YILDIZ TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİ TEKNOLOJİLERİ YÖNETİŞİM YÖNTEMLERİ VE COBIT İLE ULUSAL BİR BANKADA UYGULAMASI

Endüstri Müh. Emine HACISÜLEYMANOĞLU

FBE Endüstri Mühendisliği Anabilim Dalı Sistem Mühendisliği Programında Hazırlanan

YÜKSEK LİSANS TEZİ

Tez Danışmanı: Prof. Dr. Hüseyin BAŞLIGİL (YTÜ)

İSTANBUL,2010

İÇİNDEKİLER

Sayfa

KISALTMA LİSTESİ

ITIL : Bilgi Teknolojileri Altyapı Kütüphanesi

COBIT : Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri

CMMI : Entegre Yetenek Olgunluk Modeli

ISO : Uluslararası Standartlar Organizasyonu

COSO : Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi (Committee of Sponsoring Organizations of the Treadway Commission)

PMI : Project Management Institute – Proje yönetimi Enstitüsü

BT : Bilgi Teknolojileri

TBD : Türkiye Bilişim Derneği

CEO : Genel Müdür

IT : Bilgi Teknolojileri

BDDK : Bankacılık Düzenleme ve Denetleme Kurumu

SOX : Sarbanes Oxley

CFO : Finans Müdürü

CIO : Bilgi Teknolojileri Yöneticisi

ITGI : Bilgi Teknolojileri Yönetişim Enstitüsü

ISACA : Bilgi Sistemleri Denetim Kontrol Birliği

PO : Planlama ve Organizasyon

AI : Tedarik ve Uygulama

DS : Hizmet Sunumu ve Destek

ME : İzleme ve Değerlendirme

CMM : Yetenek Olgunluk Modeli

YOM : Yetenek Olgunluk Modeli

BTYS : Bilgi Teknolojileri Yönetim Sistemi

PCAOB : Özel Şirketler Muhasebe Gözetim Kurulu

AICPA : Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü (The American Institute of Certified Public Accountants)

GAO : Amerikan Genel Muhasebe Ofisi (Government Accountability Office)

CMDB : Konfigürasyon Yönetimi Veri Tabanı

ŞEKİL LİSTESİ

Sayfa

ÇİZELGE LİSTESİ

Sayfa

ÖNSÖZ

Ülkemizde Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) nun 2003 yılında başlattığı çalışmalar sonucu ulusal bankalara uygulanmakta olan denetim standardı olan COBIT ve diğer Bilgi Teknolojileri denetim ve kontrol yöntemleri bu çalışmada anlatılmıştır.

Risk Yönetimi ve Teknoloji Yönetimi konularına da yer verilen çalışmanın sonunda Halkbank Bilgi Teknolojilerinde uygulanan yönetim süreçlerinden ikisi için yapılan bir denetim ve sonuçları paylaşılmıştır. Bu çalışmalar esnasında Halkbank Bilgi Teknolojileri Kalite ekibinden arkadaşım Nevzat Yeğin'e yardımlarından ötürü, değerli yöneticilerime de yüksek lisans eğitimim süresince gösterdikleri anlayış için teşekkürü bir borç bilirim.

Çalışmalarım boyunca, değerli görüş ve katkılarıyla bana her konuda yardımcı olan tez danışmanım Prof.Dr. Hüseyin BAŞLIGİL'e sonsuz teşekkürlerimi sunarım.

Bu çalışmayı hazırladığım süre boyunca içten destekleriyle beni yalnız bırakmayan aileme ve ihtiyaç hissettiğim her an yanımda olan sevgili eşim Mehmet Kurt'a teşekkür ederim.

ÖZET

Bilgi Teknolojisi, bilgi ekonomisinde ve oluşumların operasyonel ve finansal yönetim merkezinde başarıya ulaşılmasında önemli bir faktördür. Bunun sonucunda artık, kurumsal yönetişim ve BT yönetimi ayrık ve farklı bir disiplin olarak ele alınamaz. Etkin bir kurumsal yönetim bireysel ve gruplar dahilinde uzmanlaşmaya ve yeteneklere odaklanır, performans ölçümleri ve takibini yapar ve de kritik sorunlar için güvence sağlar. Uzun zamanlar kurum stratejilerini mümkün kılan yalıtılmış bir süreç olarak değerlendirilen BT artık sözü edilen stratejinin ayrılmaz bir parçasıdır.

BT yönetimi, BT süreçleri, kaynakları ve bilginin kendisi ile kurum stratejileri ve amaçları arasındaki yapısal bağlantıları sağlar. BT performansının optimum yollarının entegrasyonu ve kurumsallaştırılması, sahip olma ve implementasyonu, ulaştırma ve destek hizmetleri, denetlenmesi ve değerlendirilmesini BT yönetimi üstlenir. Başarılı bir kurumsal yönetimin ayrılmaz bir parçası olan BT yönetimi, bunu ilgili kurumsal süreçler için ölçülebilir, etkili ve verimli olan iyileştirmeler ile yapmaktadır. BT yönetimi kurumların sahip oldukları bilgiden tam verim almalarını, dolayısıyla maksimum fayda sağlanmasını, rekabet gücü kazanmalarını ve fırsatlar üzerine yatırım yapmalarını mümkün kılar.

Bu çalışmada BT Yönetimi için BDDK nın da benimsediği denetleme yöntemi olan COBIT anlatılmış ve uygulama kapsamında Halkbankasında kullanılmakta olan BT Yönetim Süreçlerinin Gözden Geçirme çalışmalarının bir kısmı paylaşılmıştır.

Anahtar Kelimeler: BT denetimi, BDDK, COBIT, ITIL, ITSM

ABSTRACT

Information technology is an important factor in achieving success in the information economy and central to an entity's operational and financial management. As a result, enterprise governance and IT governance can no longer be considered separate and distinct disciplines. Effective enterprise governance focuses individual and group expertise and experience where it can be most productive, monitors and measures performance, and provides assurance to critical issues. IT, long considered solely an enabler of an enterprise's strategy, must now be regarded as an integral part of that strategy.

IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. IT governance integrates and institutionalises optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring and evaluating IT performance. IT governance is integral to the success of enterprise governance by assuring efficient and effective measurable improvements in related enterprise processes. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

COBIT, the auditing method for the IT governance which is adopted in principle by the BDDK has been studied with in the scope of the thesis implementation of the IT governance processes revision.

Keywords: IT Audit, BDDK, COBIT, ITIL, ITSM,

1. GİRİŞ

Sürdürülebilir kurumsallık ve toplumsal gelişimin güvencesi olarak ifade edilen kurumsal yönetim; adillik, şeffaflık, hesap verebilirlik ve sorumluluk ilkeleri ile dünyada olduğu gibi Ülkemizde de öncelik teşkil etmekte ve hayata geçirilmesi yönünde çaba sarf edilmektedir.

Kurumsal Yönetim İlkelerinin uygulamada yaygınlık kazanması, yatırım ortamının iyileştirilmesi, ekonomik istikrarın ve rekabet eşitliğinin sağlanması gibi sonuçlarıyla ekonomik kalkınmaya destek olacaktır.

Kurumsal Yönetim, şirketler için kurumsal varlıklarının sürdürülebilirliği, ülkemiz ekonomisi için ise sürdürülebilir ekonomik kalkınmanın sağlanmasında güvence oluşturmaktadır.

Artan kurumsal BT yönetişimi, sorunları, güvenlik tehditleri, veri kalitesi konuları ve gizlilikle ilgili mevzuatla birlikte, günümüzde kuruluşlar bilgilerin bütünlüğünü, gizliliğini ve kullanılabilirliğini hiç olmadığı kadar güvence altına alma ve temelini oluşturan sistemleri koruma ihtiyacı içindedirler. İş süreçleri, bilgisayar uygulamaları ve sistemlerle ilgili kontrollerin uygulanması ve dengelerin kurulması bu risklerin azaltılmasına yardımcı olabilir.

Bilgi sistemleri kullanımının iş hayatında yaygınlık kazanması ile artan önemi BT denetimi konusunu ön plana çıkarmıştır. Bankalarda kullanılan yazılım ve donanımın, bilgi sistemi süreçlerinin, mali veri üretiminde kullanılan bilgi sistemi ve süreçlerinin ve ilgili iç kontrollerin değerlendirilmesi amacıyla BDDK tarafından bilgi sistemleri denetimine ilişkin yayınlanan yönetmelikle BT denetimi bankacılıkta yasal bir zorunluluk haline gelmiştir.

2. DENETİM KAVRAMI

Denetim kavramının, Batı dillerindeki karşılığı (audit) kökenini oluşturan Latince audire kelimesi; işitmek, dikkatlice dinlemek anlamına gelmektedir.

Denetim kavramı ile ilgili olarak, sosyal bilimlerin birçok dalında farklı tanımlamalar yapılmaktadır. Denetimin Türkçe'de yaygın olarak kullanılan anlamı, Türk Dil Kurumunun yaptığı tanımda karşılığını bulmaktadır. Bu tanıma göre, "denetleme, bir işin doğru ve yönetime uygun olarak yapılıp yapılmadığını incelemek, murakabe etmek, teftiş etmek, kontrol etmektir." Hukuki anlamda denetleme ise "gerek devlet daire ve teşkilatının ve gerek özel hukuk hükümlerine göre kurulmuş müesseselerin kamu menfaati noktasından kanun, nizamname ve statüleri hükümlerine göre çalışıp çalışmadıklarının tetkik edilmesidir."

Avrupa Komisyonu da denetimin tanımını yapmıştır. Bu tanıma göre en genel anlamıyla denetim, bir işlem, prosedür veya raporun her bir yönünü doğrulayacak şekilde ve sonradan yapılan her türlü incelemedir.

2.1 Denetim İle İlgili Uluslar Arası Kuruluşlar

2.1.1 IIA (İç Denetçiler Enstitüsü)

İç Denetçiler Enstitüsü, kurumsal ve kamusal örgütlerin boyutlarının ve karmaşıklığının artması sonucu ortaya çıkan iç denetimdeki büyümeye ve yeni yönetsel ihtiyaçlara cevap olarak 1941 yılında New York'ta kurulmuştur. Enstitü, 1944'de Toronto'da ABD dışındaki ilk birliğini, 1948'de de Londra'da Avrupa'daki ilk birliğini kurmuştur.

IIA, günümüzde dünya çapındaki yaklaşık 90,000 üyesine iç denetim, iç kontrol, BT denetimi gibi konularda hizmet vermektedir. Ayrıca enstitü, iç denetime ilişkin standartların ve etik kuralların belirlenmesi ve geliştirilmesi konusunda katkılarda bulunmaktadır. Enstitü tarafından verilen İç Denetçi Sertifikası tüm dünyada geçerli bir belge niteliğindedir.

2.1.2 INTOSAI (Uluslararası Yüksek Denetleme Kuruluşları Örgütü)

Birleşmiş Milletlere ya da Birleşmiş Milletlerin uzmanlık kuruluşlarına üye ülkelerin yüksek denetim kuruluşlarının üye olduğu bir teşkilattır. 1953 yılında kurulmuştur. Türk Sayıştay'ı 1965 yılından bu yana INTOSAI üyesidir. Örgütün amacı; yüksek denetleme kurumları arasındaki ilişkileri geliştirerek güçlendirmektir.

2.1.3 COSO (Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi)

Treadway Komisyonu olarak bilinen Sahte Mali Raporlama Ulusal Komisyonu, 1985 yılında kurulmuştur. Treadway Komisyonunun en önemli hedefi; sahte mali raporların nedenlerini belirlemek ve meydana gelme olasılığını azaltmaktır. Komisyonunun himayesinde iç kontrol literatürünün yeniden gözden geçirilmesi için bir çalışma grubu oluşturulmuş, sponsor kurumların iç kontrol sisteminin kurulması ve etkinliğinin değerlendirilmesi için genel kabul görecek standartlar belirleyen bir projeyi üstlenmesi kararlaştırılmıştır. Bu amaçla Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi "İç Kontrol Bütünleşik Çerçeve" raporu nu 1992'de yayımlamıştır. Bu rapor, COSO iç kontrol modeli olarak bilinmektedir. COSO iç kontrol modeli, Avrupa Birliği ülkeleri başta olmak üzere birçok gelişmiş ülkeye ilham kaynağı olmuştur.

COSO Modeli iç kontrol sistemlerine ilişkin standartların temelini oluşturmaktadır. Bir iç kontrol modeli olan COSO, İç Denetçiler Enstitüsü tarafından yayımlanan 'İç Kontrole İlişkin İşletme Raporunun Hazırlanmasında İç Denetçilerin Rolü' başlıklı Raporda belirtildiği şekilde, denetim sürecine dahil edilmiş bir modeldir. Modele göre iç kontrol sisteminin ana hedefleri; Organizasyonun etkin ve etkili işler yapmasını, güvenilir mali raporlar hazırlamasını ve mevzuata uyumunu sağlamaktır.

