZ SONUÇLARI VE RAPORLAMA

10.7.1. Genel Bakış

Bu çalışmada geliştirilen sürekli denetim uygulaması aşağıdaki özelliklere sahiptir:

- Bu sürekli denetim uygulamasının planlama, geliştirme veya analizi sırasında kurumun bilgi sisteminde hiçbir değişiklik yapılmamıştır. Kurumun mevcut kodlama sistemi korunarak bu uygulama geliştirilmiştir.
- Bu sürekli denetim uygulamasının planlama, geliştirme veya analizi sırasında kurumun iş süreçlerinde hiçbir değişiklik yapılmamıştır. Kurumsal politikalar ve uygulamalar dikkate alınarak bu sürekli denetim uygulaması geliştirilmiştir.
- Kurumun yetkili kişileri tarafından sağlanan kaynak veri ACL denetim yazılımına aktarılarak dijital analizler yapılmıştır.
- Dijital analizler kaynak veriden denetim yazılımına aktararak oluşturulan tabloların veri bütünlüğü kontrolü yapıldıktan sonra uygulanmıştır.
- Sipariş dosyasındaki her kayıt satın alınması planlanan malların toplam adetleri göz önüne alınarak düzenlenmiştir. Kurumsal kaynak planlama yazılımına gerçekleşen işlemler kaydedildiğinden değişik zamanda yapılan alımlar için farklı girişler yapılmıştır. Bu nedenle finans yönetimi ve stok yönetimi modüllerinden alınan raporlara dayalı tablolarla çalışılırken stok kodu bazında denetim yapılan güne kadar olan girişlerin toplamı alınmıştır. Topamlar sipariş dosyasının ilgili alanları ile

karşılaştırılmıştır. Bu tablodaki stok net birim fiyat kayıtlardaki en yüksek birim fiyat alınarak oluşturulmuştur.

- Satın alma döngüsünün denetimi için sekiz adet kontrol testi belirlenmiştir. Bunlar geçerlilik, tamlık – bütünlük, doğruluk, sınıflandırma, zamanlılık, yetkilendirme, görev ayrımları ve özetleme kontrol testleridir. Kurumdan elde edilen kaynak veri ve iş süreçleri incelendikten sonra görev ayrımları dışındaki diğer kontrol testlerinin sürekli denetim uygulamasında yer almasına karar verilmiştir.
- Benford Analizi'nin fatura numaraları üzerinde yapılabileceği belirlenmiş ve sürekli denetim modeline eklenmiştir.
- Analiz sonuçları her analiz için ayrı ayrı oluşturulan metin (text) dosyalarına gönderilmiştir. Bu dosyalar raporlama amaçlı kullanılmaktadır.
- Değerlendirmeler 1 Ocak – 31 Aralık 2012 dönemine ait kayıtların analizinin sonucudur.

Sürekli denetim uygulamasının dijital analiz kısmı için atılan adımlar aşağıdaki gibidir:

1. İlgili kontrol testleri ve yapılacak işlemler tespit edilir.
 - a. Kontrol testleri belli alanlar üzerinde yapılan işlemler veya bazı alanların birbirleriyle karşılaştırılmasına dayanmaktadır.
 - b. İlgili dosyaların adları, yapılacak filtreleme ve karşılaştırılacak alanlar belirlenir.
2. Kurumdan gelen kaynak veri ACL denetim yazılımının içine alınır (“import” işlemi).
3. Veri bütünlüğü kontrolü yapılır.
4. Tablolar filtrelenir.
5. Tabloların ilişki kurulacak alanlarının biçimleri (format) standartlaştırılır.
6. Tablolar arasında ilişki (relation) kurulur. Kayıtlar eşleştirilir.
7. İlgili analizler yapılır.
8. Analiz sonuçları denetim raporu oluşturmak amacıyla bir dosyaya gönderilir.
9. ACL denetim yazılımının komut satırları (scripts) birbirini çağırabilir. Bu nedenle analizleri gerçekleştiren komut satırları bu analizlerin uygulanma sırasına yazılır. Tüm analizlerin yer aldığı bu “script” çalıştırıldığında kontrol testleri yapılmış ve denetim raporları hazırlanmış olur.

10.7.2. Satın Alma Döngüsündeki Kontrol Testlerinin ACL Senaryoları ve Dijital Analizlerin Sonuçları

10.7.2.1. Geçerlilik Kontrol Testleri

Amaç: kayıtların proje ile ilgili olduğunun kontrolü

Süreç kontrolü: Onaylama sürecinin kanıtları dijital ortamda olmadığı için bu sürecin geçerlilik kontrol testleri yapılamamaktadır. Bilgi ve belge akışının kurumsal politikalara uygun olduğu düşünülmektedir.

Satın alma talebi kontrolü: mal alım faturalarının proje ile ilgili olması

	Sipariş Dosyası	Stok Hareketleri Raporu
Filtre	Proje kodu = 455	Proje kodu = 455
		Evrak tipi = giriş faturası
		Hareket cinsi = toptan
Karşılaştırma	Stok kodu	Stok kodu
	Cari kod	Cari kodu

ACL senaryosu:

Stok tablosundaki “stok kodu” ve “cari kodu” kayıtları sipariş dosyasında var mıdır?

Olmayanları listele.

Analiz sonuçlarının yer aldığı rapor dosyalarının adı:

stok kodu karşılaştırması: GECERLILIK_SATINALMA_STOK.txt

cari kod karşılaştırması: GECERLILIK_SATINALMA_CARI.txt

Analiz sonucu:

102 adet farklı malın alım kaydı sipariş dosyasındaki onaylanan alımlarla eşleşmemiştir. Eşleşmeyen kayıtlardan 86 adedi tek bir firmadan alınmıştır. İnceleme sonucunda bu alımların büyük bölümünün 1000 TL’nin altında olduğu ve Üretim Bölümü’nün direkt olarak aldığı anlaşılmıştır. Alımların proje ile ilgili olduğu tespit edilmiştir.

Alış faturalarının işlenmesi: mal alım faturalarının mizana doğru yansımaları

	Cari Hesap Hareketleri Raporu	Yevmiye Dökümü
Filtre	Proje kodu = 455	Proje kodu = 455
	Evrak cinsi = alış faturası	Fiş tipi = mahsup
	Hareket cinsi = toptan fatura	Açıklama = Al.fat.:
Karşılaştırma	Cari hesap ismi	Hesap adı
	Cari hesap alacak	Alacak

ACL senaryosu:

Cari tablosundaki cari hesap isimleri ve ilgili alacak tutarları yevmiye tablosunda yer alıyor mu? Olmayanları listele. (Cari hesap isimlerinin ilk beş harfi eşleştirilecek.)

Analiz sonuçlarının yer aldığı rapor dosyalarının adı:

GECERLILIK_ALIS_FAT_ISIM.txt

GECERLILIK_ALIS_FAT_ALACAK.txt

Analiz sonucu:

Cari tabloda olan isimler yevmiye tablosunda yer almaktadır. Bir alacak kaydının cari ve yevmiye tablolarında farklı tutarlarda olduğu görülmüştür.

Ödemenin kontrolü: yapılan ödemenin proje ile ilgili alımlara ait olması

	Sipariş Dosyası	Yevmiye Dökümü
Filtre	Proje kodu = 455	Açıklama <> Al.fat.
	Evrak no > 0	Açıklama <> Sat.fat.
		Hesap kodu = 12 veya 32 (başlayanlar)
		Fiş tipi = tediye, mahsup
		Borç > 0
Karşılaştırma	Muhasebe cari kodu	Hesap kodu

ACL senaryosu:

Sipariş tablosunda yer alan “muhasebe cari kodu” yevmiye tablosunda var mıdır? Olmayanları listele.

Analiz sonuçlarının yer aldığı rapor dosyasının adı:

GECERLILIK_ODEME.txt

Analiz sonucu:

İki satın almanın dışında proje ile ilgili yapılan alımların ödemesinin gerçekleştiği görüşüne varılmıştır.

