T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
MUHASEBE VE DENETİM ANABİLİM DALI
MUHASEBE VE DENETİM YÜKSEK LİSANS PROGRAMI

BİLGİ SİSTEMLERİ UYGULAMALARINDA İÇ KONTROL VE DENETİM

Yüksek Lisans Tezi

Osman AYDIN

1350Y74126

İstanbul 2015

T.C.

İSTANBUL TİCARET ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
MUHASEBE VE DENETİM ANABİLİM DALI
MUHASEBE VE DENETİM YÜKSEK LİSANS PROGRAMI

BİLGİ SİSTEMLERİ UYGULAMALARINDA İÇ KONTROL VE DENETİM

Yüksek Lisans Tezi

Osman AYDIN

1350Y74126

Danışman: Yrd. Doç. Dr. Ali Altuğ Biçer

İstanbul, Haziran 2015

T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

ONAY SAYFASI

Yüksek lisans öğrencisi Osman AYDIN'ın "Bilgi Sistemleri Uygulamalarında İç Kontrol ve Denetim" konulu tez çalışması jürimiz tarafından Muhasebe ve Denetim programı Yüksek Lisans tezi olarak (oy birliği ☑ / oy çokluğu ☐) ile başarılı bulunmuştur.

	Adı – Soyadı	İmza
Tez Danışmanı	: Yrd. Doç. Dr. Ali Alkış Bicer	.....
Jüri Üyesi	: Doç. Dr. Fatma Pancaroğlu	.....
Jüri Üyesi	: Yrd. Doç. Dr. Berak Erdem Ben	.....
Jüri Üyesi	:	.....

Hazırlamış olduğum tez özgün bir çalışma olup YÖK ve İTİCÜ Lisansüstü Yönetmeliklerine uygun olarak hazırlanmıştır. Ayrıca, bu çalışmayı yaparken bilimsel etik kurallarına tamamıyla uyduğumu; yararlandığım tüm kaynakları gösterdiğimi ve hiçbir kaynaktan yaptığım ayrıntılı alıntı olmadığını beyan ederim. Bu tezin ihtiva ettiği tüm hususlar şahsi görüşüm olup İstanbul Ticaret Üniversitesinin resmi görüşünü yansıtmamaktadır.

ÖZ

Bilgi teknolojilerinde 19. yüzyılın son çeyreğinden itibaren yaşanan gelişmeler, her alanı olduğu gibi işletmeleri de etkilemiş, bilgi teknolojilerinin daha yoğun kullanıldığı iş süreçlerinin oluşmasına neden olmuştur. Önceleri kağıt ortamında yapılan ve uzun zaman alan işlemler artık bilgi sistemleri ile çok daha kısa sürelerde yapılır hale gelmiştir. Bu durum işletmelere büyük faydalar sağlamanın yanı sıra bir takım riskleri de beraberinde getirmiştir. Bu çalışmada, bilgi sistemleri ve bilgi teknolojileri ile ilgili temel kavramlara değinilmiş, bilgi sistemi ortamında iç kontrol düzenlemeleri sınıflandırılması ele alınmış ve konu özellikle uygulama kontrolleri örnekleri ile irdelenmiştir. Ayrıca söz konusu kontrollerin etkinliğinin test edilmesi için kullanılan teknik ve araçlara değinilmiştir. Konu ile ilgili olarak muhasebe bilgi sistemi denetimi yaklaşımları kısaca ele alınmıştır. Çalışmanın sonunda bir işletmede bilgi sistemleri kontrolleri ve bunların test edilmesine ilişkin örnekler kısaca aktarılmaya çalışılmıştır. Bu çalışma ile iç denetçilerin ve bağımsız denetçilerin denetimde bilgisayar kullanımı ile sağlayacağı faydalara da kısaca değinilmiştir.

ABSTRACT

The developments that took place since the end of the last quarter of 19th century, effected the enterprises as it did to every aspects of our lives. This situation caused to emergence of the intenser usage of the information technologies in business processes. The proceses which were being done on papers and taking long time, have started to take shorter time by the help of information systems. This situation provided great benefits to enterprises along with some risks. In this study, the basic concepts related to information systems and information Technologies have been discussed and the classification of internal controls on informaton system environment has been analyzed. Also the subject especially scrutinzed by application control instances. In addition to that such techniques and tools that are used for testing the effectiveness of controls are discussed. Related to the subject, approches to the audit of accounting information systems have been briefly discussed. At the end of the study, examples of information systems controlls and testing of these controlls have been shown. By this study, it has been aimed to show the benefits of computer usage in audit process for the auditors.

İÇİNDEKİLER

Sayfa No.

TABLO LİSTESİ

Sayfa No.

ŞEKİL LİSTESİ

Sayfa No.

KISALTMALAR

a.g.e. **:** Adı Gecen Eser

ACFE **:** Association of Certified Fraud Examiners - Uluslararası Suistimal İnceleme Uzmanları Derneği

ACL **:** Audit Command Language

B2B **:** Business to Business

BDDK **:** Bankacılık Düzenleme Denetleme Kurumu

BDS **:** Bağımsız Denetim Standartları

CAAT's **:** Computer Assisted Audit Technic and Tools - Bilgisayar Destekli Denetim Teknikleri

CAP : Computerized Audit Program

CISA **:** Certificated Information Systems Audit – Sertifikalı Bilgisayar Sistemleri Denetçisi

CISM **:** Certified Information Security Manager - Sertifikalı Bilgi Güvenliği Yöneticisi

COBIT **:** Control Objectives For Information And Related Technology

COSO : Committee of Sponsoring Organizations of Treadway Commission

CRM **:** Customer Relationship Management

ERP **:** Enterprise Resource Planning –Kurumsal Kaynak Planlaması

GTAG **:** Global Technology Audit Guide

GAS **:** Generalized Audit Software- Genelleştirilmiş Denetim Yazılımları

IFAC : International Federation of Accountants - Uluslararası Muhasebeciler Federasyonu

IAASB **:** International Auditing and Assurance Standarts Board Uluslararası Denetim ve Güvence Kurulu

IDEA : Interactive Data Extraction and Analysis

IIA **:** Institute of Internal Auditors Uluslararası İç Denetim Enstitüsü

IS : Information Systems – Bilgi Sistemleri

ISA : International Standarts on Auditing -Uluslararası Denetim Standartları

ISACA : Information Systems Audit and Control Association

IT : Information Technology - Bilgi Teknolojileri

ITF : Integreated Test Facility - Bütünleşik Veri Test Tekniği

IP : Internet Protocol Number

İDDK : İç Denetim Koordinasyon Kurulu

KGK : Kamu Gözetim Kurumu

MİY : Müşteri İlişkileri Yönetimi

MRP : Materials Resource Planning - Malzeme İhtiyaç Planlaması

ODBC : Open Database Connectivity

s. : Sayfa

S. : Sayı

SQL : Structured Query Language - Yapılandırılmış Sorgu Dili

UDS : Uluslarası Denetim Standartları

YBS : Yönetim Bilgi Sistemleri

Giri·

Bütün işletmelerin, etkin ve verimli çalışmalarını sağlamak amacıyla yazılı ve etkin olmasa da bir takım plan, kural, tedbir ve düzenlemeleri vardır. Bu kural ve tedbirler, işletme içi suiistimalleri önlemek, kaynakları etkin ve verimli kullanmak, hataları en aza indirmek gibi faydaların yanı sıra işletmenin verimliliğini artırıp hedeflerine ulaşmasına yardımcı olacak düzenlemelerdir. Bu düzenlemelerin yeterliliği ve etkinliğinin test edilmesi ve gerektiğinde geliştirilmesi için çalışmalar yapılmalıdır. Son zamanlarda sermaye hareketlerinin ve rekabetin artması, işletme faaliyetlerin çeşitliliği ve fazlalığı, işletme içi hile ve usulsüzlüklerin artması ve teknolojik gelişmeler gibi nedenler ile bu tür düzenleme ve kurallara olan ihtiyaç daha da artmıştır.

Bunun yanı sıra teknolojide, özellikle bilgi teknolojilerinde meydana gelen gelişmeler işletmeleri de etkilemiş, işletmeler, faaliyetlerini gerçekleştirirken bilgi teknolojilerini daha çok kullanır hale gelmiştir. Daha önce ihtiyaç duyulmayan CRM (Customer Relationship Management - Müşteri İlişkileri Yönetimi), MRP (Materials Resource Planning - Malzeme İhtiyaç Planlaması), ERP (Enterprise Resource Planning –Kurumsal Kaynak Planlaması), e-ticaret gibi bir takım bilgisayar yazılımları birçok işletme için vazgeçilmez olmuştur. Özellikle, internet ve mobil cihazların yaygınlaşması, bilgi teknolojileri ile gerçekleştirilen elektronik ticaretin artmasını dolayısı ile bilgi sistemlerinin işletme, tedarikçiler ve müşterileri tarafından kullanılmasını yaygınlaştırmıştır.

Faaliyetlerinin büyük çoğunluğunu bilgi sistemlerinde gerçekleştiren işletmelerin söz konusu kural ve düzenlemelerde bilgi sistemlerini dikkate alması zorunlu hale gelmiştir. Bilgi sistemleri, işletme faaliyetlerini kolaylaştırmasının yanı sıra, gerekli kontrol ve denetimlerinin yapılmadığı durumlarda işletme içi ve işletme dışı hile ve usulsüzlüklerin de kolayca yapılmasına zemin hazırlamaktadır. Bu nedenle işletmeler, bilgi sistemlerini iyi kurgulamaları, iç kontrol ile ilgili düzenlemelerini bilgi sistemlerini dikkate alarak planlamalı, bunlara ilişkin politika ve prosedürlerini oluşturmalıdır.

İşletmelerin bilgi sistemlerinde kurgulanmış iç kontrol sisteminin etkinliği ve verimliliğinin test edilmesi, gerekli güncellemelerin yapılması için iç denetim

faaliyetleri de bilgi sistemleri ile yapılmalıdır. Bilgi sistemleri dikkate alınmadan yapılan bir denetimin işletme faaliyetlerine değer katması ve geliştirmesi mümkün değildir.

Bilgi sistemlerinde kontroller ve bilgi sistemlerinin denetimi konusu her geçen gün önemi artarak devam etmektedir. Konu ile ilgili uluslararası mesleki kuruluşlar oluşturulmuş (Örneğin ISACA), bu kuruluşlar tarafından bilgi sistemlerinin kontrolü ve denetimi konusunda standartlar ve rehberler yayınlanmıştır. Artık iç denetçi ve bağımsız denetçilerin bilgi sistemleri denetimini dikkate almadan bir denetim çalışması yapması mümkün değildir. Bu durumda iç denetçi ve bağımsız denetçi işletmenin kullandığı bilgi sistemlerini ve bunların nasıl çalıştığını anlayacak derecede bilgi sahibi olması gerekmektedir.

1. Temel Kavramlar

İşletmeler için her geçen önemi artan bilgi teknolojileri-bilgi sistemleri, iç denetim ve iç kontrol birbirinden farklı konular olmasına rağmen, işletmelerde bilgisayar kullanımının yaygınlaşması ile birbirleri ile iç içe geçmiş bir duruma gelmiştir. Bilgisayarsız bir işletme yönetimi düşünülemediği gibi bilgi teknolojileri ve bilgi sistemlerinden bağımsız bir iç kontrol ve iç denetim de mümkün değildir. Bu çalışmada her iki alanda da konunun detaylarına değinilmesi mümkün olmamakla birlikte, çalışmanın anlaşılması için bir takım temel kavramlara asgari düzeyde değinilmiştir.

1.1. İç Kontrol ve İç Denetim

Yönetimin temel fonksiyonlarından biri olan kontrol, daha çok sonuçlanmış işlem ve faaliyetlerin değerlendirilmesi, hata ve sapmaların tespiti olarak, işi yapanın dışında kişiler tarafından yapılan bir faaliyet olarak algılanmaktadır. Ancak Uluslararası İç Denetim Standartları'nda kontrol, işlemlerin kontrol altında tutulması, işlemlerin gerçekleştirilme aşamasında uygulanan bir süreç olarak kabul edilmektedir[1]. Kontrol, tek seferlik bir işlem olmayıp işletme faaliyetleri boyunca devam eden ve tekrarlayan işlemlerdir.

COBIT'in tanımına göre kontrol; "işle ilgili hedeflerin başarılmasına ve istenmeyen olayları önlenmesi, tespit edilmesi ve düzeltilmesine makul güvence sağlamak amacıyla tasarlanmış politikalar, usuller, uygulamalar ve kurumsal yapılar[2]" olarak tanımlanmıştır.

İşletmelerin varlıklarını sürdürebilmeleri için yönetim kurulu ve üst yöneticiler tarafından belirlenmiş hedeflere ulaşmaları gerekmektedir. Bu hedeflere ulaşmak amacıyla gerçekleştirdikleri faaliyetler için bir takım kural, prosedür ve politikalar tanımlanmıştır. Bu düzenlemeler ile işletmenin hedeflerine ulaşmada daha etkin ve

[1] Çetin Özbek, **İç Denetim Kurumsal Yönetim Risk Yönetimi ve İç Kontrol**, İstanbul: TİDE Yayınları, 2012 s.136

[2] http://www.isaca.org/COBIT/Pages/default.aspx, (Erisim Tarihi: 25.01.2015),

verimli olması, işletme kaynaklarının korunması, karşılaşılacak risklerin önceden tespit edilip etkilerinin en aza indirilmesi beklenmektedir. Bu amaçla işletmenin tüm faaliyetlerini kapsayacak şekilde yapılan bu tür düzenlemeler iç kontrol sistemini oluşturmaktadır. Bu kural ve prosedürlerin etkin olarak çalışması işletme tarafından hazırlanan finansal raporların güvenirliliğini de etkileyecektir. İç kontrol, sadece finansal nitelikli işlemleri değil, işletme faaliyetlerinin tamamını kapsayan tüm kontrolleri içerir[3]. Örneğin, bir üretim işletmesinde işçi giriş-çıkış saatlerinin tespit edilmesi için kart okuma sisteminin kullanılması kuralı, iç kontrol sisteminin bir parçasını oluşturmaktadır.

1985 yılında hileli finansal raporlamaların önlenmesi amacıyla kurulan Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi (Committee of Sponsoring Organizations of Treadway Commission-COSO) tarafından 1992 yılında yayınlanan "İç Kontrol-Bütünleşik Çerçeve (Internal Control-Integrated Framework) adlı raporda iç kontrol kavramının uluslararası düzeyde kabul edilen tanımı yapılmış, temel ilkeleri ortaya konulmuştur. Birçok ülke ve kuruluş iç kontrol ile ilgili düzenlemelerde söz konusu raporu dikkate almıştır. Avrupa Birliği üyelik görüşmeleri devam eden ülkemizde de, Avrupa Komisyonu tarafından tüm aday ülkelere tavsiye edilen COSO modeli ile uyumlu Kamu İç Kontrol sistemlerinin kurulması yönünden adımlar atılmıştır. Bu kapsamda 2003 yılında 5018 sayılı Kamu Mali Yönetimi Kontrol Kanunu çıkarılmış, bu kanunla kamu idarelerinde iç kontrol sistemi kurulmasına rehberlik etme görevi Maliye Bakanlığı'na verilmiş buna istinaden 2007 yılında Kamu İç Kontrol Standartları Tebliği yayınlanmıştır[4]. Söz konusu kanunda iç kontrol ile ilgili düzenlemeler yapılmış olup 55. maddesinde iç kontrolün tanımına yer verilmiştir. Buna göre iç kontrol;

> "İdarenin amaçlarına, belirlenmiş politikalara ve mevzuata uygun olarak faaliyetlerin etkili, ekonomik ve verimli bir şekilde yürütülmesini, varlık ve kaynakların korunmasını, muhasebe kayıtlarının doğru ve tam olarak tutulmasını, malî bilgi ve yönetim bilgisinin zamanında ve güvenilir olarak

[3] Ersin Güredin, **Denetim ve Güvence Hizmetleri SMMM ve YMM'lere Yönelik İlkeler ve Teknikler,** 13. b., İstanbul: Türkmen Kitabevi, 2012, s.316.

[4] T.C. Maliye Bakanlığı Bütçe ve Mali Kontrol Genel Müdürlüğü (07 Şubat 2014), Kamu İç Kontrol Rehberi http://www.bumko.gov.tr/Eklenti/8227,kamuickontrolrehberi1versiyon12.pdf?0 – (Erişim Tarihi: 29.12.214)

üretilmesini sağlamak üzere idare tarafından oluşturulan organizasyon, yöntem ve süreçle iç denetimi kapsayan malî ve diğer kontroller bütünü"

olarak tanımlanmıştır[5].

Uluslararası İç Denetim Standartları Terimler Sözlüğü'nde kontrol; yönetimin, denetim kurulunun, yönetim kurulunun ve diğer uygun birimlerin riski yönetmek ve belirlenen amaç ve hedeflere ulaşma ihtimalini arttırmak amacıyla aldığı tedbirler olarak tanımlanmaktadır[6].

Uluslararası Muhasebeciler Federasyonu (International Federation of Accountants - IFAC) yayınlanan Uluslararası Denetim Standartları ve bunun paralelinde Kamu Gözetim Kurumu tarafından yayınlanan Bağımsız Denetim Standartlarında iç kontrol aşağıdaki şekilde tanımlanmıştır[7].

"Finansal raporlamanın güvenilirliği, faaliyetlerin etkinliği ve verimliliği ile ilgili mevzuata uygunluk açısından işletmenin amaçlarına ulaştığına dair makul güvence sağlamak amacıyla üst yönetimden sorumlu olanlar, yönetim ve diğer personel tarafından tasarlanan, uygulanan ve sürekliliği sağlanan süreçtir. "Kontroller" terimi bir veya daha fazla iç kontrol bileşeninin herhangi bir yönünü ifade eder."

Söz konusu iç kontrol faaliyetlerinin etkinliği, yeterliliği ve sürekliliği iç denetim faaliyetleri ile değerlendirilir. İç denetim, yaptığı faaliyetler ile iç kontrol sistemine ilişkin güvence sağlar, aynı zamanda değerlendirmeler ile iç kontrol faaliyetlerinin oluşturulması ve geliştirilmesine danışmanlık yapmış olur[8].

İç denetim, işletmelerde belirlenen kontrollerin etkinliğini denetler[9]. Uluslararası İç Denetim Enstitüsü (Institute of Internal Auditors IIA) tarafından yapılan

[5] 5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu md. 55.
[6] Türkiye İç Denetim Enstitüsü, **İç Denetim Standartları Terimler Sözlüğü, http://www.tide.org.tr/uploads/IcDenetimTerimlerSozlugu.pdf** (Erişim Tarihi: 12.01.2015)
[7] Kamu Gözetim Kurumu, Türkiye Denetim Standartları - Bağımsız Denetim Standardı 315, İşletme ve Çevresini Tanımak Suretiyle "Önemli Yanlışlık" Risklerinin Belirlenmesi ve Değerlendirilmesi. http://www.kgk.gov.tr/contents/files/BDS/BDS_315.pdf (Erişim Tarihi: 12.01.2015)
[8] Özbek, **a.g.e.**, s.553.
[9] Güredin, **a.g.e.**, s.20.

tanımda iç denetim; bir kurumun faaliyetlerini geliştirmek ve onlara değer katmak amacını güden bağımsız ve objektif bir güvence ve danışmanlık faaliyetidir. İç denetim, kurumun risk yönetim, kontrol ve kurumsal yönetim süreçlerinin etkinliğini değerlendirmek ve geliştirmek amacına yönelik sistemli ve disiplinli bir yaklaşım getirerek kurumun amaçlarına ulaşmasına yardımcı olur[10].

Son dönemde işletmelerde bilgi teknolojilerinin yoğun olarak kullanılması ile, dünyada ve ülkemizde meydana gelen bir takım usulsüzlükler, bilgi teknolojileri denetimini gündeme getirmiş, bu konu ile alakalı çalışmalar yoğunluk kazanmıştır. Bilgi teknolojilerinin denetimi konusunda uluslararası meslek örgütleri oluşturulmuş, bu örgütler tarafından bir takım standartlar yayınlanmıştır.

1.2. Bilgi Sistemleri

Teknolojideki gelişmeler tüm dünyada ve her alanda değişikliğe neden olduğu gibi, işletmelerin faaliyetlerinde bilgi teknolojilerinin kullanımını da kısa sürede yoğun bir şekilde artmıştır. Önceleri basit borç alacak takibi için kullanılan elektronik tablolar daha sonraları, birbirleri ile entegre çalışan alt sistemlerden oluşan karmaşık bilgi sistemlerine dönüşmüştür. İşlem sayılarının çokluğu, işlemlerin birbirleri ile olan ilişkileri, işlemlerde karmaşık hesaplamaların yapılması, zamanında doğru bilgiye ulaşma ihtiyacı ve benzeri birçok nedenle bilgi sistemleri ve bilgi teknolojilerinin kullanılmadığı bir işletmede faaliyetlerin sağlıklı yürütülmesi mümkün değildir. Bu nedenle özellikle büyük işletmelerde, finans, insan kaynakları, üretim gibi fonksiyonlarına ait günlük işlem ve faaliyetlerin tamamı bilgi sistemleri kullanılarak yerine getirilmektedir. İşletmenin iyi tasarlanmış bir bilgi sistemine sahip olması, maliyet, zaman, verimlilik ve etkinliğine önemli ölçüde katkı sağlayacaktır[11].

Bilgi sistemleri (Information Systems IS), Bilgi Teknolojileri (Information Technology IT), Bilişim Teknolojileri terimleri bazen birbirlerinin yerine kullanılmakta olup çalışmada aşağıda yapılan tanımlar esas alınmıştır.

---

[10] Türkiye İç Denetim Enstitüsü, **a.g.e.**

[11] O'Brein J., Marakas G., **Manegement Information Systems**, **(10. Ed.)**, New York: The McGraw-Hill Companies, 2007, s.4.

Bilgi Sistemleri; verinin saklanması, yönetilmesi, işlenerek kullanılabilir faydalı bilgiye dönüştürülmesi ve işletme içinde ilgili kişi ve birimlere zamanında ve doğru bir şekilde iletilmesi amacıyla bir araya getirilen bilgisayar donanımı, yazılım ve diğer bileşenlerinden oluşan bir bütün olarak tanımlanabilir[12].

Bilgi sistemleri, bir organizasyonda karar verme ve kontrolü destekleyen bilgileri işleyen, saklayan ve dağıtan, birbirleri ile ilişkili bileşenlerden oluşan bir sistemdir[13]. Bilgi sistemleri süreci, girdi, işlem ve çıktı faaliyetlerinden oluşur. Süreçlere ait kullanıcılar tarafından girilen ve diğer kaynaklardan alınan veriler bilgi sisteminin girdisidir, bu veriler belirli işlemlerden geçirilip sınıflandırılarak saklanır, daha sonra ya başka bir bilgi sistemine kaynak veri olarak aktarılır veyahut kullanıcılara rapor şeklinde sistem çıktısı olarak iletilir.

İşletmelerin faaliyetlerinin çokluğu ve faaliyetleri sonucunda oluşan verilerin oldukça fazla olması verilerin yönetimi ve işlenmesi ancak bilgi sistemleri ile mümkün olmaktadır. Bilgi teknolojilerindeki gelişmeler, işletmenin ihtiyaç duyduğu bilgilerin daha hızlı, daha doğru ve daha kolay bir şekilde yönetilmesine yardımcı olmaktadır. İşletme bilgi sisteminin bileşenleri olan muhtelif uygulamalar ile, sisteme veri girişleri, verilerin saklanması ve yönetilmesi, işlenerek ihtiyaç duyulan bilgiler-raporlar üretilmesi, üretilen bu rapor ve bilgilerini, internet ve iletişim araçları ile ihtiyaç duyulan kişiler ile paylaşılması mümkün olabilmektedir.

Bilgi Teknolojileri ise; bilgi sistemlerinde girdi, işleme ve çıktı faaliyetleri için kullanılan fiziki ve fiziki olmayan teknolojilerin tamamıdır. Bilgisayar donanımları, bunları kontrol eden yazılımlar, bilgi sistemlerinde iletişimin sağlanmayan ağ ve telekomünikasyon teknolojileri, verinin yönetilmesi için kullanılan veritabanı uygulamaları ve internet bilgi teknolojilerinde kullanılan araçlardır[14].

Bilgi sistemleri genelde bilgisayarlardan oluşmakla birlikte artık günümüzde birçok makine ve alet bilgi sistemlerinin bir parçası olmaktadır. Örneğin kapı girişlerine kurulan bir turnike personel bilgi sistemine personelin giriş ve çıkış saat bilgilerini göndererek sisteme bilgi girişi sağlayan bir cihaz olarak bilgi sisteminin bir

[12] Hasan DURUCASU vd., **İ˙letme Bilgi Sistemleri**, Eskişehir: Anadolu Üniversitesi Yayınları, s.7.
[13] Kenneth C. Laudon ve Jane P. Laudon, **Manegement Information Systems Managing The Digital Firms**, New Jersey: Pearson Education, 2012, s.16.
[14] **a.g.e.**, s.20.

parçası olabilmektedir. Bilgisayar yazılımları, barkod okuyucular, otomasyon sistemleri gibi birçok teknoloji bilgi sistemlerinin parçası olarak kullanılmaktadır. Bazı kaynaklarda çalışanlar ve iletişim ağları da bilgi sisteminin bir parçası olarak değerlendirilmektedir.

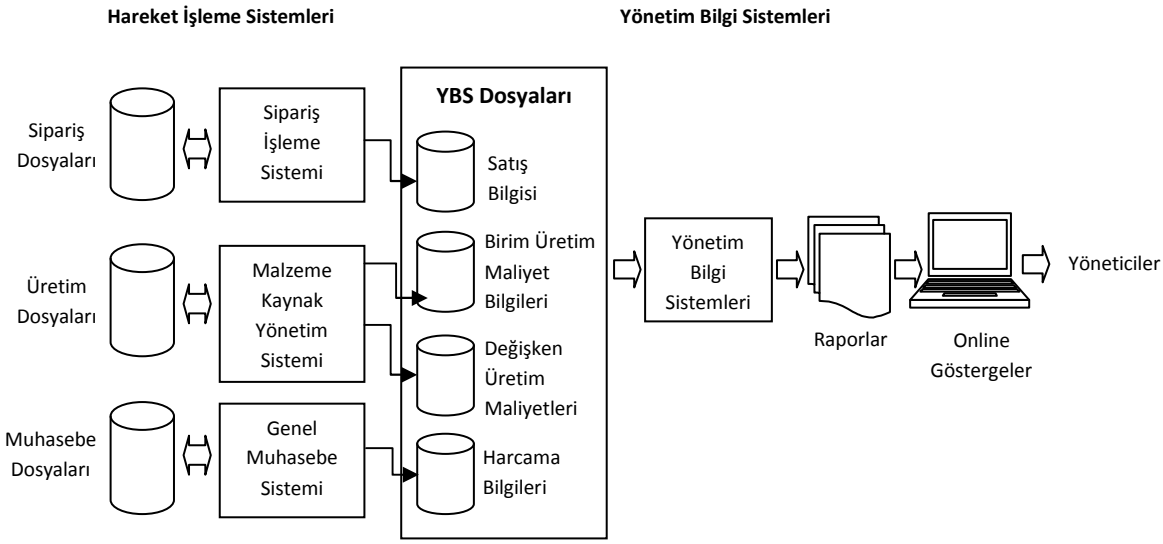
Son zamanlarda, internet, ağ teknolojisi ve mobil cihazlardaki gelişmeler cep telefonu tablet bilgisayar gibi cihazları da bilgi sisteminin vazgeçilmez bir parçası haline getirmiş, işletme dışında dahi işletme bilgi sistemini kullanma imkanı sağlamıştır. Ofis dışı çalışanlar, herhangi bir cihaz ile işletme bilgi sistemine rahatlıkla bağlanıp işlerini yapabilmekte veyahut bilgi sisteminin gönderdiği rapor ve bilgileri takip edebilmektedir. Örneğin, herhangi bir işlem için bilgi sistemlerinde tasarlanan miktar-tutar limit kontrolleri sonucu işlem onay için yetkili çalışanın akıllı telefonuna gönderilebilir, akıllı telefon ile yapılan onay sonrası işleme devam edilebilmektedir.

İşletmelerde kullanılan bilgi sistemleri temel olarak iki gruba ayrılmaktadır, Operasyon Destek Sistemleri, Yönetim Destek Sistemleri. **Operasyon destek sistemleri**, işletmenin günlük faaliyetlerini yerine getirirken kullanmış olduğu uygulamalardır. İşletmelerin günlük faaliyetlerine ait, banka hareketleri, cari hesap hareketleri, faturalar, üretim hareketleri gibi kayıtların takip edildiği sistemlerdir. Bunlara hareket işleme sistemleri (Transaction Processing System) de denilmektedir. Hareket işleme sistemleri diğer yönetim sistemleri için temel bilgi üreticisidir, bu nedenle buradaki bilgilerin doğruluğu ve eksiksiz olması durumunda karar sistemleri doğru çalışacaktır. İşletmelerde hareket işleme sistemlerinin kısa süreli çalışmaması durumunda bile ciddi kayıplara neden olabilir[15]. İleriki bölümlerde detaylı olarak anlatılacağı üzere uygulama kontrolleri daha çok hareket işleme sistemlerinde planlanmaktadır. Hareket işleme sistemlerinin dışında e-posta, kelime işlem ve elektronik tablo uygulamaları gibi yardımcı uygulamalar da operasyon destek sistemleri olarak değerlendirilmektedir.

Yönetim destek sistemleri, yöneticilerin etkili karar vermeleri için bilgi ve destek sağlayan uygulamalar olup hareket işleme sistemleri tarafından sağlanan verileri raporlayarak işletmenin faaliyetlerini özetleyip raporlamaktadır. Orta düzey yöneticilerin karar vermelerine yardımcı olacak önceden belirlenmiş standart raporlar

[15] Laudon, **a.g.e.**, s.44.

üretir. Karar destek sistemleri ise rutin olmayan konularda karar almada yöneticilere yardımcı olur[16].



Şekil 1. Hareket İ˙leme Sistemleri ve Yönetim Bilgi Sistemleri

Kaynak: Laudon, a.g.e., s.46

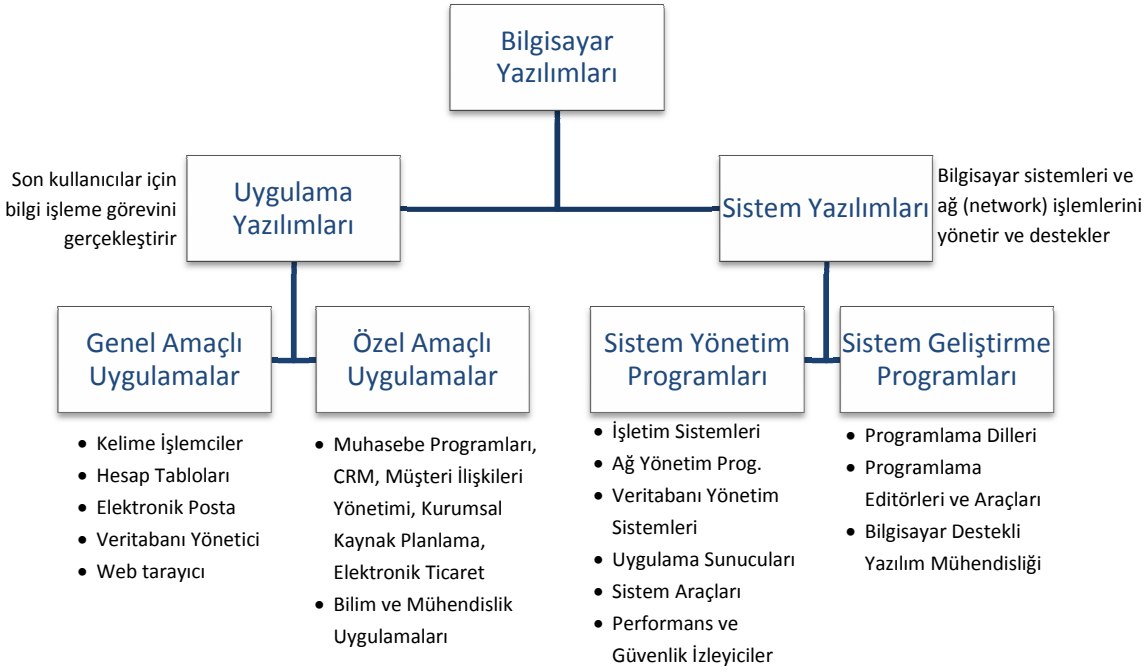
1.2.1. Bilgi Sistemleri ve Bile˙enleri

Bilgi sistemlerinin ana unsuru bilgisayarlar olduğu için işletmeler en çok bilgisayarlardan faydalanacaktır. Bilgisayar donanım (hardware) ve yazılım (software) olarak temel iki bileşenden oluşur. Donanım, bilgisayarları oluşturan ve fiziksel olarak çalışmasını sağlayan fiziki aygıt ve cihazların tümüdür. Bilgisayarın haricinde bilgi sisteminde girdi ve çıktı ve iletişim işlevlerinde kullanılan çevre birimleri - çevre donanımları adı verilen yazıcı, tarayıcı ve benzeri diğer fiziki aygıtlar bilgi sistemlerinin bir parçası olan donanımlardır.

Yazılım, elektronik aygıtların belirli bir iş yapmasını sağlayan programların tümüne denir. Bilgisayarlarda ise yazılım, bilgisayar donanımlarının fonksiyonlarının yerine getirilmesini ve kullanıcıların bilgisayar ile iletişimini sağlayan programlardır[17].

[16] O'Brein, **a.g.e.**, s.13.