COSO Modeli; kontrol ortamı, risk değerlendirme, kontrol faaliyetleri, bilgi ve iletişim ile izleme olmak üzere beş unsurdan oluşmaktadır.

Kontrol Ortamı: Yönetim ve çalışanlar bütün bir örgüt içinde, iç kontrole ve dikkatli bir yönetime yönelik olarak pozitif ve destekleyici bir tavrı geliştiren ortamı oluşturmalı ve sürdürmelidirler.

Risk değerlendirme, amaçlara ulaşılırken karşılaşılabilecek risklerin tanımlanıp analiz edilmesi ve risklerin ne şekilde yönetilmesi gerektiğine karar vermek için bir temel oluşturulmasıdır.

Kontrol Faaliyetleri, yönetimin talimatlarının yerine getirilmesini sağlamaya yardımcı olan politikalar ve yöntemlerdir. Kurumun hedeflerine ulaşırken karşılaştığı riskleri işaret etmek için gerekli önlemlerin alınmasını sağlamaya yardımcı olur.

Bilgi ve İletişim: Uygun bilgi, kişilerin sorumluluklarını yerine getirebilmelerini sağlayacak şekilde tanımlanmalı, elde edilmeli ve paylaşılmalıdır. Etkili iletişim, kurumun en altından en üstüne dolaşacak şekilde geniş anlamda gerçekleşmelidir. Tüm çalışanlara iç kontrol sistemindeki rolleri anlatılmalıdır.

İzleme: İç kontrol izlemesi zaman dilimi içindeki performansın kalitesini değerlendirmeli ve denetim ya da diğer inceleme bulgularının derhal çözüme bağlanmasını güvence altına almalıdır.

2.1.4 ISACA (Bilgi Sistemleri Denetimi ve Kontrolü Derneği)

ISACA, 1967'de bilgisayar sistemleri denetimi işi ile uğraşan küçük bir grup tarafından, merkezi bir bilgi kaynağı ve rehberlik ihtiyacına cevap olarak tasarlanmış ve 1969'da EDPAA (Elektronik Bilgi İşlem Denetçileri Derneği) adıyla Los Angeles'da kurulmuştur. 1976'da bir eğitim vakfı kurarak bilgi teknolojileri yönetimi ve kontrolü alanlarında geniş ölçekli araştırma çalışmaları yürütmeye başlamıştır.

Günümüzde ISACA, 100'den fazla ülkede 35,000'den fazla üyeye sahiptir ve yaklaşık 60 ülkede temsilcilikleri bulunmaktadır.

ISACA'nın yayınladığı bilgi sistemleri denetimi ve bilgi sistemleri kontrolü standartları tüm dünyadaki uygulayıcılar tarafından benimsenmiştir. Ayrıca verdiği Bilgi Sistemleri Denetçisi sertifikası tüm dünyada geçerli bir belge niteliğindedir.

2.2 İç Denetim Türleri

Uygulamada, iç denetim beş temel faaliyet alanını kapsar. Bu faaliyetler mali denetim, uygunluk denetimi, performans denetimi, sistem denetimi ve bilgi teknolojileri denetimidir.

Mali denetim, mali raporlardaki verilerin, denetlenen birimin varlık ve yükümlülüklerinin gerçek değeriyle, finansman kaynaklarıyla, varlıklarının yönetimiyle ve tahsis edilen bütçe ödenekleriyle uyumlu olup olmadığının değerlendirilmesidir. Yapılan denetimde çok sayıda işlemsel kusur tespit edilirse kayıtların doğruluğu, mevzuata uygunluğu ve düzenliliği üzerine daha fazla hesap denetimi yapılmasında yarar vardır.

Uygunluk denetimi, bir örgütün mali işlemlerinin ve diğer faaliyetlerinin belirlenmiş yöntemlere, kurallara ve mevzuata uygun olup olmadığını belirlemek amacıyla incelenmesidir. Bu denetim türünde belirlenmiş kriterler farklı kaynaklar tarafından oluşturulur. Uygunluk denetimi, iç denetçiler ve dış denetçiler ile kamu denetçileri tarafından yürütülür. Bu tür denetimin yürütümü göreli olarak daha kolay olduğundan daha az deneyimli denetçiler tarafından yerine getirilmesi mümkündür.

Uygunluk denetimi üst makamlar ve yasal mevzuat tarafından önceden saptanmış kurallara uyulup uyulmadığının araştırılmasıdır. Bu üst makamlar kuruluş içinden olabileceği gibi kuruluş dışından da olabilir. Uygunluk denetiminde ulaşılan sonuçlar geniş bir kitleye değil,

sınırlı olarak ilgili ve yetkili kişi ve kuruluşlara raporlanır. Bu nedenle uygunluk denetimi çoğunlukla iç denetçiler tarafından, gerekli durumlarda ise dış denetçiler tarafından yapılır.

Performans denetimi, kurum ya da kuruluşun görevlerini yerine getirirken kullandığı fiziki, mali ve beşeri kaynakların ekonomiklik, etkinlik ve verimlilik derecelerinin değerlendirilmesidir. Bu değerlendirme yapılırken, riske dayalı maliyet unsuru ile kaynakların etkin ve etkili şekilde kullanımı göz önünde bulundurulmalıdır. Uygulama zorluğu dolayısıyla bu denetimin kıdemli denetçiler tarafından yerine getirilmesi daha doğru olur.

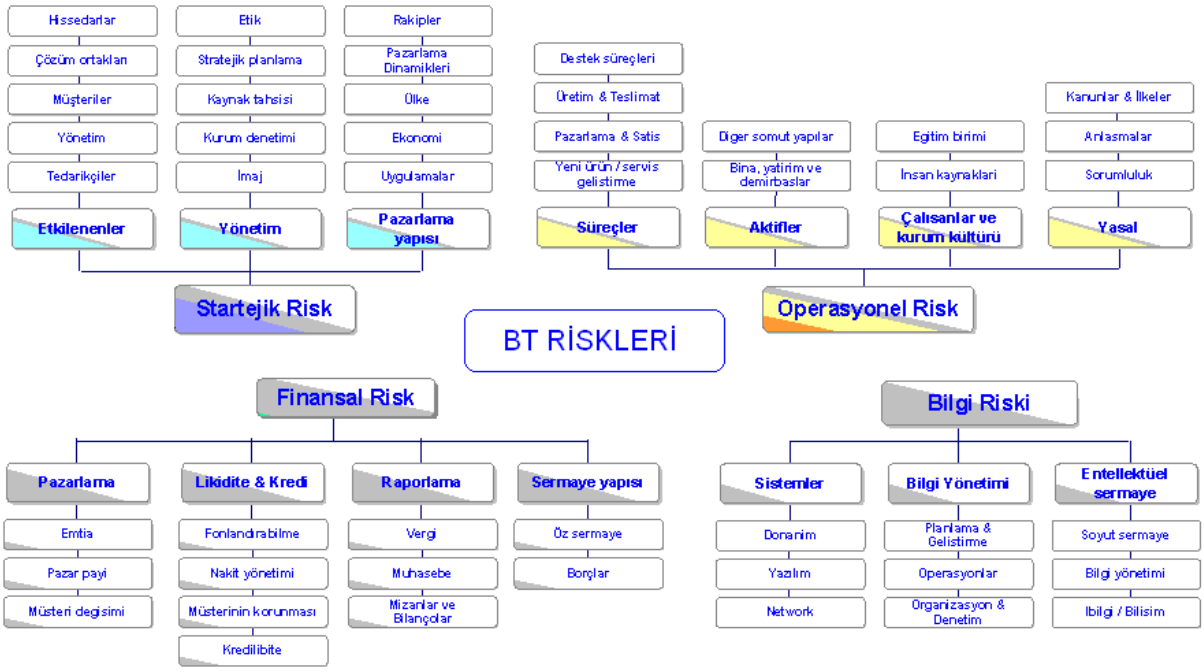
Sistem denetimi, denetlenen birimin mali yönetim usullerinin eksikliklerini tespit etme ve giderme konusunda etkili olup olmadığının değerlendirilmesidir. Sistem denetimi ayrıca mali işlemlerin ekonomiklik, etkinlik ve verimliliklerinin yanı sıra genel bağlayıcı hukuki düzenlemeler ve iç yönergelerle uyumunu inceler.

Bilgi sistemleri denetimi, denetlenen birimin bilgi sistemlerinin güvenli olup olmadığının değerlendirilmesidir. Bu denetim türü ayrıca denetlenenin bilgi sisteminde depolanan veri ve bilgilerin yeterliliğini ve doğruluğunu değerlendirmek için kullanılır. Bilgi sisteminin güvenliği, depolanmış bilgilerin yanlış kullanılmasının, zarara uğratılmasının ya da yok edilmesinin önlenme derecesi olarak tanımlanabilir.

İç denetçi, değerlendirmeye tabi tutacağı ve inceleyeceği iç yönetim ve kontrol faaliyetinin içerisinde yer almamalıdır. Buna karşın, hazırlanan bir faaliyet ya da programa ilişkin sistem ve prosedürler temelinde bir ‘ön denetim’ faaliyeti yürütebilmesi ya da fikir beyan etmesi beklenecektir. Ancak iç denetim, asla devamlı surette iç kontrol faaliyetinin bir parçası haline gelmemelidir. İç denetimin iç kontrol faaliyeti ile mesafeli olması oldukça önemlidir. Bu sayede yönetim, taşıdığı iç kontrol sorumluluğunun farkında olabilecek ve etkin bir iç kontrol faaliyeti oluşturma ve sürdürme konusunda gerekli girişimlerde bulunabilecektir.

2.3 Bilgi Teknolojileri Denetimi

Bilgi teknolojileri sistemleri de diğer sistemlerde olduğu gibi dışarı ile temas halinde oldukları için bir takım risklerle karşı karşıyadırlar. Şekil 2.1 de bilgi sistemlerinde karşılaşılabilen riskler görülmektedir.



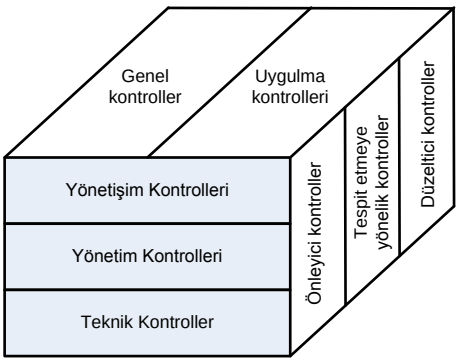
Şekil 2.1 Bilgi sistemlerinde karşılaşılabilen riskler

Bilgi Tekonolojileri denetimi bu riskleri ve derecelerini belirlemek ve önlem almak için sistemin bir takım özelliklerinin belirlenmiş standartlara uygunluğunun kontrol edilmesidir.

Kurumun bilgi sistemleri temel olarak aşağıdaki özellikler açısından kontrol edilir.

- İlgili kanunlara, mevzuata, kurumun hedef ve amaçlarına uygunluk ve tutarlılık;
- Faaliyetlerin yönetimin kurumsal yönetim politikalarına uygun ve kurumun risk alma isteğine uygun ve tutarlı olduğuna dair güvenilir kanıtlar (makul güvence) için kendi çerçevesini oluşturmak ve kaydetmek.

2.3.1 Bilgi Teknolojileri Denetimi Sınıflandırması



Şekil 2.2 BT denetimi sınıflandırması

Şekil 2.2 de görülebileceği üzere BT denetimini çeşitli sınıflandırmalara tabi tutmak

mümkündür.

Denetim çalışmalarının en başında gelen ve temelinde yatan sistemin teknik açıdan denetlenmesidir. Teknik açıdan değerlendirilen sistemin bu defa yönetim açısından değerlendirilmesi gerekecektir. Yönetim açısından da değerlendirildikten ve sonuç olumlu çıktıktan sonra sırada yönetişim açısından değerlendirme gerekecektir. Yine bunun gibi kontrolleri değişik özelliklerine göre sınıflandırmak mümkün olacaktır. Bankacılık Düzenleme ve Denetleme Kurumu (BDDK); bu sınıflandırmalar içinde Genel Kontrol ve Uygulama Kontrollerini takip etmektedir.