10.7.2.2. Tamlik – Bütünlük Kontrol Testleri

Amaç: gerçekleşmiş işlemlerin kurumsal kaynak planlama yazılımına kaydedilmiş olması

Sıra numarası kontrolü: eksik belge olma riskine karşı sıra numaralarında atlamalar aranır

	Sipariş Dosyası
Komut = Gaps	Sıra no

ACL senaryosu:

Sıra numarası üzerinde “gaps” analizi yapılır. Ardışık olmayan numaralar ve sıra numarası boş olan kayıtlar listelenir.

Analiz sonuçlarının yer aldığı rapor dosyasının adı:

TAMLIK_SIRANO_GAPS.TXT

Analiz sonucu:

Sipariş tablosunun sıra numaralarında hata bulunamamıştır. Bu nedenle sipariş dosyasında eksik belge olmadığı görüşüne varılmıştır.

Etkilenen hesapların kontrolü: farklı modüllerden alınan bilgi karşılaştırılarak kayıtların bütünlüğü kontrol edilir

	Sipariş Dosyası	Stok Hareketleri Raporu
Filtre	Proje kodu=455	Proje kodu = 455
	Evrak no > 0	
		Evrak tipi = giriş faturası
		Hareket cinsi = toptan
İlişkilendirme	Stok kodu	Stok kodu
	Cari kod	Cari kodu

ACL senaryosu:

Sipariş tablosundaki “stok kodu” ve “cari kod” stok tablosunda yer alıyor mu?
Olmayanları listele.

Analiz sonuçlarının yer aldığı rapor dosyalarının adı:

TAMLIK_ETKILENEN_HESAP_STOK.txt

TAMLIK_ETKILENEN_HESAP_CARI.txt

Analiz sonucu:

Stok kodu analizinden sonra sipariş dosyasına girilen kayıtlardan üç tanesinin, cari kod analizinden sonra da sekiz kaydın kurumsal kaynak planlama yazılımına farklı aktarıldığı anlaşılmıştır. İnceleme sonucunda bu hataların evrak numarası olarak bir modülde fatura numarasının diğer modülde irsaliye numarasının kullanılması, farklı carilerden giriş yapılması ve hareket cinsinin hatalı girilmesi olduğu tespit edilmiştir.

10.7.2.3. Doğruluk Kontrol Testleri

Amaç: işlemlerin planlanan şekilde gerçekleşmesi ve doğru şekilde kayıt edilmesi

İşlemlerin doğru kaydedildiğinin kontrolü: farklı modüllerden yapılan girişlerin birbirleriyle olan tutarlılığı

	Cari Hesap Ekstresi	Stok Hareketleri Raporu
Filtre	Proje kodu = 455	Proje kodu = 455
	Evrak cinsi = alış faturası	Evrak tipi = giriş faturası
	Hareket cinsi = toptan fatura	Hareket cinsi = toptan
Karşılaştırma	Stok net tutar (ana)	Giren net tutar

ACL senaryosu:

Cari ekstre tablosundaki “stok net tutar” stok tablosunda yer alıyor mu? Farklı olanları listele.

	Cari Hesap Hareketleri Raporu	Yevmiye Dökümü
Filtre	Proje kodu = 455	Proje kodu = 455
	Evrak cinsi = alış faturası	Fiş tipi = mahsup
	Hareket cinsi = toptan fatura	
İlişkilendirme	Evrak no	(Açıklama)
	Muhasebe fiş tarihi	Tarih
Karşılaştırma	Cari hesap alacak	Alacak

ACL senaryosu:

Cari tablosundaki “cari hesap alacak” yevmiye tablosunda yer alıyor mu? Farklı olanları listele.

Analiz sonuçlarının yer aldığı rapor dosyalarının adı:

DOGRULUK_KAYDEDILME_STOK.txt

DOGRULUK_KAYDEDILME_CARI.txt

Analiz sonucu:

Satın alınan malın stok bazında tutarlarının karşılaştırılmasında 8 adet faturada sorun olduğu tespit edilmiştir. İnceleme sonucunda bu faturalardaki aynı stok koduna sahip bazı malların iki kalem halinde girildiği görülmüştür. Bu uygulamada tablolar arasında bağlantı (relation) satın alınan malın stok kodu ve mal alım faturasının numarasının (evrak no alanı) birlikte kullanımı ile sağlanmaktadır. Bu iki unsur birlikte kullanıldığında özgün alanlar yaratmaktadır. Ancak, aynı mal alım faturasında aynı stok iki farklı tutarda girildiğinde denetim yazılımı kayıtları eşleştirmede sorun yaşamaktadır.

Satıcıların toplam alacağı üzerinde yapılan denetimde bir faturada sorun olduğu tespit edilmiştir. İnceleme sonucunda Mikro kurumsal kaynak yazılımının faturaları girerken her kalem için kullanıcıya “hareket cinsi”ni tanımlayabilme yetkisi verdiği ve aynı fatura içinde kullanıcının farklı hareket cinsleri tanımlayabileceği ortaya çıkmıştır. Denetim yazılımının sorunlu olarak raporladığı fatura kalemlerinin bir bölümü “hizmet” olarak tanımlanmış, bir kalem “toptan” olarak tanımlanmıştır. Denetim mal alım faturaları üzerinde yapıldığı için ilgili faturanın sadece hareket cinsi toptan olarak belirtilen kısmı finans yönetimi modülünden alınan cari hesap hareketleri raporuna yansımıştır. Oysa genel muhasebe modülünden alınan yevmiye dökümünde ilgili faturanın toplam alacağı ilgili satıcının alacağı olarak görülmektedir.

Sonuç olarak kurumsal kaynak planlama yazılımının farklı modüllerinden girilmiş olan bilgilerin diğer modüllere doğru yansıdığı anlaşılmıştır.

Hesaplanan tutarlarının kontrolü: hesaplamaların doğru yapılması

	Sipariş Dosyası
Karşılaştırma	Birim fiyat x Adet = Giren net tutar

ACL senaryosu:

Sipariş tablosunda “birim fiyat” ile “adet” alanları çarpıldığında “giren net tutar” alanındaki veriye eşit midir? Eşit olmayanları listele.

	Cari Hesap Ekstresi
Karşılaştırma	Stok net birim fiyat (ana) x Giriş miktarı = Stok net tutar (ana)

ACL senaryosu:

cari tablosunda “stok net birim fiyat” ile “giriş miktarı” alanları çarpıldığında “stok net tutar” alanındaki veriye eşit midir? Eşit olmayanları listele.

Analiz sonuçlarının yer aldığı rapor dosyalarının adı:

DOGRULUK_HESAPLANAN_SIPARIS.txt

DOGRULUK_HESAPLANAN_CARI.txt

Analiz sonucu:

Denetim yazılımı bazı kayıtları hatalı olarak raporlamıştır. Bu kayıtlar incelendiğinde aşağıdaki durumlar ortaya çıkmıştır:

- Sipariş dosyasında bazı kayıtlarda malın toplam değeri belirtilmiş, ancak birim fiyat ve/veya adet sıfır olarak girilmiştir. Bu kayıtlar için hesaplanan tutar sıfırdır ve “giren net tutar” ile uyuşmamaktadır. Bu durum özellikle satın alma öncesi yapılan fiyat anlaşmasının alımın toplam değeri üzerinden yapıldığı durumlarda görülmektedir.
- Mikro kurumsal kaynak planlama yazılımı kendi içindeki uygulamalarda birim fiyat hanesinin ondalık bölümünü çok basamaklı olarak kullanmaktadır. Ancak, bu uygulamada kullanılan rapor ve dökümlerde fiyat hanesi iki basamaklıdır. Özellikle, giriş miktarı çok olan faturalarda rapora göre hesaplanan ile Mikro

yazılımına girilmiş gerçek fatura tutarları arasında fark olmaktadır. Örneğin, hatalı olarak raporlanan faturaların büyük bölümünde adet 15000 ve üzeridir. Birim fiyatta 0.001’lik bir fark olduğunda hesaplanan ile gerçek fatura arasındaki fark 15 TL olacaktır.