Temel olarak sistem yazılımı ve uygulama yazılımı olarak iki gruba ayrılmaktadır. Sistem yazılımları, bilgisayarın çalışmasını ve yönetilmesini sağlayan yazılımlar ve sistem geliştirmede kullanılan programlardır; işletim sistemi, aygıt sürücüleri, programlama dilleri gibi. Uygulama yazılımları ise, işletim sistemi üzerinde çalışan, belirli bir amaca yönelik hazırlanmış özel programlardır. Metin editörleri, hesap tabloları, muhasebe programları bu tür yazılımlardır. Kullanıcılar, bilgisayar ile uygulama yazılımları ve işletim sistemi vasıtasıyla iletişim kurarlar. Bilgisayarların kullanımının artması ve kullanıcıların ihtiyaçlarının çeşitliliğine bağlı olarak uygulama yazılımları sayılamayacak derecede çoktur.



Şekil 2. Bilgisayar Yazılımlarının Sınıflandırılması

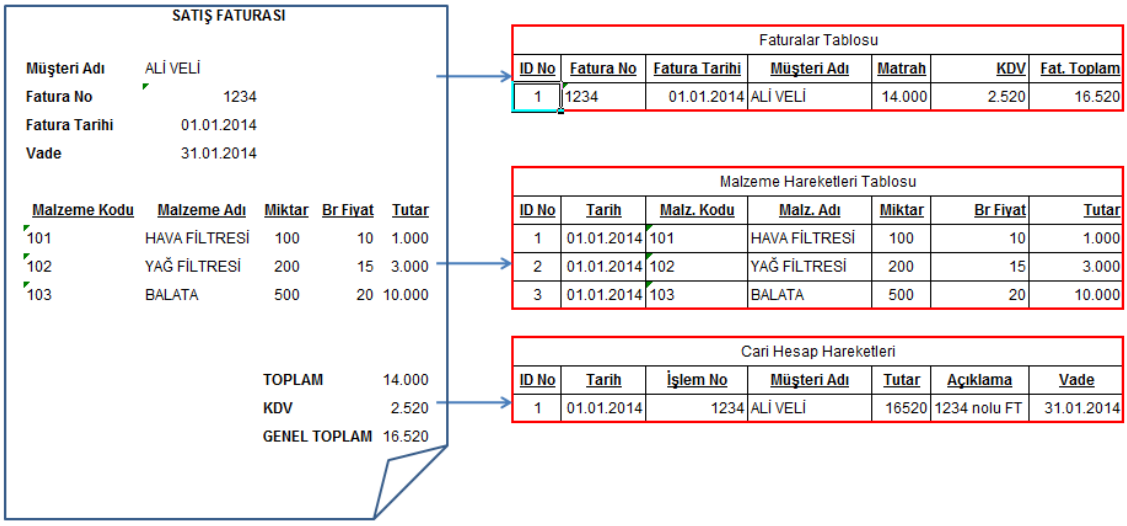
Kaynak : O'Brein, a.g.e., s.133.

Bilgi sistemlerine girilen verilerin kaydedilip saklanması için veritabanı uygulamaları kullanılır. Birbirleri ile ilişkili büyük verilerin depolandığı ve yönetildiği yazılımlara veritabanı denir. Önceleri basit bilgi ihtiyaçları tablolarda kaydedilip, saklanırken daha sonraları verilerin büyümesi, veriler arası ilişki kurulması ihtiyacı, veri güvenliğinin sağlanması ve detaylı raporlamalar gibi nedenler ile veritabanı

[17] O'Brein, **a.g.e.**, s.130.

yazılımlarına olan ihtiyaç artmıştır[18]. Veritabanı ilişkili verilerin saklandığı tablolardan oluşur. Bilgi sisteminde bilgi işleme amaçlı kullanılan her bir yazılımın verileri sakladığı muhtelif tabloları vardır. Uygulamaya herhangi bir işlem kaydedildiğinde bu işleme ait onlarca veri, veritabanında ilgili tablolara kaydedilir.

Örneğin, benzer uygulamalarda farklılıklar olmakla birlikte basit olarak, bilgi sisteminde bir satış faturası oluşturulduğunda, bu faturaya ait bütün veriler birçok tabloya kaydedilir. Fatura tarihi, fatura numarası, sipariş numarası, fatura tutarı, irsaliye tarihi vb genel bilgiler **fatura tablosuna**, fatura satırlarını oluşturan malzeme/hizmet kodu, birim fiyatı, miktarı gibi detaylar, **fatura detayları tablosuna**, fatura ile oluşan borç/alacak hareket kaydı **hesap hareketleri tablosuna**, faturadaki malzeme hareketleri de **malzeme hareketleri tablosuna** kaydedilir.



Şekil 3. Bilgi Sisteminde Satı˙ Faturası ve İli˙kili Tablolar

İyi tasarlanmış bir veritabanı, verimli ve etkin bir yönetim bilgi sisteminin temelini oluşturur, aynı zamanda kaydedilen verilerin zamanında, doğru ve tam olarak raporlanması veritabanının etkinliğine bağlıdır. En çok kullanılan veritabanı yazılımları Microsoft SQL ve Oracle SQL yazılımlarıdır.

[18] Nancy A. Bagranoff, Mark G. Simkin, Carolyn S. Norman ,**Core Concepts of Accounting Information Systems**, John Wiley & Sons Inc., 2011, s.116.

1.3. Yönetim Bilgi Sistemi ve Muhasebe Bilgi Sistemi

İşletme faaliyetlerine ilişkin verilerin anlamlı bilgiler haline dönüşmesi için bilginin yönetilmesi ve işlenmesi gerekmektedir. Bilgi yönetimi, Bilgi yönetimi günümüzde işletmeler için oldukça önemli hale gelmiştir. Rekabetin artması, teknolojik gelişmeler, müşteri talepleri, kâr oranlarının düşmesi ve benzeri nedenler ile işletmeler iş süreçlerini tekrar gözden geçirmiş, kaynakların daha etkin ve verimli kullanılmasına sağlamak için daha fazla bilgiye ihtiyaç duymuştur. Geleceğe yönelik uzun dönem yatırım kararları veyahut kısa dönem satış, üretim gibi kararlar için de bilginin doğru ve zamanında oluşması, analiz edilebilecek kalitede olması ve ilgililere ulaşması gerekmektedir.

Her türlü bilgi kayıtlarının eksiksiz tutulması, bilgilerin analiz edilip doğru kararlar verilmesi, birimler arası iletişimin hızlı sağlanabilmesi, uzun zaman alacak hesaplama ve raporlama gibi işlemlerin çok daha kısa sürede yapılabilmesi için işletmenin kullanmış olduğu bilgi teknolojileri ve uygulamalar yönetim bilgi sistemlerini oluşturur.

İşletmenin faaliyetlerinin büyük çoğunluğunu gerçekleştirmek için bilgi sistemlerini kullandığı durumlarda yönetim bilgi sistemlerinden söz edilebilir[19].

İşletmelerin fonksiyon ve süreçlerini gerçekleştirebilmeleri için farklı özelliklere sahip bilgi sistemlerine ihtiyaç duymaktadır. Örneğin pazarlama bilgi sistemi, insan kaynakları bilgi sistemi, üretim bilgi sistemi, muhasebe bilgi sistemi gibi. Önceleri birbirinden bağımsız olarak çalışan bu sistemler daha sonraları Kurumsal Kaynak Planlama (ERP - Enterprise Resource Planning) adı verilen uygulamalar adı altında birbirleri ile entegre hale gelmiştir. Örneğin; satış bilgi sisteminde girilen bir satış siparişinin bilgisi, hammadde tedariği için satınalma bilgi sisteminde, üretimin planlanması için üretim bilgi sisteminde, finansal kaynak planlaması için muhasebe bilgi sisteminde kayıtlar oluşmasını sağlar. Bu şekilde işletmeler bütün faaliyet ve işlemlerini bilgi sistemlerinde takip edip, kayıt altına alır ve ilgililere bu sistemler ile

[19] Şenay Lezki vd., **İ˙letme Bilgi Sistemleri**, Açıköğretim Fakültesi Yayınları, Eskişehir, 2012, s.62.

raporlar. Kullanıcılar ve yöneticiler bu bilgi ve raporlar ile kararlar alır, yorum ve analiz yapar[20].

Yönetim bilgi sistemi, işletmenin kaynaklarının, işletme amaçları doğrultusunda etkin ve verimli bir biçimde kullanılmasını planlamak, örgütlemek, kontrol etmek için, yönetimin ihtiyaç duyduğu işletme içi ve işletme dışı finansal ve finansal olmayan bilgileri, gerektiği yer ve zamanda, gerekli kişilere kullanabilecekleri şekilde sürekli olarak sağlamak amacıyla kurulan, çalıştırılan sistemler bütünüdür[21].

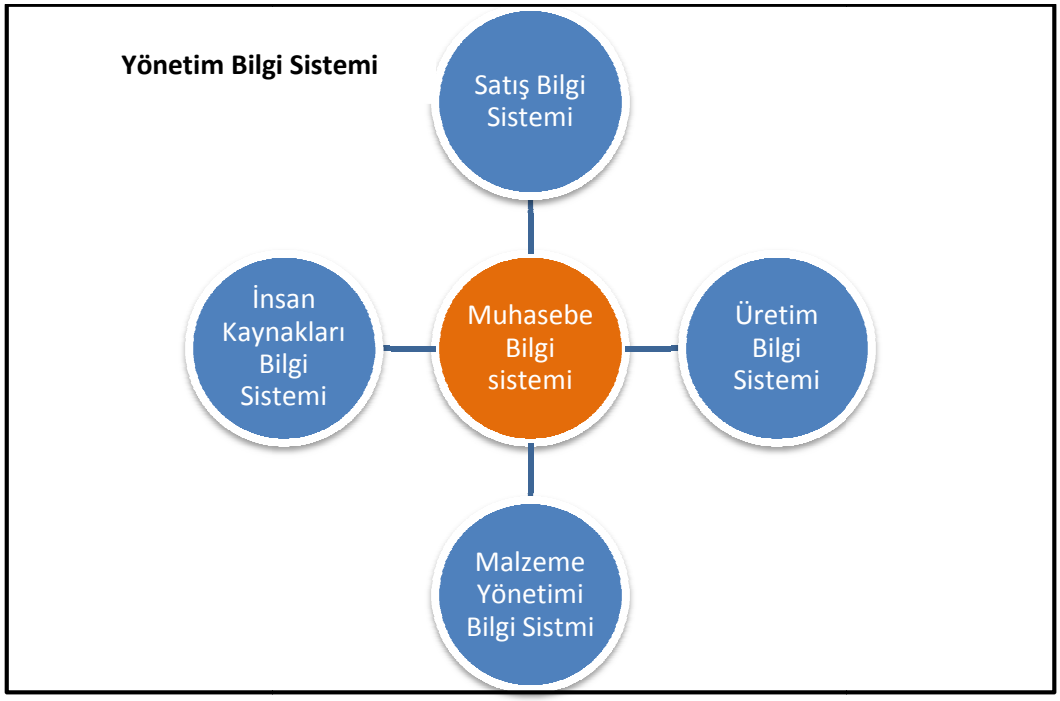
Muhasebe bilgi sistemi ise; mali nitelikteki verileri kaydeden, sınıflayan, ihtiyaca göre işleyen ve kullanıcılara raporlayan bir bilgi sistemidir[22]. Muhasebe bilgi sistemi aynı zamanda varlıklar üzerinde koruyuculuk ve hesap verebilirlik görevi üstlenmiştir[23].

Yukarıdaki tanımlardan anlaşılacağı üzere muhasebe bilgi sistemi, yönetim bilgi sisteminin bir alt sistemi olmakla birlikte diğer bilgi sistemleri ile birebir ilişkilidir. İşletmenin diğer faaliyetlerinin de muhasebe bilgi sisteminde izleri oluşur. Yöneticilerin karar verebilmesi için işletmenin muhasebe dışındaki birimlerce yapılan finansal faaliyetlerin muhasebe bilgi sistemi tarafından sınıflandırılıp raporlanması gerekmektedir.

İşletmelerde ilk kullanılan sistem genellikle muhasebe bilgi sistemi olmaktadır. Muhasebe bilgi sistemi aynı zamanda işletmenin yasal olarak tutmak zorunda olduğu defter ve kayıtların oluşturulduğu ve raporlandığı bilgi sistemidir.

---

[20] O'Brien ve Marakas, **a.g.e.** s.289.
[21] Lezki vd., **a.g.e.**, s.62.
[22] Fevzi Sürmeli, Melih Erdoğan, Nurten Erdoğan vd. **Muhasebe Bilgi Sistemi**, (T.C. Anadolu Üniversitesi Yayını No:1644, Eskişehir, 2005), s.32.
[23] Lezki vd., **a.g.e.,** s.62.



Şekil 4. Yönetim Bilgi Sistemi – Muhasebe Bilgi Sistemi İli˙kisi

Son yıllarda e-fatura, e-defter, e-arşiv gibi uygulamalar ile bazı işletmelerde muhasebe bilgi sistemi yasal zorunluluk haline gelmiştir. Ayrıca 29.12.2013 tarihinde yayınlanan 431 sıra no'lu Vergi Usul Kanunu Genel Tebliği ile, bazı işletmelerin alış kayıtları, satış kayıtları, envanter kayıtları, ithalat ihracat kayıtları ve üretim kayıtlarının bilgi sistemlerinde tutulması zorunluluğu getirilmiş olup, belirli bir süre sonra bu düzenlemenin kapsamının genişletileceği düşünülmektedir.

> "Vergi denetim faaliyetlerinin gelişen teknolojilere uygun bir şekilde yürütülebilmesi amacı ile belirlenen konulara ilişkin kayıtların elektronik ortamda oluşturulması, muhafazası ve ibraz edilmesine (Kayıt Saklama Gereksinimleri) dair usul ve esaslar bu Tebliğin konusunu teşkil etmektedir[24]."

İşletmenin mali durumunu gösteren temel mali tablolar da yine muhasebe bilgi sisteminde oluşturulmaktadır. Mali tabloların güvenilirlik düzeyinin yüksek olması için, bu tabloların oluşturulduğu bilgi sistemlerinin de denetlenmiş, kontrol edilmiş,

[24] 431 Sıra No'lu Vergi Usul Kanunu Genel Tebliği, http://www.gib.gov.tr/index.php?id=1079&uid=dmPFSoYSC7YfpYzQ&type=teblig (Erişim Tarihi: 10.12.2014)

hesaplamaların ve raporlamaların hatasız olduğu, işlemlerinde hile ve hata ihtimalinin olmadığı konusunda güvence sağlanmalıdır. Bu da bu sistemlerin standartlar çerçevesinde denetlenmesi ile olacaktır.

1.4. Bilgi Sistemleri Denetimi ve Bilgi Sistemi Denetimine İli˙kin Düzenlemeler

İşletmelerin bilgi sistemlerine olan bağımlılığı nedeni ile denetimde de bilgisayarların kullanılması kaçınılmaz olmuştur. Yine işletmenin faaliyetleri sonucu oluşan verilerin çokluğu, işlemlerin karmaşıklığı ve sadece bilgi sistemlerinde oluşan kayıtlar gibi nedenler ile bazı durumlarda da bilgisayarsız denetim imkansız hale gelmektedir. Örneğin yeni düzenlemeler ile zorunlu hale gelen e-fatura ve e-defter uygulamaları kapsamında oluşan kayıtlara yönelik bir denetimin bilgi sistemleri olmadan yapılması mümkün değildir. Bilgisayar kullanımı ile hesaplamalar, doğrulamalar, analizler daha kısa sürede yapılabilir hale gelmiştir. Yine bu sayede bilgi sistemindeki işletme kayıtlarının tamamının denetlenebilme imkanı doğmuştur.

Konun daha iyi anlaşılabilmesi için öncelikle, bilgi sistemleri denetimi ile bilgisayarlı denetim konularını açıklamak gerekmektedir. **Bilgisayarlı denetim**, denetim faaliyetlerinde bilgisayar ve yazılımlarının kullanılmasıdır. Bilgisayarlı denetim konusuna sonraki sayfalarda detaylı olarak yer verilmiştir.

Bilgi sistemleri denetimi ise, işletmenin faaliyetlerinde kullandığı bilgi teknolojileri kaynaklarının değerlendirilmesi sürecidir. Bilgi sistemlerinin işletmenin hedef ve amaçlarına uygun, ihtiyaçlarına cevap verebilecek, kaynakların verimli kullanılmasını, varlıkların korunmasını ve veri bütünlüğünü ve güvenliğini sağlayacak şekilde tasarlanıp tasarlanmadığının tespit edilmesine yönelik kanıt toplama ve değerlendirme süreci olarak tanımlanabilir[25].

[25] Topkaya, Adem, "Bilişim Sistemleri Denetiminde Sayıştay Modeli", **Dı˙ Denetim**, Y.Y. 2011, S.3, Ocak-Mart, s.118.

Bilgi sistemlerinin işletmede yaygın olarak kullanılması denetime olumlu katkılarının yanı sıra olumsuz etkileri de olmaktadır. Kullanılan uygulamalardaki hatalar, kullanıcı hataları, yanlış yetkilendirmeler gerekli iç kontrollerin bilgi sistemlerinde uygulanmaması ve benzeri durumlarda hatalı ve hileli kayıtların kolaylıkla oluşmasına neden olabilir. Bu durum bilgi sistemlerinde oluşturulan kayıtların ve raporların güvenirliliğini olumsuz yönde etkileyecektir. Yine, bilgi sistemlerinde oluşan kanıt niteliği taşıyan kayıtların fiziksel ortamdaki kanıtlara göre daha kolay değiştirilip silinebileceği gibi riskleri de göz ardı etmemek gerekir.

Bilgi sistemleri denetiminde denetçi temel olarak aşağıdaki şu üç soruya cevap aramaktadır[26],

- İşletmenin bilgi sistemi iş akışını aksatmayacak şekilde her zaman kullanıma uygun mudur?
- Sistemdeki bilgilere sadece yetkili kişiler tarafından mı erişilebilmektedir?
- Sistemdeki veriler her zaman ulaşılabilir, doğru ve güncel midir?

Konunun diğer bir boyutu ise sadece bilgi sistemlerinde kaydedilen ve saklanan verilerin değil, uygulamaların çalıştığı sistemlerin risklerinin de belirlenip denetlenmesi gerekmektedir. Bu denetimin gerçekleştirilebilmesi için bilgi teknolojileri konusunda ileri düzeyde bilgi gerekmekte veyahut uzman kişilerden yardım alınması gerekmektedir[27]. Bilgi sistemlerini oluşturan bileşenlerin fiziki ve digital güvenliği, hizmet sürekliliğinin sağlanması, uygulama geliştirme ve değişiklik ihtiyaçları ve bunların karşılanması, yedekleme ve acil durum planları gibi konular da bilgi sistemleri denetiminde dikkate alınmalıdır.

Konu ile ilgili uluslararası meslek kuruluşları standartlar ve düzenlemeler yayınlamıştır.

Uluslararası Denetim ve Güvence Kurulu (International Auditing and Assurance Standarts Board - IAASB) tarafından mali tabloların denetiminde kullanılmak üzere yayınlanan Uluslararası Denetim Standartları (International Standarts

[26] Lütfiye Defne YALKIN, "Bilgi Teknolojileri Denetimi" (Ankara Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı Yayınlanmamış Doktora Tezi), Ankara, 2011, s. 19.
[27] İzzet Gökhan Özbilgin "Bilgi Teknolojileri Denetimi ve Uluslararası standartlar", **Sayı˙tay Dergisi**, S.49. s.123

on Auditing - ISA), denetimin kalitesine yönelik bir takım düzenleme ve ilkeleri içermektedir. Bu standartlarda bilgi sistemleri ve bilgi sistemleri ortamında denetime yönelik bir takım düzenlemeler bulunmaktadır. Önceleri UDS (Uluslarası Denetim Standartları) 401 - Bilgi Sistemleri Ortamında Denetim (ISA - 401 Auditing in a Computer Information Systems Environment) numaralı standartta düzenlenmiş iken daha sonra bu standart yürürlükten kaldırılmış olup, diğer standartlarda bilgi sistemleri ile ilgili muhtelif düzenlemeler getirilmiştir[28].

Örneğin, UDS - 240 Finansal Tabloların Bağımsız Denetiminde Bağımsız Denetçinin Hileye İlişkin Sorumlulukları, standardında bilgisayar destekli denetim tekniklerinin kullanılabileceği, UDS-300 Finansal Tabloların Bağımsız Denetiminin Planlaması standardında, planlamada, verilerin erişebilirliği ve bilgisayar destekli denetim tekniklerinin uygulanabilirliğinin dikkate alınması, UDS - 315 İşletme ve Çevresini Tanımak Suretiyle "Önemli Yanlışlık" Risklerinin Belirlenmesi ve Değerlendirilmesi standardında, iç kontrol sisteminin değerlendirilmesi için bilgi sistemlerindeki genel ve uygulama kontrollerine, bilgi sistemlerinin mali tabloların oluşturulmasında kullanılması halinde bilgisayar destekli denetim tekniklerinin kullanılması, ve girdi, işlem ve çıktı kontrollerine değinilmiştir. Ayrıca diğer bazı standartlarda da bilgi sistemleri denetimi ve bilgisayar destekli denetim tekniklerine yönelik çeşitli düzenlemeler bulunmaktadır.

UDS'lere paralel olarak, Kamu Gözetim Kurumu (KGK) tarafından yayınlanan Bağımsız Denetim Standartları'nda da (BDS) bilgi sistemlerinde denetime yönelik düzenlemeler bulunmakla birlikte, kurum tarafından 2014 yılı içerisinde "Türkiye Bilgi Sistemleri Denetim Standartları"nın yayınlanması, bu konuda denetim yapacak kuruluşların ve denetçilerin mesleki yeterliliklerinin belirlenmesine yönelik çalışmaları devam ettiği belirtilmesine rağmen henüz yayınlanmamıştır[29].

Bilgi sistemlerinin denetlenmesine yönelik standartların belirlenmesi amacıyla 1967 yılında kurulan ve şu an 180 ülkede şubesi bulunan Bilgi Sistemleri Denetim ve Kontrol Derneği (Information Systems Audit and Control Association - ISACA) tarafından COBIT (Control OBjectives for Information and elated Technology) "Bilgi

[28] International Federation Of Accountants (IFAC) “International Standards on Auditing” , http://www.iaasb.org/publications-resources (Erişim Tarihi: 15.01.2015)
[29] Kuzu Dursun Ali, Bilgi Sistemleri Denetimi, http://kgk.gov.tr/contents/files/dalikuzusunum.pdf (Erişim Tarihi: 10.01.2015)

ve İlgili Teknoloji için Kontrol Amaçları" adlı bir kılavuz yayınlanmıştır. Bu yayın, işletme hedeflerine yönelik ihtiyaçlara bilgi sistemlerinin ne ölçüde cevap verdiğinin tespitine yönelik bir takım kontrol kriterleridir, bilgi teknoloji yönetiminde ulaşılması gereken hedefleri ortaya koymaktadır[30].

İlk olarak 1996 yılında yayınlanan COBIT, daha sonraları farklı tarihlerde güncellenmiş, son olarak 2012 yılında COBIT5 versiyonu yayınlanmıştır. COBIT bilgi sistemlerindeki kontrollerinin hedeflerini ve ne olması gerektiğini ortaya koyar nasıl yapılması gerektiği ile ilgilenmez. Beş temel unsuru vardır, yönetici özeti, çerçeve, kontrol amaçları, denetim ilkeleri ve yönetim ilkeleridir. COBIT çerçevesi, işletmenin bilgi sistemlerindeki kontrol hedeflerini dört ana başlık altında toplamış olup, bunlar; planlama ve organizasyon, tedarik ve uygulama, teslimat ve destek, izleme ve değerlendirmedir. Bu dört ana başlık altında belirlenen kontrol hedeflerinin herbiri için 0'dan 5'e kadar derecelendirmeler yapılarak değerlendirilir.

Ülkemizde de Bankacılık Düzenleme Denetleme Kurumu (BDDK), İç Denetim Koordinasyon Kurulu (İDDK) ve Sayıştay tarafından bilgi sistemleri denetim ile ilgili bir takım yasal düzenlemeler ve rehberler yayınlanmıştır. Bunlardan BDDK tarafından 14.10.2007 tarihli resmi gazete yayınlanan "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ"de bilgi sistemlerindeki riskler ve bunların yönetilmesi konusuna değinilmiş, bilgi sistemlerinde yapılacak iç kontrol düzenlemelerini "Uygulama Kontrolleri" ve "Genel Kontroller" olarak sınıflandırarak tanımlaması yapılmıştır[31].

1.5. Bilgi Sistemleri ve Denetçi

Bilgi sistemlerinin işletmelerde her aşamada yoğun olarak kullanılması, denetim yapacak bağımsız denetçiler ve iç denetçilerin bu konu hakkında yeterli seviyede bilgi sahibi olmasını gerektirmektedir. Denetçi denetime başlamadan önce, denetlenecek işletmenin bilgi sistemi ve kontrollerine ilişkin değerlendirmeler yapıp,

[30] Information Systems Audit and Control Association, http://www.isaca.org (01.04.2014).
[31] Deniz Umut Erhan, "BDDK Tebliği Çerçevesinde Bilgi Sistemleri Kavramının İrdelemesi ve Güncel Gelişmeler", **Muhasebe ve Denetime Bakı˙ Dergisi**, (Ocak 2009), s.91.

denetimde bilgisayar ve bilgisayar destekli denetim tekniklerinden ne derecede yararlanacağı, uzman bir bilgi sistemleri denetçisine ihtiyaç olup olmadığı konusunda planlama yapmalıdır. Bu nedenle denetçinin bilgi teknolojileri ve bilgi sistemleri hakkında temel düzeyde bilgi sahibi olması, iş süreçlerinin bilgi sistemlerindeki işleyişini anlayabilmesi gerekmektedir.

Uluslararası Muhasebeciler Federasyonu (International Federation of Accountants - IFAC) tarafından yayınlanan Uluslararası Eğitim Bildirileri El Kitabı'nda muhasebe meslek mensuplarının ruhsatlandırma öncesi ve sonrası bilgi teknolojileri (Information Technologies) bilgisi ve yeterlilik şartları belirlenmiş, denetçinin bilgi teknolojileri bilgisi ve yeterlilik şartlarını konu konu detaylı olarak ele alınmıştır. Bu yayında bilgi teknolojileri bilgisi ve yeterlilik şartları temel konu başlıkları aşağıdaki gibidir[32].

a. Genel IT (Information Technology) Bilgisi
b. IT kontrol bilgisi,
c. IT kontrol yeterlilikleri,
d. IT kullanıcı yeterlilikleri,
e. Bilgi sistemleri yöneticisi, değerlendiricisi, ya da tasarımcısı rollerinin yeterliliklerinin biri ya da bunların karışımı.

Ayrıca IIA "İç Denetçiler Enstitüsü" (The Institute of Internal Auditors - IIA) tarafından Uluslararası İç Denetim Standartlarından 1210 – Yeterlilik ve Azamî Meslekî Özen ve Dikkat standardı A3. nolu paragrafında bilgi teknolojileri ve denetçiler konusuna değinmiştir[33].

> **1210- A3.** İç denetçiler, verilen görevi yerine getirebilmek için kilit bilgi teknolojisi riskleri ve kontrolleriyle ilgili yeterli bilgiye ve mevcut teknoloji tabanlı denetim tekniklerine sahip olmak zorundadır.

[32] Uluslararası Eğitim Bildirileri El Kitabı - IFAC, Çev. Öztürk, Y., TURMOB Yayınları, Ankara, 2010, s.126.
[33] İç Denetim Standartları, Türkiye İç Denetim Enstitüsü, http://www.tide.org.tr/uploads/UMUC_2013.pdf (Erişim Tarihi:10.05.2014).

ISACA, bilgi sistemleri denetçileri için rehber olacak, mesleki etik kuralları ve denetim standartlarının, belirlendiği "Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araç ve Teknikleri" bir rehber yayınlamıştır. ISACA tarafından uluslararası geçerliliği olan, denetçinin bilgi sistemlerinin denetiminde yeterliliğini belgeleyen, Sertifikalı Bilgisayar Sistemleri Denetçisi (Certificated Information Systems Audit - CISA) sertifikaları düzenlenmektedir.

1.6. Bilgi Sistemleri Güvenliği ve Bilgi Sistemlerindeki Riskler

İşletmelerin bilgi sistemlerine olan bağımlılıkların artması nedeni ile bilgi sistemlerindeki güvenlik boşlukları ve bunları meydana getirebileceği risklerin yönetilmesi önem kazanmıştır. Önceleri fiziki ortamda saklanan ve her geçen çok daha önemli hale gelen bilgi, günümüzde artık bilgi sistemlerinde sanal ortamda bulunmakta ve öncekinden daha fazla tehdit ve saldırılara maruz kalmaktadır. Yapılan araştırmalar her geçen gün bu saldırı ve tehditlerin artığını ve giderek daha tehlikeli hale geldiğini göstermektedir[34]. Uluslararası büyük şirketler, devlet kurumları dahi zaman zaman bu tür tehdit ve saldırılar sonucu maddi ve manevi kayıplara uğramakta, hizmetlerinde aksamalar yaşanabilmektedir.

Bilgi sistemleri, faaliyetler ve yönetim süreçlerinde kolaylıklar sağlarken aynı zamanda sistemlerin karmaşıklığı kontrolünü zorlaştırmıştır. Önceleri belge üzerinde yapılan hile ve usulsüzlükler, bilgi sistemlerinde çok daha kolay yapılabilmekte ve geleneksel yöntemler ile tespiti neredeyse imkânsız olmaktadır. Bilgi sistemlerinin olmadığı durumlarda işlenilemeyen suçlar bilgi sistemleri ile işlenir hale gelmiştir. Bu nedenle hile ve suiistimallerin önlenmesi için bilgi sistemlerindeki kontroller ve denetimler önem kazanmıştır. Bilgi sistemindeki açıklar, kontrol eksikliği veyahut kullanıcı hataları gibi nedenler ile işletme içi ve işletme dışı hile ve usulsüzlüklere neden olabilecektir. Bu durumun işletmeler için maddi ve manevi kayıplara neden olması kaçınılmazdır.

[34] Mete Eminağaoğlu ve Yılmaz Gökşen, "Bilgi Güvenliği Nedir Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri" **Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, (2009) Cilt 11, S.4., s.1.

Bilgi güvenliği, bilginin yetkisiz kişiler tarafından erişilmesi, kullanılması, değiştirilmesi veyahut silinmesini engelleyecek önlemler alınmasıdır. Bilgi güvenliğinin sağlanması sadece bir takım teknik önlemler alınması değildir, aynı zamanda yönetim tarafından bir takım kural ve prosedürlerin belirlenmesi ve çalışanların bunlara uyumunun sağlanması da gerekmektedir. Bilgi güvenliği yönetimi bir seferlik yapılan bir işlem olmayıp sürekli devam eden bir süreçtir[35]. Bilgi varlıkları ve bilgi sistemlerinin güvenliğinin sağlanabilmesi için karşılaşılacak tehditlerin önceden tahmin edilip risk analizi yapılarak önlemler alınmalıdır.

Bilgi güvenliğinde temel olarak gizlilik, bütünlük ve erişebilirlik kavramları üzerinde durulmakla birlikte bazı kaynaklarda gerçeklik ve inkâr edilemezlik de bunlara eklenmiştir. Bilgi güvenliğinin sağlanabilmesi içi bu temel kavramların sağlanmış olması gerekmektedir. İşletme "kurumsal kontroller" kapsamında hazırlayacağı politika, prosedür ve kurallarda bilgi güvenliği ile ilgili temel kuralları belirlemiş olmalıdır.

Gizlilik, işletme verilerine içeriden ve dışarıdan yetkisiz kişilerce ulaşılmasının engellenmesidir. Özellikle internet ve ağ teknolojilerindeki gelişmeler, mobil cihazların kullanımındaki artış dış kaynaklı tehditlerin artmasına neden olmuştur, bilgi hırsızlığına yönelik suç olayları da artmıştır. İşletme içinde kullanıcı yetkilendirmelerde yapılan hata ve eksiklikler veyahut uygulamanın yetkilendirmedeki yetersizliği de gizliliğin ihlal edilmesine neden olmaktadır.

Gizlilik ihlalleri sadece işletmeyi ilgilendiren bir durum değildir, örneğin bir bankadaki müşteri verilerinin yetkisiz kişilerin eline geçmiş olması milyonlarca kişi ve kuruluşu olumsuz etkileyecek bir durum olacaktır.

Bütünlük, bilginin kaynağından kullanıcıya eksiksiz, tam ve doğru olarak ulaştırılmasıdır, bu kullanıcı bir kişi veyahut bir sistem olabilir. Erişebilirlik ise, bilgi sistemlerinden beklenen işlerin zamanında kullanıcılar tarafından ulaşılabilir olmasıdır. Erişebilirlik bazen bir kötü niyetli yazılım ve kişiler tarafından engellenebileceği gibi, bazen de iyi tasarlanmamış bir bilgi teknolojileri altyapısı da erişimi riskine neden olabilir.

[35] Mehmet Tekerek, "Bilgi Güvenliği Yönetimi", **KSÜ Fen ve Mühendislik Dergisi**, S.11(1), 2008, s.133.

Bilgi sisteminin güvenliğinin bir diğer unsuru da inkâr edilemezlik, kayıt (log) tutma, sistemde yapılan her bir işlemin kim tarafından, ne zaman ve ne yapıldığının detaylı olarak kaydedilmesidir. Bu sayede işletme içinde yapılan herhangi suiistimal ve usulsüzlükler daha kolay bir şekilde tespit edilebilecek, inkâr edilemeyecektir.