2.3.2 Bilgi Teknolojileri Denetim Süreci

1. Denetim yaklaşımının belirlenmesi ve planlama.
   - Denetim amacının ve çerçevesinin belirlenmesi.
   - Eldeki bilgilerin değerlendirilmesi
   - Bilinen risklerin değerlendirilmesi
   - Denetim plan ve programının oluşturulması.
2. Denetimin gerçekleştirilmesi.
   - Görüşmeler.
   - Uygunluk incelemesi.
   - Prosedürlerin analitik incelemesi
   - Detaylı testler.
   - Kanıt elde etme.
3. Denetimin sonuçlandırılması
   - Sonuçların değerlendirilmesi.
   - Raporun oluşturulması ve yayınlanması

2.3.3 Bilgi Teknolojileri Denetim Alanları

Kurumun bilgi sistemleri kontrol edilirken bütün olarak sistemin kontrolü değil sistemin belirli bileşenleri teknik açıdan ele alınır. Bilgi sistemleri yapısal olarak 4 ana başlık altında ele alınarak incelenir. Bunlar;

1. Sistem Geliştirme Süreçleri
2. Sistemler Yazılım Kontrolleri
3. Uygulama Kontrolleri

4. Veri Yapıları

Öte yandan bütün olarak bakıldığında, BT denetimi aşağıdaki alanlarda yapılır. Bu 7 alanda yapılan kontrollerin başarı ile tamamlanması gerekmektedir. Böylece kurum bilgi sistemlerinin güvenli olduğundan bahsedebiliriz.

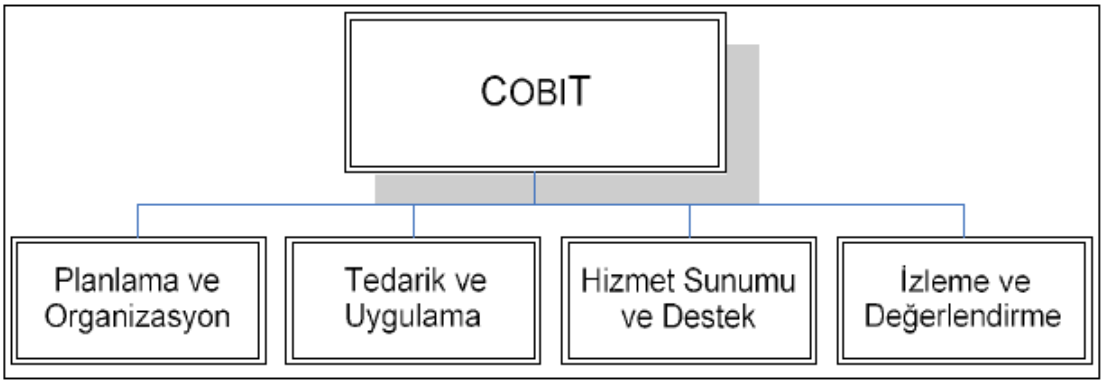
1. Bilgi Teknolojileri Süreçleri
2. Uygulamalar ve modülleri
3. Spesifik yazılımlar, donanımlar, altyapı vb.
4. Belirlenmiş standartlara göre yapılan denetimler.
5. Spesifik konfigürasyonlar.
6. İş süreçleri ile uygulama uygunluğu.
7. Sahtekârlık denetimi.

Denetim alanlarına kurumun yapısına göre yenileri de eklenebilecektir. Daha önce de bahsedildiği üzere; BDDK ya göre Bilgi Sistemleri iç kontrolleri Genel ve Uygulama Kontrolleri olmak üzere iki ana alanda yürütülmektedir.

2.3.3.1 Bilgi Teknolojileri Genel Kontrolleri

BDDK' nin yayınladığı yönetmeliğe göre bir bankanın bilgi sistemi aşağıda belirtilen unsurlar çerçevesinde denetlenmelidir. Gerçekleştirilen her bir kontrol hedefi; uygulanabilirlikleri ölçüsünde bilgi kriterleri, teknoloji kaynakları ve yönetsel ölçütlerin birlikte dikkate alınması suretiyle COBIT çerçevesinde yer alan yöntemlere uygun olarak değerlendirilip derecelendirilmelidir. Yönetsel ölçütlerin varlığı, uygunluğu ve bilgi sistemi gelişimine katkıları, bu hükmün uygulanmasında dikkate alınır ve güvenilir hale getirilmelidir.

COBIT ana kriterleri Şekil 2.3 te görülmektedir.



Şekil 2.3 COBIT Ana Kontrol Hedefleri

2.3.3.2 ,Bilgi Sistemi Uygulama Kontrolleri

BDDK Uygulama kontrolleri, bilgi sistemleri içerisinde yer alan ve bankacılık faaliyetlerini yürütmek veya desteklemek için kullanılan finansal verilerin; tanımlanması, üretilmesi, kullanılması, bütünlüğü, güvenilirliği, erişimi ve yetkilendirme gibi tüm süreçlerin denetlenmesinde kullanılacak kontrolleri kapsar.

Uygulama kontrolleri asgari aşağıdaki unsurları içerir:

- Veri oluşturma ve yetkilendirme
- Bilginin akışı ve uygulamalara girilmesi
- Veri İşleme ve Onaylar
- Üretilen bilgi ve Raporlama

3. ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi)

ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi) operasyonel BT hizmetlerinin verimli ve etkin bir şekilde yürütülmesi için geliştirilmiş kalite yönetim yöntembilimidir (metodolojisidir). ITIL BT hizmetlerinin bütünleşik süreçler olarak yürütülmesinde esas alınacak ilkelere açıklık kazandırır.

ITIL'ın organizasyonlara katacağı değer BT süreçlerinin yapılandırılması, müşteri odaklı bir yaklaşımla maliyetlerin kontrol altına alınabilmesi, ölçülebilir ve daha etkin yönetilen bir yapının ortaya konmasıdır.

BT hizmet yönetimi konusunda kabul görmüş referanslardan biri olan ITIL dünyada de-facto standart olarak benimsenmiş, teoriden çok pratiğe dayalı bir yapı olması ile dikkat çekmektedir. ITIL bazı çalışma şekillerini dikte etmek yerine tavsiyelerde bulunur. BT organizasyonları da bu tavsiyeleri kendilerine adapte ederek en uygun yapıyı tasarlayabilir. İhtiyaçlar ve öncelikler daha kolay belirlenir. Bu öncelikler doğrultusunda bir çalışma planı belirlenir.

ITIL Birleşmiş Krallık Ticaret Ofisi tarafından 1980'li yılların sonlarına doğru geliştirilmiş olan standartlardır. Hazırlanma amacı, Birleşik Krallık hükümetinde BT hizmet yönetimini iyileştirmektir. ITIL, BT hizmetlerini en başarılı yöneten örnek uygulamaları esas alarak oluşturulan, süreçleri entegre olarak anlatan bir dizi yazılı rehberdir.

- Eğitim programı,
- Sertifikalandırması,
- Danışmanlık hizmetleri,
- Yazılım destek programları olan uluslararası bir standarda dönüşmüş durumdadır.

3.1 BT Hizmet Süreçleri

ITIL, BT hizmet yönetimi süreçlerini iki bölümde ele almaktadır.

3.1.1 Hizmet Destek

Hizmet Destek, işlerini desteklemek için müşterilerin uygun BT hizmetlerine nasıl erişebileceklerini tanımlar. Hizmet Destek, müşteri ihtiyaçlarını karşılamak için kullanılan günlük operasyonel hizmet temelini birçok biçimde tanımlar.

Hizmet Destek süreçleri şunlardır:

a) Konfigürasyon Yönetimi

BT teknik altyapısını kontrol etmek, sadece onaylanmış yazılım ve donanımların kullanımını sağlamak.

b) Değişiklik Yönetimi

Her türlü değişikliği etkin şekilde yönetmek

c) Olay yönetimi

İşlevi belirlenen hizmet düzeylerinin sürekliliğini sağlamak, hizmet kesintilerini etkin ve hızlı bir şekilde gidermektir.

d) Problem Yönetimi

İşlevi Hizmet kesintilerini en aza indirmektir.

e) Sürüm Yönetimi

İşlevi; Değişim sürümlerini yönetmek, sürüm dağıtımını otomatikleştirmek ve onaylı yazılımların kullanımını sağlamak.

3.1.2 Hizmet Sunumu

Hizmet Sunumu, BT organizasyonlarının zaruri iş hizmetleri sunmalarına yardım eden beş süreci tanımlar. Doğasında dönüşümsel olan süreçler, kaliteli BT hizmetlerinin planlanması ve sunulmasıyla ilgilidir. Hizmet Sunum süreçleri şunlardır:

a) Hizmet (Seviyesi) Yönetimi

İşlevi; iş hedefleri ve müşteri istekleri doğrultusunda hizmet ve hizmet düzeylerini belirlemek, takip ve kontrol etmektir.

b) Kapasite Yönetimi

İşlevi; BT kaynaklarını verimli ve etkin kullanmaktır.

c) Finansal Yönetim

İşlevi; BT hizmet maliyetlerini hesaplamak, kontrol etmek ve en alt seviyede tutmaktır.

d) Erişilebilirlik Yönetimi

İşlevi; BT hizmetlerinin kullanırlılık düzeylerini en üst seviyede tutmaktır.

e) BT Hizmet Sürekliliği Yönetimi

İşlevi; bir felaket sonrasında hizmetlerin aksamamasını sağlamaktır.

10 süreçten oluşan bu yapıya tüm şirket ve BT organizasyonunu etkileyen Altyapı Yönetimi, Güvenlik Yönetimi süreçleri ile Yardım Masası fonksiyonu eklendiğinde ITIL tamamlanmış olur.

ITIL süreçleri birbirleriyle entegredir ve aralarındaki ilişkiler nettir. Sık yaşanan bir senaryo üzerinde süreçler arasındaki ilişki rahatlıkla görülebilir. Örneğin;

1. Bir şirket elemanı Yardım Masasını arasın ve bir hizmet konusunda yaşadığı sorunları aktarsın.
2. Olay Yönetimi süreci devreye girer, olayı kayıt altına alır.
3. Problem Yönetimi süreci sorunu inceler ve nedenini araştırır. Kapasite Yönetimi süreci bu çalışmaya destek verir. Hizmet Düzey Yönetimi sorunun daha önceden belirlenen sürede giderilip giderilmediğini takip eder. Gerektiği takdirde, Değişiklik Yönetimi süreci devreye girer ve bir değişim talep edilir.
4. Değişiklik Yönetimi süreci değişim talebini takip ve koordine eder.
5. Servis Sürekliliği süreci Değişiklik süreci ile birlikte güncel yedekleme konfigürasyonu ile geri almanın mümkün olup olmadığını kontrol eder.
6. Finansal Yönetim süreci bir üst sürüm maliyetinin çıkarılmasına yardımcı olur.
7. Sürüm Yönetimi süreci, değişim bünyesindeki donanım veya yazılım değişikliklerinin uygulanmasını kontrol eder.
8. Sürüm Yönetimi, Konfigürasyon Yönetimini yeni sürümün detayları ile günceller.
9. Kullanırlılık Yönetimi süreci sürüm değişikliğinin istenen kullanırlılık ve güvenirlilik düzeyini sağlayacağından emin olur.
10. Konfigürasyon Yönetimi süreci bütün bu akış sırasında Konfigürasyon Yönetim Veritabanının (CMDB) güncellenmesini sağlar.

ITIL, temel süreçlerin planlanması, rol ve aktivitelerin ilişkilendirilmesi ve roller arasındaki bilgi akışının nasıl olacağı konularında denenmiş yöntemler sunar. Roller arasındaki bilgi akışı veya işbirliği eksikliğinden çıkabilecek sorunları en baştan tümüyle engeller veya en aza indirir.

ITIL'in bir diğer önemli özelliği her sektörde ve her büyüklükteki organizasyonda uygulanabilmesidir. Belli bir sektöre dönük hazırlanmamıştır. BT şirketleri ile ister üretim, ister hizmet, ister kamu sektöründe olsun tüm organizasyonların BT grupları tarafından kullanılabilir.

BT hizmetleri şirket içindeki BT grubunca verilebileceği gibi başka firmalardan hizmet olarak alınıyor olabilir. Örneğin; kullanıcılara donanım ve yazılım desteği veren Yardım Masası hizmetleri BT elemanları tarafından sağlanabildiği gibi, yardım masası hizmetlerinde uzmanlaşmış bir başka şirketten de alınabilir. ITIL süreçleri her iki durumda da rehber olarak kullanılabilir.

ITIL uygulamaları ile ISO 9000 ve Avrupa Kalite Yönetimi Vakfı Mükemmellik Modeli

(EFQM - European Foundation for Quality Management) kalite sistemleri arasında sıkı ilişki vardır. ITIL'de BT süreçleri kalite sistemlerinin öngördüğü şekilde tanımlanıp dokümante edildiğinden ISO sertifikası alınması çabuklaşır.

Böylece Kurumlar öncelikle kendi BT ihtiyaçlarını doğru bir şekilde tespit edebilecek; kendilerine uygun hizmet modelini belirleyebilecektir

Türkiye'de son zamanlarda büyük şirketlerin ITIL'a ilgilerinin arttığını, elemanlarını ITIL konusunda eğittiklerini, aynı zamanda bazı süreçlerini uyarladıkları gözlemlenmektedir.