İnceleme sonucunda kayıtlarda olan ile hesaplanan değerler arasında çıkan farkların hesaplama hatasından kaynaklanmadığına karar verilmiştir.

Satın almanın planlanan şekilde gerçekleştiğinin kontrolü: satın almanın onaylanan şekilde yapılması

	Sipariş Dosyası	Cari Hesap Ekstresi
Filtre	Proje kodu = 455	Proje kodu = 455
		Evrak cinsi = alış faturası
		Hareket cinsi = toptan fatura
Karşılaştırma	Cari kod	Cari hesap kodu
	Adet	Giriş miktarı
	Birim fiyat	Stok net birim fiyat (ana)
	Giren net tutar	Stok net tutar (ana)

ACL senaryosu:

Cari ekstre tablosundaki “cari hesap kodu” sipariş dosyasında aranır. İlgili veri sipariş dosyasında yoksa listelenir.

Cari ekstre tablosundaki “giriş miktarı”, “stok net birim fiyat” ve “stok net tutar” sipariş dosyasındaki ilgili alanlardaki veriye eşit veya küçük olmalıdır. Bu kurala uymayan kayıtlar hatalıdır. Cari ekstre tablosundaki değer sipariş tablosundaki değerden büyükse listelenir.

Analiz sonuçlarının yer aldığı rapor dosyalarının adı:

DOGRULUK_PLANLANAN_CARI.txt

DOGRULUK_PLANLANAN_ADET.txt

DOGRULUK_PLANLANAN_FIYAT.txt

DOGRULUK_PLANLANAN_TUTAR.txt

Analiz sonucu:

Planlanan ile gerçekleşen kayıtlar üzerinde yapılan incelemede denetim yazılımının hata olarak raporladığı 102 kayıt bulunmaktadır. Bu uygulamada kullanılan denetim modeline göre belirlenen hataların nedenleri aşağıdaki gibidir:

- 8 adet satıcı onaylanan satın alma planında yoktur. Üretim sürecinde ihtiyaç duyulan bazı mallar planlama sürecinde yer almamış, onaylanmamış carilerden alınmıştır.
- Satın almanın planlama aşamasında birim fiyat üzerinden anlaşma yapılmadığı durumlarda sipariş dosyasının birim fiyat alanına sıfır girilmektedir. Ancak, ilgili malların gelen faturalarının birim fiyatlarıyla karşılaştırıldığında denetim modeli bu farkı planlanan ile gerçekleşen arasındaki uyumsuzluk olarak nitelendirmekte ve hata olarak raporlamaktadır. Denetim modelinin sipariş dosyasındaki birim fiyat alanına sıfır girilmesinin bilinçli bir seçim mi yoksa hatalı bir giriş mi olduğunu değerlendirmesine olanak yoktur. Bu nedenle modele birim fiyatları sıfır olan kayıtların değerlendirilmeye alınmaması için bir filtre konulmamıştır.
- Planlanan ve gerçekleşen alımların adetleri karşılaştırıldığında raporlanan hataların büyük ölçüde sipariş dosyasındaki adet alanına sıfır girilmesinden kaynaklandığı ortaya çıkmıştır. Bunun dışında kalan birkaç alımda bazı stokların planlanandan daha fazla alındığı belirlenmiştir. Planlanan ile gerçekleşen arasındaki adet bazında fark %2 ile %50 arasındadır. Bu stokların birçoğunun birim fiyatının çok düşük olduğu anlaşılmaktadır. Yapılan incelemede adetlere ilişkin ek bir filtrelemenin denetim modelini iyileştirmesinin mümkün olmadığı görülmüştür.
- Planlanan ile gerçekleşen mal alımlarının değerlendirilmesi sırasında eşleşmeyen kayıtlar, planlanandan fazla miktarda ve/veya pahalı alınan mallar tespit edilmiştir. Bu kayıtların bir bölümünün tutarları da planlanandan daha fazla olmuştur.

Satın almanın bir bölümünün onaylanan şekilde yapılmadığı tespit edilmiştir.

10.7.2.4. Sınıflandırma Kontrol Testleri

Amaç: satın alma işlemlerinin doğru hesaplara kaydedilmesi

	Yevmiye Dökümü
Filtre	Proje kodu=455
	Fiş tipi = mahsup
	(Açıklama) = Al.fat.
	Hesap kodu <> 7**
Karşılaştırma	Alacak > 0 ise, Hesap kodu = 12 veya 32 (başlayanlar)
	Borç >0 ise, Hesap kodu = 15 (başlayanlar) veya 191*

* Yevmiye dökümünde alış faturaları için borçlu hesap stok hesabı veya 191 İndirilecek KDV hesabı olabilir.

** 7 Maliyet hesaplarına ilişkin kayıtlar analiz kapsamına alınmamıştır.

ACL senaryosu:

Yevmiye tablosunda “alacak” alanı sıfırdan büyük kayıtların “hesap kodu” 12 veya 32 ile başlıyor mu? Farklı olanlar listelenir.

Yevmiye tablosunda “borç” alanı sıfırdan büyük kayıtların “hesap kodu” 15 veya 191 ile başlıyor mu? Farklı olanlar listelenir.

Analiz sonuçlarının yer aldığı rapor dosyalarının adı:

SINIFLANDIRMA_ALACAK.txt

SINIFLANDIRMA_BORC.txt

Analiz sonucu:

Yapılan analiz sonucunda proje ile ilişkilendirilmiş olan bazı alımların beklendiği gibi tek düzen hesap planına göre “15 stoklar” sınıflandırılmadığı tespit edilmiştir. Bazı mallar 255 demirbaşlar olarak sınıflandırılmıştır. İncelemenin sonucunda bu malların kaynak makinası, kompresör, vb. cihazlar olduğu anlaşılmıştır. Bu mallardan bazılarının 253 tesis makine ve cihazlar olarak sınıflandırılması daha uygun olacaktır. Ayrıca, bu cihazların ekonomik ömürleri projeye sınırlı değildir. Bu mallar ilgili projeyi tamamlamak için alınmış olmakla birlikte daha sonra farklı projeler için de kullanılabilir. Kurum politikası olarak bir proje için alınan makineler ve demirbaşlar o proje için yapılan bir masraf olarak değerlendirilmektedir. Ancak, demirbaşların

üretim girdisi olan diğer stoklarla aynı bakış açısıyla değerlendirilmesi sınıflandırma hatasına yol açmaktadır.

10.6.2.5. Zamanlılık Kontrol Testleri

Amaç: satın alma işlemlerinin doğru tarihlere kaydedilmesi

Bilgi sistemine kayıt: belgelerin kurumsal kaynak planlama yazılımına kaydı için geçen sürenin tespit edilememiştir.

Belge tarihi: mal alım faturalarının kanuni süresi içinde muhasebeleştirildiğinin kontrolü

	Stok Hareketleri Raporu
Filtre	Proje kodu = 455
	Evrak tipi = giriş faturası
	Hareket cinsi = toptan
Doğrulama	(Muhasebe fiş tarihi) =< (Tarih + 10)

ACL senaryosu:

Stok tablosundaki “tarih” alanına on gün eklenir. Bu tarih “muhasebe fiş tarihi”ne eşit veya daha büyük olmalıdır. Hesaplanan tarih muhasebe fiş tarihinden daha küçük olanlar listelenir.

Analiz sonuçlarının yer aldığı rapor dosyasının adı:

ZAMANLILIK.txt

Analiz sonucu:

Belgelerin kurumsal kaynak planlama yazılımına ne süre içinde girileceğine dair bir yönetim kararı bulunmamaktadır. Kurum politikası olarak belgelerin kanuni süreleri içinde muhasebeleştirilmelerine dikkat edilmektedir. Analiz sonucunda sadece bir kayıta alış faturasının resmi süresini aşan bir tarihte muhasebeleştirildiği tespit edilmiştir.