İşletmede bilgi güvenliğinin sağlanmış olması, ilişkili olunan kişilere ait bilgilerin güvende olduğu güvencesini sağlar. Meydana gelebilecek herhangi bir olumsuz durumda işin devamlılığını sağlayarak kaybı en aza indirir. İşletme bilgilerinin istenmeyen kişilerin eline geçmesi engellenmiş olur.

İşletmeler tarafından kullanılan uygulamalar, teknolojinin doğası gereği, uygulama kullanıcıları ve uygulamanın yönetilmesinden kaynaklanan bir takım riskleri her zaman içermektedir. Bu risklerin yönetilmemesi durumunda bilginin tam, doğru ve zamanında oluşmasına olumsuz etkisi olacaktır. Tespit edilen bu risklerin yönetilmesi için uygulama kontrolleri kullanılmaktadır[36].

Denetim faaliyeti için ayrılan kaynaklar sınırsız değildir, bu nedenle denetimin daha etkin olması için risk odaklı denetim yaklaşımı ile bilgi sistemlerinde risklere göre bir plan yapılmalıdır. İç denetçi veyahut bağımsız denetçi, denetimi planlarken işletmenin bilgi sistemlerindeki risklerinin ne olduğunu değerlendirmeli, risklere karşı alınan genel ve uygulama kontrol tedbirlerinin yeterli ve etkin olup olmadığını analiz etmeli, geliştirilmesine katkı sağlamalıdır.

Bilgi sistemlerini olumsuz etkileyip işletmenin faaliyetlerini yerine getirmesini engelleyecek riskler beş ana başlıkta toplanabilir[37].

a. Personel riski; işletme çalışanlarının bilinçsiz kullanımı veyahut kötü niyetli kullanımı nedeniyle oluşan risklerdir.

b. Teknolojik riskler; kullanılan donanım ve yazılımdan kaynaklanan risklerdir. Antivirüs programının bulunmaması, yazılımdaki hatalı kodlamalar ve benzeri durumlarda oluşabilir.

[36] Christine Bellino, Jefferson Wells ve Steve Hunt, **Global Technology Audit Guide 8 – Auditing Application Controls**, USA:The Institute of Internal Auditors (IIA), 2007. s.2.
[37] Fatih Akyol, "Cobit Uygulayan Şirketlerde Bilgi Güvenliği Politikalarının Şirket, Personel ve Süreçleri Etkileri" (Beykent Üniversitesi Sosyal Bilimler Enstitüsü İşletme Yönetimi Ana Bilim Dalı Yönetim Bilişim Sistemleri Dalı), İstanbul, 2013, s. 12.

c. Organizasyon riski; bilgi sistemlerinin ve kullanıcıların, yanlış planlanması gibi hatalar nedeni ile ortaya çıkar.

d. Yasal riskler

e. Dış riskler; Fiziki veyahut fiziki olmayan saldırılar, doğal afet ve benzeri nedenler sonucu oluşabilecek riskler.

Yukarıda bahsedilen risklerden en önemlisi kötü niyetli personel tarafından sistem içinde yapılabilecek suiistimallerdir. ACFE'nin (Association of Certified Fraud Examiners - Uluslararası Suistimal İnceleme Uzmanları Derneği) 2014 Küresel Suiistimal Çalışması'na göre suiistimallerin işletmelere maliyetinin cirolarının %5'i oranında olduğu tahmin edilmektedir. 100 den fazla ülkede 1.483 vakıa üzerinde yapılan çalışma sonucu oluşturulan raporda suiistimalin tarifi yapılmış, en sık da varlıkların kötüye kullanılması yolu ile suiistimalin gerçekleştiği ortaya konulmuştur. Bu suiistimaller de işletmenin faaliyetlerini takip etmek için kullandığı bilgi sistemleri yolu ile yapılmaktadır. Örneğin, sistemde oluşturulan hayali şirketler veyahut hayali çalışanlara ödeme yapılması, gelir kaydetmeme, gider yazma, alacak kaydırma, sahte satışlar gibi[38].

Bu tür suiistimallerin önlenmesi için genel kontroller ve uygulama kontrolleri kullanılmakta, meydana gelmesi durumunda tespit edilebilmesi için de bilgi sistemlerinde çeşitli veri analiz teknikleri uygulanmaktadır. Proaktif yöntem denilen bu yöntemde, işletme verilerinin örnekleme yolu ile alınan bir kısmı üzerinde hile denetimi yapılan geleneksel yönteme karşılık, veri analizi teknikleri ile bütün veride denetim yapılabilmektedir. Bilgi sistemleri kullanılarak gerçekleştirilen proaktif yöntemlerde herhangi bir talep veyahut ihbar olmaksızın, hile olma ihtimaline karşın bir denetim vardır[39].

Bilgi güvenliği konusu ulusal ve uluslararası birçok kurum tarafından gündeme alınmış bu konuda bazı standartlar ve düzenlemeler yapılmıştır. Örneğin BDDK tarafından yayınlanan "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ"inde "Banka, bankacılık faaliyetlerinde bilgi teknolojilerini kullanıyor

[38] ACFE, Report To The Nations On Occupational Fraud And Abuse, http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf (Erişim Tarihi 06.01.2015)
[39] Yıldırım Ercan Çalış, Emrah Keleş, Ahmet Engin, "Hilenin Ortaya Çıkartılmasında Bilgi Teknolojilerinin Önemi ve Bir Uygulama" **Muhasebe ve Finansman Dergisi**, S.64, (Temmuz 2014), s.93.

olmasından kaynaklanan riskleri ölçmek, izlemek, kontrol etmek ve raporlamak üzere gerekli önlemleri alır. Bilgi sistemlerine ilişkin risklerin yönetilmesi, bilgi sistemleri yönetiminin önemli bir bileşeni olarak ele alınır[40]." Yine ülkemizde Tübitak bünyesinde bilgi güvenliği ile ilgili güncel uyarılar ve bilgilendirici yayınlar yapmak üzere "Ulusal Bilgi Güvenliği Kapısı" programı yürütülmektedir[41]. Konu ile ilgili Türk Standartları Enstitüsü tarafından 02.03.2006 tarihinde "ISO 27001 ve ISO 27002 Bilgi Güvenliği Yönetim Sistemi Standartları" yayınlanmıştır[42].

[40] BDDK, Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ, Resmi Gazete 14.09.2007 Sayı 26643.
[41] https://www.bilgiguvenligi.gov.tr/hakkimizda.html , (Erişim Tarihi: 24.12.2014)
[42] http://www.tse.org.tr/tr/Default.aspx , (Erişim Tarihi: 24.12.2014)

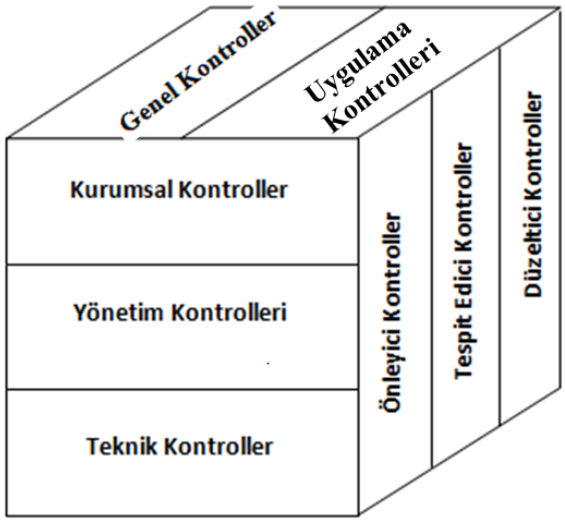
2. Bilgi Sistemlerinde İç Kontrol

Bilgi teknolojilerinin, işletme faaliyetlerinin gerçekleştirilmesinde yardımcı olmasının yanı sıra, işletmenin, hile, aldatma, hırsızlık, yetkisiz erişim, bilgi sistemlerinin çalışılamaz duruma getirilmesi gibi tehdit ve risklere maruz kalma ihtimalini de artırmıştır. Özellikle internet ve ağ teknolojilerindeki gelişmeler ile ağa bağlı herhangi bir yerden bilgi sistemlerine müdahale edilebilmesi mümkündür. Yine fiziki ortamda bulunan ve işletme dışına çıkarılması mümkün olmayacak derecede büyük hacimli işletmeye ait bir çok bilgi, bilgi sistemlerinde saniyeler içinde yetkisiz erişim, suistimal veyahut kaybolma gibi durumlara maruz kalması mümkün hale gelmiştir. Bu tür tehditler işletme dışından olabileceği gibi, işletme içi tehditlerin çok daha fazla olduğu görülmektedir. Bilgi sistemlerinde kontrol, işletmenin bilgi sistemleri kullanması ile karşılaşacağı risklerin ortadan kaldırılmasına veyahut etkilerinin en aza indirilmesine yardımcı olur[43]. Bilgi sistemlerinde düzenlenen bu kontroller iç kontrol sisteminin birer parçasıdır, işletmede bilgisayar kullanımın yoğunluğu derecesinde bu kontrollerin, iç kontrol sistemindeki konumu ve önemi artmakta veyahut azalmaktadır.

2.1. Kontrollerin Sınıflandırılması

Bilgi sistemleri kontrollerinin amaçlarının ve genel iç kontrol sistemindeki yerinin daha iyi anlaşılması için farklı açılardan aşağıdaki şekilde sınıflandırmalar yapılmaktadır.

[43] Steve MAR, vd., **Global Technology Audit Guide 1 – Information Technology Controls**, USA, The Institute of Internal Auditors, 2012, s.



Şekil 5. Kontrollerin Sınıflandırılması

Kaynak: Mar, a.g.e., s.2

2.1.1. Genel Kontroller ve Uygulama Kontrolleri

Genel Kontroller, işletmede kullanılan bilgi sisteminin tüm süreç ve bileşenleri ile ilgili tüm kontrollerdir. Uygulama kontrolleri, işletmelerin faaliyetlerini gerçekleştirmek için kullandığı uygulamalar kapsamında belirlenen kontrollerdir. İşletme faaliyetlerinin çokluğu nedeni ile kullandığı uygulamalar da bu derece fazladır ve birbirlerinden farklıdır. Bu nedenle uygulama kontrolleri her bir işletme ve uygulama için, kontrol ihtiyaçları kapsamında belirlenmelidir. Sonraki bölümlerde uygulama kontrolleri ile ilgili daha detaylı bilgiler verilecektir.

ISACA tarafından yayınlanan, Denetim, Güvence ve Kontrol Uzmanlarının Bilgi Teknolojileri Standartlarından S15 BT Kontrolleri standardında bilgi sistemlerindeki kontroller, genel kontroller ve uygulama kontrolleri olarak sınıflandırılmış, yine birçok standardında konuya detaylı olarak değinilmiştir.

2.1.2. Yönetim Açısından Kontrollerin Sınıflandırılması

Kontroller için bir diğer sınıflandırma ise, kurumsal, yönetsel ve teknik kontrollerdir. Kurumsal kontroller (Governance Controls), yönetim kurulunun, işletmenin bilgi sistemleri politika ve prosedürlerinin var olduğunu ve etkin bir şekilde işlediğinin güvencesini sağlamasıdır. Yönetim kontrolleri (Management Controls), işletmenin üst düzey yöneticileri tarafından, yönetim kurulu tarafından belirlenen politika ve prosedürler çerçevesinde işletme hedeflerini gerçekleştirecek bir şekilde bilgi sistemleri kontrollerinin varlığının ve işlerliğinin güvencesini sağlamaktır. Yönetim kontrollerinin temelini oluşturan teknik kontroller (Technical Controls), bilgi sistemlerinin teknik alt yapısı ile ilgili kontrollerdir. Yetkisiz erişim, değişiklik kontrolleri, veritabanı kontrolleri, günlük kayıtlar gibi kontrollerdir[44].

2.1.3. Önleyici, Tespit Edici ve Düzeltici Kontroller

İç kontroller bir başka açıdan önleyici, tespit edici ve düzeltici olarak sınıflandırılmaktadır. Önleyici kontroller, istenmeyen bir durumun meydana gelmesini, ortaya çıkabilecek bir hatayı önlemek için düzenlenmiş kontrollerdir. Örneğin, bilgi sistemine veri girişi esnasında verilerin uygulama mantığına uygun olduğunu doğrulamak ve sadece doğru verilerin girişine izin vermek, yanlış ve geçersiz verilerin girişini engellemek bir önleyici kontrol tipidir[45]. Bilgi sistemlerinde uygulama kontrollerinden girdi kontrolleri önleyici kontrollere örnek olarak verilebilir.

Tespit edici kontroller, uygulama mantığına, iş süreçlerindeki kurallara uygun olmayan kayıtların tespit edilmesine yönelik kontrollerdir. Bu kontroller aynı zamanda önleyici kontrollerin etkinliğinin ölçülmesinde de kullanılır[46]. Her ne kadar girdi kontrolleri ile istenmeyen ve uygun olmayan verilerin girişi kontrol altına alınmak istense de zaman zaman hatalı giriş riski devam etmektedir. Bazı durumlarda önleyici

[44] Mar vd., **a.g.e.**, s.17
[45] Bellino vd., **a.g.e.** s.6.
[46] Özbek, **a.g.e.** s.541.

kontrollerin bulunmaması veyahut olsa bile etkin ve yeterli olmaması durumunda istenmeyen bilgi sisteminde istenmeyen kayıtlar oluşabilir. İşte bu durumlarda hatalı verilerin tespit edilmesi için bu kontrol tipleri kullanılmaktadır. Örneğin kasa ödeme hareketlerinin incelenip limitlerin üzerindeki ödemelerin tespit edilmesine yönelik kontroller, tespit edici kontrollerdir.

Düzeltici kontroller ise, istenmeyen bir olayın gerçekleşmesi ve bunun tespit edilmesi halinde hatanın düzeltilmesi için belirlenmiş kontrollerdir[47]. Örneğin, bir satış faturası girişinde sisteme tanımlanan fatura serisinin son numarası kontrol edilir, kullanıcının farklı bir numaralandırma yapması durumunda, belge kayıt aşamasında yeni numara uygulama tarafından sıradaki numara ile kaydedilmesi sağlanabilir.

2.2. Genel Kontroller

Bilgi sisteminin tüm bileşenleri ve süreçlerini kapsayan, düzgün çalışmasını sağlayan ve riskleri en aza indirmeyi hedefleyen kontrollerin bütünüdür. Genel kontroller daha çok sistemi oluşturan bilgi teknolojileri ile ilgili teknik kontroller olmakla birlikte bir kısmı da işle ile ilgili kontrollerdir. Genel kontroller bilgi sistemi kontrollerinin temelini oluşturur, bu nedenle genel kontrollerin zayıf ve güvensiz olması diğer kontrolleri de etkileyecektir dolayısı ile denetçinin bilgi sistemi kontrollerine bakışı ve kontrolleri test yöntemleri de buna göre belirlenecektir[48]. Etkin olmayan bir genel kontrol ortamının bulunduğu durumda uygulama kontrollerine olan güven de sorgulanması gerekmektedir.

Genel kontroller şunları içerir;

Bilgi teknolojileri güvenliği,

Risk yönetimi,

Kaynak yönetimi,

Uygulama geliştirme ve kullanıcı yönetimi,

[47] **a.g.e.** s.541.
[48] Mar vd., **a.g.e.**, s.16.

Fiziksel ve dijital (logical) güvenlik,

Yedekleme ve veri kurtarma,

İş süreçlerinin devamlılığı ve felaket sonrası kurtarma kontrolleri.

2.3. Kullanıcı Tanımlama ve Yetkilendirme – Kimlik Tespiti

Uygulama kontrollerine geçmeden önce hem genel kontroller hem de uygulama kontrolleri kapsamında değerlendirilen kullanıcı tanımlamaları ve yetkilendirme konusunun incelenmesi gerekmektedir. Bu konuda işletme politikaları, personel görev ve yetkileri ile işletmede kullanılan uygulamaların yetkilendirme ile ilgili kabiliyetleri birlikte değerlendirilmelidir. İşletme organizasyonunda bilgi sistemlerini kullanan personellerin görev ve sorumlukları birbirinde farklı olması nedeni ile bilgi sistemlerini kullanma ve erişim yetkilerinin de bunlara uygun olması gerekmektedir.

Yapılan anketlerde bilgi sistemlerinin güvenliğinde en önemli konunun kullanıcı erişim ve yetkilendirme olduğu görülmektedir. Bu durum, konunun karmaşık olması, işletmelerde görev ayrılığı ilkesinin tam oturmamış olması ve uygulamalardaki yetkilendirme ile ilgili eksiklikler gibi nedenler ile meydana gelmektedir.

Bu yetki ve erişim tanımlamaları, bilgi sistemindeki verilerin güvenliği, yapılan işlemlerin izlenebilir olması gibi nedenler ile oluşturulan "kullanıcı hesapları" ile yapılmaktadır. Hemen hemen her uygulama, giriş anında daha önce oluşturulan bu hesap bilgilerini kullanıcından talep eder, kullanıcı, kullanıcı hesabı ve şifresi olmadan programa giriş yapamaz, uygulama tarafında kimlik tespiti yapıldıktan sonra giriş sağlanır. Bu kontrol bilgi sistemindeki kontrol düzenlemelerinin en önemlilerindendir, çünkü uygulamalardaki her türlü yetkilendirme bu kullanıcı hesaplarına tanımlanmaktadır.

Kullanıcılar, sisteme giriş esnasında doğrulama sağlayan bu şifreleri kolayca hatırlamak için basit ve zayıf belirleyebilmekte veyahut başkaları ile paylaşabilmekte, kolayca hatırlayabilmek için bir yerlere yazabilmektedirler. Bu durum bilgi sisteminin

güvenliğini tehlikeye sokmaktadır. Bu nedenle veri güvenliği amacıyla birçok işletmede uygulamalarda tanımlanan kullanıcı hesaplarına ait şifreler de yönetilmektedir. Örneğin, belirli aralıklar ile kullanıcı şifrelerinin değiştirilmesinin zorunlu olması, şifrenin belirlenen format ve uzunlukta olması, kolay şifrelerin engellenmesi gibi kontroller ile kullanıcı hesabının dolayısı ile işletme verilerinin güvenliği sağlanmış olmaktadır. Bazı bankaların uygulamalarında, kullanıcıların, doğum günü, kimlik numarası veyahut cep telefonu numarası gibi bilgilerin şifre olarak belirlenmesine izin verilmemektedir. Şifrenin yanı sıra bazı sistemlerde, jeton, akıllı kart veyahut biometrik doğrulama yöntemleri de kullanıcı erişimi için kullanılmaktadır[49].

Birçok uygulamada farklı yetkilendirme mantıkları oluşturulmuş olmakla birlikte bu çalışmada örnek olayda kullanılan Logo-Tiger uygulamasındaki yetkilendirme işlemleri dikkate alınarak konunun detayına inilmeye çalışılmıştır.

Uygulamalarda her bir kullanıcı için tek tek yetkilendirme yapılabileceği gibi, grup bazında yetkilendirilmeler de yapılabilmektedir. Grup bazında yetkilendirmede her bir görevin gerektirdiği ve ihtiyaç duyduğu erişim ve işlem yetkileri belirlenir, bu yetkiler gruplara tanımlanır ve kullanıcılara bu grubun yetkisi verilir. Böylelikle aynı görevde çalışan kullanıcılar için yetkilendirmede bir standart oluşturulacaktır. Sonraki yetkilendirme ihtiyaçlarında grup bazında yapılacak değişiklikler ile tüm kullanıcıların yetkileri güncellenmiş olacaktır. Grup bazında yetkilendirme işlemine rol tabanlı erişim kontrolü de denmektedir. Grup bazında yetkilendirme, işlemleri ve kontrolü kolaylaştırmakla birlikte özellikle küçük ve orta büyüklükteki işletmelerde görev ayrılığının olmaması ve görevlerin net olmaması nedeni ile uygulanması imkansız hale gelmektedir. Bu durumda her bir kullanıcı için bütün yetkilerin tek tek tanımlanması gerekmektedir. Bu da sistemde kontrol edilemez bir yetkilendirmenin doğmasına neden olmakta, suistimallere maruziyeti artırmaktadır.

Kullanılan yazılımlarda farklılıklar olmasına rağmen yetkilendirmenin temelde birkaç boyutu vardır. Bunlar; erişim yetkisi, işlem yetkisi, hareket/kayıt yetkisi, alan yetkisi gibi yetkilendirmelerdir. Kullanıcı yetkilendirmede işletme organizasyon ve ihtiyaçlarına göre bu yetki türlerinin tamamı veyahut birkaçı kullanılır.

[49] Laudon, **a.g.e.**, s.350

Erişim yetkisi, kullanıcının programa ilk girişi aşamasında kimlik tespiti ve hangi modül, ekran ve menüleri kullanacağının belirlenmesi işlemidir. Özellikle ERP programlarında işletmenin tüm fonksiyonlarına ait modüllerin tamamı tek bir uygulamada bulunmaktadır, herhangi bir yetkilendirme yapılmadığı durumda kimlik tespiti kontrolünden sonra programa giriş yapan kullanıcı, bu modüllere ait tüm menülere erişmiş olacaktır. İşletmede, uygulamaları kullanan çalışanların birimleri ve görevleri farklı olacağından uygulamadaki menülere erişim hakları da görevleri ve yetkileri çerçevesinde olmalıdır. Örneğin depo bölümünde çalışan bir kullanıcının insan kaynakları uygulaması ve verilerine ulaşması istenilmeyecektir.

Bazı uygulamalarda erişim yetkisi ile işlem türleri bazında yetkilendirme de yapılabilir, örneğin satış faturalarına erişim yetkisi olan kullanıcıları mal satış faturası, hizmet satış faturası, iade faturası gibi fatura türlerinin her biri için ayrı ayrı yetkilendirmek mümkündür.

İşlem yetkisi, kullanıcıların erişim hakkı verilen kayıt ve hareketlerde hangi işlemleri yapmaya yetkili olduklarının belirlenmesidir. Kayıt ve hareketlerde görüntüleme, oluşturma, değiştirme, silme, kopyalama, iptal etme gibi farklı işlemlerinin kimler tarafından yapılacağının belirlenmesi gerekmektedir. Görevler ayrılığı ilkesi gereği kullanıcıların kayıtlar üzerindeki yetkileri de farklı olmalıdır. Bazı kullanıcılara, ekleme, değiştirme yetkisi verilirken sadece silme yetkisi tek bir kullanıcıda olması istenebilir.

Hareket yetkisi, kayıtlara ait farklı hareket türlerinin yetki seviyelerinin belirlenmesidir. Örneğin bir stok kartına ait, alış hareketi, satış hareketi, iade hareketi gibi hareket türleri bulunmaktadır, satış biriminde çalışan bir kullanıcının alış hareketini görmesi istenmeyebilir, ama aynı zamanda satış hareketlerini de görmesi gerekmektedir, bu durumda sadece malzeme hareketlerine yetki verilmesi yeterli olmayacak hareket türlerine göre de yetkilendirme yapılması gerekecektir. Ayrıca TIGER uygulamasında tüm kayıt ve hareketlerin yetki kodu alanları bulunmakta olup bu alanlar ile de yetki kontrolü yapılabilmektedir. Örneğin kullanıcılar tüm kayıtlar içinde sadece “A” yetki kodlu kayıtları görmesi sağlanabilir. Yetki kodları ile aynı hareketler ve kayıtlar arasında bir sınıflandırma yapılarak yapıp kullanıcıların erişimleri kontrol edilebilir. Örneğin, ödemeler arasında personellere yapılan ödemelerin diğer finans kullanıcıları tarafından görülmesi engellenebilir.

Alan yetkisi ise hareket yetkisine benzer bir yetkilendirmedir, yukarıdaki örnek ile devam ettiğimizde depo çalışanları malzeme hareketlerinin tamamını görmelidir ancak bu hareketlerdeki birim fiyatların görülmemesi istendiğinde alan bazında yetkilendirme ile bu kontrol sağlanabilir.

Bu yetkilendirme türlerinin yanı sıra, uygulamalarda işyeri, depo, bölüm, fabrika ve benzeri temel sınıflandırmalar ile yetkilendirmeler yapılabilmektedir. Bu yetkilendirme daha genel bir yetkilendirme olup işletme organizasyonuna göre belirlenebilir. Bu yetkilendirmelerin tamamı sadece varolan verilere ulaşım için değil aynı zamanda veri girişi esnasında sadece yetkili olduğu alan ve kayıt girişlerinin yapılmasını da sağlamaktadır. TIGER uygulamasında, kullanıcılara tanımlanan, varsayılan (default) kullanıcı bilgileri ile sadece yetkili olduğu işyeri, bölüm ve yetki kodu ile kayıt girmesi sağlanabilir. Özellikle birden fazla işyeri veya bölümü olan büyük işletmelerde bu yetkilendirme kontrollerinin iyi planlanmadığı durumlarda ciddi kayıt karmaşaları meydana gelebilecektir.

Kullanıcı yetkilendirme tek seferlik bir işlem olmayıp görev değişikliği, kullanıcı talepleri vb. durumlarda güncelleme ihtiyaçları ortaya çıkacaktır. Bu tür değişiklik ve talepler göz önünde bulundurulacak şekilde bir yetkilendirme politikası oluşturulmalıdır.

Bilgi sistemlerinde yetkilendirme, sadece işletme içi kullanıcıların yetkilendirilmesi ile sınırlı değildir. Günümüzde e-ticaretteki artış nedeni ile çalışanların dışında müşteri ve tedarikçilerden işletme bilgi sistemini kullanan diğer kullanıcıların da yetkilendirilmesi bu kapsamda değerlendirilmelidir. Bankaların sayıları milyonlara varan kullanıcılarının her biri tanımlanan yetkiler ile banka bilgi sistemlerine erişerek işlem yapmakta, kişisel bilgilerine ulaşmaktadır.

2.4. Uygulama Kontrolleri

Uygulama kontrolleri, işletme tarafından kullanılan, finans, üretim, pazarlama gibi iş süreçlerini takip ettiği özel bilgisayar programlarına ait kontrollerdir. Uygulama kontrolleri, programların içerisinde gömülü olan, veri girişi, verinin işlenmesi ve veri çıkışını kontrol etmek için kullanılan manuel veyahut otomatik teknikler olarak tarif

edilebilir[50]. Genel kontroller, uygulama kontrolleri ile entegre bir halde çalışır ve uygulama kontrollerinin daha etkin ve doğru işlemesine yardımcı olur[51].

Uygulama kontrolleri, münferit iş süreçlerinin bilgi sistemine giriş, işlem ve çıktı aşamasındaki kontrollerdir, bu nedenle uygulama kontrollerinin amacı[52];

- Veri girişlerinin tam, yetkilendirilmiş ve doğru olduğu,
- Verilerin geçerli zaman içinde işlendiği,
- Saklanan verilen tam ve doğru olduğu,
- Çıktıların tam ve doğru olduğu,
- Verilerin giriş, işlem ve çıktı aşamaların izlemek için kayıt tutulduğundan emin olmaktır.

İşletmelerde kullanılan uygulamalar ihtiyaçlar doğrultusunda çok farklı olmasına rağmen her birinde kendi içinde tasarlanmış bir takım yetkilendirme ve kontroller mevcuttur. Bu kontrollerin bir kısmı sabit ve değişmezdir, örneğin herhangi bir uygulamaya giriş için kullanıcı bilgilerine ihtiyaç duyulması gibi, bir kısmı ise ihtiyaca bağlı olarak parametrik olarak kullanılabilir. İşletme, bilgi sistemlerinde yapacağı iç kontrol modellemesinde uygulamaların yetkilendirme ve kontrol özelliklerini de dikkate almalıdır. Uygulamada teknik olarak gerçekleştirilemeyecek bir kontrol faaliyetinin planlanması pratikte mümkün olmayacağı için faydalı da olmayacaktır. Etkin olmayan bir kontrolün varlığı, başka bir kontrol önleminin alınmasını da etkileyecektir.

Uygulama kontrollerin olmadığı durumlarda aşağıdakiler gibi olumsuz sonuçlar ile karşılaşılması muhtemeldir[53];

- Hileli ver girişi ve işlenmesi,
- Alacaklılara veyahut diğer hak sahiplerine yanlış ödemeler yapılması,
- Uygun olmayan varlık çıkışları, ödeme çekleri gibi,
- Ticari bilgilerin ifşa olması,

[50] Sandra Senft, Frederick Gallegous, **Information Technology Control and Audit**, Newyork, Auerbach Publications, 2009, s. 386.
[51] Bagranof vd, s.396.
[52] Mar vd., **a.g.e.**, s.8
[53] The Chartered Institute of Public Finance and Accountancy (CIPFA), **Computer Audit Guidelines**, London, 2002 6. Ed., s.230

- İşletmenin itibar ve kredibilite kaybı,

Uygulama kontrolleri, temel olarak girdi kontrolleri, işlem kontrolleri ve çıktı kontrolleri olmak üzere üç sınıfa ayrılabilir. Bu üç kontrol ile ilgili açıklamalara aşağıda detaylı olarak değinilmiştir.

2.4.1. Girdi Kontrolleri

Birçok işletmede bilgi sistemlerine veri girişleri tarayıcı, barkod okuyucu gibi cihazlarla yapılmasına rağmen el ile veri girişlerinden tamamen vazgeçilmesi mümkün değildir. Bu durum hatalı girişlerin olmasını da mümkün kılmaktadır. Bu nedenle veri girişi esnasında meydana gelecek hatalı giriş riskini en aza indirmek için bir takım kontrollere ihtiyaç vardır. Girdi kontrolleri bilgi sistemine girilen verinin doğruluğu, tamlığı ve geçerliliğini sağlar.

Bilgi sistemlerinde veri girişi sistemin doğru işlemesi için birinci önceliktir. Girdi kontrolleri, verinin sisteme doğru girilmesinin yanı sıra verinin bilgiye dönüşmesi için işlenmesine uygun olmasını da sağlar. Örneğin hatalı formatlarda girilen tarih verilerin uygulama tarafından hesaplanması, sıralanması, filtrelenmesi gibi işlemleri de mümkün olmayacaktır.

İşletmenin kullandığı hareket işleme sistemlerindeki uygulamalar birbirinden farklı olmasına rağmen, programlama mantığı gereği veyahut ilgili kayıt hareketine ait verinin standart olması nedeni ile bazı uygulamalarda bu tür kontroller hazır olarak bulunmaktadır. Örneğin çek girişi esnasında çekin vadesinin girileceği alanın “Tarih” formatında olması gerektiğinden uygulama yazılımcıları bu alana tarih dışında herhangi bir veri girilmesini standart olarak hataların önüne geçilebilecektir.

Uygulamaların özellikleri, işletmelerin ihtiyacı ve veriye göre farklı girdi kontrolleri tasarlanıp uygulanabilir. Genel olarak kullanılan girdi kontrollerine aşağıdaki gibidir.

2.4.1.1. Kaynak Belge Kontrolleri

Bilgi sistemine veri girişine kaynaklık eden belgelerin giriş öncesi kontrollerin sağlanması gerekmektedir. Giriş esnasında yapılan hatalı ve yanlış girişler sistemde yanlış olarak devam edecektir. Kullanıcılar tarafından, olmayan bir satınalma fatura girişi, veyahut varolan bir faturanın birden fazla girilmesi durumunda, işletme kaynaklarında kayıplar meydan gelecektir. Bu tür hataların önüne geçilmesi için işletme bilgi sistemlerinde aşağıdaki şekilde kontroller planlamalıdır[54].

Kaynak belgeler, kendi aralarında gruplandırılarak numaralandırılmalıdır. Bilgi sistemine bu numaralar ile girilmeli, aynı numaranın birden fazla girişi engellenmelidir. Yapılan kontroller ile söz konusu numaranın aralık kontrolleri yapılıp, varsa eksiklikler incelenmelidir. Bu yöntemde aralıkta bulunan tüm belgelerin iptal veyahut deforme olmuş olsa bile eksiksiz girilmesi gerekmektedir. Müteselsil numaralandırma ile takip edilen satış faturalarında herhangi bir eksiklik olması durumu, satışın kayda girmeden kaynak evrakın imha edildiğine işaret olabilir.

2.4.1.2. Doğrulama Rakamı - Data Kodlama Kontrolleri

Yönetim bilgi sistemlerinde müşteri kodları, malzeme kodları, muhasebe hesap kodları gibi bir takım kodlamalar yaygın olarak kullanılmaktadır. Bu kodlamalar ile söz konusu öğeler gruplanarak toplu işlemlerde, raporlamalar, tanımlamalar gibi benzeri işlemler doğru ve daha kolay yapılabilir. Giriş esnasında yanlış kodlanan bir verinin daha sonraki işlemleri de hatalı olacaktır.

Örneğin, müşteri hesaplarında kullanılan kodlama sistemindeki bir karakter müşteri grubu için kullanılıp, bu karakter ile müşteri gruplarına özel iskontolar tanımlanabilir. Yanlış kodlanan bir müşteride bu iskonto tanımlamaları da hatalı olacaktır.

[54] James A.Hall, **Information Technology Auditing and Assurance,** USA:Cengage Learning, 2011, s.290

Bu kodlamalarda hatalı girişleri engellemek için doğrulama rakamı (Check Digit) kullanılır. Bu durumda uygulama tarafından hesaplanan doğrulama rakamı koda eklenir, bir sonraki kod girişinde ilk kod ile karşılaştırır, hatalı olması durumunda izin vermez.

Bu kontrol yönteminde en çok kullanılan teknik 11'e bölme yöntemidir. Aşağıdaki işlem basamakları konunun anlaşılmasına yardımcı olacaktır[55].

1. Her bir basamak için farklı ağırlıklar atanır, ve o basamaktaki rakam bu ağırlıklar ile çarpılır. 5372 kodu ile tanımlanmış bir müşteri kaydını ele alalım.