3.2 ITIL Kitapları

- **ITIL Service Strategy (ITIL Hizmet Stratejisi)**

Hizmet stratejisi modülü, BT Hizmet yönetiminin stratejik bir varlık olarak tasarlanmasını, geliştirilmesini ve uygulanmasını sağlar. Odak konusu Neden sorusuna cevap bulmaktır, Nasıl yapılacağı konusu bu aşamada öncelikli değildir. Bu modülün hedefi politikaların ve hedeflerinin tanımlanmasıdır.

- **ITIL Service Design (ITIL Hizmet Tasarımı)**

Hizmet Tasarım modülü, belirlenen servislerin ve Servis süreçlerinin tasarlanmasını ve geliştirilmesini sağlar.

- **ITIL Service Transition (ITIL Hizmet Geçiş)**

Bu modül, yeni/değişen servislerin uygulamaya alınış aşamasının verimli olmasını sağlar.

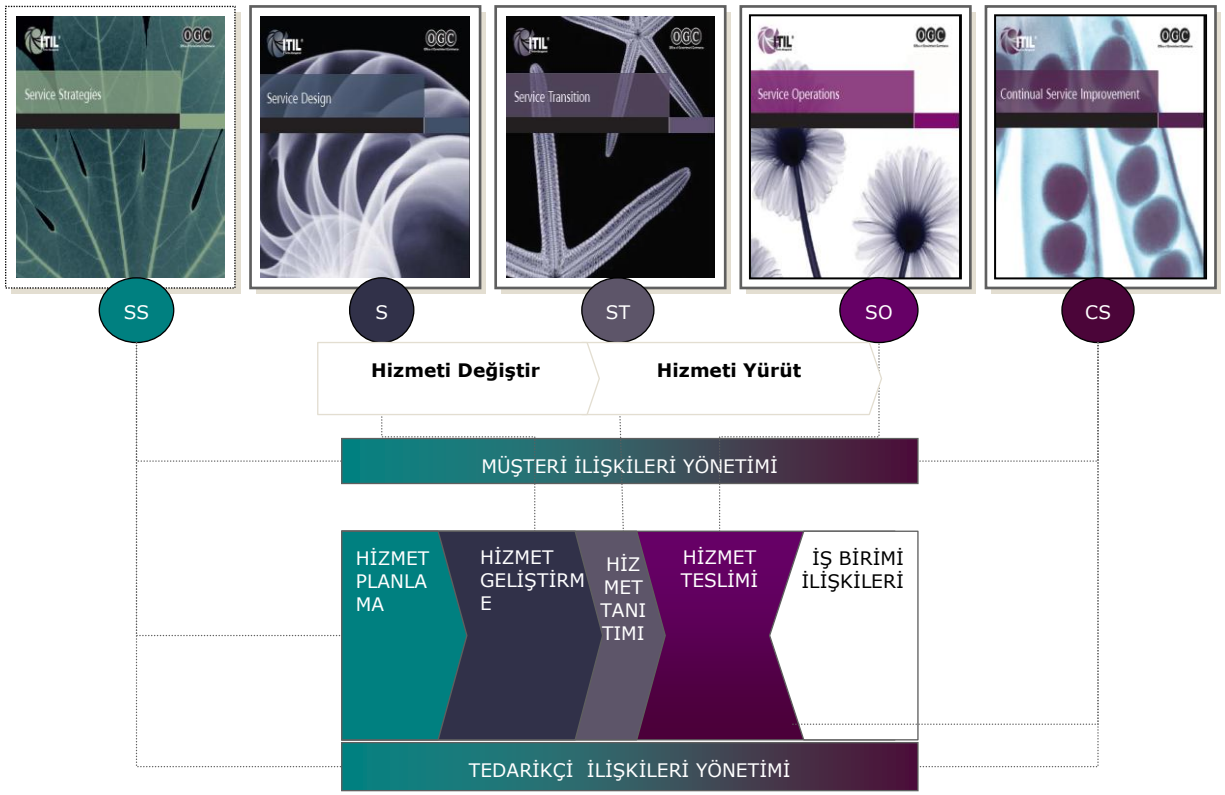
- **ITIL Service Operation (ITIL Hizmet İşletimi)**

Servislerin, taahhüt edilen seviyede işletilmesi ve yönetilmesi için süreç ve aktivitelerin yerine getirilmesi ve koordine edilmesini sağlar.

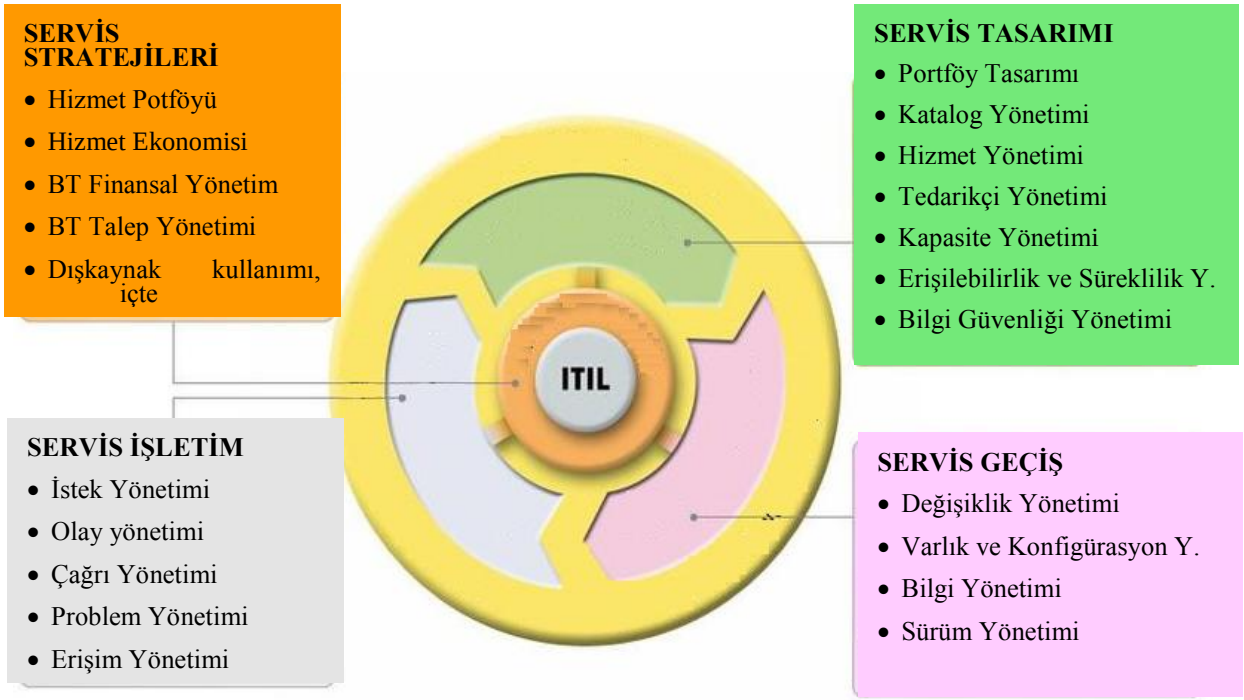
- **ITIL Continual Service Improvement (ITIL Sürekli İyileştirme)**

Sürekli Servis İyileştirme modülü, servis kalitesinin ve ilgili süreçlerin kalitesinin değerlendirilmesi ve iyileştirmesine yönelik öneriler sunar.

Şekil 3.1 ITIL Kitaplarını gösterirken, Şekil 3.2 ITIL Hizmet Yönetimi Yaşam Döngüsüdür.



Şekil 3.1 ITIL Kitapları



Şekil 3.2 ITIL Hizmet Yaşam Döngüsü

Şekil 3.3 ITIL Versiyon 3 te yer alan proseslerin, ITIL yaşam döngüsü adımlarına göre nasıl gruplandırıldığını göstermektedir.

Temel Süreçler		Servis Strateji	Servis Tasarım	Servis Geçiş	Servis İşletim	Sürekli Servis İyileştirme
Servis Strateji	SS					
Finansal Yönetim	SS					
Servis Portfolyo Yönetimi	SS					
Talep Yönetimi	SS					
Servis Seviyesi Yönetimi	ST					
Servis Katalog Yönetimi	ST					
Erişilebilirlik Yönetimi	ST					
Kapasite Yönetimi	ST					
Bilgi Güvenliği Yönetimi	ST					
Servis Süreklilik Yönetimi	ST					
Tedarikçi Yönetimi	ST					
Değişiklik Yönetimi	SG					
Servis Varlık ve Konfigürasyon Yönetimi	SG					
Sürüm ve Yaygınlaştırma	SG					
Durum Yönetimi	SI					
Olay Yönetimi	SI					
Taleplerin Yerine Getirilmesi	SI					
Problem Yönetimi	SI					
Erişim Yönetimi	SI					
7 Aşamalı Servis İyileştirme Planı	SIY					

Şekil 3.3 ITIL Versiyon 3 Prosesleri

4. COBIT (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri)

CobiT, Türkçe karşılığı Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri olan “Control OBjectives for Information and related Technology” kelimelerinden üretilmiş bir kısaltmadır. ISACA ve ITGI tarafından 1992 yılında geliştirilmiş, BT Yönetimi için en iyi uygulamalar kümesidir. CobiT; ISO teknik standartları, ISACA ve AB tarafından yayınlanan yönetim kanunları, COSO, AICPA, GAO tarafından yayınlanan profesyonel iç kontrol ve denetim standartları tarafından biçimlendirilmiştir. Bir şirkette teknolojinin kullanımından ve BT yönetişimi ile kontrol geliştirmekten türeyen faydayı en üst düzeye çıkarmaya yardım etmesi için yöneticilere, denetçilere ve BT kullanıcılarına genel olarak kabul görmüş ölçüler, göstergeler, süreçler ve en iyi uygulamalar sağlar. CobiT’in vizyonu; bilişim teknolojileri yönetişim (IT governance) modeli olmaktır. CobiT sadece bir denetim aracı değil, aynı zamanda bir yönetişim aracı olma amacını da taşır. Bu nedenle yönetimden bilişim teknolojileri personeline kadar kurum içi ve dışında, kurumun varlığı ve sağlıklı faaliyet göstermesi konularında risk üstlenen çeşitli taraflara fayda sağlama amacını da yerine getirmeyi hedeflemektedir (Uzunay, 2007).

COBIT; Bilgi Teknolojilerinin kullanıldığı süreçlerin kontrol ve ölçümlemelerinin nasıl yapılması gerektiğini anlatan metodolojidir. Organizasyonların iş hedef ve gereksinimlerini karşılayacak bilgilerin üretimi ve aktarımının hızlı, sürekli ve güvenli sağlanabilmesi için teknoloji kullanımından kaynaklanan risklerin belirlenmesi, yönetim ve kontrolünün etkin ve verimli olarak yapılması gerekmektedir. Kısaca “Teknoloji risklerini nasıl yöneteceğiz ve bağlı oldukları yapıyı daha güvenli hale nasıl getireceğiz?” sorularının yanıtları, sadece BT yöneticileri değil, teknoloji yoğun çalışan ve iş süreçlerine teknolojiyi entegre etmiş tüm kurum yöneticileri için önem taşımaktadır.

COBIT, bu sorulara sistematik bir yaklaşım sergileyerek ve yönetsel ihtiyaçlara da yanıt verecek şekilde oluşturulmuş bir yöntemdir. İş Hedefleri’nin BT Hedefleri’ne dönüşümü, bu hedeflere ulaşmak için gerekli kaynakları ve gerçekleştirilen süreçleri bir araya getiren COBIT, Bilgi Teknolojileri için Kontrol Hedefleri anlamına (Control Objectives for IT and related Technologies) gelmektedir (Artinyan, 2008).

COBIT ilk olarak 1996 yılında yayımlanmıştır. Misyonu "araştırma, geliştirme, ilan ve yetkili tanıtmak, güncellik, uluslararası alanda kabul görmüş genel bilgi teknolojileri kontrol hedeflerinin iş yöneticileri ve denetçiler tarafından kullanılmasıdır." Yöneticiler, denetçiler ve kullanıcılar COBIT gelişmelerinden yararlanırlar; çünkü COBIT onlara BT sistemlerini

anlamada, şirketlerin varlıklarını korumak için BT yönetişim modeline göre gerekli olan güvenlik ve kontrol seviyelerine karar vermede yardımcı olur.