10.7.2.6. Yetkilendirme Kontrol Testleri

Amaç: satın alma sürecindeki işlemlerin belirlenen yetkiler çerçevesinde ilgili kişiler tarafından yapılması

	Sipariş Dosyası	Stok Hareketleri Raporu
Filtre	Proje kodu = 455	Proje kodu = 455
		Evrak tipi = giriş faturası
		Hareket cinsi = toptan
Karşılaştırma	Stok kodu	Stok kodu

ACL senaryosu:

Stok tablosundaki “stok kodu” sipariş tablosunda var mıdır? Olmayanlar listelenir.

Analiz sonuçlarının yer aldığı rapor dosyasının adı:

YETKILENDİRME.txt

Analiz sonucu:

Stok tablosunda sipariş tablosunda yer almayan birçok malın giriş kaydına rastlanmıştır. Bu durum yetkili olmayan kişilerin mal alımı yaptığını ya da Satın Alma Bölümü’nün bilgisi dahilindeki bir alımı sipariş dosyasına işlemediğini gösterir. Bu uygulamada yetkilendirme kontrol testi dolaylı olarak yapılabildiği için planlanan ve gerçekleşen alımların tamamının eşleşmesi durumunda yetkilendirmenin yeterliliği konusunda görüş bildirilebilir.

10.7.2.7. Görev Ayrımları Kontrol Testleri

Amaç: satın alma sürecindeki faaliyetlerin farklı kişiler tarafından gerçekleştirilmesi

Bu konuda dijital analiz yapılamamıştır. Ancak, kurumda görev ayrımları olduğu ve etkin olarak işlediği düşünülmektedir.

10.7.2.8. Özetleme Kontrol Testleri

Amaç: ilk kaydın yapıldığı hesaplar ile toplam tutarların aktarıldığı hesapların uyumlu olması

	Stok Hareketleri Raporu	Yevmiye Dökümü
Filtre	Proje kodu=455	Proje kodu=455
	Evrak tipi = giriş faturası	Fiş tipi = mahsup
	Hareket cinsi = toptan	
	Giren net tutar > 0	Borç > 0
Karşılaştırma	Muhasebe kodu	Hesap kodu

ACL senaryosu:

Stok tablosundaki “muhasabe kodu” yevmiye tablosunda aranır. Stok tablosunda olup da yevmiye tablosunda bulunamayan kayıtlar listelenir.

Analiz sonuçlarının yer aldığı rapor dosyasının adı:

OZETLEME.txt

Analiz sonucu:

Analiz sonucu sadece bir kayıtta stok tablosunda belirtilen muhasabe hesap kodu yevmiye tablosunda belirtilen hesap kodu ile uyumlu değildir. Bu durum iki şekilde oluşabilir: ilgili tablolardaki kayıtların doğru eşleşmemesi veya faturanın muhasabe entegrasyonu yapıldıktan sonra hesap numarasının değiştirilmiş olması.

10.7.2.9. Benford Analizi

Amaç: Alış faturalarının belge numaraları üzerinde yapılacak Benford Analizi ile kurumsal kaynak planlama yazılımına kaydedilen faturalarda hile olup olmadığına dair görüş bildirmek.

ACL senaryosu:

Stok tablosunun “evrak no” alanı üzerinde Benford Analizi yapılır. Evrak numaraları faturaların seri numaralarından arındırıldıktan sonra Benford Analizi yapılmalıdır.

Analiz sonuçlarının yer aldığı rapor dosyasının adı:

BENFORD_ON_STOK.txt

Analiz sonucu:

Mal alım faturalarının numaralarının ilk hanesinin istatistiki dağılımı ve Benford Kanunu'na göre olması gereken dağılım aşağıda verilmiştir:

İlk hanenin sayısı	Gerçekleşen	Olasılık- gerçekleşen	Olasılık-Benford
1	18	5,34	30,1
2	2	0,59	17,6
3	260	77,15	12,5
4	7	2,08	9,7
5	35	10,39	7,9
6	3	0,89	6,7
7	10	2,97	5,8
8	0	0,00	5,1
9	2	0,59	4,6
toplam kayıt:	337		

Gerçekleşen dağılım teorik dağılımdan çok farklıdır. Önceki analizlerde planlanan ve onaylanan alımların dışında yapılmış mal alımları tespit edilmiştir. Bu durumda gerçek olmayan faturaların kurumsal kaynak planlama yazılımına kaydedilmiş olma ihtimalinden söz edilebilir. Ancak, faturalar incelendiğinde bazı satıcılarla yoğun çalışıldığı ve bu satıcılardan gelen faturaların analiz setini olumsuz etkilediği ortaya çıkmıştır. Örneğin, Burç Makina adlı satıcıdan gelen faturaların belge numaraları 3 ile başlamakta ve toplam faturaların % 6'sını oluşturmaktadır. Analize konu olan faturaların belli satıcılar üzerinde yoğunlaştığı görülmektedir. İlgili satıcının belge numaraları hep aynı sayı ile başladığı için rassal bir veri seti elde edilememiştir. Bu durumda Benford analizine dayanarak hile tespiti ihtimali çok düşüktür.

10.8. GELİŞTİRİLEN SÜREKLİ DENETİM UYGULAMASININ ETKİNLİĞİ VE ÖNEMİ

10.8.1. Geliştirilen Sürekli Denetim Uygulamasının Etkinliği

Yapılan analiz sonuçları incelendiğinde bu çalışmada geliştirilen sürekli denetim modelinden kaynaklanan önemli hatalara rastlanmamıştır. Yapılmış olan modellemenin ilgili kontrol testleriyle uyumlu olduğu görülmüştür.

Kurumsal kaynak planlama yazılımının kodlama sistemi farklı modüllerden sağlanan rapor ve dökümlerdeki kayıtları eşleştirmeye çok uygun değildir. Kayıtların eşleştirme işlemi ilgili kayda ait özgün bir değer ile gerçekleştirilebilir. Ancak, denetim tablolarında özgün alanlar mevcut değildir. Genellikle iki alanın birleştirilmesiyle her kayıt için özgün değerler yaratılmaya çalışılmıştır. Büyük ölçüde başarılı olunmasına karşın az sayıda eşleştirilemeyen kayıtlar hata olarak raporlanmıştır. Bilgi sisteminin mevcut kodlaması geliştirilen sürekli denetim uygulamasının etkinliğini azaltıcı bir unsur olarak karşımıza çıkmaktadır.

Denetim kanıtlarının önemli bir bölümünün dijital ortamda bulunmaması bazı kontrol testlerinin modellenmesinde dolaylı yöntemler kullanılmasını zorunlu kılmıştır. Bu tür analizlerin sonucunda çıkan hataların gerçekte planlanan denetimle ilgili bulgular olup olmadığını anlamak zordur.

10.8.2. Geliştirilen Sürekli Denetim Uygulamasının Önemi

Bu çalışmada geliştirilen sürekli denetim uygulaması denetimi yapılan kurumun bilgi sisteminde, iş süreçlerinde ve kurumsal politikalarında herhangi bir değişikliğe yol açmadan kullanılmak üzere tasarlanmıştır.

Literatürde yer alan sürekli denetim sistemleri yapılmak istenen analizler göz önüne alınarak modellenmiştir. Bu modellere uygun olarak geliştirilen bilgi sistemleri üzerinde çalıştırılmışlardır. Hatta geliştirilen birçok uygulama kurumsal iş süreçlerinin ve bilgi akışının yeniden düzenlenmesine yol açmıştır.

Sürekli denetim modelini geliřtirdikten sonra bu model ile uyumlu bilgi sistemini yaratmak ve belge akışını düzenlemek denetim etkinliğini arttıracaktır. Ancak bu yöntem sürekli denetim modellerinin uygulanabilirliğini önemli ölçüde azaltmaktadır. Bölüm 6’da açıklanan sürekli denetim uygulamaları geliřtirirken karşılaşılan zorlukların büyük bölümü denetim modeliyle birlikte kurumsal bilgi sisteminin ve kurumsal uygulamaların da değıştirilmeye çalışılmasından kaynaklanmaktadır. Sürekli denetim sisteminin kurulması için harcanacak emek, zaman ve para bu sistemden elde edilecek faydayı büyük ölçüde gölgelemektedir. Bu nedenle birçok kurum böyle bir çalışmadan kaçınmaktadır.