Rakamlar		**Ağırlık**	**Çarpım**
5	X	5	25
3	X	4	12
7	X	3	21
2	X	2	4

2. Çarpım sonuçları toplanıp 11'e bölünür. (25+12+21+4=62) / 11 = 5 kalan 7

3. Bölümden kalan sayı 11'den çıkarılır kalan doğrulama rakamıdır. => 11-7= 4

4. Doğrulama rakamı kodlamanın sonuna eklenir, bu durumda yeni kod 53724 olacaktır.

Kredi kartı numaraları ve kimlik numaraları gibi kodlamalarda buna benzer kontroller ile kendi içinde bir sağlama bulunmaktadır.

2.4.1.3. Alan Kontrolleri

Uygulamalarda veri girilen alanlarda yapılan bazı kısıtlamalar ile verinin doğru ve eksiksiz girilmesi sağlanabilir. Genel olarak kullanılan bazı alan kontrolleri aşağıdaki gibidir.

[55] James A.Hall, **Accounting Information Systems**, USA:Cengage Learning, 2011, s.746.

Karakter Sayısı Kontrolü; bazı verilerde karakter sayısı önemli olabilir, bu durumda verinin eksiksiz olması için ilgili alana girilecek verinin karakter sayısı belirlenebilir, böylelikle karakter sayısında fazla veyahut eksik karakter girilmesi engellenerek verinin tam girilmesi sağlanacaktır. Bu kontrol özellikle muhasebe bilgi sistemlerinde kimlik numaraları ve vergi numaraları alanlarında sıklıkla kullanılmaktadır.

Geçerli Karakter Kontrolü; ilgili alanda özellikle girilmesi istenen bir karakter için kontroller konulabilir. Örneğin müşteri kartı tanımlamalarında e-posta alanına girilen verinin geçerli bir e-posta adresi olup olmadığının kontrolü "@" karakterinin varlığı test edilip bu alanda bu karakter zorunlu tutulabilir.

Sayısal ve Alfabetik Karakter Kontrolü; verinin türüne göre ilgili alana doğru girişin yapılabilmesi için sayısal veyahut alfabetik karakter kontrolleri konulabilir. Örneğin, herhangi bir sayısal alanında harf girilmesinin engellenmesi gibi.

2.4.1.4. Doğrulama Kontrolleri

Bilgi sistemine girilen verinin istenilen doğru verilerden olması için daha önce belirlenmiş ve sisteme tanıtılmış listeler ile karşılaştırılması yapılır, eşleşmesi durumunda veri girişi gerçekleşir. Bu kontrol daha çok belirli ve sabit olan veriler için kullanılır. Örneğin ülkeler, şehirler, daha önce belirlenmiş değer aralıkları, unvanlar gibi.

Bu kontrol aynı zamanda ilgili alana girilen verinin tekil ve her seferinde doğru olarak girilmesini sağlar. Bir uygulamada herhangi bir alana birden çok kullanıcı tarafından veriler giriliyor olabilir veyahut tek kullanıcı dahi olsa farklı zamanlarda veri girişi yapılacaktır. Bu durumda istenilen verinin her giriş işleminde farklı olmaması için doğrulama kontrolleri kullanılabilir. Örneğin müşteri kartı tanımlamalarında müşterinin bulunduğu şehir alanı için "İst.", "İstanbul", "Istanbul" gibi farklı girişler daha sonra kayıtların kullanılmasında, filtrelemesinde hatalara neden olacaktır. Bu alan için tanımlanan doğrulama kontrolü, verinin "İstanbul" olarak doğru şekilde girilmesini sağlayacaktır.

İlgili alan için belirlenen doğru değerler az sayıda ise, kullanıcın veri girişi esnasında ekranda listelenen kayıtlardan seçim yapması sağlanabilir.

Doğrulama kontrolleri, ödeme sistemlerinde de sıklıkla kullanılmaktadır. Muhasebe bilgi sistemine tanımlanan tedarikçilerin banka hesaplarının haricinde ödeme yapılmasını engellemek için doğrulama kontrolleri uygulanmaktadır[56].

2.4.1.5. Limit Kontrolleri

Limit kontrolleri, verinin herhangi bir alan için önceden belirlenmiş alt ve üst limitler arasında olmasını sağlar. Uygulama sistemlerinde birçok işlemde kullanılmaktadır. Yönetimin iç kontrol düzenlemelerinde, nakit ödemeler, harcamalar, sipariş tutarı gibi işlemler için üst limit; ekonomik sipariş miktarı, kritik stok seviyesi ve üretim sipariş miktarı gibi işlemler için alt limitler belirlenmiş olabilir. Bu durumda ilgili işlemler için tanımlanan limit kontrolleri, iç kontrol sistemine yardımcı olacaktır. Girilen değerin belirlenen limitler aralığında olmaması durumunda uygulama ilgili kaydın yapılmasına izin vermeyecektir.

Limit kontrolleri, organizasyon kademeleri arasında farklı tutarlarda belirlenebilir. Örneğin, iç kontrol sisteminde, satış temsilcisinin azami indirim yetkisi %10 olup bunun üzerinde bir indirim uygulanması durumunda satış müdürünün onaylaması kurgulanmış olabilir.

2.4.1.6. Eksik Veri Kontrolleri / Zorunlu Alan Kontrolleri

Bilgi sistemlerine girilen veri kümelerinin / kayıtlarının eksiksiz olması için konulan kontrollerdir. Bu kontrolde ilgili veri kümesinde istenilen kritik veriler zorunlu alan olarak tanımlanır, bu alanların boş bırakılması durumunda uygulama kaydın tamamlanmasına izin vermez, kullanıcıyı uyarır. Örneğin, bir müşteri kartı tanımlaması

[56] Hall, Accounting…, **a.g.e.**, s.747.

aşamasında müşteriye ait, telefon, e-posta, vergi kimlik numarası gibi alanların eksiksiz olması istendiğinde bu alanların zorunlu olması eksik veri girişini engelleyecektir.

Fatura girişi esnasında her bir satıra fatura satırı için birim fiyat alanına veri girişi yapılması zorunlu hale getirildiğinde, birim fiyatı olmayan fatura satırları var ise faturanı kaydedilmesi engellenmiş olur.

2.4.1.7. Zaman Kontrolleri

Veri girişi esnasında en çok kullanılan kontrollerden biri de zaman kontrolleridir. Kayıtların belirlenen aralıklar arasında olması veyahut belirlenen tarih öncesine giriş yapılmaması istendiğinde uygulamada zaman kontrolleri kullanılır. Özellikle malzeme hareketleri, kasa hareketleri gibi kayıtların sadece aynı gün girilmesi istenmekte, geçmiş tarihli kayıtlara izin verilmemektedir. Yasal beyannameler verildikten sonra ilgili döneme ait mevcut kayıtların değiştirilmemesi veyahut kayıt eklenip çıkarılmaması için de tarih kontrolleri kullanılmaktadır.

Herhangi bir tarih kontrolünün olmaması durumunda geçmiş tarihli kayıtların hata, suiistimal ve hilelere maruz kalması mümkündür. İşletmelerde özellikle muhasebe birimlerinde dönemsellik ilkesi gereği o döneme ait kayıtlar tamamlanıp, kontrol edildikten sonra tasnif edilip kaldırılır ve yönetim raporları, maliyetlendirme, mutabakat vb işlemler yapılır. Tüm bu işlemler yapıldıktan sonra döneme ait işlemler tamamlandığı düşüncesi ile tekrar ilgili döneme dönüş olmayacaktır. İşte bu durumda ilgili döneme ait verilerin güvenliği tarih kontrolleri ile sağlanmalıdır.

Zaman kontrolleri sadece ilgili kaydın tarihinin kontrolü için kullanılmaz, kaydın yapıldığı zamanın kontrolleri için de bu kontrol kullanılabilir. Örneğin mesai saatleri dışında veri girişi engellenebilir veyahut sevkiyat planlaması için satış siparişlerinin gün içince belirlenene saatten önce girilmesi istenebilir.

2.4.2. Bilgi İ˙leme Kontrolleri

Bilgi sistemine veri girişi aşamasından sonra verinin bilgiye dönüşmesi için uygulamada bir takım matematiksel ve mantıksal işlemlerden geçer. İşleme kontrolleri verinin bu işlemler esnasında herhangi bir kayıp, hata ve değişiklik olması riskine karşılık düzenlenmiş kontrollerdir[57].

2.4.2.1. Yığın Kontrolleri (Batch Controls)

Bu kontrol, çok sayıda verinin bilgisayara toplu olarak işlenmesi durumunda kullanılan bir kontrol yöntemidir. Bu kontrol ile, tüm kayıtların işlendiği ve herhangi bir kaydın mükerrer işlenmediğinin kontrolü sağlanmış olur[58]. Örneğin bir satış sisteminden gün sonunda tüm satış faturalarının listelenerek muhasebe bilgi sistemine toplu olarak girişi yapılıyor olsun, bu durumda veri girişinden önce faturada tutar, numara vb. herhangi bir sayısal alan için toplamlar alınır ve bir kontrol toplamı oluşturulur. Veri girişi tamamlandıktan sonra kontrol toplamı ile bilgisayarda ilgili alan toplamının eşitliği kontrol edilir.

Bazı işletmeler, iş süreçlerindeki özel durumlar nedeni ile finans, satış, envanter, insan kaynakları gibi işlemlerini farklı uygulamalarda takip etmek zorunda kalabilir. Bu durumda işletme bünyesinde kullanılan ve işletme bilgi sisteminin bir parçası olan bu farklı uygulamaların birbirleri online-entegre olarak veri alışverişine ihtiyaç duyulmaktadır. Bu veri alış verişinin entegre bir şekilde yapılamadığı durumlarda yığın veri işleme söz konusu olacaktır. Bu yığın veri işleme elle-manuel şekilde yapılabileceği gibi ara yazılımlar vasıtasıyla bilgisayar ile toplu olarak işlenebilir. Her iki durumda da kaynak veriler ile işlenen verilerin doğruluğunu test etmek için yığın kontrolleri kullanılabilir.

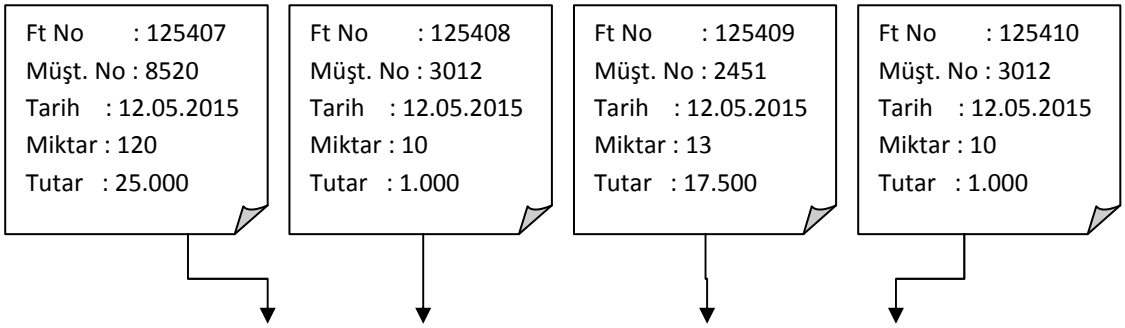
---

[57] Gallegous, **a.g.e.**, s.388.
[58] Hall, Accounting…, **a.g.e.**, s.747.

Yığın kontrolleri, sisteme veri girişi aşamasında başlar ve verinin işlendiği her aşamada devam eder. Yığın kontrolleri, benzer verilerin bir yığın olarak gruplandırılması ve işlem aşamasında bir bütün olarak kontrol edilmesidir[59]. Yığın kontrollerinde, tek bir alanı kontrol için kullanmak yeterli olmayabilir, bu nedenle uygun olan birden fazla sayısal alanların toplamları ile kontrol daha doğru olacaktır. Bu belge detayındaki toplamlar için Hash Total – detay toplam terimi kullanılmaktadır[60].

Örneğin, elimizde kaynak olarak 4 adet satış faturası olduğunu varsaydığımızda, fatura sayısı, fatura numaraları, müşteri numaraları, miktar ve fatura tutarı verilerinin toplamları (hash total), yığın kontrolleri amacıyla kullanılabilir.

[59] **a.g.e.**, s.747.
[60] Hall, Information…, **a.g.e.**, s.295.



Sıra No	Ft No	Müşteri No	Tarih	Miktar	Tutar
1	125407	8520	12.05.2012	120	25.000
2	125408	3012	12.05.2012	10	1.000
3	125409	2451	12.05.2012	13	17.500
4	125410	3012	12.05.2012	10	2.300
Toplamlar	**4 Adet**	**501634**	**16995**	**153**	**45.800**

Şekil 6. Yığın Kontrolleri

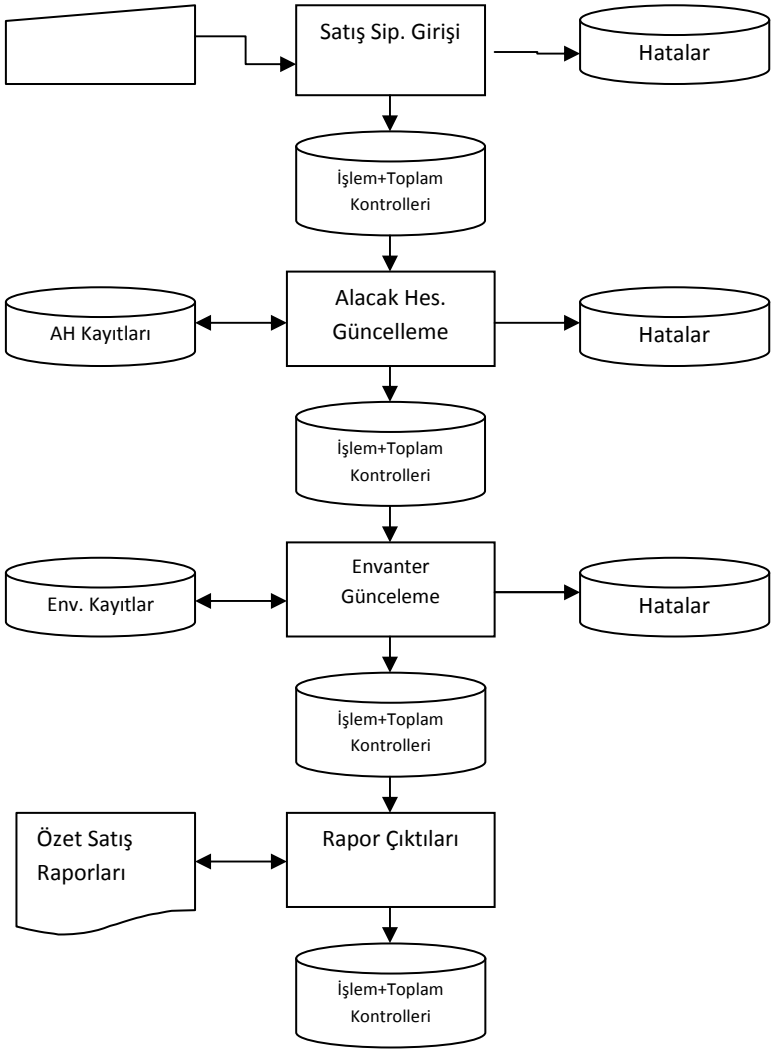
2.4.2.2. Geçi˙ Kontrolleri (Run to Run – Adım Adım Kontrol)

Geçiş kontrolleri, yığın kontrol toplamlarını kullanan bir kontrol yöntemidir. Bu kontrol ile bilgi sistemi içindeki her bir işlemden sonra değerler kontrol toplamları ile karşılaştırılır ve kaydın doğru işlendiğinin sağlaması yapılır[61]. Bilgi sistemine girilen veriler adım adım işlemlerden geçer ve her bir aşamada ilgili tablolarda kayıtlar oluşturur, geçiş kontrolleri ile ilgili kaydın her aşamada doğruluğu test edilmiş olur.

Bir satış sürecini ele alıp, 4 aşamadan oluşan bir süreç olduğu düşünüldüğünde; veri girişi (1) aşamasında daha önce belirlenen kontrol toplamları (hash total) ile karşılaştırılır, doğru olması durumunda bir sonraki aşama olan, alacak kaydı yapılır (2) aynı kontroller tekrar edilip, doğruluk sağlandıktan sonra, envanter kayıtlarının

[61] Melih Erdoğan vd., **Denetim**, Eskişehir:Anadolu Üniversitesi Yayınları, 2012, s.126

güncellenmesi (3) işlemine geçilir, buradaki kontrolden sonra son aşama raporlama (4) aşamasıdır. Her bir aşamada varsa hatalı kayıtlar tespit edilerek işaretlenir (red flags) ve hata dosyasına işlenir. Geçiş kontrolleri aşağıdaki şema ile anlatılmaya çalışılmıştır[62].



Şekil 7. Geçi˙ Kontrolleri (Run to Run Controls)

Kaynak: Hall, Information…, a.g.e., s.304.

2.4.2.3. Kullanıcı Müdahale Kontrolleri

[62] Hall, Accounting…, **a.g.e.**, s.748-749.

Uygulamalar, bir işleme devam etmek, veyahut yeni bir işlem başlatmak gibi durumlarda kullanıcının müdahale etmesini gerektirebilir. Bu durum insan kaynaklı hataların meydana gelme olasılığını arttırır. Bu olasılığın tamamen ortadan kalkması mümkün olmasa da bazı sistemlerde bu hataların en aza indirilebilmesi için kullanıcı hareketleri sınırlandırılır. Uygulamalarda belirlenen bazı parametreler ile bu tür hataların önüne geçilmesi sağlanmış olur[63].

Muhasebe bilgi sistemlerinde kullanılan uygulamalarda, herhangi bir finansal harekete ilişkin yevmiye kayıtlarının doğru olması için bu yöntem kullanılmaktadır. Bilgi sistem kullanıcıların muhasebe bilgileri yeterli olmayabilir veyahut bu tür kayıtlar muhasebe dışında birimlerce oluşturulmuş olabilir. Bu durumda her bir kayda ilişkin muhasebe kayıtlarının tekrar tekrar oluşturulması yerine belirlenen şablonlar dâhilinde muhasebe hesabı default olarak getirilebilir. Örneğin kalem grubu malzemelerin satışında satış kodu 600.01, defter grubu malzemelerde ise 600.02, %18 kdv oranında hesaplanan kdv hesabının 391.18, %8 oranında 391.08 olarak belirlenmiş olması belirlenmiş olabilir, bu durumda kullanıcın müdahalesine ihtiyaç kalmadan her bir satış faturasında belirlenen yevmiye kayıtları oluşur.

2.4.2.4. Denetim İzi Kontrolleri (Audit Trail)

İşlem kontrollerinden en önemlilerinden biri, denetim izlerinin korunmasıdır. Denetim izi, bir işlemin, verinin kaynağından işlendiği her aşamada raporlandığı sonuca kadar takip edilebilir olmasının mümkün olması demektir. Örneğin bir muhasebe bilgi sisteminde kaynak belgeden, mali verilerin raporlanmasına kadar her aşamada takip edilmesi gerekmektedir. Manüel sistemlerde bu belgeler üzerinde kolayca yapılabilmektedir. Ancak bilgi sistemlerinde denetim izinin şekli değişmiştir[64].

İşlem günlükleri (Tansaction Logs); sistemde başarıyla işlenen her bir işlemin günlüğü kaydedilmiş olmalıdır. Bilgisayar uygulamalarında yapılan işlemlere ait izler iki türlüdür. Birincisi veri girişi esnasında işlem tamamlanıp bir sonraki aşamaya geçinceye kadar olan geçici dosyalar şeklindeki izler, diğeri tamamlanan veri girişinin

[63] Hall, Information…, **a.g.e.**, s.304.
[64] O'Brein, **a.g.e.**, s.569.

izleridir. Bunlar denetçi için gerekli olan tamamlanan kayıtlara ilişkin izlerdir, çünkü finansal ve finansal olmayan raporları etkileyecek olan bu tamamlanmış kayıtlardır[65].

Hareket işleme uygulamalarının birçoğunda bulunan denetim izlerinde, ilgili kaydın hangi kullanıcı tarafından, hangi zamanda, oluşturulduğu, var olan kaydın kim tarafından güncellendiği, silindiği, yazdırıldığı, açıldığı, okunduğu gibi bilgiler tutulmaktadır. Bazı uygulamalarda alan bazlı loglama yapılmaktadır, kayıtlardaki hangi alanların güncellendiği, güncelleme öncesi ve sonrası değerinin ne olduğu gibi detaylı bilgiler de tutulmaktadır.

Denetim izleri sadece kullanıcılar ile ilgili bilgileri değil diğer uygulamalar tarafından yapılan hareketlerin izlenmesinde de kullanılır. Denetim izleri ile güvenlik ihlalleri, sistem performansı ve sorunları tespit edilebilir. Denetim izleri, yapılan işlemlerde bireysel kullanıcıların sorumluluk bilincinin artmasına fayda sağlar. Denetim izlerinin önceden belirlenen kural ve kriterlere göre izlenip analiz edilmesi gerekmektedir. Bu tür gözden geçirmeler, belirli bir olay sonrası yapılabileceği gibi, periyodik olarak da yapılabilir[66].

Örneğin, eski tarihli kayıtlar üzerinde yapılan değişiklikler, kayıtlara yetkisiz erişim, kayıt silme ve benzeri olaylar loglardan süzülerek standart dışı durumlar yorumlanması gerekmektedir.

2.4.3. Çıktı Kontrolleri

Bilgi sistemine verilerin girilmesi ve işlenmesinden sonra karar vericiler tarafından kullanılabilmesi için, ekran, yazıcı, rapor gibi farklı ortamlarda özetlenip sunulması gerekmektedir. Verilerin bu sunumu bilgi sistemlerinin çıktısıdır. Çıktı kontrolleri, bu çıktıların kullanıcılara doğru, eksiksiz, zamanında ve gizliliği ihlal edilmeden iletilmesi için tasarlanmış kontrollerdir[67]. Bu kontroller, çıktıları girdiler ile kıyaslayarak doğruluğunu sağlar. Çıktıların doğruluğu ve güvenilirliği girdi ve işlem

[65] Hall, Accounting…, **a.g.e.**, s.750.
[66] http://csrc.nist.gov/publications/nistbul/itl97-03.txt, Erişim Tarihi:12.05.2015.
[67] Gallegous, **a.g.e.**, s.390.

kontrollerinin varlığına bağlıdır ancak bunların doğru çalışması çıktıların da kesinlikle doğru olacağının güvencesini sağlamaz. Bu nedenle hangi ortamda olursa olsun bilgi sistemi tarafından üretilen çıktı için bir takım kontroller düzenlenmelidir. Çıktıların yanlış, eksik ve geç üretilmesi sonucu uygulama, beklenen faydayı sağlayamayacaktır, çıktıların başka bir uygulama için kaynak oluşturan veriler üretmesi durumunda sonraki uygulamanın da yanlış çalışmasına neden olacaktır[68].

Çıktıların kontrol edilmemesi işletme için ciddi maddi ve manevi kayıplara neden olabilir. Örneğin, müşteri bilgileri, ticari sırlar, araştırmalar gibi bilgi sistemlerine kaydedilmiş kritik verilerin yanlış yönlendirme sonucu üçüncü kişilere ulaşması gibi[69].

Bilgi sisteminin çıktıları bilgisayar ortamında (digital-online) veyahut basılı (hard copy) ortamda olabilir. Her iki ortamda da olası risklere karşı kontrollere ihtiyaç vardır.

Büyük verilerin işlendiği sistemlerde yazdırma araçlarının kapasitesinin üzerinde (örneğin şerit yazıcılar) çıktı ihtiyacı olabilir. Bu durumda yazıcıya gönderilen çıktı aynı anda yazdırılamaz, bilgisayar ortamında biriktirilir, yazıcının kullanılabilir olduğu zaman yazdırılır. Çıktıların biriktirilmesi esnasında ilgili dosyalara erişilip, verilerin değiştirilmesi, silinmesi, kopyalanması gibi suiistimallere maruz kalabilir[70]. Örneğin bilgisayarlar ile yazdırılan çek, dekont, bordro gibi benzeri evraklara müdahale edilerek tutarları değiştirilebilir.

İş süreçlerinin takibi için kullanılan uygulamalarda bir takım standart raporlar bulunmakla birlikte her bir işletmenin farklı rapor ihtiyaçları olabilmektedir. Ve bu ihtiyaçlar tek seferlik olmayıp, işletme faaliyetlerine devam ettiği müddetçe mevcut raporlarda güncellemeler ve yeni rapor ihtiyaçları da devam edecektir. Bu ihtiyacın karşılanması için uygulama raporlarında değişikliklere ve yeni raporlar oluşturmaya izin verilmektedir. İşletme, raporlardaki bu tür müdahaleleri sadece yetkin ve kişiler tarafından yapılmasını sağlamalı, bunun dışındaki son kullanıcıların raporlarda değişikliklere izin verilmemeli kontrol altına alınmalıdır. Değiştirilen veyahut yeni oluşturulan her bir raporun detaylı kontrolleri yapılmadan sisteme dahil edilmemelidir.

[68] CIPFA, **a.g.e.**, s.248.
[69] Hall, Information…, s.306.
[70] **a.g.e.**, s.306.

Raporlamalardaki bu tür değişiklikler için bir prosedür belirlenmeli, değişiklik ihtiyacı, nelerin değiştirildiği, önceki ve sonraki örnek raporların saklanması gibi kurallar belirlenebilir.

Basılı olan raporlamalarda kullanılan bir kontrol türü de numaralandırmadır. Sayfa ve bölüm numaralandırmalarının kullanılması raporun bütünlüğü hakkında kullanıcılara bilgi verir. Numaralandırmada sadece sayfa numarası kullanılacağı gibi, sayfa numarasının yanında raporun toplam sayfa sayısı yazılı olarak da kullanılabilir. Yine bazı durumlarda kaç kopya yazdırıldığı da raporlarda belirtilebilir.

Uygulamalarda bazı durumlarda ilgili fiş veyahut raporun yazdırılıp yazdırılmadığı, yazdırıldı ise kaç kez yazdırıldığına dair bilgiler de çıktı kontrolleri olarak kullanılabilir. Örneğin bilgi sisteminde oluşturulan herhangi bir fatura matbuu evraka tek bir kez yazdırılmalıdır, bu nedenle uygulamada yazdır komutu ile ilgili fatura için yazdırıldığına dair bir kayıt oluşturulur ve bir sonraki yazdır komutunda faturanın daha önce yazdırıldığı bilgisi ile kullanıcı uyarılır. Bu kontrol ile yazdırılan bir fatura, irsaliye gibi işlemlerin uygulamada değiştirilmesi de kontrol edilebilir. Çek, senet, yevmiye defteri, defteri kebir gibi çıktıların bir kez yazdırılması gerektiğinden bu kontrol kullanılabilir.

İşletmeler tarafından kullanılan bazı uygulamalarda yazdırılan işlemlerin kayıtları (log) tutulmaktadır. Hangi işlem ve raporun kim tarafından, ne zaman, hangi filtreleme seçenekleri ile yazdırıldığının kayıtları tutulur, böylelikle sistemdeki verilerden hangilerine kimler tarafından ulaşıldığı da tespit edilmiş olur. İşletmede bu tür uygulamaların bulunması, kullanıcılara, raporlar üzerinden oluşacak suiistimaller için caydırıcı bir kontrol olacaktır.

Bilgisayar ortamındaki çıktıların türüne göre farklı kontroller uygulanabilir. Bu çıktıların bir kısmı baskı öncesi ekran görüntüleri olup, dijital ortamda bilgisayar dosyası olarak saklanmakta ve ilgililer ile paylaşılmaktadır. Bu çıktı türlerinde basılı çıktılardaki kontroller kullanılabilir. Ayrıca bu çıktı dosyalarının kopyalanması ve yetkisiz kişilere ulaşmasının engellenmesi için bilgi güvenliği ve bilgi sistemleri genel kontrollerindeki prosedür ve kurallara da dikkat edilmesi gerekmektedir.

3. Bilgi Sistemleri Uygulamalarında Kontrollerinin Test Edilmesi ve Bilgisayar Destekli Denetim

3.1. Bilgi Sistemleri Uygulamalarında Kontrollerin Test Edilmesi

İşletmeye mali durumu hakkında ilgililere bilgi veren mali tablolar, işletmede kullanılan bilgi sistemleri uygulamalarının çıktılarıdır. Dolayısı ile bilgi sistemleri denetimini dikkate almadan finansal denetimin yapılması mümkün olmayacaktır. Özellikle genel kontrollerin yanı sıra uygulama kontrollerinin incelenmesi ve test edilmesi gerekmektedir[71].

Bilgi sistemlerinin temel unsurlarının neler olduğunu bilen denetçi, denetim yapacağı işletmenin bilgi sistemleri hakkında da bilgi sahibi olmalıdır. Bilgi sistemlerini işletmede ne derecede kullanıldığı, işletmenin iş süreçlerinin neler olduğu hangi süreçlerinin bilgi sistemleri ile gerçekleştirildiğini, bilgi sisteminin donanım ve yazılım altyapısının özellikleri, bilgi sistemindeki risklerin neler olduğu ve risk değerlendirilmesinin nasıl yapıldığı, sistemdeki risklere karşın alınan genel ve uygulama kontrollerinin neler olduğunu araştırmalıdır[72]. Denetimin planlama aşamasında yapılacak bu çalışmalar ile ayrıca denetimde teknik konular için bir bilgi sistemleri denetçisine ihtiyaç olup olmadığının belirlenmesi gerekmektedir. Yine denetimin planlanması aşamasında sistemdeki risklere ilişkin bir değerlendirme yapılmalıdır.

Bilgi sistemleri denetimi genel kontroller ve uygulama kontrollerinin test edilmesini kapsamakla birlikte bu çalışmada daha çok uygulama kontrollerinin denetimi üzerinde durulacaktır.

Tüm teknolojik uygulamalarda olduğu gibi operasyon destek uygulamalarında da bir takım riskler bulunmaktadır. Bu risklerin yönetilmesi için işletmeler,

[71] Yalkın, **a.g.e.**, s.16.
[72] T.C. Sayıştay, **Bili˙im Sistemleri Denetim Rehberi**, Ankara:2013, s.4.

uygulamada var olan veyahut daha sonra uyarlanan uygulama kontrollerini kullanmaktadırlar. İç denetim yöneticileri tarafından uygulama kontrollerinin uygun bir biçimde tasarlanıp tasarlanmadığının, ne derece etkin ve faydalı olduklarının periyodik olarak denetlenmesi ve test edilmesi gerekmektedir[73]. Yapılan bu denetim ile tasarlanan uygulama kontrollerine güven derecesi de belirlenmiş olur.

Uygulama kontrollerinin denetlenebilmesi için işletmenin kullanmış olduğu programların yeterince anlaşılması gerekmektedir. Bu nedenle bilgi hazırlanması, girişi, işlenmesi ve çıktı aşamaları süreçlerindeki iş akışları ele alınıp, işletme tarafından oluşturulan uygulama kontrolleri belirlenmelidir[74]. İşletmenin oluşturduğu kontrollerde eksik olduğu düşünülen işlemler ile ilgili denetimin danışmanlık hizmeti kapsamında önerilerde bulunabilir.

Uygulama kontrollerinin denetimlerinde kapsamın belirlenmesi için iki farklı yöntem uygulanmaktadır. Bunlar[75];

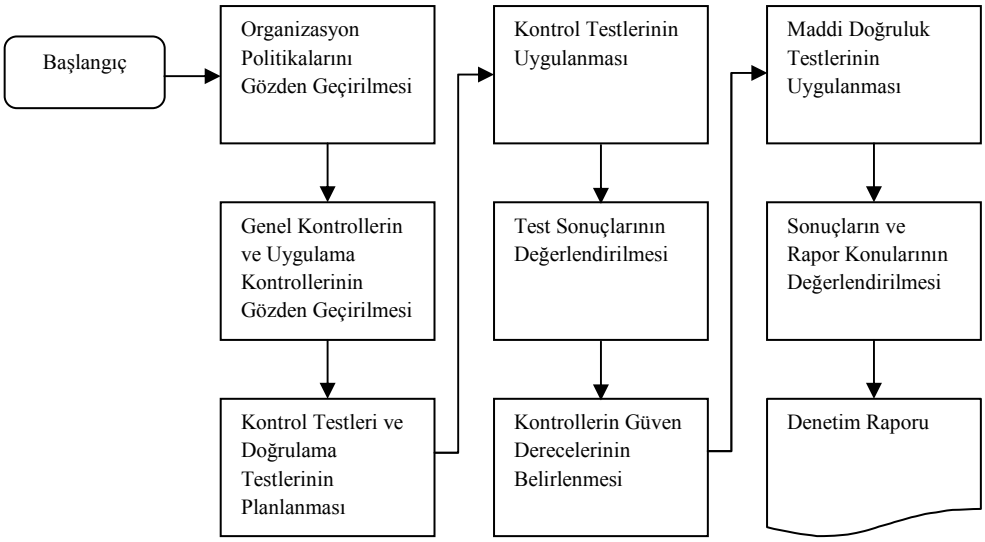
İ· Süreci Yöntemi; belirli bir iş sürecinde kullanılan uygulamaların veyahut modüllerin tamamındaki kontrollerinin değerlendirilmesi yöntemidir. Örneğin bir satınalma işleminde, siparişten ödemenin yapılmasına kadar sipariş, tedarik, envanter, fatura ve ödeme gibi birçok işlem söz konusudur, bu işlemler işletme tarafından farklı uygulamalarda takip edilebilir, bu durumda sadece tek bir uygulama değil süreçte kullanılan tüm uygulamalar denetim kapsamına dâhil edilmelidir. Özellikle birbirleri ile entegre çalışan ERP modüllerinin kullanıldığı işletmelerde iş süreci yöntemi tercih edilmektedir.