COBIT 4.1 34 tane üst düzey işleme sahiptir. Bunların kapsadığı 318 adet kontrol hedeflerinin de dört ana kategorisi bulunur: Planlama ve Organizasyon, Tedarik ve Uygulama, Hizmet Sunumu ve Destek, İzleme ve Değerlendirme. COBIT, yöneticilere, BT kullanıcılarına ve denetçilere çeşitli faydalar sağlar. Yöneticilerin COBIT'ten yararlanma nedeni, BT alanında daha etkili kararlar verme ve kuruluş için doğru yatırımlar yapma olarak açıklanabilir. İçerdiği stratejik BT planı, bilgi mimarisi, stratejiyi işletmek için gerekli BT donanım ve yazılımları, sürekli hizmet sağlaması ve BT performansını izleme sistemi ile COBIT karar vermeyi daha etkili hale getirmektedir. BT kullanıcılarının COBIT'ten yararlanma nedeni, kontrol, güvenlik ve süreç yönetimi güvencesi sağlanmasıdır. Denetçilere ise BT altyapısı içindeki sorunları kontrol esasları çerçevesinde belirlemelerine yardımcı olur. Ayrıca denetçilerin kendi denetim bulgularını onaylar.

4.1 COBIT Versiyonları ve Tarihçesi

COBIT dört ana yayımdan oluşmuştur:

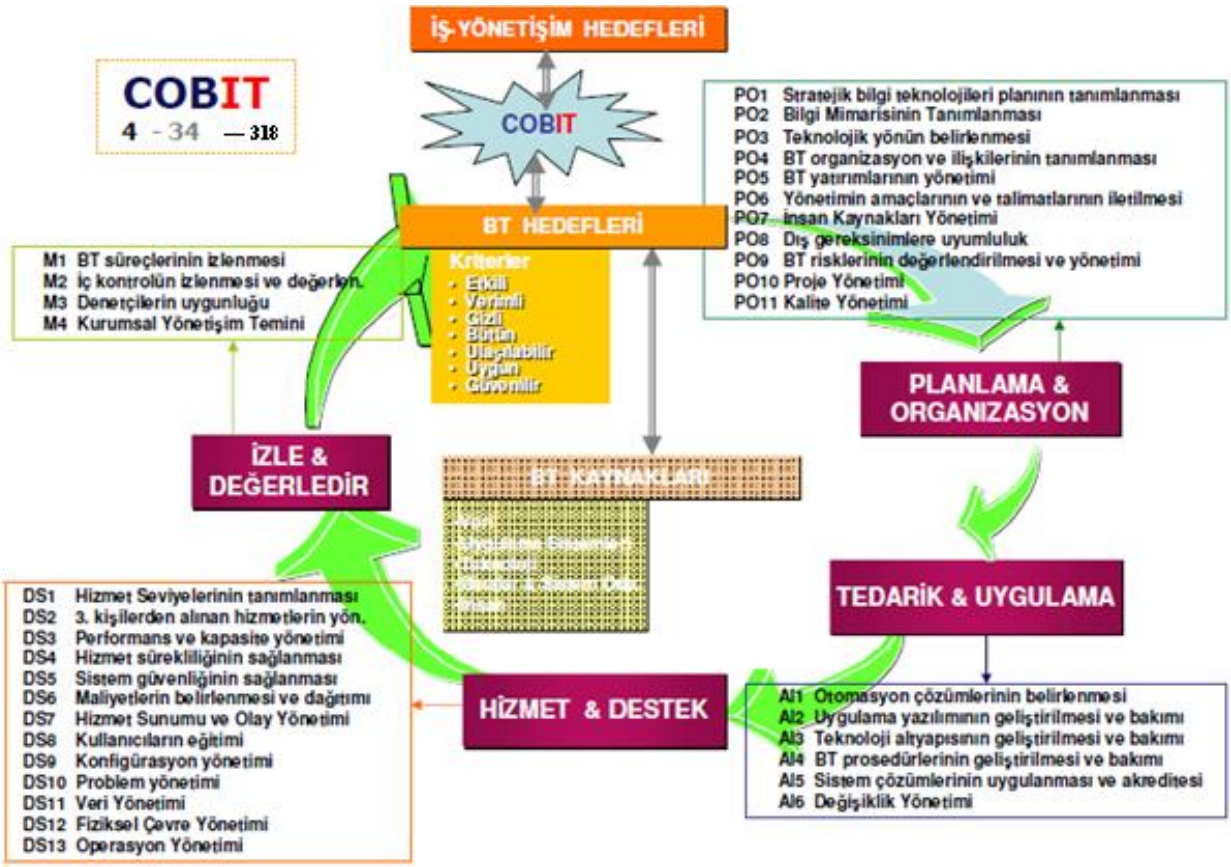
- 1996, COBIT birinci baskı yayımlandı.
- 1998, İkinci baskıda yönetim yönergelerine eklendi.
- 2000, Üçüncü baskı yayımlandı.
    - 2003, COBIT online sürümü kullanıma sunuldu.
- 2005 Aralık, Dördüncü baskı yayımlandı.
    - 2007 Mayıs, Güncel versiyonu 4.1 yayımlandı.

CobiT'in ilk sürümü 1996 yılında yayımlandı. Amacı; iş yöneticileri ve denetçilerinin günlük kullanımı için geçerli, güncel, uluslararası kabul görmüş BT amaçlarını araştırmak, geliştirmek ve teşvik etmektir. "Yönetim Rehberi", 1998'de yayınlanan 2. sürüme eklendi. 2000 yılında 3. sürüm yayınlandı. 2003 yılında bilgisayar bağlantılı versiyonu kullanılır duruma geldi. 2005 yılının aralık ayında 4. basım ilk olarak yayınlandı. 2007 yılının mayıs ayında, şu anda kullanılan 4.1 sürümü yayınlandı. Yayında olan bu versiyona ISACA'nın web sitesinden erişilebilmektedir.

CobiT'in jenerik bir model olarak herhangi bir kurumda yer alabilecek tüm teknoloji süreçlerini kapsayan yapısı içerisinde, gruplanmış 4 süreç alanı ve 34 tane temel BT süreci yer

almaktadır.

Bu süreçlerin altında, 318 adet kontrol hedefi veya alt aktivite tanımlanmıştır. CobiT, BT güvenliği için kapsamlı ve en iyi uygulama niteliğinde bir yaklaşım ortaya koymaktadır. IT Governance Institute, CobiT'in oluşturulmasında tüm en iyi uygulamalar ve standartları (COSO, ISO 9000, Spice, CMM, ITIL, BSI7799 vb.) referans olarak ele almış, dünya çapında akademisyen, uzman, danışman ve analistler ile ortak bir çalışma yürütmüştür. CobiT'de yer alan "Yönetim Rehberi-Management Guidelines" içerisinde tüm teknoloji süreçleri için Olgunluk Modeli (Maturity Model), Kritik Başarı Faktörleri (Critical Success Factors), Ana Hedef Göstergeleri (Key Goal Indicators) ve Ana Performans Göstergelerinin (Key Performance Indicators) tanımlanmış olması sayesinde, 34 süreç dahilinde, organizasyonun hedeflere ulaşma derecesi ölçümlenebilmektedir. Hedefler, kaynaklar ve süreç grupları ve süreçler bir araya getirildiğinde oluşturulan CobiT Mimarisi ana hatları ile aşağıda yer almaktadır (Artinyan, 2008):



Şekil 4.1 COBIT İş Hedefleri (Artinyan, 2008)

4.1.1 COBIT Versiyon 4

COBIT Versiyon 4, COBIT 3 'teki ayrı kitapların tek bir ses halinde ve kullanım kolaylığına sahip olarak geliştirilmiş halidir.

4.1 versiyonundaki temel değişiklikler;

- Olgunluk modeli için destek,
- Amaçların basitleştirilmiş tarifi,
- İş, BT Hedefleri ve BT Süreçleri arasındaki çift yönlü ilişkileri ve süreçleri basamaklandırmak şeklinde listelenebilir.

Ayrıca her işlem için oluşturulan yeni alt kısımlar şunlardır:

- Girdilerin çapraz referansları ve diğer COBIT süreçlerinin çıktıları
- Sorumlu bir atama ile her işlem için faaliyetler (CFO, CEO, BT Hizmetleri Müdürü ve Geliştirme Müdürünün ne yapması gerektiğini gösteren)

Bu versiyon aşağıdaki yayınlardan oluşmaktadır;

- Yönetici Özeti
- Yönetim ve Kontrol Çerçevesi
- Kontrol Nesneleri
- Yönetim Kılavuzu
- Uygulama Kılavuzu
- BT Güvence Kılavuzu

4.1.2 COBIT Versiyon 4.1

COBIT sürümü 4.1 simdi ISACA web sitesinde mevcuttur. Yapılan büyük değişiklikler şunlardır:

- Hedef açıklamaları basitleştirildi
- Süreçler ile "İşletme", "BT hedefleri" ve "BT süreçleri" arasındaki çift yönlü ilişki basamaklandırıldı.

Bu son versiyon aşağıdaki 4 yayından oluşmaktadır;

- Yönetimsel Özet,
- Çatı
- Esas İçerik (Kontrol Hedefleri, Yönetim Kılavuzu ve Olgunluk Modelleri)
- Ekler

4.1.2.1 Yönetimsel Özet

İş kararları, uygun zamanda iyi seçilmiş öz bilgilere dayanmaktadır. Özellikle zaman sıkışıklığı olan kıdemli yöneticiler için tasarlanan COBIT Yönetimsel Özet, COBIT'in temel kavram ve kurallarının anlaşılması için bir özet niteliğindedir. COBIT'in anahtar konuları ve kurallarına ilişkin anahtar bilgileri sağlar.

İşletme yönelimli COBIT; işletmenin amaçlarının bilgi teknolojisi amaçlarına odaklanması, başarıyı değerlendirmek için vade modellerinin oluşturulması, işletme ve bilgi teknolojisi süreç sahiplerinin birleşik sorumluluklarının teşhis edilmesi faaliyetlerinden oluşur.

4.1.2.2 Çatı

Başarılı bir organizasyon veri ve bilgilerin sağlam bir çatı üzerine kuruludur. Bu çatı esas bileşenlere, süreçler, kontroller, hedefler ve metrikler arasındaki ilişkilere genel bir açıklama sağlar. İşe tam destek için gerekli BT kaynakları kadar önemli olan yedi bilgi kriterini (etkinlik, verimlilik, gizlilik, bütünlük, uygunluk, uyum ve güvenilirlik) de tanıtır. İşletmenin gereksinimleri ile bağlantı kurar. Bilgi teknolojisi faaliyetlerini genel kabul görmüş bir süreç modeli şeklinde örgütler. Ana bilgi teknolojisi kaynaklarını tanımlar. İşletme kontrol hedeflerini açıklar.

4.1.2.3 Esas İçerik

Başarılı bir işletme sağlamak için, iş süreçleri ve bilgi sistemleri arasındaki birliği etkili bir şekilde yönetmek gerekir. Yeni Yönetim Yönergeleri, Olgunluk Modellerinden oluşur; bu da kontrol aşamalarını ve beklenen kontrol düzeylerini sanayi normlarıyla karşılaştırmak içindir. Kritik Başarı Faktörleri, BT işlemleri kontrolü için en önemli faaliyetleri içerir. Anahtar Hedef Göstergeleri, performans hedef seviyelerini tanımlamak içindir. Anahtar Performans Göstergeleri de BT kontrol sürecinin amaca ulaşmasına uygun olup olmadığını ölçmek içindir. Bu yönetim yönergeleri kurumsal yatırıma sahip olanların sorunlarına çözüm bulabilmelerinde yardımcı olur.

CobiT kılavuzunun esas içeriği 34 BT sürecine göre bölümlenmiştir. Her bir süreç, kendine ait 4 sayfada detaylandırılmıştır. Bu sayfaların içeriği aşağıdaki gibidir;

1.Sayfa – Süreç için üst seviye kontrol amacını içerir; süreç tanımı, amaçlar, hedefler, metrikler, uygulamalar ve süreçten süreç alanlarına eşleme, bilgi kriterleri, BT kaynakları ve BT odak alanları tarif edilir.

2.Sayfa – Süreç için detaylı kontrol hedefleri açıklanır.

3.Sayfa – Yönetim kılavuzları, süreç girdileri/çıktıları, RACI (Sorumlu, tarif edilir ve/veya bilgilendirilmiş) grafiği, hedef ve metrikler anlatılır.

4.Sayfa – Süreç için olgunluk modeli açıklanır.