Bu çalışmada geliřtirilen uygulama sürekli denetim sisteminin kuruma büyük bir yük getirmeden yaratılabileceğini göstermiştir. Bu uygulamadaki bakış açısı sürekli denetim kavramına yeni bir yaklaşım getirmiş, maliyetine değil faydasına odaklanılabileceğini göstermiştir.

11. SONUÇ

Yatırımcılar finansal tabloları esas alarak yatırım kararlarını verirler. Piyasalarda işlem gören kurumların finansal tablolarına olan inanç yatırımcıların kararlarında önemli rol oynamaktadır. Özellikle son yıllardaki ekonomik skandallar yatırımcıların kurumların açıklamalarına ve finansal bilgilerine olan inancını azaltmıştır.

Hızla değişen ekonomik şartlar ve rekabetçi piyasalar yöneticilerin doğru ve hızlı karar almalarını başarının ilk şartı haline getirmiştir. Yöneticiler açısından bakıldığında doğru ve iyi analiz edilmiş kurumsal bilgi verilen kararların başarılı sonuçlar doğurması için ön şarttır.

Hem yatırımcılar hem de yöneticiler açısından günümüzde denetimin etkin ve zamanlı olmasının önemi artmıştır. Aylarca önce denetlenmiş finansal veriler ilgili kurumun güncel durumunu açıklamada yetersiz kalmaktadır. Doğru kararlar verebilmek için kurumsal bilgi güvenilir olmalıdır. Bu nedenle kurumsal bilginin etkin ve hızlı bir denetim sürecinden geçmesi gerekmektedir.

Etkin bir denetimi klasik denetim yöntemleriyle sağlamak mümkündür. Ancak, zamanlilik ilkesini sağlayabilecek en uygun yöntem sürekli denetimdir. Güncel, kapsamlı ve etkin bir denetim ihtiyacı sürekli denetim kavramını yaratmıştır.

Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü (American Institute of Certified Public Accountants, AICPA) ile Kanadalı Yetkili Muhasebeciler Enstitüsü'nün (Canadian Institute of Chartered Accountants, CICA) birlikte hazırladıkları raporda sürekli denetim “bağımsız denetçinin, denetim konusunun temelini oluşturan olayların gerçekleşmesi ile eşzamanlı veya bu olayların gerçekleşmesinden kısa bir süre sonra yayınlanan bir dizi denetçi raporunu kullanarak, denetim konusu üzerine yazılı bir güvence vermesine imkan tanıyan bir metodoloji” (CICA, 1999) şeklinde tanımlanmıştır. Sürekli denetim ile ilgili birçok tanım yapılmış olsa da bu tanım literatürde referans olarak kullanılmaktadır.

Günümüzde sürekli denetim ile ulaşılmak istenen gerçek zamanlı ve bilgi sistemleri ile otomatik olarak yapılan denetimdir. Sürekli denetim kavramı çok yenidir ve uygulama yöntemleri araştırma safhasındadır. Bu denetim yöntemi henüz yaygın olarak kullanılmamakta ve uygulamada önemli zorluklar içermektedir. Bu alanda araştırmaların

devam etmesi ve bilgi sistemlerinin gelişmesiyle sürekli denetim uygulamalarını hayata geçirmede yaşanan sorunlar giderilecek ve kullanımı artacaktır.

Bu çalışmada sürekli denetim kavramı, modelleri, hukuki çerçeve, uygulama geliştirmek için atılması gereken adımlar, veri analizinde kullanılan dijital analiz teknikleri, ilgili bilgisayar teknolojileri ve bugüne kadar geliştirilmiş belli başlı uygulamalar üzerinde durulmuştur. Bu dijital analiz tekniklerinden bazıları kullanılarak ACL denetim yazılımı ile satın alma döngüsü için bir sürekli denetim uygulaması geliştirilmiştir. Geliştirilen sürekli denetim modeli ile denetimi yapılan kurumun bilgi sisteminde ve iş süreçlerinde değişiklik yapmadan denetim etkinliği sağlanmıştır. Bu da sürekli denetim uygulamaları geliştirmenin önündeki engelleri kaldırma yolunda önemli bir adımdır.

EKLER

EK 1: Denetim Öncesi Veri Bütünlüğü Analizi

Denetime ilişkin analizleri yapmadan önce denetim yazılımına aktarılan tablolardaki verinin mekanik doğruluğunu teyit etmek gerekir. Bu uygulamada Mikro kurumsal kaynak yazılımı veritabanında bulunan bilgi ilgili kurum yetkililerince Excel'e aktarılmakta ve e-posta yoluyla denetçiye gönderilmektedir. Denetçi e-posta yoluyla gelen bu Excel dosyalarını ACL denetim yazılımının kullanabileceği bir formata dönüştürmektedir. Denetimde kullanılan tablolar iki kez format dönüşümü, bir kez de veri transferiyle karşı karşıya kalmaktadırlar.

Bu dönüşümler ve transfer sırasında kaynak verinin değişikliğe uğramadan tam ve doğru olarak denetim tablolarına yansıdığını çeşitli analizler yaparak teyit edebiliriz. Bu amaçla kullanılabilecek analizler ve denetim tablolarının hangi alanları üzerinde uygulandığı aşağıdaki tabloda belirtilmiştir.

Bu analizler belirtilen alanlara uygulanmış, kaynak verinin tam ve doğru olarak denetim tablolarına yansıdığı sonucuna varıldığında sürekli denetim planlandığı gibi yapılmıştır.

Veri bütünlüğü testlerinin uygulandığı tablolar ve ilgili alanlar:

	Sipariş Dosyası	Yevmiye Dökümü	Stok Hareketleri Raporu	Cari Hesap Hareketleri Raporu	Cari Hesap Ekstresi
tablo adı:	siparis	yevmiye	stok	cari	cari ekstre
Verify	tüm alanlar	tüm alanlar	tüm alanlar	tüm alanlar	tüm alanlar
Count	tüm tablo (alan seçilmesi gerekmiyor)	tüm tablo (alan seçilmesi gerekmiyor)	tüm tablo (alan seçilmesi gerekmiyor)	tüm tablo (alan seçilmesi gerekmiyor)	tüm tablo (alan seçilmesi gerekmiyor)
Total	Adet Giren net tutar	Borç Alacak	Giren net tutar Çıkan net tutar	Cari hesap borç Cari hesap alacak	TL borç TL alacak
Statistics	Tarih Birim fiyat Adet Giren net tutar	Tarih Borç Alacak	Tarih Giren net tutar Çıkan net tutar Muhasebe fiş tarihi	Tarih Cari hesap borç Cari hesap alacak Muhasebe fiş tarihi	Tarih TL borç TL alacak

Between()	Tarih	Tarih	Tarih	Tarih	Tarih
Isblank()	Stok kodu Tarih Cari kodu Birim fiyat Adet Giren net tutar	Yevmiye no Tarih Sıra no Hesap kodu Borç Alacak	Stok kodu Muhasebe kodu Tarih Cari adı Evrak tipi Evrak no Muhasebe fiş tarihi Muhasebe fiş no	Tarih Evrak no Evrak cinsi Vade Cari hesap kodu Muhasebe fiş tarihi Muhasebe fiş sıra no	Tarih Evrak no Evrak cinsi Vade Cari hesap kodu
Duplicates	Stok kodu				
Hesaplanmış Alanlar	Birim fiyat x adet = giren net tutar				Giriş miktarı x stok net birim fiyat (ana) = stok net tutar (ana)

EK 2: Kaynak Veri Dosyalarındaki Kolon Adları

Aşağıdaki tablolara ait kolon adları kurumdan gelen kaynak veri dosyasında yer aldığı sıralamadır.