Tekli Uygulama Yönteminde ise, iş süreci yerine tek bir modül veyahut uygulamanın kontrolleri denetim kapsamına dahil edilir. Sadece envanter hareketlerinin kaydedildiği bir uygulamada giriş ve çıkış hareketlerine ilişkin kontrollerin test edilmesi durumunda bu yöntemden bahsedilebilir.

Bilgi sistemleri denetimi temel olarak üç aşamada gerçekleştirilir bunlar; denetimin planlanması (1), kontrollerin test edilmesi (2) ve son olarak test sonuçlarının değerlendirilmesi (3) aşamalarıdır. Planlama aşamasında denetçi, hangi testleri

[73] Bellino, **a.g.e.**, s.8.
[74] Sayıştay, **a.g.e.**, s.107.
[75] Bellino, **a.g.e.**, s.17.

uygulayacağına karar verebilmesi için işletmenin bilgi sistemleri altyapısı, işletme politikaları ve uygulamaları hakkında bilgi edinmelidir. Bu aşamada daha çok risk analizleri yapar, uygulamalar üzerindeki kontrolleri anlamaya çalışır. İkinci aşamada, çeşitli teknikler ile uygulama kontrollerinin etkinliğini test eder. Kontrollerin var olduğunu etkin ve düzgün çalıştığından emin olmak için çalışmalar yapar. Son aşamada maddi doğruluk testleri ile hesap bakiyelerinin araştırılması detaylı soruşturmalar yapar. Bu aşamada daha çok bilgisayar destekli denetim tekniklerini (BDDT - CAATT's) kullanır[76].



Şekil 8. Bilgi Sistemi Denetiminin A˙amaları

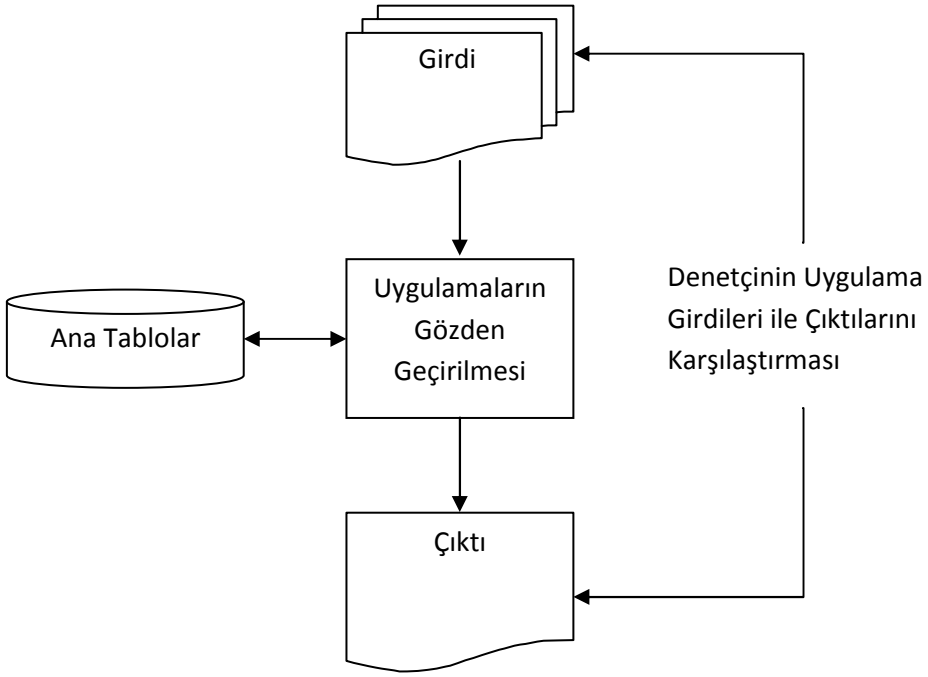
3.2. Bilgisayarlı Muhasebe Sistemlerinde Denetim Yakla˙ımları

Faaliyet ve süreçlerinde bilgi sistemlerini kullanan işletmelerin denetiminde temel olarak üç yaklaşım bulunmaktadır[77].

[76] Hall, Information…, **a.g.e.,** s.11.
[77] Erdoğan vd., **a.g.e.,** s.113.

3.2.1. Bilgisayar Etrafından Denetim (Black Box)

Bu yaklaşım işletmenin kullandığı bilgi sistemleri dikkate alınmadan geleneksel yöntemlerle yapılan denetim yaklaşımıdır. Denetçi sadece girdi ve çıktı ile ilgilenir, bilgi sistemlerinde girilen verilerin hangi süreçlerden geçerek raporlandığı ile ilgilenmez. Dolayısı ile bilgi sistemlerinin yapısı ve işleyişi ile herhangi bir değerlendirme ve çalışma yapmaz. Bu yaklaşımda denetçinin bilgi sistemlerine ait teknik bilgi ihtiyacı yoktur. Küçük ve bilgi sistemlerini daha az kullanan işletmelerde kullanılması mümkündür ancak denetimde etkinliği ve verimliliği önemli ölçüde düşürecektir[78].



Şekil 9. Bilgisayar Etrafından Denetim Yaklaşımı

Kaynak: Hall, Information…, **a.ge.,** s.311.

Örneğin, bu yaklaşımda denetçi, örnekleme yöntemi ile belirleyeceği girdi olan herhangi bir fatura evrakı ile bu faturanın mali defterlere kaydedilip kaydedilmediğinin

[78] Hall, Information…, **a.g.e.**, s.311.

tespitini yapacaktır. Bu evrakın bilgi sistemine, girişi, işlemesi ve raporlama aşaması ile ilgili herhangi bir inceleme yapmaz.

3.2.2. Bilgisayarın İçinden Denetim (Through The Computer - White Box)

Bu yaklaşımda denetçi, bilgi sistemlerinin işleyişi, uygunluğu, genel ve uygulama kontrolleri, girdi, işlem ve çıktıların denetimini yapmalıdır. Bu yaklaşımda denetçi, bilgi sistemleri ile ilgili temel bilgilere sahip olması gerekmektedir. Bilgi sistemlerinde belirlenmiş olan iç kontrollerin ne derecede etkin olduğunun tespit edilmesi risk analizinde denetçiye önemli derecede yardımcı olacaktır. Yine bilgi sistemlerinde yapılan hesaplamalar ve raporlamaların doğru olması, verilerin maddiliğinin test edilmesi, kayıtların tamamının kontrol edilebilmesi denetimin güven derecesini arttıracaktır.

Bilgisayarın içinden denetimde denetçinin kullandığı testlerden bazıları aşağıdaki gibidir[79];

- Doğruluk Testleri,
- Geçerlilik Testleri
- Tamlık testleri,
- Fazlalık Testleri
- Erişebilirlik Testleri
- Denetim İzleri Testleri

Bu yaklaşımda denetimde Genelleştirilmiş Denetim Yazılımları (Generalized Audit Software-GAS) ve Bilgisayar Destekli Denetim Teknikleri (Computer Assisted Audit Technic and Tools - CAAT's) kullanılır, bazı durumlarda uzman bilgi sistemleri denetçisi, veyahut bilgi teknolojilerinde uzman personele ihtiyaç duyulabilir.

3.2.3. Bilgisayarla Denetim

[79] Hall, Information…, **a.g.e.**, s.311.

Bu yaklaşım, işletmenin verilerinin analizi ile denetim yaklaşımıdır. Bu yaklaşımda bilgi sistemlerinin iç yapısı değil bilgi sistemlerinde kaydedilmiş veriler dikkate alınır, yukarıda bahsedilen yazılım ve teknikler kullanılır. İşletmenin faaliyetlerinin karmaşık olması, bilgi sistemlerinin anlaşılmasının zor olduğu durumlarda bu yaklaşım ile denetim, daha etkin ve hızlı olacaktır.

Denetçi kullandığı herhangi bir veri analiz programı ile (Excel, Access, Sql vb.) işletmenin kullandığı uygulamanın veritabanına bağlanarak veyahut uygulamalardan alınan verileri analiz programına aktararak çalışma yapar. Örneğin, kasa hareketlerinde limitler dışında herhangi bir ödeme olup olmadığının sorgulanması gibi.

3.3. Bilgisayar Destekli Denetim Teknik ve Araçları (BDDT-CAATT's)

3.3.1. Genelle˙tirilmi˙ Denetim Yazılımları – GDY (Generalized Audit Software GAS)

Bilgisayarla denetimde, denetçiler genel amaçlı kullanılan kelime işlem, elektronik tablolar ve veri tabanı yönetim programı gibi uygulamalardan faydalanabilmektedir. Örneğin mutabakat mektupları veyahut denetçi raporu için kelime işlem programına ihtiyaç duyacaktır, elektronik tablolar ile karmaşık hesaplamaları kolayca yapabilirler ya da büyük verilerin analizi için veri tabanı yönetim programlarında raporlar hazırlanabilmektedir.

Bunların yanı sıra özel olarak denetim amaçlı yazılımlar da üretilmiştir. Bu yazılımlara genel olarak, Genelleştirilmiş Denetim Yazılımları (Generalized Audit Software - GAS) denilmekte olup, denetçilerin devamlı kullandıkları genel formlar ve yazışmalar ile bilgisayarlı denetim tekniklerini içermektedir. Denetçi, denetlenecek işletmeye ait verileri bilgisayar ortamında alıp GDY yazılımlarına aktarır ve denetim çalışmalarını bu programlar ile yapar. Bir çok işletmede rahatlıkla kullanılabilen bu programlar, denetçinin yapmış olduğu çalışmaları standart içermektedir. Standart şablonlar ile denetim ile ilgili temel hesaplama ve analizler, kısa sürede

gerçekleştirilebilir[80]. Bu programlar ile denetçi, uzman seviyede bilgisayar bilgisine sahip olmadan kısa eğitimler ile detaylı analizler yapabilir. Bu yazılımlarda bulunan standart veri analiz yöntemleri ile verinin tamamının denetlenmesi mümkün olmaktadır. Ancak daha çok muhasebe bilgilerinin analizlerine yönelik uygulamalar olduğu için bağımsız denetçiler tarafında daha fazla kullanılmaktadır[81]. Verilerin bilgisayara işlendikten sonraki sonuçların denetime tabi tutulması nedeni uygulamalar üzerindeki kontrollerin test edilememesi bu tür programların dezavantajlarındandır[82].

Bu programlardan en çok kullanılanları, **ACL** (Audit Command Language), **IDEA** (Interactive Data Extraction and Analysis) ve **CAP** (Computerized Audit Program) programlarıdır. Bunlardan CAP adlı program Türkiye'de geliştirilmiş olup, Türkçe olması ve bağımsız denetime ait müşteri kabulünden denetçi raporunun oluşturulmasına kadar tüm süreçlerin takip edildiği bir uygulama olması nedeni ile Türkiye'de çokça tercih edilmektedir. Ayrıca CAP programını geliştiren aynı firmanın iç denetimin tüm süreçlerini izlendiği bir uygulaması da mevcuttur[83].

Şekil 10. CAP Programı Ana Ekranı

[80] Selvi, Yakup, Türel, Ahmet ve Şenyiğit, Bora, "**Elektronik Bilgi Ortamlarında Muhasebe Denetimi**", 7. Muhasebe Denetimi Sempozyumu Nisan 2005, İstanbul.,
[81] Serhan Gürkan, "Bilgisayar Destekli Denetim Tekniklerinin (BDTT) Muhasebe Denetimine Etkileri ve Türkiye'dki Bağımsız Denetim Kuruluşlarının BDTT Uygulamalarına İlişkin Bir Araştırma", (Karaelmas Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Bilim Dalı, Yüksek Lisans Tezi), Zonguldak, 2008, s.68.
[82] Cemal Elitaş, Arman Aziz Karagül, "Bilgisayar Destekli Denetim Teknikleri", **Sosyal Bilimler Dergisi**, S.2, Aralık 2010, s.145.
[83] http://futurecom.com.tr/, (Erişim tarihi, 15.02.2015)

3.3.2. Bilgisayar Programlarının Test Edilmesi

Bilgisayar programlarının test edilmesindeki amaç, sisteme girilen verinin giriş ve işlenmesi aşamasında uygunluğunun sağlanmasında programın başarılı olup olmadığıdır. Denetçiler programların test edilmesinde aşağıdaki üç yöntemden birini kullanır[84].

3.3.2.1. Veri Testi Tekniği

Bu teknikte denetçi, işletmenin bilgi sistemlerinde planlamış olan kontrollerin etkinliğini test eder. Denetçi tarafından tespit edilen, işletme faaliyetlerine ilişkin veriler kullanılan bilgi sistemlerine girişleri yapılarak elde edilen sonuçlar değerlendirilir. Beklenen sonuçlar ile elde edilen sonuçların uyumlu olması durumunda kontrolün yeterli olduğu kanaatine varılır[85]. Bu teknikte sistemin kontrollerinin etkinliğini test etmek amacıyla hatalı kayıt girişleri de yapılabilir. Veri testinin avantajı bilgisayar sistemindeki kontroller ile ilgili direkt bilgi vermesidir, bununla birlikte veri testlerinin hazırlanmasının uzun sürmesi ve denetçinin tüm kontrollere hakim olamaması gibi dezavantajları da vardır[86].

Tablo 1. Örnek Test Verileri Tablosu

Program Giri˙ Testi	Programdan Beklenen	Test Verisi
Tamlık	6 karakter gerekliliği	12345
Numerik alan	Sadece numerik karakter	123C45
İşaret (+ veya -)	Sadece pozitif sayılar	-1234
Kabul Edilebilirlik	Haftalık çalışma 45 saati aşmaması	60
Doğrulama Kodu	Fatura için "I", Ödeme için "P" kabul edilebilir	C
Değer Aralığı	01.01.2014 – 31.12.2014 tarih aralıklarındaki tarih girilebilir.	01.01.2010

Kaynak: Bagranoff, **a.g.e.,** s.461.

[84] Bagranof vd., **a.g.e.**, s.461.
[85] Hall, Accounting…, **a.g.e.**, s.756.
[86] Elitaş ve Karagül, **a.g.e.**, s.158.

3.3.2.2. Bütünle˙ik Veri Test Tekniği (Integreated Test Facility-ITF)

Veri testinin benzeri bir teknik olup, farkı testin tüm muhasebe bilgi sistemini içerecek şekilde yapılmasıdır[87]. Denetçi sistemde verilerin biriktiği hayali kayıtlar oluşturup, bu kayıtlara bir takım gerçek olmayan veriler girer, veri girişi sonucunda ortaya çıkan sonuç ile beklenen sonuç karşılaştırır. Örneğin bilgi sisteminde hayali bir cari hesap kartı açılır, bu cari hesap kartına, fatura, havale, çek tahsilatı ve benzeri veriler girilir, sonuçlar beklenen sonuçlar ile karşılaştırılıp değerlendirilir. Veri testi tekniği programa veri girişi esnasında uygulanan kontroller ile ilgili sonuçlar verirken, özellikle veri girişi sonrası işlenmesi aşamasındaki kontrollerin test edilmesinde etkili değildir. Bu nedenle bütünleşik veri testi tekniğinin kullanılması gerekmektedir[88].

Bu tekniğin dezavantajı, test amaçlı girilen verilerin bilgi sisteminde gerçek veriler ile birlikte bulunması ve test sonucunda silinmesi aşamasında bir takım riskleri taşımasıdır. Bilgi sistemindeki gerçek verilen silinmesi ciddi kayıplara neden olabilir[89].

3.3.2.3. Paralel Benzetim (Simülasyon) Tekniği

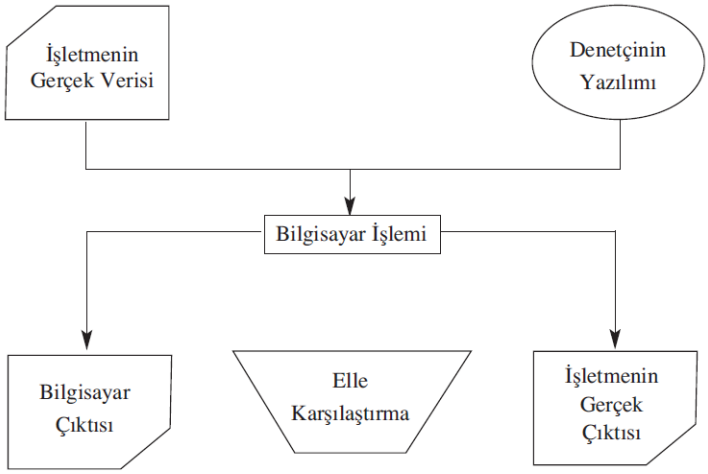
Bu teknikte gerçek veriler, işletmenin bilgi sistemi ile denetçinin programına paralel olarak işlenir, daha sonra her iki programın çıktıları karşılaştırılır. Bu teknikte amaç, birbirinden bağımsız her iki programın, girdi, işlem ve çıktı sonuçlarının test edilmesidir[90]. Bu teknikte denetçi işletmenin bilgi sistemini, her bir aşamada detaylı olarak test edebilecek, uygulamaların kontrolleri ile ilgili daha kesin sonuçlar elde edebilecektir.

---

[87] Erdoğan vd, **a.g.e.**, s.128.
[88] Özgür TERAMAN, "Elektronik Bilgi Ortamında Bilgi Ortamında Bilgisayarlı Denetim Programları Aracılığı ile Muhasebe Denetimi ve CAP Uygulaması", (Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü İşletme Ana Dilim Dalı Muhasebe Programı Yayınlanmamış Yüksek Lisans Tezi), İzmir:2011, s.88.
[89] Serhan Gürkan, **a.g.e.**, s.79.
[90] Murat Kiracı, "Bir Bilgisayar Destekli Denetim Tekniği Olarak Paralel Simulasyon Tekniği", **Mali Çözüm Dergisi**, S.(68), İstanbul, 2004, s.145.

Verilerin gerçek ortama girilmemesinden dolayı, veri karmaşıklığına neden olmayacak, test sonra verilerin temizlenmesindeki riskler ile karşılaşılmayacaktır. Ancak denetçinin alternatif bir uygulama kullanmasının maliyeti bu tekniğin en büyük dezavantajıdır.

Simülasyon programları ile ortaya çıkan sonuçların karşılaştırılmasında farklılıklar iki nedenle olabilir. Ya gerçekten denetlenen uygulamadaki işlemlerin ve kontrollerin eksik olması, veyahut simülasyon uygulamasının eksikliği nedeniyle olabilir. Bu nedenle denetçi farklılıkları değerlendirirken dikkatli olmalıdır[91].



Şekil 11: Paralel Simülasyon Tekniği

Kaynak: KİRACI, **a.g.e.**, s.145.

3.3.3. Veri Analiz Teknikleri

İşletme faaliyetlerine ilişkin bilgi sisteminde oluşan büyük verilerin anlamlı hale gelmesi için analiz edilmesi gerekmektedir. Veri analizi mevcut verilerin çeşitli istatistiki ve matematiksel yöntemler ile karar verme ve destek amacıyla kullanılabilir hale getirilmesidir[92]. Birçok bilim alanında kullanılan veri analiz yöntemleri işletme bilgi sistemlerinin yaygınlaşması ile denetimde de kullanılmaya başlanılmıştır. IAA

[91] Hall, Information…, **a.g.e.**, s.320.
[92] http://en.wikipedia.org/wiki/Data_analysis (Erişim tarihi:01.04.2015)

tarafından yayınlanan İç Denetim Standartları'nda veri analiz tekniklerinin kullanımına aşağıdaki paragrafta değinilmiştir[93].

> "1220.A2 – Azamî meslekî özen ve dikkati gösterirken, iç denetçiler, teknoloji destekli denetim ve diğer veri analiz tekniklerini kullanmayı düşünmek zorundadır."

Önceki konularda anlatılan teknikler ile uygulamaların kontrollerini test eden denetçi, söz konusu kontrollerin etkin bir şekilde çalıştığından emin olduktan sonra bilgi sistemlerinde oluşan verilerin doğruluğunu Genelleştirilmiş Denetim Yazılımları veyahut genel amaçlı kullanılan MS Excel, MS Access, MS SQL, ORACLE SQL gibi bir takım veri işleme programları ile test etmesi gerekmektedir Bu tür programlar ile, işletmenin bilgi sistemindeki denetlenecek verilere doğrudan ulaşılarak gerekli hesaplama ve analizler yapılır.

Veri analizinde en çok kullanılan teknikler bu bölümde alt başlıklar halinde anlatılacaktır, bununla birlikte işletmenin faaliyetlerine, denetçinin tecrübesi ve bilgi teknolojilerindeki yeterliliğine ve denetimin amacına göre farklı analizler de yapılabilir.

3.3.3.1. Yeniden Hesaplama

Veri analiz programları ile ulaşılan işletme bilgi sistemindeki veriler yeniden hesaplanarak işletme tarafından raporlanan hesap bakiyelerinin ve diğer hesaplamaların doğruluğu test edilebilir. Birçok programda kullanıcıların kendi kullandıkları raporlara müdahale izini verilmektedir. Bu tür durumlarda kötü niyetli ve programa hâkim bir kullanıcı raporların hesaplamalarına müdahale edebilecek düzenlemeler yapabilir, yeniden hesaplama yöntemi ile bu şekilde yapılan usulsüzlüklerin tespiti yapılabilir.

[93] http://www.tide.org.tr/uploads/UMUC_2013.pdf (Erişim tarihi: 01.04.2015)

3.3.3.2. Katmanlara Ayırma ve Özetleme

Bu teknik büyük ve karmaşık verileri belirli kriterlere göre alt katmanlara ayırma ve gruplandırma tekniğidir. Büyük miktardaki veriler bütün halde analizleri anlamlı sonuçlar vermeyebilir. Bu tür durumlarda verinin özelliğine göre muhtelif alt konular belirlenebilir. Örneğin, zaman, müşteri, malzeme, lokasyon, satıcı, personel gibi. Satış verilerinin yer aldığı bir tablonun bütününe bakıldığında herhangi bir dikkat çekici durum gözlenmezken, bu veri satıcılar bazında alt katmanlara ayrılarak analizinde satıcıların satış tutarları arasında farklılık olup olmadığı değerlendirilebilir[94].

Örneğin, cari hesapların denetiminde, hesapların tedarikçi, müşteri gibi türlerine ayrılarak incelenmesi katmanlara ayırma işlemidir. Bu hesap hareketlerinin müşteri, lokasyon, tarih gibi alt sınıflara ayrılarak hesaplanması, sayılması ve benzeri işlemelere tabi tutulması ise özetlenmesi olarak ifade edilebilir.

Hatalı bir fatura tutarının tespiti için tüm faturalar için de yapılacak bir incelemede tutarsal olarak ortalamanın altında kalan bir satış faturası, müşteri, tarih, ürün vb. alt kriterler ile özetlendiğinde ortaya çıkabilir.

3.3.3.3. Örnekleme

Örneklemenin bir sistem dahilinde bilgisayar yazılımları kullanılarak yapılması yöntemidir, denetçinin bilgi sisteminde örnek seçmesini sağlar. Genelleştirilmiş denetim yazılımlarında kullanılan temel örnekleme yöntemleri aşağıdaki gibidir[95].

- Para birimine dayalı örnekleme
- Katman Örneklemesi
- Tesadüfi Örnekleme
- Sistematik Örnekleme

[94] Kürşat Taşkın, (2011). "Yolsuzluğun Tespit ve Önlenmesinde Bilgisayar Destekli Denetim Teknikleri" **3. Ulusal Kurumsal Yönetim, Yolsuzluk, Etik ve Sosyal Sorumluluk Konferansı**, Nevşehir, 07-11 Haziran 2011.
[95] Emine Yarar, **Bilgisayar Destekli Denetim Teknikleri Kurs Notları**, Ankara: Sayıştay , 2011, s.11.

3.3.3.4. Tekrarlanan Kayıt Kontrolleri

En kolay kullanılabilen yöntemlerden biridir. Fatura, tahsilat, ödeme vb. kayıtların birden fazla kez sisteme girilip girilmediğinin kontrol edilmesidir. Bir çok sistemde bu tür kontroller mevcut olmakla birlikte suiistimal niyeti ile bu tür kontrolleri atlatma girişimleri olabilir. Bu nedenle işlemlerin mükerrerliğini farklı kombinasyonlarının da kontrol edilmesi gerekmektedir. Örneğin sistemin fatura numarası bazında mükerrerlik olduğunu varsayalım, bu kontrol kullanıcılar tarafından, başında herhangi bir karakter eklenerek veyahut rakamların yerleri değiştirmek suretiyle numarada basit değişiklikler ile atlatılabilir[96]. Bu tür durumların engellenmesi için, fatura tarihi, tutarı, fatura carisi, fatura numarası, irsaliye numarası gibi diğer bilgileri ile birlikte değerlendirilmelidir.

Tekrarlanan kayıt kontrollerinde hata ile yapılan kayıtlar tespit edilebilirken, özellikle suiistimal ve hile amacı ile yapılan kayıtlarda kullanıcı yanıltma amacı ile benzer kayıtlar kullanacaktır. Bunların tespit edilebilmesi ise Bulanıklık Eşleştirilme (Fuzzy Matching) teknikleri geliştirilmiştir. Daha çok bilgisayar tabanlı çeviri programlarında kullanılan bu yöntemde farklı gibi görünen verilerin aynı olma ihtimalleri göz önünde bulundurularak değerlendirmeler yapılır. Bu teknikte verilerin %100 eşleşmesi yerine benzerleri ile eşleştirme yapılır[97]. Kötü niyetli hareketlerin haricinde özellikle uygulamalarda metin alanı gibi serbest girişe izin verilen alanlara kullanıcı tarafından hatalı girişlerde de bu yöntem kullanılabilir. Genelleştirilmiş denetim yazılımlarında bu tür karşılaştırmalar için en yaygın kullanılan alanlar, isim, adres, telefon numaraları, doğum yeri, ilişkili kişi gibi alanların karşılaştırılması olarak görülmektedir.

3.3.3.5. Bo˙luk Belirleme ve Dizi Kontrolleri

[96] Kürşat, **a.g.e.**, s.
[97] http://www.techopedia.com/definition/24183/fuzzy-matching (Erişim Tarihi:02.04.2015)

Bilgi sistemlerinde girilen bazı kayıtlarda veyahut kaynak belgenin üzerinde matbuu olarak seri takibi yapılmaktadır. Bu yöntem, kayıtların serileri arasında kullanılmayan boşlukları olup olmadığının kontrol edilmesidir. Bu kontroller ile varolan bir belgenin kaydedilmemesi, kaydedilen bir belgenin sonradan silinmesi gibi hata ve usulsüzlüklerin tespiti yapılabilir. Dizi kontrollerinde ise seri içindeki hatalı ve tekrarlanan numaralandırmaların tespiti yapılır.

4. Örnek Uygulama

4.1. Uygulamanın Amacı

Örnek uygulama ile amaç, çalışmamızda bahsedilen genel ve uygulama kontrollerinin bir işletmede pratikte nasıl ve nerelerde kullanıldığına dair fikir vermektir. Senaryo bir işletmenin tüm süreçlerini içerecek şekilde kapsamlı olmamakla birlikte, bazı yerlerde kontrollere örnekler verebilmek için detaylandırılmıştır. Unutulmalıdır ki her bir işletmenin risk değerlendirmesi, kullandığı yazılım, bulunduğu sektör, büyüklüğü ve benzeri birçok kriter farklı olacağı için belirleyeceği kontrol uygulamaları birbirinden farklı olacaktır. Ancak kullanılan araç ve teknikler aşağıdaki örneklere benzerlik gösterecektir.

Örnek uygulamada otomotiv sektöründe faaliyet gösteren kobi ölçeğinde ve günlük hareketlerinde bilgi sistemlerini kullanma zorunluluğu bulunan ve planlı bir bilgi sistemi olmayan bir işletme ele alınmıştır. Öncelikle mevcut durumun analizi yapılmış, genel uygulamalardaki kontrollere kısaca değinilmiş ve uygulama kontrollerine örnek olacak düzenlemeler süreç bazında incelenmeye çalışılmıştır. Daha sonra bazı veri analiz teknikleri ile denetim amaçlı bir takım rapor örnekleri oluşturulmuştur.

4.2. Mevcut Durum ve İhtiyaç Analizi

ABC Otomotiv Aş., otomotiv sektöründe araç satış, satış sonrası servis hizmetleri ve toptan yedek parça dağıtımı faaliyetlerinde bulunmaktadır. Faaliyetlerini bir merkez iki şube olmak üzere üç farklı işyerinde, farklı organizasyonlar ile gerçekleştirmektedir.

Mevcut durumda işletmenin faaliyetlerini takip ettiği tek bir bilgi sistemi yoktur, merkezde muhasebe defterleri, beyanname ve bordro gibi yasal zorunlulukları,

yerine getirmek amacı ile sadece muhasebe kayıtlarının tutulduğu bir muhasebe programı kullanmakta, şubelerde ise birbirinden bağımsız hareket işleme uygulamaları ile günlük faaliyetler takip edilmektedir. Günlük işlemler şubelerde detaylı olarak girilmesine rağmen ortak bir uygulama kullanılmadığından, muhasebe kayıtları için merkezde yeni veri giriş işlemine ihtiyaç duyulmaktadır. Bu da işletmenin her bir işlemi için ikinci bir iş yükü getirmektedir. Ayrıca mali tablolara kaynak olan kayıtlar ile günlük hareketler farklı uygulamalarda takip edildiği için birbirleri ile bağlantısı oluşmamaktadır.

Birbirinden bağımsız bu uygulamalar etkin kullanılmamakta, her bir uygulama sürecin ilgili adımını gerçekleştirmekten öte bir fayda sağlamamaktadır. Bilgi sisteminden alınan raporlamalar ihtiyaca cevap vermediğinden uygulama dışında çeşitli düzenlemeler ile birimlere ait yeni raporlar hazırlanmaktadır. Bilgi sisteminin dışında hazırlanan bu raporlar zaman zaman hatalı olduğu görülmektedir. Uygulamalarda öngörülen herhangi bir kontrol bulunmadığı gibi yetki tanımlamaları da detaylı olarak yapılmamıştır. Herhangi bir kullanıcı sistemde geçmiş tarihli herhangi bir kaydı silebilmekte veyahut olamayan bir kayıt girişi yapılabilmektedir.

Faaliyetlerin artması sonucu, yevmiye kayıtlarına dayalı bu süreç de artık devam ettirilemez bir hale gelmiştir. Mevcut durumun hata ve suiistimallere açık olduğu açıkça görülmekte ve bu durumun büyük riskler içerdiği kabul edilmektedir. Tekrarlanan işlemler sonucu oluşan iş yükü mevcut kadro ile altından kalkılamaz bir durumdadır. Bilgi sisteminin plansız ve düzensiz olması, uygulamaların sağlayacağı faydaları en aza indirmekte verimsiz bir çalışma ortamının oluşmasına neden olmaktadır.

Her bir işyerinin tüm faaliyetleri birbirinden bağımsız personel tarafından yerine getirilmekle birlikte tek vergi kimlik numarası olduğu için vergi bildirimlerini tek beyanname ile vermektedir. Bu nedenle farklı işyerindeki iş süreçlerinin ortak bir uygulamada takip edilmesi gerekmektedir. Aynı zamanda yönetim kurulu ve ortaklara yönelik yapılan raporlamaların eksiksiz olması için de tek bir uygulamanın kullanılması tercih edilmektedir. Tek bir uygulama kullanılmasının, işyerlerindeki iş süreçlerinin ve iç kontrollere ilişkin tanımlamaların bütünlüğü, ek bir uygulama maliyetinin olmaması ve raporlama kolaylığı gibi faydaları da vardır.

Her bir işyerinin etkinliği ve verimliliğinin ölçülebilmesi işletmeye ait tüm raporlamaların işyeri bazında yapılması istenmektedir. Bu nedenle işletmedeki iş süreçlerine ait tüm işlem ve hareketlerin işyeri bazında kaydedilmesi gerekmektedir. Her bir işyerinin cari hesapları, banka kayıtları, stok hareketleri ve muhasebe hareketleri gibi bilgi sistemlerine girilen tüm hareketlerin, sadece o işyerindeki personel tarafından görülmesi istenmektedir. Merkezde bütünü gören ve vergi beyannamelerini düzenleyen, ortak bildirimleri yapan bir muhasebe müdürü bulunmaktadır. Muhasebe müdürünün bu bildirimleri eksiksiz vermesi için ilgili kayıtların tamamına ulaşma yetkisi gerekmektedir.

Günlük faaliyetlerin takibi ve kaydedilmesi için kullanılan uygulamalarda hata ve suiistimallerin önlenmesi için bir takım kontrollere ihtiyaç olduğu görülmüş, bu kontrollerin azami düzeye kullanılmasına karar verilmiştir.

İşyerleri fiziki olarak farklı ortamlarda bulunduğu için ortak kullanılması düşünülen uygulamaya erişimin nasıl olacağı, yetkisiz erişim tehdidi, kayıtların anlık bilgi sistemine kaydedilmesi gibi sorunların varlığı da işletmeyi kaygılandırmaktadır.

İşletme yönetimi mevcut durumun iyileştirilmesi için bilgi sisteminin daha etkin kullanılması gerektiği görüşünde fikir birliğindedir. İşletme, hizmet aldığı danışmanları ve birim amirleri ile yapmış olduğu uzun toplantı ve çalışmalar sonucu, kısmen kullanılan ve alternatif programlara göre daha az maliyet ile güncelleme yapılarak ihtiyaçları karşılayabileceğini düşündükleri LOGO – TIGER programını kullanmaya karar vermiş ve bir proje ekibi oluşturmuştur.

4.3. Bilgi Sistemleri Genel Kontrolleri

Çalışmamızın konusu bilgi sistemlerinde uygulama kontrolleri olmakla birlikte, konunun bütünlüğü ve anlaşılması için örnek uygulama içinde genel kontrollere kısaca yer verilmiştir. Genel kontroller konusunun daha kapsamlı ve daha çok, teknik bilgi gerektiren bir konu olduğu unutulmamalıdır. Bu nedenle bu konuda uzman teknik kişilerden yardım alınması gerekmektedir.