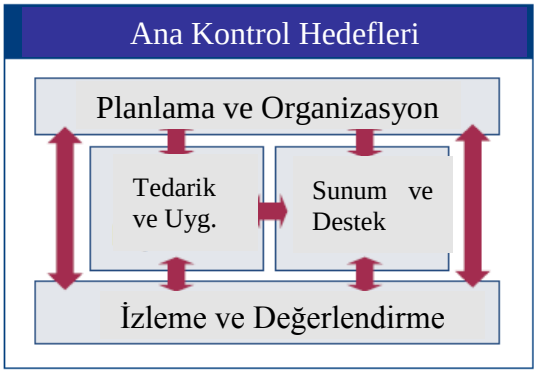
4.1.2.4 Ekler

Eşleştirmeler ve çapraz başvurular, ilave olgunluk modeli bilgileri, referans materyalleri, proje tanımı ve sözlük yer alır.

4.2 COBIT'in Ana Kontrol Hedefleri

COBIT ana kontrol hedefleri Şekil 4.2 de de gösterildiği gibi dört etki alanını kapsar:

- Planlama ve Organizasyon
- Tedarik ve Uygulama
- Hizmet Sunumu ve Destek
- İzleme ve Değerlendirme



Şekil 4.2COBIT Ana Kontrol Hedefleri

4.2.1 Planlama ve Organizasyon

Bu bölüm işletme amaçlarının gerçekleştirilebilmesi için Bilgi teknolojilerinin katkısının hangi yolla olması gerektiğini belirler. Bu bölümde strateji ve taktikler vardır. Stratejik planın gerçekçi olabilmesi için farklı açılardan ele alınması gerekir. Organizasyonun teknolojik açıdan altyapı uygunluğu incelenir.

Planlama ve Organizasyon alanı teknoloji kullanımını ve kurumun amaç ve hedeflerini gerçekleştirmeye yardımcı olmak için nasıl en iyi şekilde kullanılabileceğini kapsamaktadır. Bu alan en uygun sonucu elde etmek ve bilgi teknolojileri kullanımından en iyi şekilde faydalanmak için bilgi teknolojilerinin alması gereken organizasyonel ve altyapısal şekli ortaya çıkartmaktadır.

Planlama ve Organizasyon alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır:

- *PO1 Stratejik bir BT Planı Tanımlama*
- *PO2 Bilgi Mimarisini Tanımlama*
- *PO3 Teknolojik Yönü Belirleme*
- *PO4 BT Prosesleri, Organizasyon ve İlişkilerini Tanımlama*
- *PO5 BT Yatırımını Yönetme*
- *PO6 Yönetim Hedefleri ve Yönünü Bildirme*
- *PO7 BT İnsan Kaynaklarını Yönetme*
- *PO8 Kaliteyi Yönetme*
- *PO9 BT Risklerini Değerlendirerek Yönetme*
- *PO10 Projeleri Yönetme*

4.2.1.1 PO1 Stratejik bir BT Planı Tanımlama

PO1.1 IT Değer Yönetimi
PO1.2 İş ve BT Arasındaki Uyumun Sağlanması
PO1.3 Mevcut Performansın Değerlendirilmesi
PO1.4 BT Stratejik Planı
PO1.5 BT Taktik Planları
PO1.6 BT Portföy Yönetimi

PO1.1 IT Değer Yönetimi

BT ’nin etkinleştirildiği yatırımlardan oluşan işletme portföyünün sağlam iş olurluk incelemeleri olan programları içermesini sağlamak için işletme ile çalışmalıdır. Karmaşıklık ve fon tahsisindeki özgürlük derecesi bakımından farklılık gösteren zorunlu, destekleyici ve isteğe bağlı yatırımların olduğu hatırlatılmalıdır. BT süreçleri, programların BT bileşenlerinin etkili ve verimli bir şekilde teslimini ve maliyet ile işlevsellik programı dahil programların beklenen sonuçlarını etkileyebilecek olan, plandan öteye gerçekleşen tüm sapmaların erken uyarısını sağlamalıdır. BT hizmetleri, adil ve yürütülebilir hizmet seviyesi sözleşmeleri ile tatbik edilmelidir. Menfaat elde etme ve maliyetleri kontrol etmenin sorumluluğu net bir şekilde tahsis ve takip edilir. İş durumlarının, mali değer, kapasiteye ulaşamama riski ve beklenen menfaatleri elde edememe riski dahil, adil, şeffaf, tekrarlanabilir ve kıyaslanabilir

bir şekilde değerlendirilmesi sağlanmalıdır.

PO1.2 İş Birimleri ve BT Uyumu

Yöneticiler zamanın teknoloji imkanları ve gelecekteki yönler, BT 'nin sağladığı imkanlar ve bu fırsatlardan istifade etmek için ticari işletmenin ne yapması gerektiği konusunda eğitilmelidir. BT 'nin entegre edildiği iş yönünün anlaşılması sağlanmalıdır. İş ile BT stratejileri, işletme hedefleriyle BT hedefleri net bir şekilde birbirine bağlanacağı ve fırsatlar ile geçerli imkan sınırlarının akılda bulundurulacağı şekilde entegre edilmelidir ve geniş çapta duyurulmalıdır. İşletmenin (iş stratejisinin) kritik derecede BT 'ye bağlı olduğu noktalar belirlenmelidir ve kararlaştırılmış öncelikler tespit edileceği şekilde iş ile teknolojinin şartları arasında ara yol çizilmelidir.

PO1.3 Mevcut Yetenek ve Performans Değerlendirmesi

Mevcut plan ve bilgi sistemlerinin performansını, iş hedeflerine katkı, işlevsellik, istikrar, karmaşıklık, maliyetler, güçlü ve zayıf noktalar açısından değerlendirilmelidir.

PO1.4 BT Stratejik Planı

İlgili paydaşlarla işbirliği içinde BT 'nin işletmenin stratejik amaçlarına (hedeflerine) ve ilgili maliyet ile risklere nasıl katkı sağlayacağını belirleyen bir stratejik plan oluşturulmalıdır. BT 'nin BT etkili yatırım programları ve işlevsel hizmetlerin sağlanmasını nasıl destekleyeceği buna dahil olmalıdır. Plan, hedeflere nasıl ulaşılacağı ve ölçüleceğini belirler ve paydaşların resmi onayından geçirilmelidir. BT stratejik planı yatırım/işlemler bütçesi, finansman kaynakları, kaynak stratejisi, tedarik stratejisi ile yasa ve yönetmenliklerin şartlarını kapsamalıdır. Stratejik plan, BT taktik planlarının belirlenmesine izin verecek şekilde yeterince ayrıntılı olmalıdır.

PO1.5 BT Taktik Planları

BT stratejik planından türetilen BT taktik planlarından oluşan bir portföy oluşturulmalıdır. Bu taktik planları gerekli BT inisiyatifleri, kaynak ihtiyaçları ve kaynak kullanımı ile menfaatlerin elde edilmesinin nasıl takip edilerek yönetileceği tanımlanmalıdır. Taktik planları, proje planlarının belirlenmesine izin verecek şekilde yeterince ayrıntılı olmalıdır Belirlenen taktik BT planları ve inisiyatiflerini proje ve hizmet portföylerinin analizi yoluyla aktif bir şekilde yönetilmelidir. Bu, düzenli olarak ihtiyaç ve kaynakların dengelenmesi,

bunların stratejik ve taktik hedeflere ve beklenen menfaatlere ulaşılmasıyla kıyaslanması ve sapmalar halinde gerekenin yapılmasını kapsamalıdır

PO1.6 BT Portföy Yönetimi

İşin yanı sıra, programları tespit ederek, tanımlayarak, değerlendirerek, önceliklerini belirleyerek, seçerek, başlatarak, yöneterek ve kontrol ederek, spesifik stratejik iş hedeflerine ulaşabilmek için gerekli BT-etkili yatırım programlarından oluşan portföy aktif bir şekilde yönetilmelidir. İstenilen iş sonuçlarının netleştirilmesi, program hedeflerinin sonuçlara ulaşılmasını desteklemesinin sağlanması, sonuçlara ulaşmak için gerekli çabaların tam kapsamının anlaşılması, destekleyici önlemlerin net bir sorumluluğunun tahsis edilmesi, program içindeki projelerin tanımlanması, kaynak ve finansmanın bulunması, yetkilerin verilmesi ve ilgili projelerin program başlangıcında uygulamaya konulması bu kapsama dahil olmalıdır.

4.2.1.2 PO2 Bilgi Mimarisini Tanımlama

PO2.1 İşletme Bilgisi Mimarisi Modeli
PO2.2 İşletme Veri Sözlüğü ve Veri Sentaks Kuralları
PO2.3 Veri Sınıflandırma Şeması
PO2.4 Bütünlük Yönetimi

PO2.1 İşletme Bilgisi Mimarisi Modeli

Stratejik bir BT Planı tanımlamada tarif edildiği gibi, BT planlarıyla uyumlu uygulamaların geliştirilmesi ve karar almayı destekleyen faaliyetleri sağlamak için işletme bilişim modeli oluşturulmalıdır. Bu model, bütünlüğü sağlayacak, esnek, işlevsel, uygun maliyetli, zamanlı, güvenilir ve başarısızlığa karşı dayanıklı bir yoldan işletme tarafından bilginin optimum olarak oluşturulması, kullanımı ve paylaşılması sağlanmalıdır.

PO2.2 İşletme Veri Sözlüğü ve Veri Sentaks Kuralları

Müessesenin veri sentaks kuralarını içeren işletme veri sözlüğü tutulmalıdır. Bu sözlük, veri unsurlarının uygulama ve sistemler arasında paylaşılmasını sağlamalıdır, BT ve iş kullanıcıları arasında verilerin ortak olarak anlaşılmasını kolaylaştırmalıdır ve uyumsuz veri unsurlarının oluşturulmasını önlemelidir.

PO2.3 Veri Sınıflandırma Şeması

İşletme verilerinin kritiklik ve hassasiyet derecesine (örn. kamuya açık, gizli, çok gizli) dayalı, işletmenin tamamında geçerli olarak bir sınıflandırma şeması oluşturulmalıdır. Bu şema, verinin mülkiyeti hakkındaki bilgiler, ilgili güvenlik dereceleri ve koruma kontrollerinin tanımı ve verinin tutulması ve imha edilmesi şartları, kritikliği ve hassasiyetinin kısa tanımını içermelidir. Şema, erişim kontrolleri, arşivleme yada şifreleme gibi kontrollerin uygulanması için temel teşkil etmelidir.

PO2.4 Bütünlük Yönetimi

Veri tabanları, veri depoları ve veri arşivleri gibi, elektronik biçimde muhafaza edilen tüm verilerin bütünlük ve tutarlılığını sağlamak için gerekli prosedürler tanımlanmalıdır ve uygulanmalıdır.

4.2.1.3 PO3 Teknolojik Yönü Belirleme

PO3.1 Teknolojik Yönün Planlanması
PO3.2 Teknolojik Altyapı Planı
PO3.3 Gelecekteki Eğilimler ve Yönetmenliklerin Takibi
PO3.4 Teknoloji Standartları
PO3.5 BT Mimarisi Kurulu

PO3.1 Teknolojik Yönün Planlanması

Mevcut ve yeni ortaya çıkan teknolojileri analiz ederek BT stratejisi ile iş sistemleri mimarisini gerçekleştirmek için hangi teknolojik yönün uygun olduğu planlanmalıdır. Ayrıca plan içinde hangi teknolojilerin iş fırsatlarını yaratma potansiyeli olduğu belirtilmelidir. Plan sistemlerin mimarisi, teknolojik yön, göç stratejileri ve altyapı bileşenlerinin ihtimal dahilindeki unsurlarını içermelidir.

PO3.2 Teknolojik Altyapı Planı

BT stratejik ve taktik planlarıyla uyumlu olan bir teknolojik altyapı planı oluşturarak tatbik edilmelidir. Plan teknolojik yöne dayalı olup risk düzenlemeleri ve teknoloji kaynaklarının dağıtımı için talimatı içermelidir. Planda rekabet ortamındaki değişiklikler, bilişim sistemlerine personel alınması ve yatırım yapılması boyutunu taşıyan ekonomiler ve platformlar ile uygulamaların arasında geliştirilmiş ara-çalışabilirlik ele alınmalıdır.

PO3.3 Gelecekteki Eğilimler ve Yönetmenliklerin Takibi

İş sektörü, teknoloji, altyapı, mevzuat ve düzenleme çevre eğilimlerini takip etmek amacıyla bir süreç oluşturulmalıdır. Bu eğilimlerin sonuçlarını, BT teknoloji altyapı planının geliştirilmesine dahil edilmelidir.

PO3.4 Teknoloji Standartları

İşletme çapında tutarlı, etkili ve güvenli teknoloji çözümlerini sunmak için teknoloji ilkeleri, altyapı ürünlerin üzerine danışmanlık ve teknoloji seçimi konusunda rehberlik sağlamak için bir teknoloji forumunu kurunuz ve bu standart ile ilkelere uyumu ölçülmelidir. Bu forum, iş ilgililiği, risk ve dış şartlara uyumları bazında teknoloji standartlarını yönetmelidir.