Tablo adı: siparis

Sıra No	Stok kodu	Stok ismi	Muhasebe stok kodu	Tarih	Cari Kod	Muhasebe cari kodu	Cari adı	Proje kodu	Proje adı
---------	-----------	-----------	--------------------	-------	----------	--------------------	----------	------------	-----------

Evrak no	Birim Fiyat	Adet	Giren Net Tutar	Ünite kodu	Muhasebe Fiş Tarihi	Muhasebe Fiş No
----------	-------------	------	-----------------	------------	---------------------	-----------------

Tablo adı: yevmiye

Yevmiye no	Tarih	Sıra no	Fiş tipi	Hesap kodu	Hesap adı
------------	-------	---------	----------	------------	-----------

Açıklama	Borç	Alacak	Birim 1 miktar	Birim 2 miktar veya vergi matrahı	Proje kodu
----------	------	--------	----------------	-----------------------------------	------------

Tablo adı: stok

Stok kodu	Stok ismi	Muhasebe kodu	Muh.Grupsu kodu	Stok hareket kayıt no	Tarih	Cari kodu	Cari adı
-----------	-----------	---------------	-----------------	-----------------------	-------	-----------	----------

Proje kodu	Proje adı	Evrak tipi	Hareket cinsi	Hareket tipi	Normal İade	Evrak no
------------	-----------	------------	---------------	--------------	-------------	----------

Giren (Birim 1)	Birimi	Çıkan (Birim 1)	Birimi	Giren Net Tutar	Çıkan Net Tutar	Muhasebe Fiş Tarihi	Muhasebe Fiş No
-----------------	--------	-----------------	--------	-----------------	-----------------	---------------------	-----------------

Tablo adı: cari

Tarih	Evrak No	Evrak Cinsi	Hareket Cinsi	Vade	Açıklama	Cari Hesap Kodu	Cari Hesap İsmi
Proje Kodu	Cari Hesap Borç	Cari Hesap Alacak	Muhasebe fiş tarihi	Muhasebe fiş sıra no	Muhasebe fişi yevmiye no		

Tablo adı: cari ekstre

Tarih	Evrak No	Belge No/Tarih	Evrak Cinsi	Hareket Cinsi	Referans No	Vade	Açıklama	Cari Hesap Kodu	Cari Hesap İsmi
Stok/ hizmet/ masraf demirbaş/ ithalat Kodu	Stok/ hizmet/ masraf demirbaş/ ithalat Adı	Giriş Miktarı	Çıkış Miktarı	Stok Birimi	Stok Brüt Birim Fiyat (Ana)	Stok Net Birim Fiyat (Ana)	Stok Net Tutar (Ana)	Stok Vergi dahil Net Tutar(Ana)	
Stok Net Birim Fiyat (Cari.Orj)	Stok Net Tutar (Cari.Orj)	Stok Vergi dahil Net Tutar (Cari.Orj)	Proje kodu	Proje adı	TL Borç	TL Alacak	TL Borç bakiye	TL Alacak bakiye	

EK 3: Denetim Tablolarının Alan Formatları

Bu uygulamada planlanan bazı kontrol testlerini yapabilmek için tablolar arasında ilişki kurulması gerekmektedir. ACL denetim yazılımında tablolar arasında ilişki “relation” komutu ile kurulur. Bu komutun işlevini yapabilmesi için ilişki kurulacak tabloların ilgili alanlarının biçimsel uyumlarının sağlanması gerekir.

Bu uygulamada kullanılan denetim tablolarının ilişkili alanlarına ait meta data aşağıda belirtildiği gibidir:

	Sipariş Dosyası	Cari Hesap Hareketleri Raporu	Cari Hesap Ekstresi	Stok Hareketleri Raporu	Yevmiye Dökümü	T:text D:date N:numeric	uzunluk
Tablo adı:	siparis	cari	cari ekstre	stok	yevmiye		
	Proje kodu=455	Proje kodu=455	Proje kodu=455	Proje kodu=455	Proje kodu=455	T	4
	Proje adı	Proje adı		Proje adı		T	21
	Evrak no	Evrak no	Evrak no	Evrak no		T	8
	Muhasebe fiş tarihi	Muhasebe fiş tarihi		Muhasebe fiş tarihi	Tarih	D	19
		Muhasebe fişi yevmiye no			Yevmiye no	N	3
		Muhasebe fiş sıra no		Muhasebe fiş no	Sıra no	N	2
	Muhasebe stok kodu			Muhasebe kodu		T	6
	Muhasebe cari kodu				Hesap kodu	T	13
	Tarih	Tarih	Tarih	Tarih		D	19
	Stok kodu		Stok/ hizmet/ masraf demirbaş/ ithalat kodu	Stok kodu		T	5
	Stok ismi		Stok/ hizmet/ masraf demirbaş/ ithalat adı	Stok ismi		T	50

	Cari kod	Cari hesap kodu	Cari hesap kodu	Cari kodu		T	4
	Cari adı	Cari hesap ismi	Cari hesap ismi	Cari adı		T	50
		Evrak cinsi	Evrak cinsi	Evrak tipi	Fiş tipi	T	14
		Hareket cinsi	Hareket cinsi	Hareket cinsi		T	20
				Hareket tipi		T	10
				Normal İade		T	10
	Adet		Giriş miktarı	Giren (Birim 1)	Birim 1 miktar	N	10
			Stok birimi	Birimi		T	10
	Birim fiyat		Stok net birim fiyat (ana)			N	10
	Giren net tutar		Stok net tutar (ana)	Giren net tutar	Borç	N	10
		Cari hesap alacak			Alacak	N	10
	Sıra no					N	5
	Muhasebe fiş no					N	5
		Açıklama	Açıklama		Açıklama	T	100
		Vade	Vade			T	10
		Cari hesap borç			Borç	N	10
			Belge no/ tarih			T	20

EK 4: Filtreler

ACL denetim yazılımında tablolar arasında ilişki kurabilmek için iki tabloda da yer alan özgün alanların bulunması gerekir. Bu uygulamada kullanılan kaynak verinin alındığı bilgi sisteminde kullanılan kodlama planlanan kontrol testleri dikkate alınarak düzenlenmediği için özgün alanların bulunmasında zorluklar yaşanmıştır. ACL tablolarını ilişkilendirmeden önce tablolar filtrelenerek ihtiyaç duyulan özgün alanlar ortaya çıkartılmıştır.

Tabloların analiz öncesi filtrelenmesinin bir başka faydası da daha az kayıt içeren tablolarla çalışılmasıdır. Kurumun tüm kayıtlarını içeren büyük tablolar yerine kontrol testlerini yapabilmek için ihtiyaç duyulan ilgili projenin kayıtlarının yer aldığı tablolarla çalışmak denetim süresini kısaltmaktadır.

Bu uygulamada kodu 455 olan projenin kayıtları üzerinde denetim yapılmaktadır. Kontrol testlerinin büyük bölümü alış faturaları ile ilgilidir. 455 kodlu projenin alış faturalarını filtrelemek için kullanılan alanlar ve ilgili filtreler aşağıda belirtilmiştir:

	Sipariş Dosyası	Cari Hesap Hareketleri Raporu	Cari Hesap Ekstresi	Stok Hareketleri Raporu	Yevmiye Dökümü
Tablo adı:	siparis	cari	cari ekstre	stok	yevmiye
	Proje kodu = 455	Proje kodu = 455	Proje kodu = 455	Proje kodu = 455	Proje kodu = 455
		Evrak cinsi = Alış faturası	Evrak cinsi = Alış faturası	Evrak tipi = Giriş faturası	Fiş tipi = mahsup
		Hareket cinsi = Toptan fatura	Hareket cinsi = Toptan fatura	Hareket cinsi = Toptan	

EK 5: Sürekli Denetim Uygulamasında Yer Alan Dijital Analizlerin Listesi

Geçerlilik Kontrol Testleri

- Satın alma talebi kontrolü
- Alış faturalarının işlenmesi
- Ödemenin kontrolü

Tamlık – Bütünlük Kontrol Testleri

- Sıra numarası kontrolü
- Etkilenen hesapların kontrolü

Doğruluk Kontrol Testleri

- İşlemlerin doğru kaydedildiğinin kontrolü:
- Hesaplanan tutarlarının kontrolü
- Satın almanın planlanan şekilde gerçekleştiğinin kontrolü

Sınıflandırma Kontrol Testleri

Zamanlılık Kontrol Testleri

- Belge tarihi

Yetkilendirme Kontrol Testleri

Özetleme Kontrol Testleri

Benford Analizi

KAYNAKÇA

Kitaplar

Association of Certified Fraud Examiners. Fraud Examiners Manual. A.B.D.: Association of Certified Fraud Examiners, Inc., 2007.