4.3.1. Kurum Seviyesi Kontroller

Yönetim kurulu, işletmenin etkin ve verimliliği için bilgi sistemlerinin daha iyi kullanılması gerektiğini, bu sayede müşteri memnuniyetinin artacağı ve rekabette üstünlük sağlayacaklarını, bununla birlikte bilgi güvenliğinin vazgeçilmez olduğunda fikir birliğindedir. Finansal raporlamalara kaynağı olan verilerin girildiği, işlendiği ve saklandığı bilgi sistemlerinin tüm süreçlerinde bilginin doğru, tam ve eksiksiz olarak girilip işlendiği ve raporlandığı bir bilgi sisteminin oluşturulması istenmektedir. Bu nedenle mevcut durumun analizi ve iyileştirilmesi için süreçlerin gözden geçirilmesi, teknik altyapının değerlendirilmesi ve gerekli prosedür ve politikaların oluşturulması için yöneticileri görevlendirmiş, bu konudaki kararlıklarını göstermek amacıyla genel bir duyuru yayınlamışlardır.

4.3.2. Yönetim Seviyesi Kontroller

Birim yöneticileri, yönetim kurulunun bilgi sistemlerine bakışı çerçevesinde işletmenin günlük işlerini yerine getirirken kullanmış olduğu yazılımlar gözden geçirilmiş, tüm sürecin bilgi sisteminde yürütülmesi için çalışmalar yapmıştır. Genel bilgisayara kullanım talimatları, güvenlik prosedürleri, personel görev ve yetkilendirme, bilgi güvenliği ve kurallar, bilgi sistemi kullanıcıların eğitimi ve benzeri konularda genel politikaları belirleyip talimatlar hazırlamışlardır.

Bilgi sistemlerindeki riskler ile ilgili çalışmalar yapılmış olup, bunlar

4.3.3. Teknik Kontroller

Proje ekibi çalışmalarına bilgi sistem altyapısını inceleyerek başlamaya karar vermiştir. İşletme, bünyesinde teknik personel yetersizliği nedeni ile genel kontrollerin gerçekleştirilmesi için dış destek almaktadır. Danışman teknik firma tarafından öncelikle bilgi sistemlerindeki mevcut teknolojilerinin bir envanteri çıkarılmış, ihtiyaçlar ile karşılaştırılıp eksiklikleri ve riskleri belirlenmiştir.

Bilgi Teknolojilerinin işletme fonksiyonlarını karşılamasının değerlendirilmesi için yapılan çalışmalarda uygulamanın kurulacağı, ana bilgisayarın mevcut durumda teknik olarak yeterli olduğu ancak, kullanıcı sayısındaki artış halinde yavaşlamalar yaşanacağı değerlendirilmektedir, ana bilgisayarın kapasitesini arttırmak için donanım yatırımı yapılması gerektiği görülmüştür. **Bilgisayar ağ yapısı** gözden geçirilmiş uygulamaların kullanımı için yeterli olduğu değerlendirilmiştir. Şubelerin uzak erişimi için kullanılmak üzere VPN (sanal ağ)'lar oluşturulmuş, sadece belirlenen IP'ler üzerinden erişime izin verilmiştir. Bu kontrol ile şubeler haricinde işletme dışı bağlantı girişimleri engellenmiştir. Uzak erişimin kalitesini arttırmak ve şubelerde bilgi sisteminin daha hızlı kullanılmasını sağlamak için yeni fiberoptik hatlar tesis edilmiştir.

Bilgi sistemlerinin **fiziki güvenliği** ile ilgili çalışmalarda, işletme verilerinin saklandığı ana bilgisayarlar için ayrılmış kapalı bir oda bulunduğu ancak anahtarların birden fazla kişide bulunduğu görülmüştür. Sistem odası fiziki olarak diğer birimlerden ayrı bir yerdedir, ancak odada bilgisayarlar uygun konumlandırılmamıştır. Sistem odasında ana bilgisayarın dışında güvenlik kamera sistemlerinin yönetildiği diğer bilgisayarlarda bulunduğu bakım vb. nedenler ile bilgi sistem çalışanları dışında kişiler rahatlıkla girebilmektedir. Mevcut durumda bilgi sistemlerinin fiziki güvenliği tehdit altında olduğu görülmektedir. Fiziki güvenliğin sağlanması için öncelikle, ana bilgisayarın bağımsız bir odada olması ve kabinet denilen özel dolaplarda bulunması gerektiği kararlaştırılmıştır.

Bilgi sisteminin **veritabanı güvenliği** ile ilgili yapılan değerlendirme çalışmasında, işletme bünyesinde kullanılan farklı uygulamaların veritabanının (MS SQL) tek bir ana bilgisayarda olduğu, uygulamalara destek almak amacıyla farklı kişiler için tam yetkili veritabanı kullanıcıları oluşturulduğu görülmüştür. Bu kişiler istediği

zaman işletme iç veyahut dışında herhangi bir lokasyondan veri tabanına erişim sağlayabilmekte istedikleri işlemleri yapabilmektedir. Bu durum veri tabanı güvenliğin ciddi tehdit altında olduğu, yetkisiz erişimlere maruz kalabileceği anlamına gelmektedir. Bu nedenle varolan kullanıcıların tamamı silinmiş, sadece yetkili olduğu veritabanına erişim sağlayabilecekleri kullanıcılar oluşturulmuştur. Ayrıca destek amaçlı oluşturulan bu tür uzak bağlantılar sınırlandırılmış sadece izin verilen IP numaralarının (Internet Protocol Number) sisteme uzak erişimine izin verilmiştir.

Veritabanı güvenliğine ilişkin incelemelerde, şirket içinde raporlama amaçlı kullanılan ve tüm verilere ulaşabilecek şekilde yetkilendirilmiş, bölüm yöneticileri ile paylaşılan bir ortak bir veritabanı kullanıcısı bulunduğu ve kullanıcı hesabının birçok kişi tarafından bilindiği tespit edilmiştir. Bu kullanıcıya sadece verileri okuma yetkisi tanımlanmıştır ancak bu kullanıcı hesabını kullanan herhangi bir çalışan veritabanına sınırsız bağlanarak bilgi sistemindeki tüm verilere ulaşabilmekte, kopyalama veyahut aktarım yapabilmektedir. Veri güvenliği ve veriye yetkisiz kişilerin erişimine neden olan bu kullanıcı hesabı iptal edilmiş, rapor ihtiyacının tamamen kullanılan uygulamalar ile karşılanması kural olarak belirlenmiştir. Bu kontrol düzenlemesi ile verilere yetkisiz kişilerin erişimi engellenmiş, hatalı rapor-çıktı üretim riski de ortadan kaldırılmıştır.

Mevcut durumda **yedekleme** sadece veritabanı için her gün bilgi işlem çalışanları tarafından el ile (manüel) yapılmaktadır, kapasite sorunu nedeni ile sadece geçmiş bir haftalık yedek tutulmakta, bir hafta sonra o güne ait yedeğin yerine yeni günün yedeği kopyalanmaktadır. Bu yedekleme işlemi için yine verilerin bulunduğu ana bilgisayar kullanılmakta dolayısı ile asıl veri ve yedek fiziken aynı ortamda bulundukları için risk oluşmaktadır. Mevcut durumun iyileştirilmesi için otomatik yedekleme yapabilen gelişmiş yedekleme uygulama ve araçları kullanılması, yedeğin fiziken ayrı bir ortamda bulundurulması ve yedeklerin saklandığı cihazların da güvenliğinin sağlanması kararlaştırılmıştır. Ayrıca işletmenin iş sürekliliğinin sağlanması için sadece veritabanı yedeklemesinin yeterli olmadığı, bununla birlikte IMAGE yöntemi ile ana bilgisayarın tamamının yedeğinin alınması kararlaştırılmıştır. Bu kontrol ile herhangi bir saldırı, doğal afet, yangın vb. nedenler ile oluşacak veri kaybının önüne geçilecek, iş sürekliliği sağlanmış olacaktır.

İşletme içi ağ erişimi için domain altyapısı bulunmakta, sistemdeki tüm bilgisayarların erişim izinleri bu yöntem ile takip edilmektedir. Mevcut durum ağ güvenliği için yeterli bir kontrol uygulaması olarak değerlendirilmiştir.

Virüs, trojan, spam ve benzeri sanal saldırılara maruz kalınmaması için firewall (Ateş Duvarı) uygulaması ve virüs programı kullanılmaktadır. Virüs programı tüm kişisel bilgisayarlara kurulmuş olup, programa kullanıcıların müdahalesi engellenmiştir. Program internet üzerinden sürekli kendi güncellemektedir. Sisteme tehdit içerecek herhangi bir çevre birimi dahil olduğunda virüs programının gerekli kontrolleri yapması sağlanmıştır.

Verilerin kopyalanması, taşınması veyahut yetkisiz kişilere ulaştırılmasının engellenmesi amacıyla bir takım kontroller tasarlanmıştır. CD yazıcı, USB bellek gibi veri depolama araçlarının kullanımı bilgisayarda yasaklanmıştır. Bazı çalışanlarda bulunan taşınabilir bilgisayarların rahatlıkla dışarı çıkarılabiliyor olması risk olarak değerlendirilmiş bununla ilgili sınırlamalar getirilmiştir. E-posta gönderimlerinde uygulanan dosya büyüklüğü kontrolleri ile veri içerecek büyük dosyaların e-posta ile gönderilmesi engellenmiştir. Yine e-posta hesaplarından, Hotmail, Gmail gibi genelde şahsi olarak kullanılan e-posta hesaplarına gönderimler yasaklanmıştır.

Elektrik kesintisi durumunda **i˙ sürekliliğinin** sağlanması amacıyla bilgisayar ve çevre birimlerini destekleyen merkezi güç üniteleri (power supply) bulunmaktadır, mevcut durumda güç ünitesine bağlı olamayan bilgisayarlar sisteme dahil edilmiş, gereksiz araçların kullanımını engellemek amacı ile özel prizler kullanılmıştır.

4.4. Uygulama Kontrolleri

Temel iş süreçleri için kullanmaya karar verdiği TIGER uygulaması incelendiğinde, farklı işyerlerindeki operasyonları uygulamada mevcut işyeri ve bölüm ayrımları ile sınıflandırarak çözmeyi planlamaktadır. Uygulamada tüm hareket ve fişlerde işyeri ve bölüm alanları bulunmakta ve kullanıcılar için varsayılan (default) değerler tanımlanabilmektedir. İşletme veri girişi esnasında tüm hareketlerde bu alanları kullanarak kayıtların işyeri bazında sınıflandırması yapabilecektir.

4.4.1. Kullanıcı Yetkilendirme Çalı˙maları

Kullanıcıların yetkilerinin belirlenmesinde, kullanıcı temelli yetkilendirmenin daha sonra karmaşıklığa neden olmaması için rol temelli yetkilendirme yöntemi belirlenmiştir. Öncelikle personelin iş süreçlerindeki görev ve yetkileri belirlenmiş buna paralel olarak TIGER uygulamasında her bir görev için asgari yetki ihtiyaçları değerlendirilip, roller oluşturulmuş belirlenen yetkiler bu rollere tanımlanmıştır. Bir personel için birden fazla rol tanımlaması yapılabilmektedir.

Ayrıca kullanıcıların programlara erişimleri sadece kendi bilgisayarları üzerinden yapılabilecek şekilde yetkilendirilmiştir. Kullanıcı tanımlamalarında kullanıcı adı olarak personelin adı ve soyadı belirlenmiştir, böylelikle işlem loglarında hangi kullanıcı tarafından oluşturulduğu açıkça görülecektir. Uygulama üzerinden, kullanıcıların şifrelerinin 60 günlük aralıklarla değiştirilmesi zorunluluğu getirilmiştir. Genel olarak kullanıcılara kayıt silme yetkisi verilmemiş, sadece belirli kayıtların birim sorumluları seviyesindeki kullanıcılar tarafından silinmesine izin verilmiştir.

Yapılan bu düzenlemeler ile hedeflenen temel kontroller aşağıdaki gibidir.

- Kullanıcılar sadece kendi işyerleri ile ilgili yetkilendirildikleri kayıtları görebilecektir.
- Sadece yetkili oldukları işlemleri yapabilmeleri sağlanacaktır,
- Kullanıcıların bir başka bilgisayarı kullanması engellenmiştir.
- Rol tanımlamaları ile kullanıcılara özel yetki tanımlamalarının önüne geçilmek istenmiştir.
- Uygulamada kullanıcıların yaptıkları her bir kayıt, değişiklik ve silme işlemi log kayıtları ile izlenebilecektir.

Ana hatları ile belirlenen roller ve yetkileri aşağıdaki gibidir. Her bir yetki için yetki derecesi belirlenmiş böylelikle yetkilendirmeler kendi içinde seviyelendirilmiştir. Yetkilendirme dereceleri kendinden önceki işlemleri de kapsamaktadır. Örneğin 5 derecesinde verilen Sil yetkisine sahip kullanıcı, aynı zamanda 4 Düzeltme, 3 Kopyalama, 2 Yeni, 1 İnceleme yetkilerine de sahip olacaktır.

0 - Yetki Yok ; 1 - İnceleme ; 2-Yeni ; 3- Kopyalama ; 4-Düzeltme ; 5-Sil

Bölüm	MALİ İŞLER							SATIŞ				SATINALMA				DEPO	
Görev	KASA	BANKA	CARİ	PERSONEL	ÇEK / SENET	MUHASEBE YETKİLİSİ - İŞYERİ	MUHASEBE YETKİLİSİ - FİRMA	FATURALAMA SATIŞ	SATIŞ PLANLAMA	SATIŞ ŞEFİ	SATIŞ MD.	FATURALAMA SATINALMA	SATINALMA	SATINALMA ŞEFİ	SATINALMA MD.	SEVKİYAT PLANLAMA	MAL KABUL	DEPO SORUMLUSU
FİNANS																		
ANA KAYITLAR																		
Cari Hesaplar	1	1	4		1	5	5	1	1	1	1	1	1	1	1			1
Ödeme Planları	1	1	1		1	1	5											
Çekler- Senetler	1	1	1		3	4	5											
Bankalar	1	4	1		1	4	5											
Kasalar	1	1	1		1	1	5											
HAREKETLER																		
Cari Hesap Hareketleri	1	1	4		1	5	5											
Çek Senet Bordroları	1	1	1		3	5	5											
Banka Hareketleri	1	3	3		1	5	5											
Kasa Hareketleri	3	1	1		1	5	5											

Şekil 12: Yetkilendirme Şablonu

Bu rollerin işletme organizasyonuna ve çalışanların görevlerine göre hangi kullanıcılara verileceği tek tek belirlenmiştir. Uygulamada ilgili modüllerde-ekranlara yetkisinin tek bir kullanıcıya verilmesine dikkat edilmiştir.

Uygulamada alan detayında yetki belirleme imkanı bulunmakla birlikte, rollerin ve işlemlerin çokluğu nedeni ile bu detaya inilmemiş, daha sonra ihtiyaç halinde alanlarda kısıtlamalar ile kontroller sağlanacaktır.

4.4.2. Ana kayıtlar ve Hareketlerde Yetki Kodları

Uygulamada cari hesap, muhasebe hesabı, malzeme kartı gibi tanımlamalara "Ana Kayıtlar", bunlara ait borç alacak, giriş çıkış gibi günlük işlemlere ilişkin kayıtlara da "Hareketler" denilmektedir. İşletmede ana kayıtlar ve hareketlerinde işyeri bazında ayrı olması ve sadece ilgili personel tarafından girilebilmesi ve görülebilmesi istendiğinden bunlara da "Yetki kodları" tanımlanmıştır. Personel bilgi sistemine herhangi bir veri girdiğinde sadece kendi kullanıcı hesabına tanımlanmış yetki kodu ile

giriş yapabilecek, sadece bu kodlu kayıt ve hareketleri görebilecektir. Bu kontrol ile ortak kullanılacak uygulamada veri karmaşasının ve yetkisiz erişimin önüne geçilmiştir.

Temel kural tüm ana kayıtların her bir işyerinde ayrı ayrı tanımlanması olmakla birlikte, stok kartlarındaki uygulamada farklılık vardır. Otomotiv sektöründe yedek parça stokları çeşit olarak çok fazla olduğu için işletme stok kartlarının tanımlanmasın da yeni bir kodlama çalışması yapmayıp üretici işletme tarafından belirlenen stok tanımlama kodlarını referans almaktadır. Aynı yedek parçalar bütün işyerlerinde kullanılmaktadır, dolayısı ise temel kural olarak işyerlerinde ayrı ayrı tanımlanmak istendiğinde aynı kodla birden fazla kez tanımlama yapılmasına uygulama izin vermemektedir. Bu durum stok kartlarının tüm işyerleri tarafından ortak kullanılmasını gerektirdiğinden işyeri temelinde yetkilendirme yapılamayacaktır. Aynı zamanda farklı işyerlerinde kullanıcıların birbirinden habersiz olarak stok kartlarını değiştirmeleri durumunda ciddi sorunlarla karşılaşılabilir, bu nedenle stok kartlarında tüm işletmede sadece tek bir kullanıcı yetkilendirilmiştir.

4.4.3. Finans Modülü ve İç Kontroller

4.4.3.1. Cari Hesap Kartlarının Tanımlanması

İşletme için cari hesap kodlaması oldukça önemlidir. Öncelikle cari hesapların işyeri bazında ayrıştılabiliyor olması gerekmektedir, ayrıca işletmenin muhtelif müşteri tipleri mevcuttur. Bu ayrımların cari hesap kodlarında olması istenmektedir. İşletme yapmış olduğu kodlama çalışması ile cari hesap kartlarının kodlamasında 10 karakter kullanacaktır. Kodlama mantığının doğru işlemesi için tüm cari kartlarının 10 karakter olarak oluşturulması gerekmektedir, bu nedenle uygulamada tanımlanan bir girdi kontrolü ile cari hesap kodlarının 10 karakterden fazla veyahut eksik olması engellenmiştir.

Cari hesapların ve bunlara ilişkin kayıt ve raporlamaların yönetilmesi için kayıt esnasında belirlenen asgari verilerin de tanımlanması zorunludur. Bu nedenle belirlenen

bu alanlar için uygulamada bulunan ve boş olduğunda kaydın tamamlanmasına izin vermeyen "Zorunlu Alan" işlevi kullanılacaktır. Cari hesaplar için belirlenen zorunlu alanlar ve bunlar ile hedeflenen kontroller aşağıdaki tabloda verilmiştir.

Tablo 2. Uygulanan Alan Kontrolleri

Alan Adı	Kontrol Şekli	Hedef Kontrol
Cari Hesap Kodu	Karakter Sayısı 10	Doğru sınıflandırma için kodlamanın eksik veyahut fazla olmasının engellenmesi
Cari Hesap Adı	Boş bırakılamaz	
Vergi Numarası / TC Kimlik Numarası	Boş bırakılamaz ve gerçek kişi ve şahıs işletmeleri içi TC alanı ve 11 karakter, kurumlar için Vergi no alanı ve 10 karakter.	Bu bilgiler, faturada yasal zorunluluk olduğu olup eksiksiz olması faturalardaki eksikliği de önleyecektir. İşyerlerinde aynı müşterilere ait cari hesap kartlarında farklı unvanlar kullanılabilir, bu alanın zorunlu olması BA ve BS beyannameleri ve benzeri ortak raporlama gerektiren durumlarda bütünlük sağlayacaktır. Karakter sayısı kontrolleri ile değerlerin yanlış alana girilmesi ve eksik fazla girilmesi engellenmek istenmiştir.
Ödeme Şekli ve Vade	Zorunlu Alan	Toptan yedek parça grubunda malzeme fiyat iskontoları müşteri tipi ve vadesine göre belirlendiği için girişi zorunlu yapılmış, belirlenen iskonto oranlarının kontrolü sağlanmıştır.
Yetki Kodu	Zorunlu Alan / Kullanıcı Yetki Kodu	Kullanıcının sadece kendi yetki kodu ile cari hesap kartı tanımlanması sağlanmış ve yetki kodu olmayan cari kartın tanımlanması engellenmiştir.
Adres Bilgileri	İl ve İlçe Kodları Zorunlu Alan	İşletme içinde muhtelif raporlamalar için adres bilgileri kullanılmakta olup, bunların doğruluğu için il ve ilçe kodları önceden tanımlanan listelerden alınarak yanlış girişler engellenmiştir.

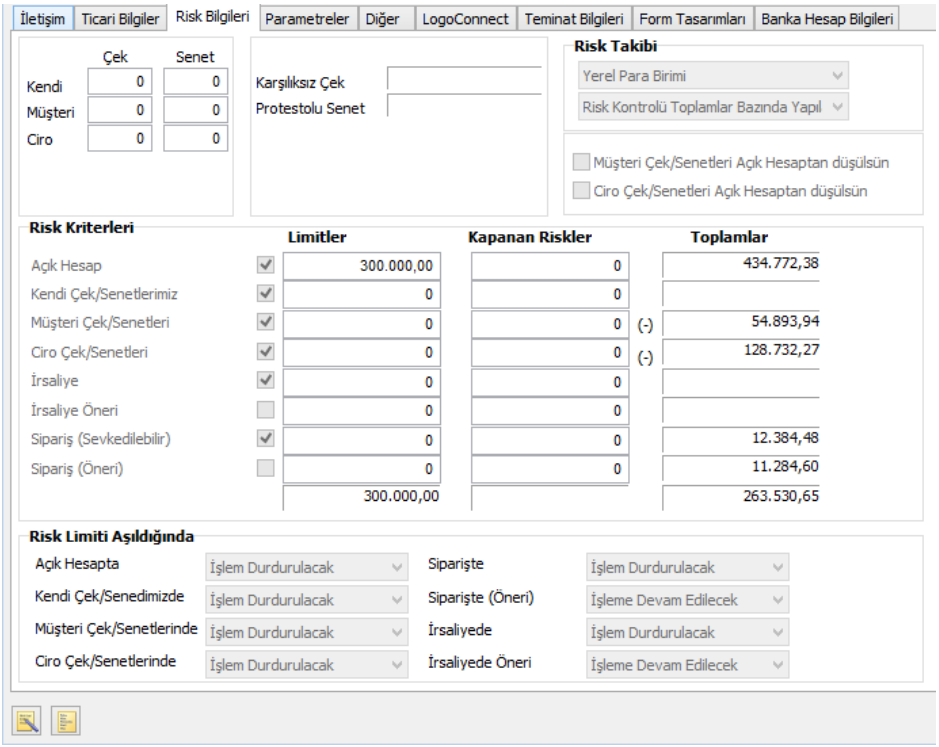
Muhasebe Bağlantı Kodu	Zorunlu Alan	Cari hesaplara ilişkin hareketlerin muhasebeleştirilmesi aşamasında sorun olmaması için bağlantı kodunun girilmesi gerekmektedir.
Özel Kod	Zorunlu Alan	Müşteri ve tedarikçileri gruplandırmak için bu alan zorunlu alan olarak belirlenmiştir. Özel kod tanımlamalarının doğruluğunun kontrolü, bu alan için önceden belirlenmiş değerler ile karşılaştırılarak yapılacaktır.

4.4.3.2. Cari Hesap Limit Risk Takibi

İşletme bazı müşterileri ile vadeli çalışmak zorundadır, bu da belirli tutarlarda açık hesap bakiyelerinin oluşmasına neden olmaktadır. Ancak bu bakiyelerinin her müşteri için belirlenen müşteri riskinin üzerinde olmaması istenmektedir. Aksi takdirde işletmenin kaynakları verimsiz kullanılmış olacak, alacaklar etkin yönetilemeyecek, alacak riski artacaktır. Bunun için uygulamada var olan limit ve risk takibinin kullanılmasına karar verilmiştir. Öncelikle her bir müşteri için en yüksek limitler belirlenmiş ve hangi işlemlerin risk olarak kabul edileceği kararlaştırılmıştır. Bu kontrol ile müşteri risklerinin belirlenen limitler dahilinde kalması sağlanmış, limit aşımında borç hareketi oluşturacak işlemlere izin verilmemiştir. Örneğin 1.000 TL limiti ve 900 TL riski bulunan bir müşteriye 100 TL satış faturası düzenlenmek istendiğinde uygulamadaki bu kontrol işleme izin vermeyecektir.

Uygulamada işlem bazında limitler tanımlanabilmektedir, ancak işletme toplam limit kontrolü yapmak istemektedir. Risk toplamına dahil edilen işlemler ve limit aşımında programın nasıl bir kontrol sağlayacağı planlanmıştır. Sipariş kayıtları cari hesabında borç kaydı oluşturmamasına rağmen işletme, onaylı siparişleri de toplam riske dahil etmiştir çünkü onaylanan siparişler depoya sevk emri olarak iletilmekte ve depo bu emre istinaden hazırlık yapmaktadır, mal toplama işlemi tamamlandıktan sonra

limit nedeni ile irsaliye dönüştürülememesi ciddi iş kayıplarına neden olmaktadır. Bu nedenle sipariş aşamasında risk limit kontrolü yapmak uygun görülmüştür.



Şekil 13. Cari Hesap Limit Kontrollerinin Uygulanması

Müşteri toplam risk limitindeki değişikliklerinin nasıl gerçekleşeceği bir prosedüre bağlanmış bu değişikliğin bilgi sisteminde finans departmanı yöneticisi tarafından güncelleştirilmesine izin verilmiştir.

4.4.3.3. Finans Diğer Ana Kayıtlar

Banka tanımlamalarında, bir banka şubesinde birden fazla işyerinin hesabı olabileceği nedeni ile banka ve şube kartları ortak olarak kullanılmış, işyerlerinin şubelerdeki hesaplarının ise işyeri temelinde yetkilendirilmiştir. Banka hesaplarının çokluğunun muhasebede karışıklığa neden olmaması için ayrı ayrı hesaplarda takip edilmesi gerekmektedir, bu nedenle her bir banka hesabının muhasebe hesap kodları da tanımlanmıştır.

Kasalar, işyeri temelinde yetkilendirilerek tanımlanmıştır, her işyerinin bir veyahut birden fazla kasası olabilir ve sadece o işyerindeki yetkilendirilmiş kullanıcılar tarafında görülebilir ve işlem yapılabilir. Kasaların muhasebe kodları da belirlenmiştir.

4.4.3.4. Finans Hareketleri ve Kontroller

Finans hareketlerinin tamamında genel kural olarak, işyeri bazında yetkilendirme yapılıp, kullanıcılara tanımlanan varsayılan değerler ile kayıtlara izin verilmiştir. Finans hareketlerinde "İşyeri" ve "Yetki Kodu" alanları için belirlenen kontroller ile bu alanların boş olması engellenmiştir.

Uygulamada mevcut borç dekontu, alacak dekontu fişleri ile tek taraflı borç-alacak kaydı oluşturan fişlerin kaydedilmesi engellenmiştir.

Finans hareketlerinin tamamının muhasebeleştirilmiş olması kuralı getirilmiş olup bu kontrol ile tüm işlemlerin muhasebe hesaplarına eksiksiz kaydedilmesi sağlanacaktır. Dönem sonlarında cari hesap hareketleri için tarih kontrolleri konulmuş, bu tarihten önceki kayıtlarda herhangi bir değişiklik, ekleme ve çıkarma işlemine izin verilmemektedir.

İşletmede kasa işlemlerinin günlük olarak işlenmesi gerekmekte, gün sonu kasa raporu alınarak mevcut tutar ile karşılaştırılması ve tutanak altına alınması istenmektedir. Bu nedenle geçmişe dönük hareketlerin oluşturulması, silinmesi veyahut değiştirilmesi tarih kontrolleri ile engellenmiştir.

Kasa hareketlerinin azaltılması amacı ile ödeme ve tahsilatlar için tutarsal sınır belirlenmiş olup 1.000 TL üzeri nakit hareketlerin banka yolu veyahut çekler ile yapılması istenmektedir. Bu nedenle uygulamada kasa hareketlerinde 1.000 TL ve üzeri kayıt girişi, kasa işlem limiti ile kontrol altına alınmıştır.

Uygulama, dönem bazlı çalışmakta her bir yıl için yeni bir dönem tanımlaması yapılıp hareketlerin toplamları sonucu oluşan bakiyeler bir sonraki döneme açılış fişi olarak aktarılmaktadır. Dönemler arasında sadece ana kayıtlar sabit ve ortak kullanılmakta olup, dönem hareketleri birbirlerinde bağımsızdır, yani devir yapıldıktan

sonra bir önceki dönemdeki herhangi bir değişiklik, sonraki dönem açılış fişini etkilememektedir. Bu nedenle devir sonrası önceki dönemde yapılacak herhangi bir değişikliğin engellenmesi amacıyla tarih kontrolleri kullanılmıştır. Aynı şekilde yeni dönemde açılış fişinde yapılan bir değişikliğin, önceki dönem ile bağlantısı olmayacağından hata ve suistimale neden olmaması için kullanıcı müdahalesine kapatılmış ve sadece uygulama tarafından açılış fişinin oluşturulması sağlanmıştır. Örneğin, açılış fişinde cari hesap bakiyelerinin herhangi birinin borç veyahut alacak tutarlarının değiştirilmesi işletmenin varlıklarında kayba neden olacak bir hareket olup, bu değişikliğin anlaşılması ancak özel raporlamalar ile mümkündür. Bu nedenle yukarıdaki kontrol uygulamaları ile bu gibi değişiklikler sınırlandırılmıştır.

4.4.4. Malzeme Yönetimi Kontrolleri

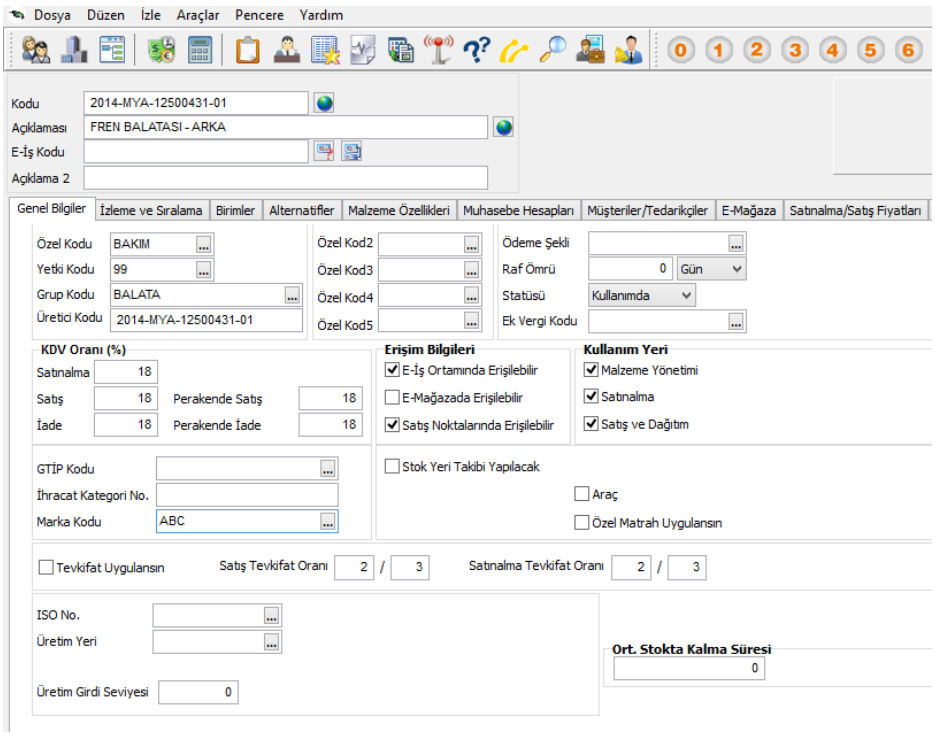
4.4.4.1. Malzeme Kartı Tanımlamaları

Malzeme kartları işyeri bağımsız ortak kullanılacağı için tek bir kullanıcı tarafından tanımlanması gerektiği kararlaştırılmış ve yetkiler bu şekilde tanımlanmıştır. Bu kontrol ile yanlış kodlamanın önlenmesi planlanmıştır. Malzeme kartları tanımlamasında kullanılacak üreticinin belirlediği kodlar 20 karakter olup hatalı kodlama yapılmaması için malzeme kodu alanı için karakter sayısı kontrolü konulmuş, 20 karakterden az veyahut fazla giriş engellenmiştir.

Malzeme kartlarının sonraki süreçlerde yönetilmesi ve bunlara ilişkin raporlamaların daha kolay yapılabilmesi için malzeme kartlarında bazı alanlar zorunlu alan olarak belirlenmiş olup bu alanlar ve kontrol amaçları aşağıdaki gibidir. Ayrıca bu alanlardan bazıları için kullanıcın herhangi bir değeri değil, sadece önceden tanımlanan değerlerden herhangi birinin girilmesi istendiği için seçimli liste kontrolleri belirlenmiştir.

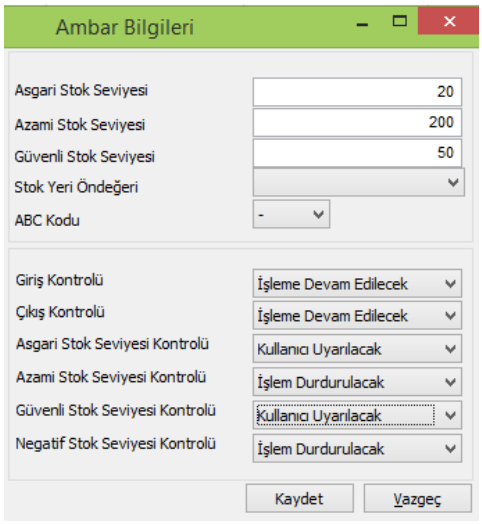
Tablo 3. Malzeme Kartlarındaki Belirlenen Kontroller

Alan Adı	Kontrol	Kontrol Amacı
Malzeme Kodu	20 karakter zorunluluğu	Malzeme kodlarının eksik veyahut faza girilmesi engellenmiştir.
Özel Kod1	Zorunlu Alan / Seçimli Liste	Malzemelerin sınıflandırılması için kullanılmaktadır
Yetki Kodu	Zorunlu Alan	Yetkilendirmeyi yönetmek için zorunludur.
Marka Kodu	Zorunlu Alan / Seçimli Liste	Malzeme hareketi raporlarında sürekli marka temelinde raporlar alınmakta ve analizler yapılmaktadır.
KDV Oranları	Zorunlu Alan	Alış ve Satış hareketlerinde KDV oranının doğru uygulanması için zorunludur.