PO3.5 BT Mimarisi Kurulu

Mimari ilkelerini sağlamak, bunların uygulaması konusunda danışmanlık vermek ve uyumluluğu kontrol etmek üzere bir BT Mimarisi Kurulu oluşturulmalıdır. Bu organ BT mimarisi tasarımını yöneterek bu tasarımın iş stratejisini etkinleşmesini sağlamalıdır ve yönetmenliklere uyum ile süreklilik şartlarını değerlendirmelidir. Bu, bilişim mimarisine ilişkilendirilmelidir / bilişim mimarisi ile ilgili olmalıdır.

4.2.1.4 PO4 BT Prosesleri, Organizasyon ve İlişkilerini Tanımlama

PO4.1 BT Proses Çerçevesi
PO4.2 BT Stratejisi Komitesi
PO4.3 BT Yönetim Komitesi
PO4.4 BT İşlevinin Organizasyon içinde Yerleştirilmesi
PO4.5 BT Organizasyon Yapısı
PO4.6 Rol ve Sorumluluklar
PO4.7 BT Kalite Güvencesi Sorumluluğu
PO4.8 Risk, Güvenlik ve Uyum Sorumluluğu
PO4.9 Veri ve Sistem Mülkiyeti
PO4.10 Denetleme
PO4.11 Sorumlulukların Ayrıştırılması
PO4.12 BT Personel Alımı
PO4.13 Ana BT Personeli
PO4.14 Sözleşmeli Personel Politika ve Prosedürleri

PO4.1 BT Süreç Çerçevesi

BT stratejik planını tatbik etmek için BT süreç çerçevesi tanımlanmalıdır. Bu çerçeve bir BT süreç yapısı ve ilişkilerini (örn. süreç boşlukları ve bindirmelerini yönetmek için), mülkiyet, vade, performans ölçümü, iyileştirme, uyum, kalite hedefleri ve bunlara ulaşmanın planlarını içermelidir. Çerçeve, BT 'ye özgü olan süreçler, işletme portföy yönetimi, iş süreçleri ve iş değişim süreçleri arasındaki entegrasyonu sağlamalıdır. BT süreç çerçevesi kalite yönetim sistemi ile iç kontrol çerçevesine entegre edilmelidir.

PO4.2 BT Stratejisi Komitesi

Kurul düzeyinde bir BT stratejisi komitesi kurulmalıdır. Bu komite, kurumsal yönetimin bir parçası olarak BT yönetiminin gerektiği şekilde ele alınması, stratejik yön konusunda danışmanlık sunması ve ana yatırımları gözden geçirmesini sağlamalıdır.

PO4.3 BT Yürütme Komitesi

Yönetici ile iş ve BT yönetiminden oluşan bir BT yürütme komitesi (yada eşdeğeri) proje statülerini ve kaynak uyumsuzluklarını çözme amaçlarıyla oluşturulmalıdır.

PO4.4 BT İşlevinin Organizasyon içinde Yerleştirilmesi

Başta BT 'nin iş stratejisi için kritiklik derecesi ve BT 'ye işlevsel bağımlılık derecesi olmak üzere BT 'nin işletme içerisindeki önemine bağlı olarak BT işlevini bir iş modeli genel organizasyon yapısı içerisinde konumlandırılmalıdır. CIO 'nun raporlama satırı, BT 'nin işletme içindeki önemiyle bağlantılı olmalıdır.

PO4.5 BT Organizasyon Yapısı

İş ihtiyaçlarını yansıtan bir iç ve dış BT organizasyon yapısı kurulmalıdır. Buna ilave olarak personel alım ihtiyaçları ve kaynak stratejilerini, beklenen iş hedeflerine ve değişen şartlara uyacak şekilde değiştirmek amacıyla BT organizasyon yapısını periyodik olarak gözden geçirmek için bir süreç uygulanmalıdır.

PO4.6 Rol ve Sorumluluklar

Bilişim sistemlerine ilişkin olarak müessesedeki tüm personel için, personele verilen rol ve sorumlulukları yerine getirmeleri için yeterli yetkinin verilmesi amacıyla, rol ve sorumluluklar tanımlanmalıdır. Rol tanımları oluşturularak bunlar düzenli olarak güncellenmelidir. Bu tanımlar hem yetki hem de sorumluluğu sınırlar, ilgili pozisyonda

gerekli yetenek ve tecrübenin tarifini içerir ve performansın değerlendirilmesinde kullanıma uygun olmalıdır. Rol tanımları iç kontrol sorumluluğunu içermelidir.

PO4.7 BT Kalite Güvencesi Sorumluluğu

Kalite güvence işlevinin yerine getirilmesinden kaynaklanan sorumluluğu yükleyerek kalite güvence grubuna uygun kalite güvence sistemleri, kontrol ve iletişim yetenek ve deneyim sağlanmalıdır. Organizasyon içinde konumlandırma, sorumluluklar ve kalite güvence grubunun büyüklüğü müessesenin ihtiyaçlarına uygun olmalıdır.

PO4.8 Risk, Güvenlik ve Uyum Sorumluluğu

İşletme içinde BT ile ilgili risklerin aidiyet ve sorumluluğunu ilgili üst düzey seviyeye entegre edilmelidir. Bilgi güvenliği, fiziksel güvenlik ve uyumdan kaynaklanan sorumluluk dahil olmak üzere BT risklerinin yönetimi açısından kritik olan roller tanımlanarak tahsis edilmelidir. Müessese çapındaki sorunları ele alabilmek için müessese çağındaki düzeyde risk ve güvenlik yönetimi sorumluluğu oluşturulmalıdır. İlgili güvenlik sorunlarının ele alınabilmesi için ilave güvenlik yönetim sorumlulukları sisteme özgü düzeyde tahsis edilmelidir. BT risklerinin alınabilirliği ve arta kalan tüm BT risklerinin onaylanması konusunda üst düzey yönetimden talimat alınmalıdır.

PO4.9 Veri ve Sistem Mülkiyeti

İşletmeye veri ve bilişim sistemlerinin mülkiyetinden kaynaklanan sorumlulukların ele alınabileceği şekilde prosedür ve araç sağlanmalıdır. Bilgi ve sistemlerin sınırlandırılması ve bu sınıflandırmaya göre korunması konusundaki kararlar sahipler tarafından verilmelidir.

PO4.10 Denetleme

Rol ve sorumlulukların gerektiği şekilde yerine getirilmesinden emin olmak, rol ve sorumluluklarını yerine getirmek için personelin tamamının yeterli yetki ve kaynaklara sahip olup olmadığını değerlendirmek ve genel olarak ana performans göstergelerini gözden geçirmek için BT işlevi içerisinde gerekli denetleme uygulamaları yürütülmelidir.

PO4.11 Sorumlulukların Ayrıştırılması

Tek bir bireyin kritik bir süreci bozması ihtimalini azaltacak şekilde rol ve sorumluluklar ayrıştırılmalıdır. Yönetim ayrıca personelin yalnızca, ilgili iş ve pozisyonlarına uygun, yetki aldıkları görevleri yerine getirmesi sağlanmalıdır.

PO4.12 BT Personel Alımı

BT işlevi için yeterli sayıda yetkin BT personelinin bulunduğundan emin olabilmek için personel alım ihtiyaçlarını işletme, işlevsel çevre yada BT çevresinde yapılan büyük değişiklikler üzerine değerlendirilmelidir. Personel alımında işletme/BT personelinin karşılıklı konumu, işlevler arası iş rotasyonu ve dış kaynak kullanımı dikkate alınmalıdır.

PO4.13 Ana BT Personeli

Ana BT personeli tanımlanmalıdır ve tespit edilmelidir ve bunlara olan aşırı bağlılık en aza indirgenmelidir. Acil durum halinde ana personele ulaşma planı bulunmalıdır.

PO4.14 Sözleşmeli Personel Politika ve Prosedürleri

Müessesenin bilgi varlıklarının korunmasının sağlamak ve kararlaştırılan sözleşeme şartlarının yerine getirmek amacıyla danışman ve diğer sözleşmeli personelin faaliyetlerinin BT işleviyle ile kontrolü için politika ve prosedür tanımlanmalıdır ve uygulanmalıdır.

4.2.1.5 PO5 BT Yatırımını Yönetme

PO5.1 Mali Yönetim Çerçevesi
PO5.2 BT Bütçesi içinde Önceliklerin Tanınması
PO5.3 BT Bütçe Oluşturma Prosesi
PO5.4 Maliyet Yönetimi
PO5.5 Fayda Yönetimi

PO5.1 Mali Yönetim Çerçevesi

Yatırım, hizmet ve varlık portföyleri bazında bütçe oluşturma ve maliyet/fayda analizini belirleyen BT için mali bir çerçeve oluşturulmalıdır. Mevcut BT bütçesinin temelini teşkil eden BT-etkili yatırım programları, BT hizmetleri ve BT varlıklarının portföyleri tutulmalıdır. Mevcut BT varlık ve hizmet portföylerini dikkate alarak yeni yatırımlar için iş olurluk incelemelerine girdi sağlanmalıdır. Hizmet ve varlık portföylerine yeni yatırımlar ve bakım BT bütçesinin geleceğini etkileyecektir. Bu portföylerin maliyet ve fayda bilgilerini bütçe içinde önceliklerin tanınması, maliyet yönetimi ve fayda yönetimi süreçleri kullanılmalıdır.

PO5.2 BT Bütçesi İçinde Önceliklerin Tanınması

İşletmenin portföyünde BT-etkili yatırım programları ve diğer BT hizmet ve varlıklarının getirisini optimum hale getirmeye yönelik BT ’nin katkısını en yüksek seviyeye çıkarmak için

işlemler, projeler ve bakım için BT kaynaklarının tahsisine öncelik tanımak amacıyla bir karar alma süreci uygulanmalıdır.

PO5.3 BT Bütçe Oluşturma Süreci

İşletmenin BT-etkili yatırım programları portföyü tarafından belirlenen öncelikleri yansıtan ve mevcut altyapıyı çalıştırma ve devam ettirmenin sürekli maliyetlerini dahil eden bir bütçeyi hazırlama ve sürdürmenin süreci oluşturulmalıdır. Bu süreç genel bir BT bütçesinin gelişmesini desteklerken aynı zamanda, programların BT bileşenlerine özel vurgu ile birlikte ayrı programlar için geliştirme bütçelerini desteklemelidir. Süreç, genel bütçe ile ayrı programlara ait bütçelerin sürekli olarak gözden geçirilmesi, ayarlanması ve onaylanmasına izin vermelidir.

PO5.4 Maliyet Yönetimi

Gerçek maliyetleri bütçelerle karşılaştıran bir maliyet yönetimi süreci uygulanmalıdır. Maliyetler takip edilerek rapor edilmelidir. Sapmalar söz konusu olduğunda bunlar zamanında tespit edilerek bunların programlar üzerindeki etkisi değerlendirilmelidir ve bu programların iş sponsoruyla birlikte uygun çözüm önlemleri alınmalıdır ve gerekirse programın iş olurluk incelemesi güncellenmelidir.

PO5.5 Fayda Yönetimi

Fayda takip süreci uygulanmalıdır. BT-etkili yatırım programlarının bileşeni yada düzenli işlevsel desteğin bir parçası olarak BT 'nin iş sonuçlarına beklenen katkısı tespit edilmelidir, kararlaştırılmalıdır, takip edilmelidir ve raporlanmalıdır. Raporlar gözden geçirilmelidir ve BT 'nin katkısını iyileştirme fırsatları söz konusu olduğunda gereken önlemler tespit edilerek alınmalıdır. BT 'nin katkısında gerçekleşen değişiklikler programı etkilediğinde ya da ilgili diğer projelerdeki değişiklikler programı etkilediğinde programın iş olurluk incelemesi güncellenmelidir.

4.2.1.6 PO6 Yönetim Hedefleri ve Yönünü Bildirme

PO6.1 BT Politikası ve Kontrol Ortamı
PO6.2 İşletme BT Riski ve İç Kontrol Çerçevesi
PO6.3 BT Politikalarının Yönetimi
PO6.4 Politikanın Yaygınlaştırılması
PO6.5 BT Amaçlarının Bildirilmesi ve Yönlendirme

PO6.1 BT Politikası ve Kontrol Ortamı

BT için, işletmenin felsefe ve çalışma tarzına göre düzenlenmiş bir kontrol ortamının unsurları tanımlanmalıdır. Bu unsurlar, BT yatırımlarından değer elde edilmesiyle ilgili beklentiler/ihtiyaçlar, risk alınabilirliği, bütünlük, etik değerler, personel yetkinliği, hesap verebilirlik ve sorumluluğu kapsamalıdır. Kontrol ortamı, ciddi riskleri yönetirken değerlerin elde edilmesini destekleyen, bölümler arası işbirliği ve takım çalışmasını teşvik eden, uyumluluk ve sürekli süreç iyileştirmeyi ilerleten ve süreç sapmalarıyla (başarısızlık dahil) iyi başa çıkan bir kültüre dayanmalıdır.