Bozkurt, Nejat. Muhasebe Denetimi. 3. Basım. İstanbul: Alfa Yayınları, 2000.

Bozkurt, Nejat. İşletmelerin Kara Deliği: Hile – Çalışan Hileleri. 2. Basım. İstanbul: Alfa Yayınları, Ekim 2011.

Coderre, David. Computer-Aided Fraud Prevention And Detection: A Step-by-Step Guide. A.B.D.: John Wiley & Sons, Inc., 2009.

Coderre, David. Internal Audit. A.B.D.: John Wiley & Sons, Inc., 2009.

Coderre, David. Fraud Analysis Techniques Using ACL. A.B.D.: John Wiley & Sons, Inc., 2009.

Dauber, Nick A. ve diğerleri. The Complete Guide To Auditing Standards And Other Professional Standards For Accountants. A.B.D.: John Wiley & Sons, Inc., 2008.

Gallegos, Frederick ve diğerleri. Information Technology Control And Audit. 2. Basım. A.B.D.: CRC Press LLC, 2004.

Goldmann, Peter. Anti-Fraud Risk And Control Workbook. A.B.D.: John Wiley & Sons, Inc., 2009.

Kaval, Hasan. Muhasebe Denetimi. 2. Basım. Ankara: Gazi Kitabevi, Ekim 2005.

Kurnaz, Niyazi ve Tansel Çetinoğlu. İç Denetim - Güncel Yaklaşımlar. Kocaeli: Umuttepe Yayınları, Mayıs 2010.

Mainardi, Robert L. Harnessing the Power of Continuous Auditing: Developing and Implementing a Practical Methodology. A.B.D.: John Wiley & Sons, Inc., 2011.

Moeller, Robert R. Brink's Modern Internal Auditing. 7. Basım. A.B.D.: John Wiley & Sons, Inc., 2009.

Pathak, Jagdish. Information Technology Auditing. Almanya: Springer, 2005.

Pehlivanlı, Davut. Modern İç Denetim. İstanbul: Beta Basım, 2010.

Pehlivanlı, Davut. Hile Denetimi Metodoloji ve Raporlama. İstanbul: Beta Basım, Ekim 2011.

Pickett, K. H. Spencer. The Essential Handbook Of Internal Auditing. 2. Basım. İngiltere: John Wiley & Sons, Inc., 2003.

Rezaee, Zabihollah ve Richard Riley. Financial Statement Fraud Prevention And Detection. 2. Basım. A.B.D.: John Wiley & Sons, Inc., 2010.

Russell, J. P. (Ed.). The Quality Audit Handbook. 2. Basım. A.B.D.: American Society For Quality, 2000.

Wells, Joseph T. (Ed.). Fraud Casebook: Lessons From The Bad Side Of Business. A.B.D.: John Wiley & Sons, Inc., 2007.

Makaleler

Ağca, Ahmet. “Sürekli Denetim: Denetimde Bir Devrim mi Yoksa Bir Hayal mi?”, MODAV Muhasebe Bilim Dünyası Dergisi 8.1 Mart 2006:63-78.

<http://www.muhasetr.com/ozelbolum/029/> (12 Aralık 2008).

Alles, Michael G., Alexander Kogan ve Miklos A. Vasarhelyi. “Accounting In 2015”, The CPA Journal. (Kasım 2000):15-20, 70-72.

Alles, Michael ve diğerleri. “Continuous monitoring of business process controls: A pilot implementation of continuous auditing system at Siemens”, International Journal of Accounting Information Systems 7. (2006): 137-161.

Alles, Michael G., Alexander Kogan ve Miklos A. Vasarhelyi. “Putting Continuous Auditing Theory into Practice: Lessons from Two Pilot Implementations”, Journal of Information Systems 22. 2 (2008): 195-214.

Aquino, Carlos Elder Maciel De, Washington Lopes Da Silva and Miklos A. Vasarhelyi. “Moving Toward Continuous Auditing: Establishing Audit Priority Areas Can Lead To A More Effective Continuous Audit Process”, Tech Forum (Ağustos 2008).

<http://www.entrepreneur.com/tradejournals/article/183444836.html> (17 Ocak 2009).

Baksa, Robert ve Murray Turoff. “The Current State of Continuous Auditing and Emergency Managemet’s Valuable Contribution”, 7th International ISCRAM Conference. Seattle, ABD: Mayıs 2010.

Best, Peter J., George Mohay ve Alison Anderson. “Machine-Independent Audit Trail Analysis – A Tool For Continuous Audit Assurance”, Intelligent Systems In Accounting, Finance and Management. 12 (2004):85-102.

Brennan, Gerard. “Continuous Auditing Comes of Age”. Information Systems Control Journal. 1. 2008. <http://www.isaca.org> (17 Ocak 2009).

Burns, Randal ve Zachary Peterson. “Security Constructs for Regulatory-Compliant Storage”, Communications Of The ACM 53. 1 (Ocak 2010): 126-130.

Cankar, İsa. “Denetimin Yeni Paradigması: Sürekli Denetim”. Sayıştay Dergisi 61 (2006): 69-81.

Chan, David Y. ve Miklos A. Vasarhelyi. “Innovation and Practice of Continuous Auditing”. <http://www.raw.rutgers.edu> (18 Şubat 2011).

Chou, Charles Ling-yu, Timon Du ve Vincent S. Lai. “Continuous Auditing with a multi-agent system”, Decision Support Systems. 42 (2007): 2274-2292.

Cleary, Richard ve Jay C. Thibodeau. “Applying Digital Analysis Using Benford’s Law to Detect Fraud: The Dangers of Type I Errors”, A Journal Of Practice & Theory 24. 1 (Mayıs 2005): 77-81.

Coderre, David. "Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment", Global Technology Audit Guide. The Institute of Internal Auditors, USA, 2005.

Coderre, David. "A Continuous View of Accounts". Internal Auditor. (Nisan 2006): 25-31.

Cohen, Eric E., Teresa Schiavina ve Oliver Servais. "XBRL: The standardised business language for 21 st century reporting and governance", International Journal of Disclosure and Governance 2. 4 (2005): 368-394.

Dal-Ri Murcia, Fernando, Flavia Cruz De Souza ve Jose Alonso Borba. "Continuous Auditing: A Literature Review". Haziran 2008. <http://www.raw.rutgers.edu> (18 Şubat 2011).

Du, Hui ve Saeed Roohani. "Meeting Challenges and Expectations of Continuous Auditing in the Context of Independent Audits of Financial Statements", International Journal of Auditing. 11 (2007):133-146.

Earnst & Young. Global İç Denetim Anketi. 2008.

Elitaş, Cemal ve Murat Kiracı. "Satın Alma Sürecinde Kontrol Testi ve Bir Nitelik Örnekleme Uygulaması", Çözüm Dergisi (Temmuz-Ağustos 2010): 45-77.

El-Masry, El-Hussein E. ve Jacqueline L. Reck. "Continuous online auditing as a response to the Sarbanes-Oxley Act", Managerial Auditing Journal 23. 8 (2008):779-802.

Flowerday, Stephen, Adrian Blundell ve Rossouw Von Solms. "Continuous Auditing Technologies and Models: A Discussion", Computers & Security. 25 (2006):325-331.

Groomer S. Michael ve Uday S. Murthy. "Continuous Auditing of Database Applications: An Embedded Audit Module Approach", Journal of Information Systems. 3(İlkbahar 1989):53-69.