Şekil 14. Malzeme Kartı Tanımlaması

Yönetim, satış ve satınalmaların yönetilmesi ve etkin stok maliyeti için bazı malzemelerde asgari ve azami stok seviyeleri belirlemek istemektedir. Bunun için ilgili malzemelerin her biri için seviyeler belirlenmiş, programda Şekil 13.'de gösterildiği gibi tanımlanmış, stoklar bu seviyelere ulaştığında kullanıcıların bu malzemelere ait herhangi bir kayıt oluşturduğunda uygulama tarafından uyarılması sağlanmıştır.

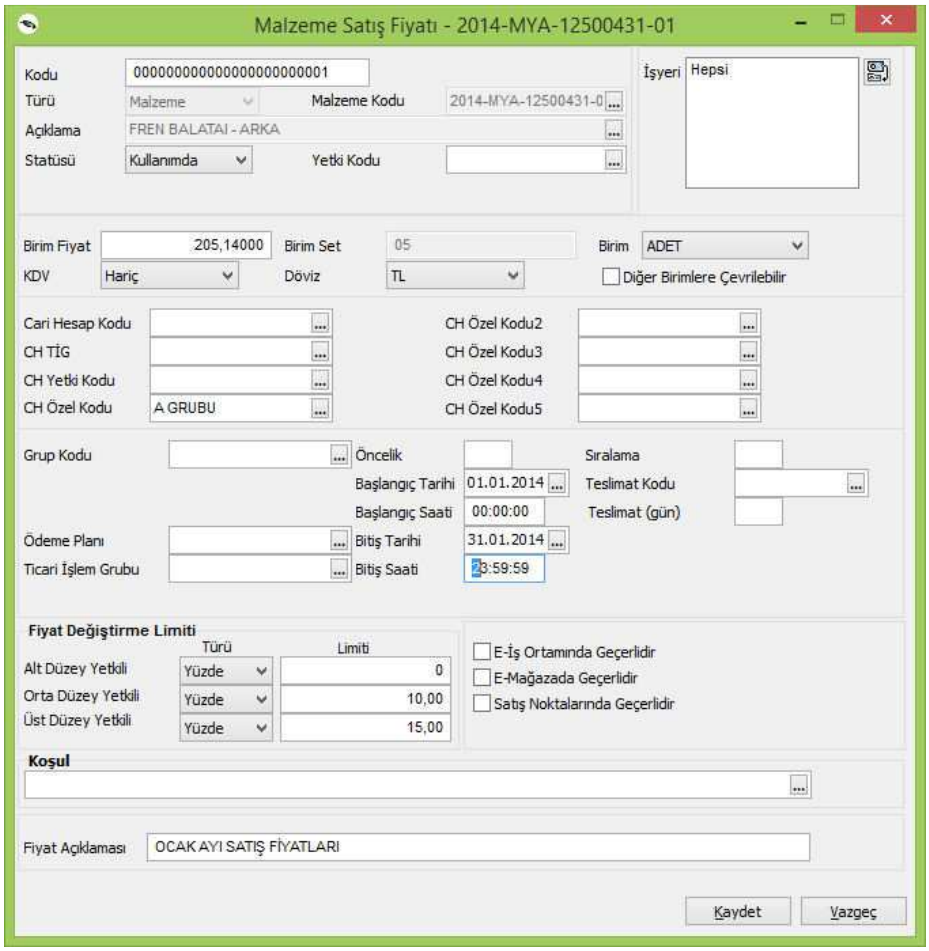


Şekil 15. Malzemelerde Miktar Kontrollerinin Uygulanması

Asgari stok seviyesinde satışın durdurulmayıp, sadece belirli müşterilere birer adet satılması istenmektedir ancak uygulamada bu isteğin kontrol edilebilmesi mümkün değildir bu nedenle geliştirme ve değişiklik yapılması gerekmektedir. Konu bilgi sistemlerinde dış destek alınan danışman firmaya iletilmiştir.

4.4.4.2. Alım ve Satı˙ Fiyatlarının Tanımlanması

Malzeme alış fiyatlarında aylık dönemlerde değişiklikler olmakta, buna paralel satış fiyatları da her ay güncellenmektedir. Bu hızlı fiyat değişikliği nedeni ile alış ve satışlarda malzeme birim fiyatlarında hata riskine karşı için her ay yeni fiyatlar sisteme tanımlanmakta olup belirlenen oranlarda sapmaların dışında fiyat farklılıklarında alış ve satış kayıtları yapılması engellenmiştir.



Şekil 16. Malzeme Satı˙ Fiyatı Tanımlaması

4.4.4.3. Malzeme Hareketleri

Malzeme hareketlerine ait fişler alış ve satış irsaliyeleri ile oluşmaktadır, dolayısı ile dönem içinde irsaliye dışında herhangi bir işlem ile giriş veyahut çıkış yapılmasına izin verilmemiştir. Dönem sonlarında yapılan sayım sonucu fazla ve eksik miktarlarının nedenleri incelenip düzenlenen tutanaklar ile sayım fazlası ve sayım eksiği fişleri ile işlenecektir. Dönem başı devir fişleri sistem tarafından bir önceki dönemden devredilecek olup herhangi bir kullanıcıya devir fişlerinde müdahale izni verilmemiştir.

Malzeme Satınalma İşlemleri

Malzeme satınalma kararları önceki dönem malzeme hareketlerinin analizi ile yapılan öngörüler ve müşteri siparişleri dikkate alınarak belirlenmektedir. Programda önceki dönem analizleri detaylı bir şekilde yapacak bir uygulama bulunmadığından bu ihtiyaç MS Access programı ile veritabanı bağlantısı oluşturarak yapılmaktadır.

Malzeme satın alma süreci talep, sipariş, teslim alma ve fatura ilişkisi kurularak yapılmakta bu sürecin dışında herhangi bir satın alma işlemi yapılmamaktır. Bu süreci uygulamada kontrol altına alınması için kaynaksız belge oluşturulması kısıtlanmıştır, süreç uygulamada aşağıdaki adımlar ve kontroller ile yürütülecektir.

Satın alınması talep edilen malzemeler için talep fişi müşteri detayı, miktarı, tedarikçisi birim fiyatı gibi detaylar ile öneri konumunda oluşturulmaktadır. Birim fiyat daha önce her bir malzeme için tanımlanan satın alma fiyatlarından gelmektedir. Satın alma yöneticisi belirli aralıklar ile öneri konumundaki talepleri kontrol edip, gerekirse değişiklikler yaptıktan sonra uygun gördüklerini satın alma olarak onaylar.

Satınalma birimi daha önce onaylanan talep fişlerindeki kayıtlar ile tedarikçi ve malzeme temelinde sınıflandırma yaparak satınalma siparişlerini oluşturmakta, bu sipariş ile depoda mal kabulü yapılmaktadır. Mal kabulünün yapılabilmesi için sistemde satınalma siparişinin olması gerekmektedir, siparişi olmayan bir malzemenin depo tarafından kabul edilmesi engellenmiştir.

Ayrıca mal kabulü esnasında sipariş miktarı ile gelen miktar arasında farklılıkların olması durumunda kullanıcının uyarılması istenmiş ancak programda bu kontrol uygulanamamıştır. Bu farklılıkların tespiti belirli aralıklarla veri analiz programları ile yapılması planlanmıştır.

Depo tarafından mal kabul işlemi yapıldıktan sonra, uygulamada satın alma irsaliyesi oluşmakta ve irsaliye muhasebe tarafından sipariş ile karşılaştırılıp faturaya dönüştürülmektedir. Faturadaki birim fiyat satın alma siparişinde fiyat ile karşılaştırılıp, yüksek birim fiyat olması durumunda faturanın kaydedilmesi önlenmiştir.

Tüm malzeme hareketlerinin muhasebe kayıtlarına geçmesi için, satın alma irsaliyelerinin mutlaka faturalanmış olması, faturaların da mutlaka muhasebeleştirilmiş olması kuralı belirlenmiştir. Uygulamada, irsaliyelerde faturalandığına dair ve

faturalarda ise muhasebeleştirildiğine dair işaretler bulunmakta olup dönem sonlarında yapılan kontroller ile eksik işlemler tamamlanmaktadır.

Hem satış hem de satınalma tarafında sürecinde işlemlerin bir önceki işlem ile bağlantılı olması ve birden fazla birim tarafından yerine getirilmesi hata ve suistimal riskini azaltmıştır. Örneğin irsaliye olmadan herhangi bir fatura girişinin engellenmesi gerçek olmayan bir fatura kaydına engel olacaktır.

Malzeme Satış İşlemleri

Müşteri siparişleri uygulamada satış siparişi fişi olarak oluşturulmakta, onaylanan siparişler depoya sevk emri olarak iletilmekte, depoda mal toplama işleminin tamamlanması ile satış irsaliyesine ve daha sonra satış faturasına dönüştürülmektedir. Satış işlemlerinin her bir aşamasında bir takım kontroller planlanmıştır.

Sipariş Fişinin Oluşturulması

Müşteri satış siparişleri satış personeli tarafından, telefon, faks, e-posta gibi iletişim araçları ile alınıp sisteme "Öneri" olarak kaydedilir. Malzeme satış fiyatları sisteme daha önce girilen o tarihe ait brüt fiyatlardan gelmekte, müşteri tipi ve vadesine göre farklı indirimler uygulanmaktadır. Tanımlı fiyatların haricinde kullanıcı tarafından birim fiyat girişi izin verilmeyerek, yanlış fiyatlama riski kontrol edilmiştir. İndirimlerin doğru uygulanması için indirim oranları programda tanımlanmış olup, fiş oluştururken müşteri ve vadeye göre ilgili oran otomatik gelmekte, kullanıcı tarafından değiştirilmesine izin verilmemektedir.

Sipariş sevkiyatlarının yönetilebilmesi için sipariş tipi, sevkiyat tipi ve sevk tarihi bilgilerine ihtiyaç duyulmaktadır, bu bilgiler için uygulamada zorunlu alan tanımlamaları yapılmış, bilgiler girilmeden sipariş fişinin kaydedilmesi önlenmiştir.

Öneri konumundaki siparişler, gerekli kontroller yapıldıktan sonra satış birim yöneticileri tarafından onaylanmakta, onay ile depoya sevk emri olarak iletilmektedir. Onay aşamasında müşteri risklerinin belirlenen limitler dahilinde olup olmadığı uygulama tarafından kontrol edilmekte, risk toplamının limit toplamını aştığı durumlarda siparişin onaylanmasına izin verilmemektedir.

Depo tarafından alınan sevk emirleri depoda kullanılan el terminalleri ile hazırlanmaktadır. Sevk emrinde malzeme kodu ve adı, sevk miktarı ve depodaki yeri belirtilmiştir, depo çalışanı bu bilgiler ile ilgili depo rafına gidip, rafta ve malzemede bulunan barkodları okutarak malzemeleri toplar. Barkod okutmadan malzeme toplama işlemine izin verilmeyerek yanlış malzeme gönderimi engellenmek istenmiştir. Sevk emri tamamlandıktan sonra sistemde satış irsaliyesi oluşturulur ve daha sonra satış faturasına dönüştürülür. Faturada kullanıcılar tarafından cari hesap, vade, birim fiyatlarda ve miktarlarda herhangi bir değişiklik yapılmasına izin verilmemiştir. Sevk irsaliyesi olmadan kullanıcının fatura oluşturulması engellenmiştir.

Dönem sonlarında yapılan kontroller ile tüm siparişlerin sevk edildiği, tüm irsaliyelerin faturaya dönüştürüldüğü ve tüm faturaların da muhasebeleştirilerek muhasebe kayıtlarına ulaştırıldığının kontrolleri yapılır. Bu kontroller program içinde yapılabileceği gibi veri analizi programlarında oluşturulacak raporlar ile de yapılabilecektir.

Satış birimi, satış politikası gereği bazı özel malzemelerin satış miktarlarını kontrol altına almak istemektedir. İlgili malzemelerin bir siparişte belirlenen adetlerde satılmasını bu adetlerin üzerinde satışa izin verilmemesi gerekmektedir, ancak bu kontrol programda gerçekleştirilememektedir.

İşletme, müşterilerinin kendi siparişlerini oluşturmalarını sağlayan, aynı zamanda bir takım cari hesap bilgilerine de ulaşabileceği B2B (Busines to Busines) benzeri bir uygulamaya ihtiyaç duymaktadır. Mevcut programın bu ihtiyacı karşılamadığı, bu nedenle uygulamada geliştirilme yapılması gerektiği görülmüştür.

4.4.5. Araç Satı˙ ve Servis İ˙lemleri

Araç satış ve servis süreçlerinin takibi işletmenin diğer faaliyetlerinden farklıdır. Her iki faaliyette de temel iş süreçlerinde kullanılan TIGER uygulamasının yeterli olmadığı sektöre özel yazılımların kullanılması gerektiği değerlendirilmiştir. Aynı zamanda üretici firma kendi yazılımlarının kullanılmasını istemektedir. Bu durumda işletmenin bu faaliyetleri ile ilgili süreçlerini yürütmek için ihtiyaç duyacağı

yazılımın tasarımı ve uyarlanması için kaynak ayırmayacak olması bir avantajdır. Bunun yanı sıra bu faaliyetlere ilişkin bilgilerin ana program olan TIGER'da olmaması da işletme için dezavantajdır.

Bu uygulamalarda da bir takım kontroller bulunmaktadır. Örneğin geçmiş tarihli fiş girişine izin verilmemektedir, hareketlerin tamamen silinmesi engellenmiştir, malzeme ve işçilik kodlarına müdahaleye izin verilmemiştir, satış birim fiyatları tanımlanan birim fiyatlar ile gelmekte, indirim oranları belirlenen kampanya ve kurallar ile müşteriye göre uygulanmaktadır.

Servis süreci kısaca aşağıdaki adımlardan oluşmakta ve tamamı bilgi sistemleri üzerinden takip edilmektedir.

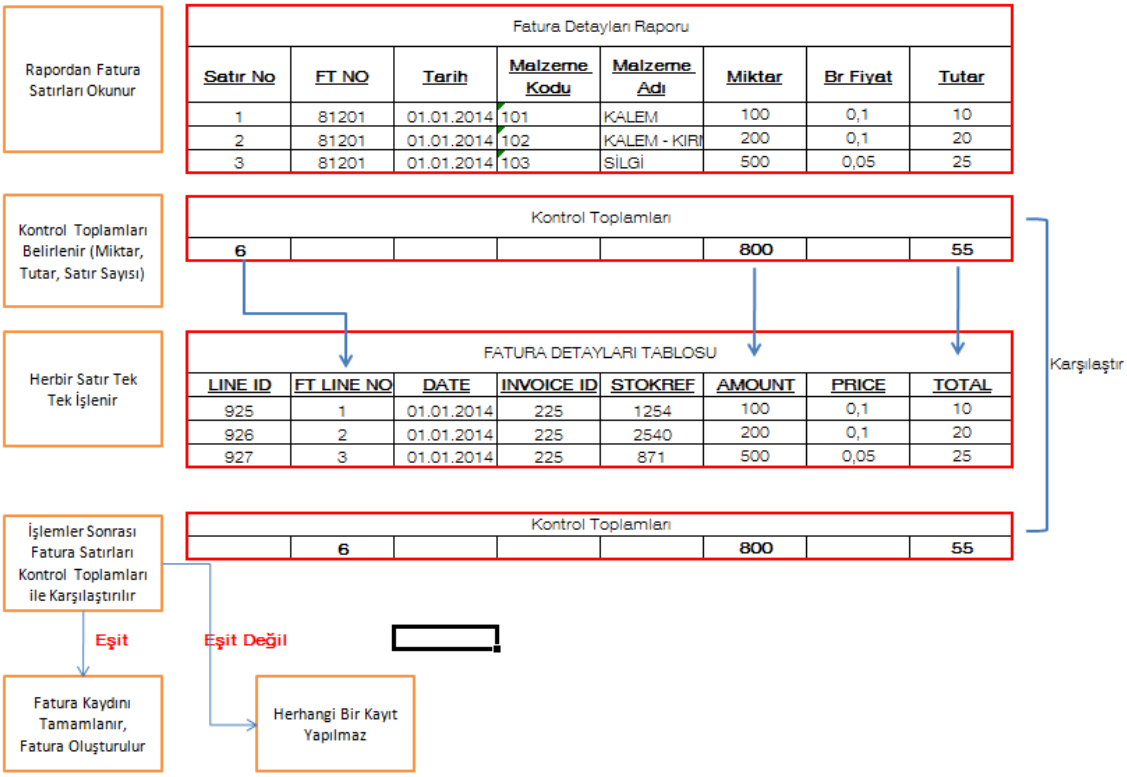
Gelen müşteri için ruhsat bilgileri ile sistemdeki bilgiler karşılaştırılarak iş emri açılır iş emri olmayan araç için serviste işleme başlanılmaz. Teknik eleman ilgili iş emri için gerekli olan yedek parçayı depodan talep eder, iş emri olmadan depodan malzeme çıkışına izin verilmez, yapılan işçilikler iş emrine hem kâğıt üzerinde hemde bilgisayar ortamında belirtilir, işlemler tamamlandıktan sonra iş emri kapatılıp faturaya dönüştürülür. Belirli aralıklar ile kapatılmayan iş emri kontrolleri yapılmaktadır.

Yapılan çalışmalar sonucunda araç satış ve servis süreçlerinde kullanılan uygulamadaki verilerin tamamının TIGER'a aktarılması mümkün değildir. En azından süreçlere ait fatura ve cari bilgilerinin ana uygulamaya aktarılması kararlaştırılmıştır. Her iki uygulama birbirleri ile entegre bir şekilde çalışmamakla birlikte üretici firmanın uygulamasında geliştirilme yapılmasına izin verilmemektedir.

Servis ve araç satış faturalarının ana uygulamaya girilmesi için iki yöntem vardır. Birincisi, üretici firmanın uygulamasında oluşturulan faturalar tekrar kullanıcılar tarafından girilebilir, ancak bu durumda her bir işlem iki kez yapılacak ve bu da çok zaman alacaktır. İkinci yöntem ise alınan raporların ana uygulamaya ara bir yazılım ile aktarılmasıdır. TIGER programına bu yöntemle veri aktarılması mümkündür.

Yapılan çalışmalar sonucunda aktarımın doğru ve eksiksiz yapılabilmesi için bir takım kontroller planlanmıştır. Yapılan aktarımlar TIGER uygulamasının belirlediği kural ve prosedürler çerçevesinde yapılması kararlaştırılmış, böylelikle ciddi riskler taşıyan veritabanına direkt veri yazılmasının (Insert Data) önüne geçilmiştir. Bu şekilde

aktarılan verilerin ana uygulama standartlarına uygun kayıtlar oluşturulmasını sağlanmış, gereksiz veritabanı müdahaleleri ile hatalı kayıtların oluşması engellenmiştir. Aynı zamanda ana uygulamada planlanan uygulama kontrollerinin de işlerliği devam edecektir. Fatura aktarımlarında önceki bölümlerde anlatılan yığın işleme kontrolleri kullanılmaktadır. Aktarım uyarlaması kaynak rapordan okuduğu verileri programa detayları ile aktaracaktır, her bir detay ilgili tablolara yazılması gerekmektedir, herhangi bir aksaklık nedeni ile detayları kaydedilemeyen fatura sisteme kaydedilmeyecektir. Örneğin A-1234 nolu üç kalem malzemeden oluşan bir satış faturasının aktarılması esnasında malzemelerin herhangi birinin uygulamada kaydı yok ise bu malzeme satırı eklenemeyecektir dolayısı ile faturanın tutarı eksik olacaktır, bu durumda yığın kontrolünde toplam fatura tutarı eşleşmeyeceği için kayıt yapılmayacak eksik kaydın önüne geçilecektir.



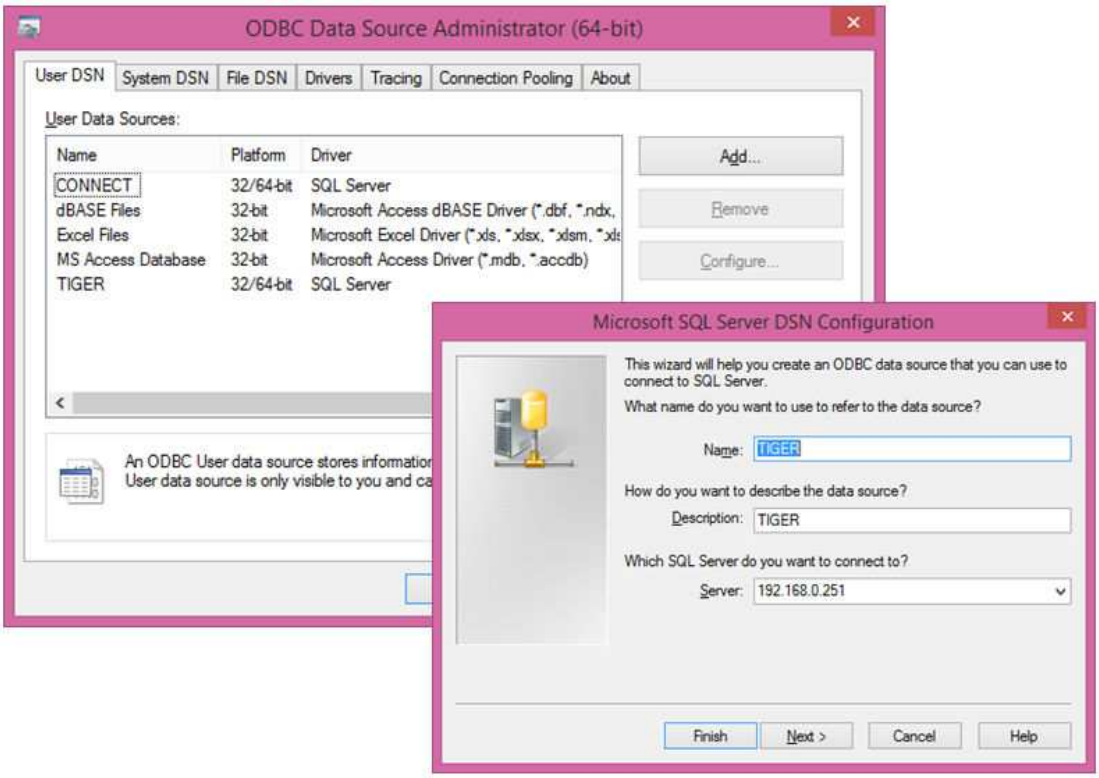
Şekil 17. Toplu Kayıt Aktarım A˙amaları

Aktarımlar sonucu tüm faturaların aktarıldığının ve herhangi bir faturanın birden fazla aktarılmadığının kontrol edilmesi gerekmektedir, bunun da uygulamalar farklı olduğu için bilgi sistemi üzerinde yapılması mümkün değildir. Bu nedenle belirli

aralıklar ile her uygulamadan alınan satış raporları çıktılarının el ile kontrol edilmesi planlanmıştır.

4.6. Veri Analiz Tekniklerinin Uygulanması

İşletme bazı işlemlerin kontrol ve denetimi için veri analiz teknikleri ile birtakım raporlar oluşturmuştur. Bu raporlar ile ilgili kayıtların tamamının kontrolü çok kısa sürede kolayca yapılabilmektedir. Bu işlemler için işletmede bulunan genel amaçlı uygulamalardan MS Excel ve MS Access uygulamaları kullanılmaktadır. Verilerin ilgili programlara online (anlık) veri aktarabilmesi için raporlama yapacak kullanıcıların bilgisayarlarında ODBC (Open Database Connectivity) tanımlamaları yapılmıştır. Bu şekilde bilgi sisteminde herhangi bir veri kaydedildiğinde raporda da aynı anda görüntülenecektir.



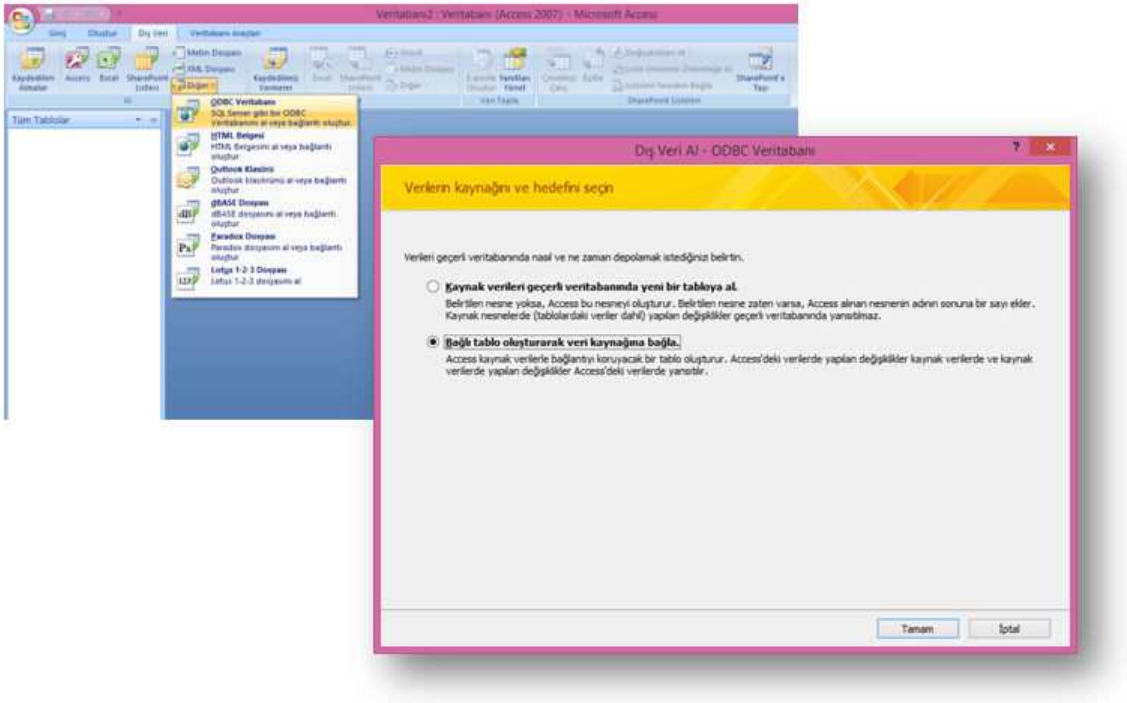
Şekil 18. Veritabanı Bağlantısı Tanımlama

Bu tür raporların oluşturulabilmesi için uygulamanın veritabanı yapısı, tablo adları, alan adları ve birbirleri ile ilişkilerinin bilinmesi gerekmektedir.

4.6.1. Kasa Hareketlerinde Tutar Kontrollerinin Test Edilmesi

İşletmede kullanılan uygulamada 1.000 TL üzerindeki kasa hareketlerine izin verilmemiş, giriş kontrolü ile bu tür kayıtlar engellenmesi planlanmıştı. Bu kontrolün etkinliğinin test edilmesi için MS Access programı kullanılarak oluşturulan rapor aşağıda adım adım anlatılmıştır.

Öncelikle Access programı ile ilgili tabloların bağlantısı yapılması gerekmektedir. Bunun için program menüsünden sırası ile "Dış Veri > Diğer > ODBC Veritabanı" butonları seçilir.

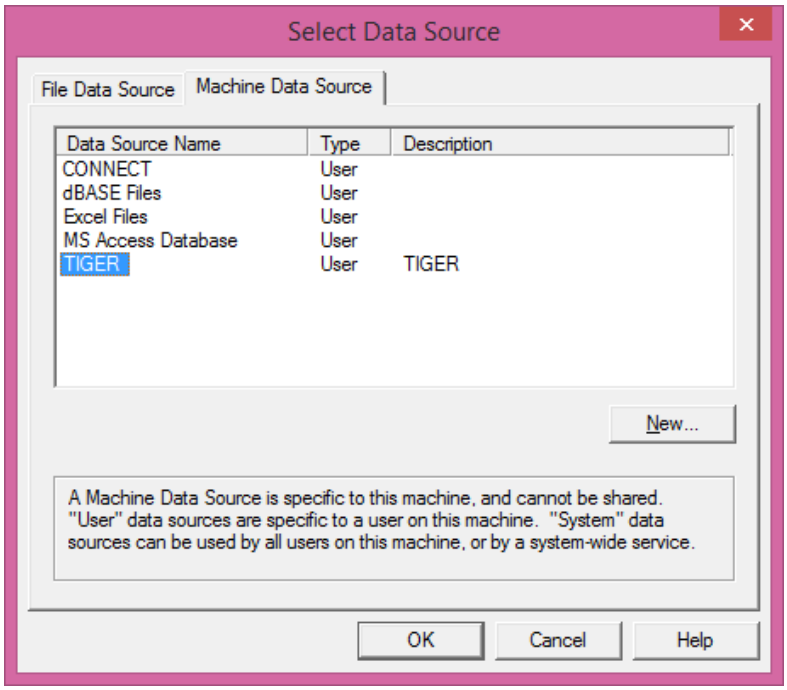


Şekil 19. Access Programı Veritabanı Bağlantısı oluˇturma

Açılan pencerede kullanıcıya iki seçenek sunulur, birincisi veritabanındaki ilgili tabloların o anki verileri Access uygulamasına aktarılır, ikincisinde ise ilgili tablo

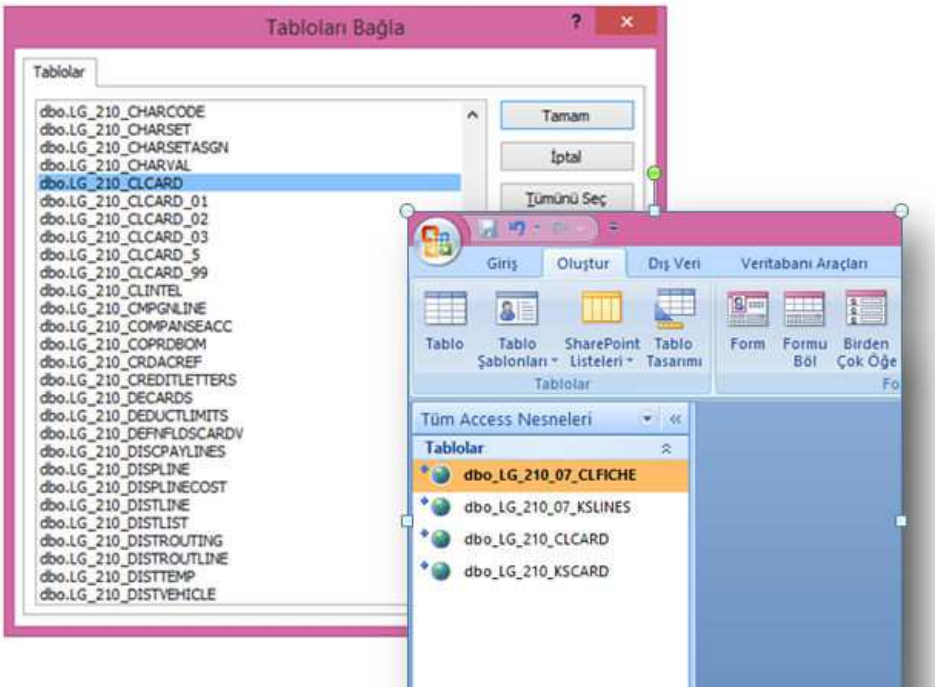
ile bağlantı kurulması sağlanır. Bu kontrol belirli aralıklarla devamlı yapılacağı için ikinci seçeneği ile devam edilmesi doğru olacaktır.

İlgili seçimden sonra tamam butonu tıklandıktan sonra gelen pencereden daha önce tanımlanmış ODBC bağlantısı seçilir.