Heffes, Ellen M. "Theory to Practice: Continuous Auditing Gains", Financial Executive. Eylül 2006: 17. <http://www.fei.org> (18 Şubat 2011).

Hunton, James E. ve Jacob M. Rose. "21st Century Auditing: Advancing Decision Support Systems to Achieve Continuous Auditing", Accounting Horizons 24. 2 (2010):297-312.

ISACA Standards Board. "Continuous Auditing: Is It Fantasy or Reality?". Information Systems Control Journal 5, 2002.

Jans, Micke, Michael Alles ve Miklos Vasarhelyi. "Process Mining Of Event Logs In Auditing: Opportunities and Challenges". Şubat 2010. <http://www.raw.rutgers.edu> (18 Şubat 2011).

Jerskey, Pamela. "Using Analytical Procedures For Continuous Auditing And Fraud Detection", 1998. Boston College. <http://www.auditnet.org/contaudit.htm> (13 Aralık 2008).

Kardeş, Seval. "Denetim Olgusunun Kurumsal Kaynak Planlaması (ERP) Sistemleriyle Bütünleştirilmesi".

<http://archive.ismmmo.org.tr/docs/sempozyum/07Sempozyum/11-SEVAL%20KARDE%C5%9E%20SEL%C4%B0MO%C4%9ELU.doc> (12 Aralık 2008).

Kenger, Erdal. “Denetçi Yardımcıları İçin Eğitim Notu”. Şubat 2001. (12 Aralık 2008).

Kiracı, Murat. “Muhasebe Denetimi”, (2008). Eskişehir Osmangazi Üniversitesi, İktisadi ve İdari Bilimler Fakültesi. (12 Aralık 2008).

Kogan, Alexander ve diğerleri. “Analytical Procedures for Continuous Data Level Auditing: Continuity Equations”. Temmuz 2010. <http://www.raw.rutgers.edu> (18 Şubat 2011).

Kuhn Jr., John R. ve Steve G. Sutton. “Continuous Auditing in ERP System Environments: The Current State and Future Directions”, Journal of Information Systems 24. 1 (2010):91-112.

Kurnaz, Niyazi. “Güncel Denetim Yaklaşımları”. www.niyazikurnaz.net (12 Aralık 2008).

Lehmann, Constance, Sridhar Ramamoorti ve Marcia Weidenmier Watson. “Maximized Monitoring”, Internal Auditor. (Haziran 2010):56-59.

Masli, Adi ve diğerleri. “Examining the Potential Benefits of Internal Control Monitoring Technology”, Eylül 2009. Rutgers University, Continuous Auditing and Research Laboratory. <http://raw.rutgers.edu/docs/wcars/19wcars/GaryPeters.pdf> (14 Aralık 2011).

Matthews, Nigel. “How Continuous Auditing and XBRL-GL Work Together to Provide Improved Business Value”. (19 Mayıs 2008). (17 Ocak 2009).

Nearon, Bruce. “Foundations in Auditing and Digital Evidence”, The CPA Journal. (Ocak 2005):32-34.

Nelson, Lee. “Stepping Into Continuous Audit”. Internal Auditor. (Nisan 2004): 27-29.

Nigrini, Mark J. “Continuous Auditing”. 2000. http://aaahq.org/audit/midyear/01midyear/papers/nigrini_continuous_audit.pdf (14 Aralık 2011).

Teeter, Ryan A., Michael G. Alles, Miklos A. Vasarhelyi. “Remote Audit: A Research Framework”. Eylül 2010. <http://www.raw.rutgers.edu> (18 Şubat 2011).

Teppler, Steven W. “Digital Data And The Meaning Of Audit”, The CPA Journal. (Şubat 2003).

Thiprungsri, Sutapat. “Cluster Analysis for Anomaly Detection in Accounting Data”. Temmuz 2010. <http://www.raw.rutgers.edu> (18 Şubat 2011).

Türkyener, Mustafa. “Benford Yasası ve Mali Denetimde Kullanımı”. Sayıştay Dergisi 64 (2007): 111-122.

Onions, Robert L. "Towards a Paradigm for Continuous Auditing". Ocak 2003. <http://www.auditsoftware.net/community/how/run/tools/Towards%20a%20Paradigm%20for%20Continuous%20Auditin1.doc> (19 Şubat 2011).

O'Reilly, Anthony. "Continuous Auditing: Wave Of The Future?". The Corporate Board. (Eylül/Ekim 2006): 24-26.

Pathak, Jagdish. "A Tale of Compatible Twins! Success of E-Commerce & Information Systems/Internal Auditors", Aralık 2002. University of Windsor, Odette School of Business. University of Windsor Working Paper No. 2002-02. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=373761 (14 Aralık 2011).

Pathak, Jagdish, Ben Chaouch ve Ram S. Sriram. "Minimizing cost of continuous audit: Counting and time dependent strategies", Journal of Accounting and Public Policy. 24 (2005): 61-75.

Pearson, Timothy A. ve Tommie W. Singleton. "Fraud and Forensic Accounting in the Digital Environment", Issues In Accounting Education 23. 4 (Kasım 2008): 545-559.

Rezaee, Zabihollah ve diğerleri. "Continuous Auditing: Building Automated Auditing Capability", A Journal of Practice & Theory 21. 1 (Mart 2002): 147-163.

Rezaee, Zabihollah, Rick Elam, Ahmad Sharbatoghlie. "Continuous auditing: the audit of the future", Managerial Auditing Journal 16. 3 (2001): 150-158.

Sarva, Srinivas. "Continuous Auditing Through Leveraging Technology", Journal Online. 2006. <http://www.isaca.org> (17 Ocak 2009).

Searcy, DeWayne L. ve Jon B. Woodroof. "Continuous Auditing: Leveraging Technology". Mayıs 2003. (17 Ocak 2009).

Searcy, DeWayne, Jon Woodroof ve Bruce Behn. "Continuous Audit: The Motivations, Benefits, Problems, and Challenges Identified by Partners of a Big 4 Accounting Firm". 2002. <http://csdl.computer.org/comp/proceedings/hicss/20> (14 Mart 2010).

Uyanık, Atilla. "XVI Dünya Muhasebe Kongresi ve Denetim İle İlgili Gelişmelerin Değerlendirilmesi", Mevzuat Dergisi 6. 62 Şubat 2003. <http://www.mevzuatdergisi.com/2003/02a/01.htm> (12 Aralık 2008)

Vasarhelyi, Miklos A. "Concepts In Continuous Assurance", 2002. Rutgers University, Continuous Auditing and Research Laboratory. <http://raw.rutgers.edu/carlab> (28 Şubat 2012).

Vasarhelyi, Miklos A., Michael G. Alles ve Alexander Kogan. "Principles of Analytic Monitoring for Continuous Assurance", Journal of Emerging Technologies in Accounting 1. (2004):1-21.

Warren Jr, J. Donald ve L. Murphy Smith. "Continuous Auditing: An Effective Tool For Internal Auditors", Internal Auditing 21. 2 (Mart/Nisan 2006):27-35.

Whitehouse, Tammy. “Whatever Happened to Continuous Auditing?”, Compliance Week. 30 Kasım 2010. www.complianceweek.com (Ocak 2011).

Woodroof, Jon ve DeWayne Searcy. “Continuous audit: Model development and implementation within a debt covenant compliance domain”, International Journal of Accounting Information Systems 2. (2001): 169-191.

Yeh, Chun-Hsiu ve Wei-Cheng Shen. “Using continuous auditing life cycle management to ensure continuous assurance”, African Journal of Business Management 4. 12 (Eylül 2010): 2554-2570.

Ye, Huanzhuo ve Ye Li. “Research of Continuous Auditing Immune Model based on Object-Oriented Rule Base”, 2nd International Conference on Computer Engineering and Technology. Chengdu, Çin: 17 Haziran 2010: V4-148 - V4-152.

“Yeminli Mali Müşavirlik Yıllık Gelir ve Kurumlar Vergisi Beyannamesi Denetim ve Tasdik Normları”. 2008.