Şekil 20. Access Programı Veritabanı Seçimi

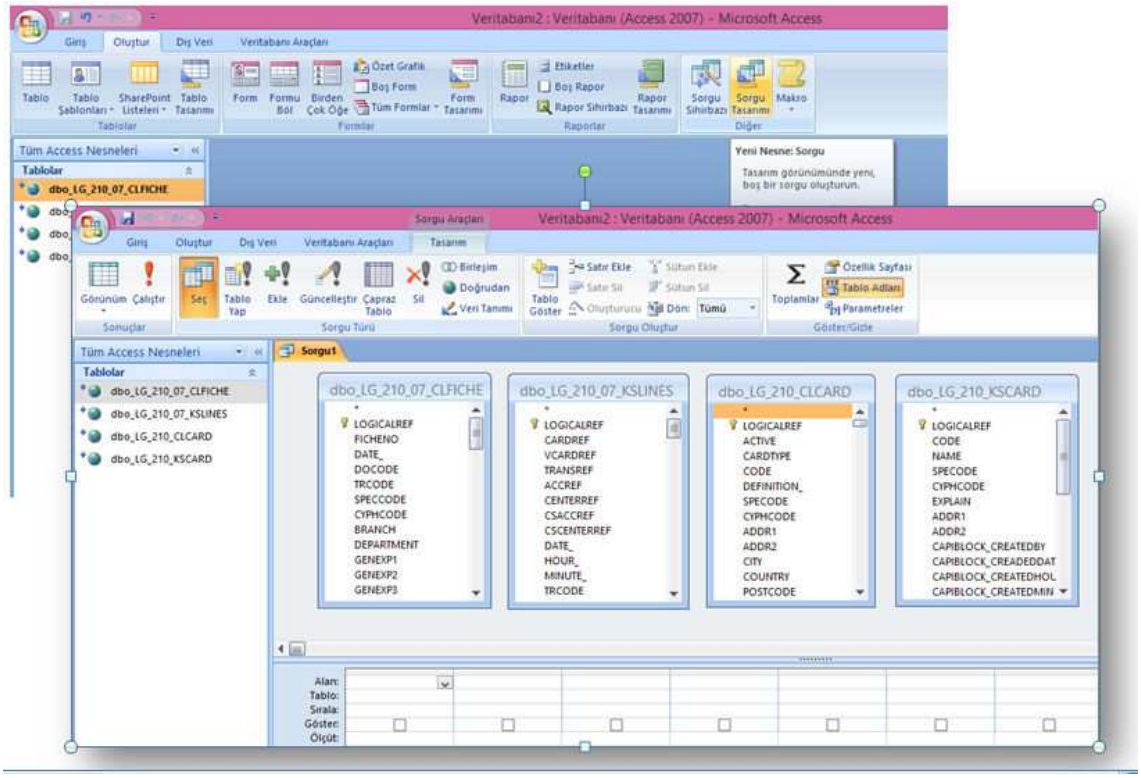
Yapılan bu işlem ile uygulamanın veritabanındaki erişim sağlanmış olur. Sonraki pencerede veri analizinde kullanacak verilerin kaydedildiği tablolar seçilip Access ile tablo bağlantısı oluşturulur. Bağlantı yapıldıktan sonra, Access uygulamasında seçilen tablolar aşağıdaki şekilde görünecektir.



Şekil 21. İlgili Tabloların Seçilmesi

Kasa hareketlerinin incelenmesi için oluşturulması planlanan raporda kullanılacak dört adet tablo bulunmaktadır. Bunlar; Kasa kartlarının kaydedildiği …_KSCARD tablosu, kasa hareketlerinin kaydedildiği …_KSLINES tablosu, cari hesapların tanımlı olduğu …_CLCARD ve cari hesap fişlerinin bulunduğu …_CLFCIHE tablosudur.

Sonraki aşamada Access sorgu aracı kullanılacaktır. Sırası ile Menü > Oluştur > Sorgu tasarımı tıklandıktan sonra, sorgu tasarım ekranı açılacaktır. Bu ekranda sorguda kullanılacak ilgili tablolar seçilir.



Şekil 22. Access Sorgusunun Oluˇturulması -1

Bu dört tabloda ilgili kayıtlara ilişkin birçok veri bulunmaktadır, bunların birçoğu oluşturulacak rapor için gerekli değildir. Bu nedenle sorgu tasarımında sadece gerekli olan alanlar seçilecektir. Alan seçiminden önce tabloların birbirleri ile ilişkili olan alanların tanımlaması yapılmalıdır. Bu ilişki aşağıdaki tabloda gösterilmiştir.

Tablo 4. Raporda Kullanılan Tablo Alan ve Alanlar Arası İli˙kiler

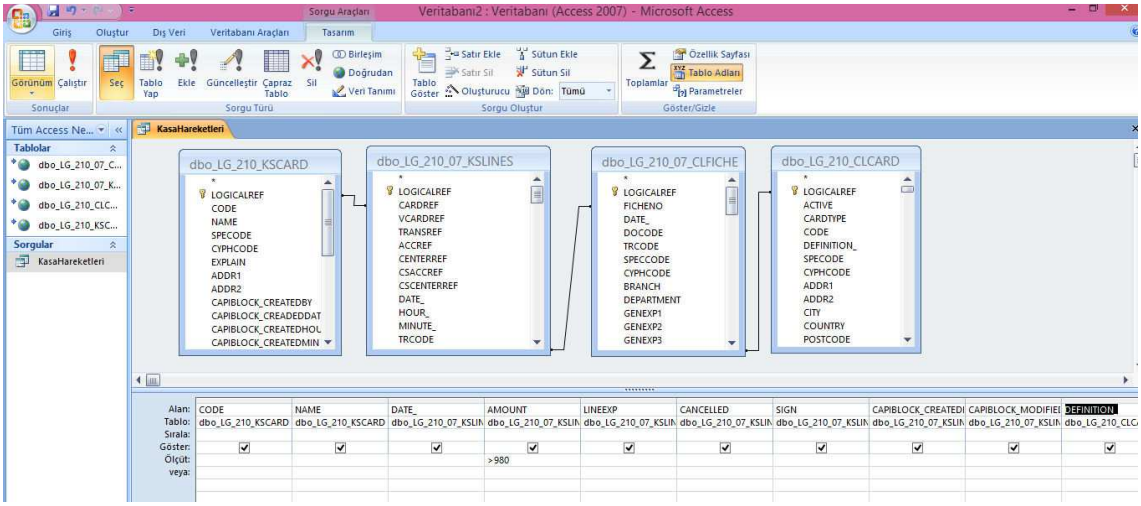
Tablo Adı	**…_KSCARD**	**…_KSLINES**	**…_CLFCIHE**	**…_CLCARD**
Tablo Açıklaması	Kasa kartlarının tanımlı olduğu tablo	Kasa hareketlerinin kayıtlı olduğu tablo	Cari hesap fiş kayıtlarının bulunduğu tablo	Cari hesap bilgilerinin kaydedildiği tablo
İlişkili Alan / Alan Açıklaması	LOGICALREF	CARDEF		
	Her bir kasa kartının tanımlanmış Uniqe değeridir.	İlgili hareketinin hangi kasaya ait olduğu bu alanda yazılıdır.		
İlişkili Alan / Alan Açıklaması		FICHENO	FICHENO	
		Kasa hareketinin fiş numarası.	Cari hesap hareketlerinin fiş numarası	
İlişkili Alan / Alan Açıklaması			CLCARDREF	LOGICALREF
			Cari hareketin ilişkili olduğu cari hesap kartının referans numarası.	Cari hesap kartlarının uniqe (tekil) değeridir.

Tablolar arası ilişki kurulduktan sonra raporda listelenmesi istenen alanlar ve bu alanlara ilişkin filtrelerin tanımlamaları yapılır. Bu alanlara ilişkin detaylar aşağıdaki gibidir.

Tablo 5. Raporda Kullanılan Tablo Alanları

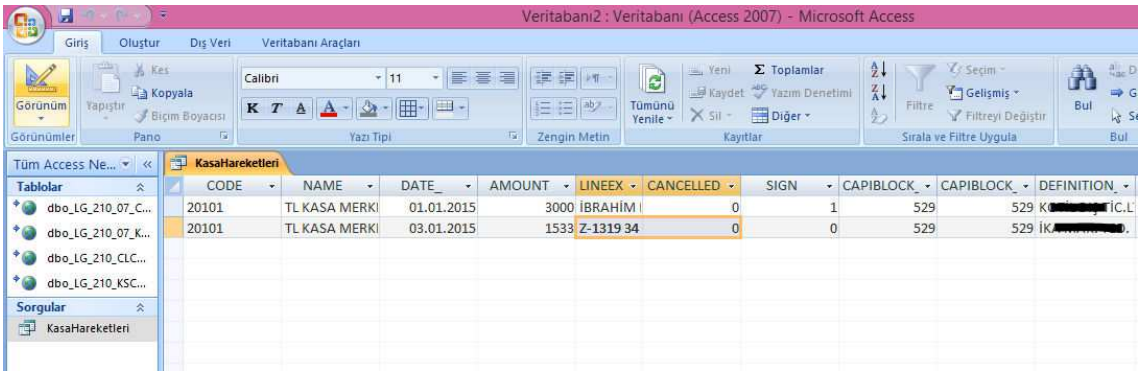
TABLO ADI	ALAN ADI	ALAN AÇIKLAMASI	FİLTRE
dbo_LG_210_KSCARD	CODE	Kasa Kodu	
dbo_LG_210_KSCARD	NAME	Kasa Adı	
dbo_LG_210_07_KSLINES	DATE_	Hareket Tarihi	
dbo_LG_210_07_KSLINES	AMOUNT	Tutar	> 980 (sınıra yakın değerlerin listelenmesi istenmiştir)
dbo_LG_210_07_KSLINES	LINEEXP	Hareket Açıklaması	
dbo_LG_210_07_KSLINES	CANCELLED	İptal Edilmiş / İptal Edilmemiş (0 değeri iptal edilmemiş, 1 değeri iptal edilmiş)	0 (iptal edilmemiş kayıtların listelenmesi istenmiştir)
dbo_LG_210_07_KSLINES	SIGN	Borç / Alacak işareti (0 değer Borç, 1 değer alacak)	
dbo_LG_210_07_KSLINES	CAPIBLOCK_CREATEDBY	Oluşturan Kullanıcı	
dbo_LG_210_07_KSLINES	CAPIBLOCK_MODIFIEDBY	Değiştiren Kullanıcı	
dbo_LG_210_CLCARD	DEFINITION_	İlgili hareketin cari hesap adı	

Tablolardaki ilgili alanları Access sorgusuna ekleyip filtrelerin tanımlaması yapılır. Son olarak sorgu görüntüsü aşağıdaki gibi olacaktır.



Şekil 22. Access Sorgusunun Oluşturulması -2

Sorguyu kaydedip çalıştırdığımızda istemiş olduğumuz hareketlere ilişkin rapor aşağıdaki şekilde gelecektir.



Şekil 23. Access Sorgusunun Sonucu Rapor

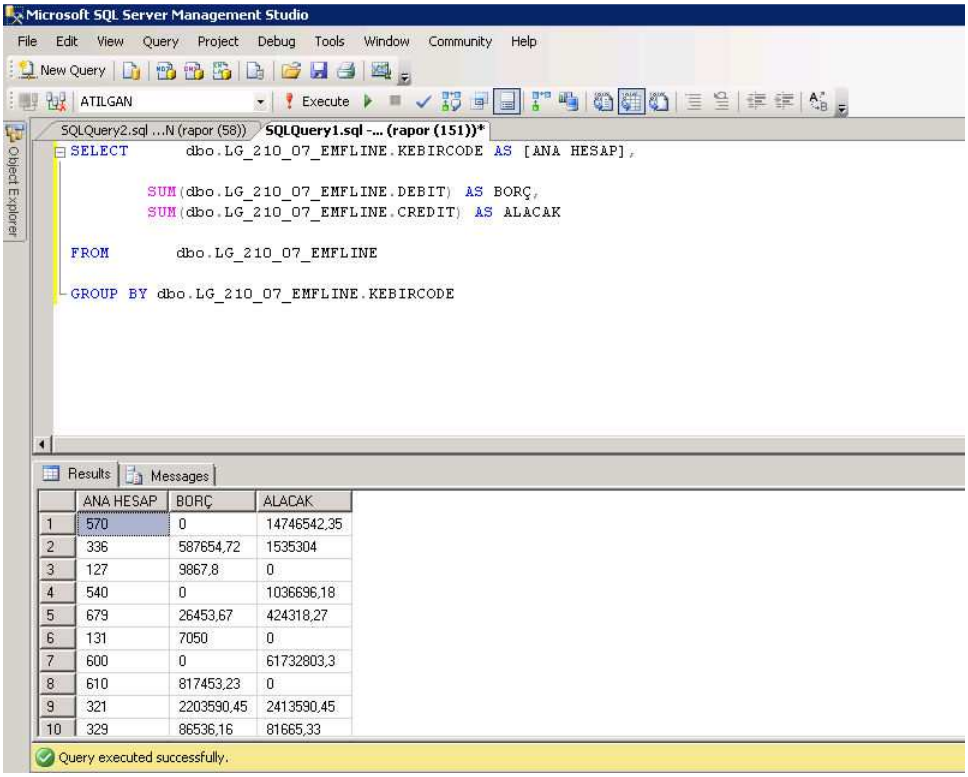
Listelenen raporda 2 adet hareketin belirlenen üst limitlerin üzerinde olduğunu göstermektedir. Bu durumda işletme tarafından uygulamada tasarlanmış kasa limit kontrolünün etkin olarak çalışmadığını veyahut kullanıcılar tarafından bir şekilde atlatıldığını göstermektedir.

Oluşturulan bu sorgu ile istenildiği her an, o anki durumda bilgi sisteminde kayıtlı tüm kasa hareketlerinden belirlenen filtreler dâhilindeki kayıtları saniyeler içinde raporlayacaktır. Özellikle hareket sayısı çok olan işletmelerde bu tür bir rapor ile alınan sonuçlara bilgisayar olmadan ulaşılması çok zaman alacak bazen de imkansız olacaktır.

4.6.2. SQL Kodları İle Ana Hesap Bakiyelerinin Test Edilmesi

İşletmenin iş süreçlerinin takibi için kullandığı TIGER programı MSSQL veritabanı yönetim programı ile çalışmaktadır. TIGER programından alınan raporlardaki tutarların doğruluğunun test edilmesi için SQL dili ile oluşturulan raporlar kullanılabilir. Bu tür raporlar için önceki raporlamada olduğu gibi SQL dilini ve TIGER tablo yapısını bilmek gerekmektedir.

Muhasebe hesap bakiyelerini oluşturan hareketler …EMFLINE tablosunda takip edilmektedir. Bu tabloda raporlama için gerekli alanlar, hesap kodunun saklandığı KEBIRCODE, borç tutarlarının saklandığı DEBIT ve alacak kayıtlarının saklandığı CREDIT alanlarıdır. Microsoft SQL Server uygulamasında yeni bir Query dosyası açılıp aşağıdaki sorgu kodu çalıştırıldığında sonuç olarak ana hesaplara ait hesap toplamları çok kısa bir sürede raporlanmış olur. Oluşturulan rapor ile işletme kayıtlarına ait 219.985 adet hareketin ana hesap bazında özeti saniyeden daha kısa sürede raporlanmıştır.



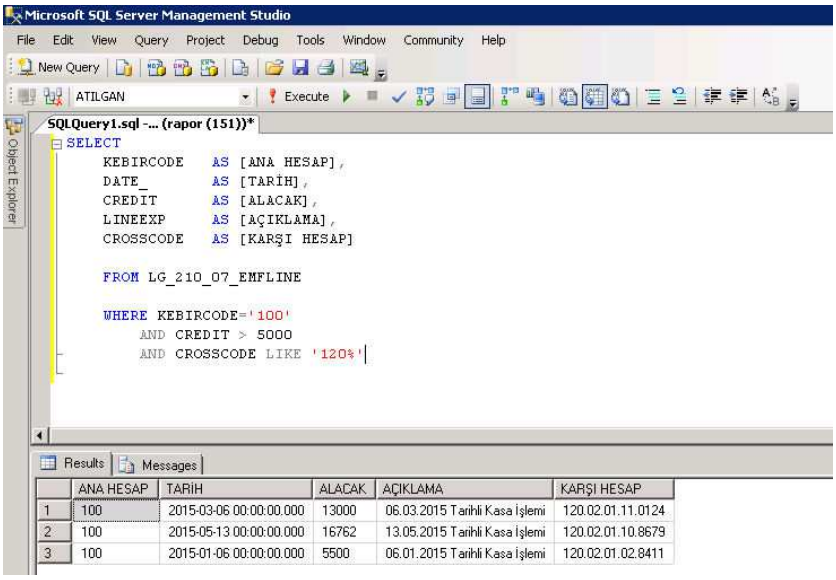

```
SELECT       dbo.LG_210_07_EMFLINE.KEBIRCODE AS [ANA HESAP],

             SUM(dbo.LG_210_07_EMFLINE.DEBIT) AS BORÇ,
             SUM(dbo.LG_210_07_EMFLINE.CREDIT) AS ALACAK

FROM         dbo.LG_210_07_EMFLINE

GROUP BY     dbo.LG_210_07_EMFLINE.KEBIRCODE
```

Şekil 24. SQL ile Ana Hesap Bakiyelerinin Test Edilmesi

Oluşturulan bu rapor, uygulamanın dışında verilerden oluşturulduğu için aynı zamanda uygulamanın işlem ve çıktı aşamalarında etkinliğinin test edilmesinde de kullanılabilecektir.

4.6.3. SQL Kodları İle Kasa Hesabındaki Yüksek Tutarların Tespiti

Bir önceki örnekte anlatılan yöntem ile kasa hesabına ait yüksek tutarlı ödemelerin listelenerek yorumlanması istenmektedir. Bu raporda da aynı tablo kullanılarak oluşturulmuştur. Kullanılacak alanlar bir önceki rapordaki alanlar ile hareket tarihinin saklandığı DATE_ alanı, hareket açıklamasının saklandığı LINEEXP alanı ve ödemenin karşı hesabı olan CROSSCODE alanlarıdır. Raporda 5.000 TL ve üzerindeki 120 hesaplara yapılan ödeme hareketlerinin raporlanması istenilmektedir bu nedenle oluşturulan SQL sorgu kodu aşağıdaki şekilde olacaktır.




```
SELECT
      KEBIRCODE   AS [ANA HESAP],
      DATE_       AS [TARİH],
      CREDIT      AS [ALACAK],
      LINEEXP     AS [AÇIKLAMA],
      CROSSCODE   AS [KARŞI HESAP]

      FROM LG_210_07_EMFLINE
            WHERE KEBIRCODE='100'
            AND CREDIT > 5000
            AND CROSSCODE LIKE '120%'
```

Şekil 25. Kasa Hareketlerinin SQL ile İncelenmesi

Sonuç

Günümüzde işletmelerin faaliyetlerini gerçekleştirmede bilgi sistemlerini yoğun olarak kullanması tüm süreçleri etkilediği gibi iç kontrol ve denetim süreçlerinde de etkili olmuştur. Söz konusu faaliyetler için tasarlanan iç kontrol düzenlemeleri ve denetimin de bilgi sistemleri ile yapılması kaçınılmazdır. Bu nedenle bu çalışmaları yapacak meslek mensuplarının bilgi teknolojileri ve bilgi sistemleri ile ilgili temel düzeyde bilgi sahibi olması gerekmektedir.

Bilgi sistemlerinin denetimi ile ilgili uluslararası mesleki örgütler oluşturulmuş ve konu ile ilgili standartlar yayınlanmış olmasına rağmen ülkemizde konu yeteri kadar ele alınmamıştır. Yapılan çalışmada, özellikle Türkçe yayınlanmış akademik çalışmaların eksikliği göze çarpmaktadır. Üniversitelerin ilgili bölümlerinin lisans düzeyi eğitimlerinde ders listelerinde konu ile ilgili derslere rastlanılmamıştır. Önemi giderek artan bilgi sistemleri ve bilgi teknolojileri denetimi konusu ülkemizde meslek örgütleri tarafından gündeme alınmalı, bu alanda eğitim veren üniversiteler bölümlerinde bu konuyu ders planlarına eklemelidirler.

Bu çalışmada bilgi sistemleri denetimi ve kontrolleri konusunda temel bilgilere değinilmiş, iç kontrol çalışanları ve denetçilerin bu konuya dikkatleri çekilmek istenmiştir. Önümüzdeki yıllarda önemi çok daha artacak olan bu konu hakkında bilgi sahibi olan ve çalışma yapmış denetçilere olan ihtiyaç da artacaktır. Özellikle ISACA tarafından verilen ve tüm dünyada geçerliliği olan CISA, CISM, (Certified Information Security Manager - Sertifikalı Bilgi Güvenliği Yöneticisi) gibi sertifika sahibi denetçiler aranır olacaktır.

Günlük faaliyetlerini gerçekleştirmek için bilgi teknolojileri ve bilgi sistemlerini kullanan işletmeler, bu faaliyetlere ilişkin kontrollerin uygulanmasında da bilgi sistemlerini kullanacaktır. Bu durum kontrol düzenlemelerinde farklılıklara neden olmuştur. Bilgi teknolojilerinin kullanılması, sağladığı faydaların yanı sıra işletmeler için yeni riskleri de beraberinde getirmiştir. Örneğin verilerin kopyalanması, kullanıcı yetkilendirme gibi konular bilgi sistemleri ile işletmeler için yeni riskler olarak ortaya çıkmıştır. İşletme bilgi sistemi risklerini iyi anlamalı ve bu riskler için gerekli kontrol

tedbirlerini almalıdır. Bu kapsamda işletme, geleneksel iç kontrol düzenlemelerin yanı sıra bilgi sisteminde genel ve uygulama kontrollerini de düzenlemeli ve etkinliğini denetlemelidir. Bu konuda işletmeler, uluslarası meslek örgütlerince bilgi sistemi denetimi ile ilgili düzenlenmiş standartlar ve rehberlere uygun çalışmalarda bulunmalıdır.

Bilgi sistemlerinin işletme faaliyetlerini destekleme ve ihtiyaçlarına cevap verebilmesi, iş sürekliliğin sağlanması için bilgi teknolojileri genel kontrolleri iyi kurgulanmalı ve sürekli denetlenmelidir. Özellikle bilgi sistemlerine bağlı süreçlerin bir anlık durması işletmeler için ciddi kayıplara neden olabilir. Bu nedenle işletmelerin bu kontrolleri tüm süreçleri kapsayacak şekilde planlamalı, etkinliğini test edip gerekli güncellemeleri devamlı yapmalıdır.

Uygulama kontrolleri her işletme ve kullandığı uygulama için farklılık göstermektedir. İşletme uygulama kontrollerini planlarken iş süreçlerini ve bu süreçlerde kullandığı uygulamaları detaylı olarak ele alıp incelemelidir. Özellikle planlanan kontrol düzenlemesinin uygulamada yapılabilirliği dikkate alınmalıdır. Uygulama tarafında mümkün olmayan bir kontrol planlanması fayda sağlamayacağı gibi süreçteki diğer kontrollerin varlığını da etkileyecektir. Bu nedenle işletme uygulama kontrollerine ilişkin çalışmaları hem süreçleri hem de uygulamayı iyi bilen kişiler ile yapmalıdır.

Uygulama kontrollerinde işletmenin fayda maliyet analizi yapması da gerekmektedir. Örneğin veri girişi esnasında planlanan kontrollerin veri giriş süresini olağandan çok daha fazla artırması veyahut veri girişini imkânsız hale getirmesi iş sürecini tıkayacaktır. Bu tür durumlarda alternatif kontroller düşünülmeli sürecin sonraki aşamalarında kontroller planlanmalıdır. Gerektiğinde önleyici kontroller yerine, tespit edici veyahut düzeltici kontroller kullanılması düşünülmelidir.

İşletmenin mali tablolarına kaynaklık eden hareketlerin kaydedildiği bilgi sistemlerinin güvenilirliği bu tablolara olan güven derecesini etkileyecektir. Bu nedenle işletme bilgi sistemlerinin standartlar çerçevesinde denetlenmiş olması gerekmektedir. Denetçi bilgi sistemlerinde, verinin giriş, işleme ve çıktı aşamalarında doğru, eksiksiz ve uygun olarak işlendiğinden emin olmalıdır. Bu nedenle denetçi bilgi sistemlerini ve

işleyişini anlayacak derecede tanımalı, gerektiğinde detaylı denetim konuları için uzman kişilerden yardım almalıdır.

Günümüzde bilgisayarsız bir denetim imkansız hale gelmiştir, denetim çalışmasının daha etkin olması ve daha kısa sürede tamamlanması için denetçinin bilgisayar destekli denetim tekniklerinden faydalanması gerekmektedir. Genelleştirilmiş denetim yazılımları ve genel amaçlı uygulamalardan faydalanan denetçi hem tüm verilerin denetimini yapmış olacak hem de etkin analiz teknikleri ile kısa sürede denetimini tamamlayacaktır. Bu çalışmanın son bölümünde de anlatılan örnek raporlamalarla ulaşılan sonuçların bilgisayar kullanılmadan elde edilmesi çok uzun zaman alacak bazen de neredeyse imkansız olacaktır.

KAYNAKÇA

Kitaplar

BAGRANOFF, N. A.. SIMKIN, M. G. ve NORMAN, C. S. (2011) **Core Concepts of Accounting Information Systems**.USA: John Wiley & Sons Inc.

BELLINO, C. WELLS, J. ve HUNT, S. (2007). **Global Technology Audit Guide 8 – Auditing Application Controls**. USA: The Institute of Internal Auditors.

ERHAN, D. U. (Ocak 2009). BDDK Tebliği Çerçevesinde Bilgi Sistemleri Kavramının İrdelemesi ve Güncel Gelişmeler. **Muhasebe ve Denetime Bakı˙ Dergisi**. s.91.

DURUCASU, H. vd. (2012). **İ˙letme Bilgi Sistemleri**. Eskişehir: Anadolu Üniversitesi Yayınları.

GÜREDİN, E. (2012).**Denetim ve Güvence Hizmetleri SMMM ve YMM' lere Yönelik İlkeler ve Teknikler**. İstanbul: Türkmen Kitabevi.

ÖZBEK, Ç. (2012). **İç Denetim, Kurumsal Yönetim, Risk Yönetimi ve İç Kontrol**. İstanbul: TİDE Yayınları.

O'BREIN, J. A. ve MARAKAS G. M. (2007). **Manegement Information Systems**, **(10. Edition)**. New York: The McGraw-Hill Companies.

LAUDON, K. C. ve LAUDON, J. P. (2012) **Manegement Information Systems Managing The Digital Firms**. New Jersey: Pearson Education..

LEZKİ, Ş. vd. (2012). **İ˙letme Bilgi Sistemleri**. Eskişehir: Açıköğretim Fakültesi Yayınları.

SÜRMELİ, F.. ERDOĞAN, M. ve ERDOĞAN, N. (2005). **Muhasebe Bilgi Sistemi**. Eskişehir: Anadolu Üniversitesi Yayını.

MAR, S. vd. (2012). **Global Technology Audit Guide 1 – Information Technology Controls**. (2rd ed). USA: The Institute of Internal Auditors.

SENFT, S. GALLEGOUS, F. (2009). **Information Technology Control and Audit**. Newyork : Auerbach Publications.

Computer Audit Guidelines. (2002). London: CIPFA, The Chartered Institute of Public Finance and Accountancy.

HALL, J.A. (2011). **Information Technology Auditing and Assurance.** (3rd ed) USA:Cengage Learning Inc.

HALL, J.A. (2011). **Accounting Information Systems**. (7rd ed). USA:Cengage Learning Inc.

ERDOĞAN M. vd. (2012). **Denetim**. Eskişehir:Anadolu Üniversitesi Yayınları.

ÖZTÜRK, Y. (2010). **Uluslararası Eğitim Bildirileri El Kitabı – IFAC**. Ankara:TURMOB Yayınları.

Makaleler

TOPKAYA, A. (2011). Bilişim Sistemleri Denetiminde Sayıştay Modeli. **Dı˙ Denetim**, (3), 118-130.

ÖZBİLGİN İ. G. (2003). *Bilgi Teknolojileri Denetimi ve Uluslararası standartlar.* **Sayı˙tay Dergisi**, (49), 123-128.

EMİNAĞAOĞLU, M. ve YILMAZ G. (2009). *Bilgi Güvenliği Nedir Ne Değildir, Türkiye'de Bilgi Güvenliği Sorunları ve Çözüm Önerileri*. **Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, 11 (4), 1-14.

TEKEREK, M. (2008). *Bilgi Güvenliği Yönetimi*. **KSÜ Fen ve Mühendislik Dergisi**, 11 (1), 132-137.

ÇALIŞ, E. Ç. KELEŞ, E. Ve ENGİN, A. (2014). *Hilenin Ortaya Çıkartılmasında Bilgi Teknolojilerinin Önemi ve Bir Uygulama*. **Muhasebe ve Finansman Dergisi**, (64), 93-108.

ELİTAŞ, C. KARAGÜL, A. A. (2010). *Bilgisayar Destekli Denetim Teknikleri*. **Afyon Kocatepe Üniversitesi Sosyal Bilimler Dergisi**, 2 (2), 145-160.

KİRACI M. (2004). *Bir Bilgisayar Destekli Denetim Tekniği Olarak Paralel Simulasyon Tekniği*. **Mali Çözüm Dergisi**, (68), 145-155.

TAŞKIN, K. (2011). *Yolsuzluğun Tespit ve Önlenmesinde Bilgisayar Destekli Denetim Teknikleri*. **3. Ulusal Kurumsal Yönetim, Yolsuzluk, Etik ve Sosyal Sorumluluk Konferansı**.

ERHAN D. E. (2009). *BDDK Tebliği Çerçevesinde Bilgi Sistemleri Kavramının İrdelemesi ve Güncel Gelişmeler*. **Muhasebe ve Denetime Bakı˙ Dergisi**,91-110.

SELVİ, Y. TÜREL, A. ve ŞENYİĞİT, B. (2005). *Elektronik Bilgi Ortamlarında Muhasebe Denetimi*. **7. Muhasebe Denetimi Sempozyumu - Nisan 2005, İstanbul.**

T.C. Sayıştay. (2013). **Bili˙im Sistemleri Denetim Rehberi**. Ankara: Sayıştay Yayınları.

YARAR, E. (2011). **Bilgisayar Destekli Denetim Teknikleri Kurs Notları**, Ankara: Sayıştay Yayınları.

Tezler

AKYOL, F. (2013). *Cobit Uygulayan Şirketlerde Bilgi Güvenliği Politikalarının Şirket, Personel ve Süreçleri Etkileri*. Yayınlanmamış Yüksek Lisans Tezi. Beykent Üniversitesi Sosyal Bilimler Enstitüsü.

TERAMAN, Ö. (2011). *Elektronik Bilgi Ortamında Bilgi Ortamında Bilgisayarlı Denetim Programları Aracılığı ile Muhasebe Denetimi ve CAP Uygulaması*. Yayınlanmamış Yüksek Lisans Tezi. Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü.

YALKIN L. D. (2011). *Bilgi Teknolojileri Denetimi.* Yayınlanmamış Doktora Tezi. Ankara Üniversitesi Sosyal Bilimler Enstitüsü.

GÜRKAN, S. (2008). *Bilgisayar Destekli Denetim Tekniklerinin (BDTT) Muhasebe Denetimine Etkileri ve Türkiye'dki Bağımsız Denetim Kuruluşlarının BDTT Uygulamalarına İlişkin Bir Araştırma*. Yayınlanmamış Yüksek Lisans Tezi. Karaelmas Üniversitesi Sosyal Bilimler Enstitüsü .

İnternet Kaynakları

COBIT 5.1. 25 Ocak 2015, http://www.isaca.org/COBIT/Pages/default.aspx

Kamu İç Kontrol Rehberi. (07 Şubat 2014). 29 Aralık 2014, http://www.bumko.gov.tr/Eklenti/8227,kamuickontrolrehberi1versiyon12.pdf?0

Türkiye İç Denetim Enstitüsü. **İç Denetim Standartları Terimler Sözlüğü**. 12 Ocak 2015, http://www.tide.org.tr/uploads/IcDenetimTerimlerSozlugu.pdf

Kamu Gözetim Kurumu. Bağımsız Denetim Standardı 315, İşletme ve Çevresini Tanımak Suretiyle "Önemli Yanlışlık" Risklerinin Belirlenmesi ve Değerlendirilmesi. 12 Ocak 2015, http://www.kgk.gov.tr/contents/files/BDS/BDS_315.pdf

431 Sıra No'lu Vergi Usul Kanunu Genel Tebliği, 10 Aralık 2014, http://www.gib.gov.tr/index.php?id=1079&uid=dmPFSoYSC7YfpYzQ&type=teblig

International Federation Of Accountants (IFAC). International Standards on Auditing. 15 Ocak 2015, http://www.iaasb.org/publications-resources

KUZU D. A. Bilgi Sistemleri Denetimi. 10 Ocak 2015, http://kgk.gov.tr/contents/files/dalikuzusunum.pdf

Information Systems Audit and Control Association. 01 Nisan 2014, http://www.isaca.org

Türkiye İç Denetim Enstitüsü. İç Denetim Standartları. 10 Mayıs 2014, http://www.tide.org.tr/uploads/UMUC_2013.pdf

ACFE, Report To The Nations On Occupational Fraud And Abuse, 06 Ocak 2015, http://www.acfe.com/rttn/docs/2014-report-to-nations.pdf

Ulusal Bilgi Güvenliği Kapısı. Hakkımızda. 24 Aralık 2014, https://www.bilgiguvenligi.gov.tr/hakkimizda.html

Türk Standartları Enstitüsü. 24 Aralık 2014, http://www.tse.org.tr/tr/Default.aspx

Audit Trails. 12 Mayıs 2015, http://csrc.nist.gov/publications/nistbul/itl97-03.txt

Data Analysis. 01 Nisan 2015, http://en.wikipedia.org/wiki/Data_analysis

IIA Uluslararası İç Denetim Standartları. 01 Nisan 2015, http://www.tide.org.tr/uploads/UMUC_2013.pdf

Fuzzy Matching. 02 Nisan 2015, http://www.techopedia.com/definition/24183/fuzzy-matching

Türkiye İç Denetim Enstitüsü. İç Denetim Standartları Terimler Sözlüğü, 12 Ocak 2015, http://www.tide.org.tr/uploads/IcDenetimTerimlerSozlugu.pdf

Kamu Gözetim Kurumu. Bağımsız Denetim Standardı 315, İşletme ve Çevresini Tanımak Suretiyle "Önemli Yanlışlık" Risklerinin Belirlenmesi ve Değerlendirilmesi.
12 Ocak 2015, http://www.kgk.gov.tr/contents/files/BDS/BDS_315.pdf

Resmi Yayınlar

5018 Sayılı Kamu Mali Yönetimi ve Kontrol Kanunu. Resmi Gazete, Tarih :24.12.2003 Sayı : 25326

BDDK, Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ, Resmi Gazete, Tarih : 14.09.2007 Sayı: 26643.

431 Sıra No'lu Vergi Usul Kanunu Genel Tebliği, Resmi Gazete Tarih: 29.12.2013 Sayı:28866