PO6.2 İşletme BT Riski ve İç Kontrol Çerçevesi

BT kaynak ve sistemlerini korurken değer sunabilmek için işletmenin risk ve iç kontrole genel yaklaşımını tespit eden bir çerçeve geliştirerek sürdürülmelidir. Çerçeve BT süreç çerçevesi ve kalite yönetim sistemiyle entegre edilerek genel iş maçlarına uymalıdır. Çerçeve, önleyici faaliyetler, düzensizliklerin zamanında tespiti, kayıpların sınırlanması ve iş varlıklarının zamanında kurtarılması yoluyla bilgi varlıklarına yönelik riskleri en aza indirgerken değer elde etme başarısını maksimum seviyeye çıkarmaya yönelik olmalıdır.

PO6.3 BT Politikalarının Yönetimi

BT stratejisini desteklemek için bir takım politikalar geliştirerek sürdürülmelidir. Bu politikalar politika niyeti, rol ve sorumluluklar, istisna süreci, uyumluluk yaklaşımı ve prosedür, standart ve kılavuzlara referansı içermelidir. Politikalar, kalite, güvenlik, gizlilik, iç kontroller ve fikri mülkiyet gibi ana konuları ele almalıdır. Bunların güncelliği düzenli olarak teyit edilerek onaylanmalıdır.

PO6.4 Politikanın Yaygınlaştırılması

İşletme işlemleri üzerine kurulu ve bu işlemlerin ayrılmaz bir parçası haline getirilmesini sağlamak için BT politikalarının ilgili personelin tamamı arasında yaygınlaştırıldığından ve yürütülerek uygulandığından emin olunmalıdır.

PO6.5 BT Amaçlarının Bildirilmesi ve Yönlendirme

İş ve BT amaçları ile yönlendirmenin bilinci ve anlaşılmasının işletme çapında bildirilerek yaygınlaşması sağlanmalıdır. Bildirilen bilgi, net bir şekilde belirtilmiş misyon, hizmet amaçları, güvenlik, iç kontroller, kalite, etik/davranış kuralları, politika ve prosedürler, vs. içermeli ve üst düzey yönetim tarafından hem konuşma hem de fiiliyat olarak desteklenen

sürekli bir iletişim programına dahil edilmelidir. Yönetim, BT güvenlik bilincini ve BT güvenliğinin herkesin sorumluluğunda olduğu mesajını yaygınlaştırma özellikle dikkat etmelidir.

4.2.1.7 PO7 BT İnsan Kaynaklarını Yönetme

PO7.1 Personel Alımı ve İstihdam
PO7.2 Personel Yetkinlikleri
PO7.3 Roller için Personel Alımı
PO7.4 Personel Eğitimi
PO7.5 Bireylere Bağlılık
PO7.6 Personel Onay Prosedürleri
PO7.7 Çalışanın İş Performansı Bakımından Değerlendirilmesi
PO7.8 İş Değişikliği ve İşe Son Verilmesi

PO7.1 Personel Alımı ve İstihdam

BT personel alım süreçlerinin kuruluşun genel personel politikaları ve prosedürlerine (örn. işe alım, pozitif çalışma ortamı ve oryantasyon) uygun olması sağlanmalıdır. Yönetim, organizasyon hedeflerine ulaşabilmek için gerekli yeteneklere sahip, gerekli şekilde istifade edilen Bilgi Teknolojileri işgücünün müessesede bulunmasını sağlamak için süreçler uygulanmalıdır.

PO7.2 Personel Yetkinlikleri

Personelin, eğitim, öğretim ve/veya tecrübeleri bazında rollerini yerine getirme yetkinliklerinin bulunup bulunmadığını düzenli olarak kontrol edilmelidir. Ana BT yetkinlik şartlarını tanımlayarak gerektiğinde kalifikasyon ve belgeleme programlarını kullanarak bunlara uyulduğunu doğrulanmalıdır.

PO7.3 Roller için Personel Alımı

Yönetim politika ve prosedürleri, etik ve mesleki uygulamalarına bağlı kalma şartı dahil olmak üzere personel için rol, sorumluluk ve telafi çerçeveleri tanımlanmalıdır, takip edilmelidir ve denetlenmelidir. İstihdam şartları çalışanın bilgi güvenliği, iç kontrol ve tüzüklere uyum konusundaki sorumluluğunu vurgulamalıdır. Denetim düzeyi, pozisyonun hassasiyetine ve tahsis edilen sorumluluk derecesine uygun olmalıdır.

PO7.4 Personel Eğitimi

BT çalışanlarına işe alındığında uygun oryantasyon ve bilgi, yetenek, imkan, iç kontrol ve güvenlik bilinçlerini, organizasyon hedeflerine ulaşabilmek için gerekli seviyede tutmak için sürekli eğitim sağlanmalıdır.

PO7.5 Bireylere Bağlılık

Bilginin belgelenmesi, bilgi paylaşımı, birbirine vekalet edebilecek pozisyonların planlanması ve personelin yedeklenmesi yoluyla ana bireylere kritik bağlılık ihtimali en aza indirgenmelidir.

PO7.6 Personel Onay Prosedürleri

Bilgi Teknolojileri için personel alım sürecine geçmiş kontrolünü dahil edilmelidir. Bu kontrollerin periyodunun derece ve sıklığı işlevin hassasiyeti ve/veya kritikliğine bağlı olup çalışan, yüklenici ve satıcılara uygulanmalıdır.

PO7.7 Çalışanın İş Performansı Bakımından Değerlendirilmesi

Müessesenin hedeflerinden türetilen bireysel hedefler, belirlenen standartlar ve işe özgü sorumluluklar bazında düzenli olarak zamanında değerlendirme yapılması talep edilmelidir. Gerektiğinde çalışanlar performans ve davranış konusunda eğitim alabilmelidir.

PO7.8 İş Değişikliği ve İşe Son Verilmesi

Bilgi Teknolojilerinde iş değişiklikleri, özellikle de işten çıkarmalar konusunda uygun önlemler alınmalıdır. Riskler en aza indirgeneceği ve işlev sürekliliğinin garantileneceği şekilde bilgi transferi düzenlemeleri yapılmalıdır, sorumluluklar yeniden tahsis ve erişim hakları iptal edilmelidir.

4.2.1.8 PO8 Kaliteyi Yönetme

PO8.1 Kalite Yönetim Sistemi
PO8.2 BT Standartları ve Kalite Uygulamaları
PO8.3 Geliştirme ve İktisap Standartları
PO8.4 Müşteri Odağı
PO8.5 Sürekli İyileştirme
PO8.6 Kalite Ölçümü, Takip ve Gözden Geçirme

PO8.1 Kalite Yönetim Sistemi

İş şartlarına uygun kalite yönetimine ilişkin standart, resmi ve sürekli bir yaklaşım sağlayan bir KYS 'ni oluşturulmalıdır ve sürdürülmelidir. KYS, kalite şart ve kriterleri, ana BT süreçleri ve bunların sıra ve aralarındaki etkileşimi ile uygunsuzlukların tanımlanması, tespit edilmesi, düzeltilmesi ve önlenmesi amaçlı politika, kriter ve yöntemleri tanımlar. KYS, rol, görev ve sorumlulukları kapsayacak şekilde kalite yönetimi için organizasyon yapısını tanımlamalıdır. Tüm ana alanlar kalite planlarını, kriter ve politikalara uygun olarak geliştirir ve kalite verilerinin kaydı tutulmalıdır. KYS 'nin etkililiği ve kabul edilebilirliğini takip edilerek ölçülmelidir ve gerektiğinde iyileştirilmelidir.

PO8.2 BT Standartları ve Kalite Uygulamaları

Kalite Yönetim Sistemi niyetine ulaşma konusunda müesseseye kılavuzluk etmek üzere ana BT süreçleri için standart, prosedür ve uygulamaları tanımlanmalıdır ve sürdürülmelidir. Müessesenin kalite uygulamaları iyileştirilmelidir ve planlarken sektörün en iyi uygulamaları kullanılmalıdır.

PO8.3 Geliştirme ve Tedarik Standartları

Nihai elde edilebilenin hayat döngüsünü takip eden tüm geliştirme ve tedarikler için standartlar oluşturulmalıdır ve sürdürülmelidir. Kararlaştırılan onay kriterleri bazında ana kilometre taşlarında onay kullanılmalıdır. Dikkate alınacak konular arasında yazılım kodlama standartları; isimlendirme kararları; dosya biçimleri; şema ve veri sözlüğü tasarım standartları; kullanıcı arabirimi standartları; karşılıklı çalışabilirlik; sistem performans verimliliği; ölçeklenebilirlik; geliştirme ve test standartları; şartlara göre doğrulama; test planları ve birim, regresyon ile entegrasyon testleri bulunmalıdır.

PO8.4 Müşteri Odağı

Müşterilerin şartlarını tespit ederek ve bu şartları Bilgi Teknolojileri standart ve uygulamalarına entegre ederek kalite yönetiminin müşterilere odaklanması sağlanmalıdır. Kullanıcı/müşteri ile BT müessesesi arasındaki anlaşmazlıkların çözümü ile ilgili rol ve sorumluluklar tanımlanmalıdır.

PO8.5 Sürekli İyileştirme

Sürekli iyileştirmeyi kolaylaştıran genel kalite planı sürdürülmeli ve düzenli açıklanmalıdır.

PO8.6 Kalite Ölçümü, Takip ve Gözden Geçirme

KYS ve KYS 'nin sunmuş olduğu değere sürekli uyumu takip etmek için gerekli ölçümler tanımlanmalı ve uygulanmalıdır. Bilgilerin ölçüm, takip ve kaydedilmesi süreç sahibi tarafından ilgili düzeltme ve önleme faaliyetlerinde bulunmak için kullanılmalıdır.

4.2.1.9 PO9 BT Risklerini Değerlendirerek Yönetme

PO9.1 BT ve İş Riski Yönetiminin Uyumlaştırılması
PO9.2 Risk Bağlamının Tespiti
PO9.3 Olay Tanımlama
PO9.4 Risk Değerlendirme
PO9.5 Risk Yanıtı
PO9.6 Risk Faaliyet Planının Sürdürülmesi ve Takibi

PO9.1 BT ve İş Riski Yönetiminin Uyumlaştırılması

BT yönetimi, risk yönetimi ve kontrol çerçevesini müessesenin (işletmenin) risk yönetimi çerçevesiyle entegre edilmelidir. Bu, müessesenin risk alınabilirlik ve riske tahammül seviyesiyle uyumlaştırmayı da kapsamaktadır.

PO9.2 Risk İçeriğinin Tespiti

Uygun sonuçları sağlamak için risk değerlendirme çerçevesinin uygulandığı içerik tespit edilmelidir. Her risk değerlendirmesinin iç ve dış bağlamının tespiti, değerlendirmenin amacı ve riskler değerlendirilirken kullanılacak kriterler bu kapsam dahil edilmelidir.

PO9.3 Olay Tanımlama

İş, yönetmenlik, yasa, teknoloji, ticari ortak, insan kaynakları ve işlevsel unsurlar dahil olmak üzere, işletmenin hedeflerine potansiyel bir etkiye sahip olan tüm olaylar tanımlanmalıdır. Olumlu ya da olumsuz olmak üzere etkinin özelliği de tespit edilerek bu bilgiler sürdürülmelidir.

PO9.4 Risk Değerlendirme

Tekrarlanabilirlik bazında nicel ve nitel yöntemler kullanarak tanımlanmış tüm risklerin ihtimal ve etkisi değerlendirilmelidir. İçsel ve arta kalan riskle ilgili ihtimal ve etki ayrı-ayrı olarak, kategoriye göre portföy bazında tespit edilmelidir.

PO9.5 Risk Yanıtı

Risk sahibi ile etkilenen süreç sahipleri tespit edilmelidir, uygun maliyetli kontrol ve güvenlik önlemlerinin sürekli olarak risklere karşı savunmasızlığı hafifletmesini sağlamak için risk yanıtı geliştirilerek sürdürülmelidir. Risk yanıtı, önleme, azaltma, paylaştırma yada kabul şeklinde risk stratejilerini tanımlamalıdır. Yanıtı geliştirirken maliyet ve faydaları dikkate alınız ve arta kalan riskleri belirli risk tahammül sınırları içerisinde tutan yanıtlar tercih edilmelidir.

PO9.6 Risk Faaliyet Planının Sürdürülmesi ve Takibi

Maliyet, fayda ve uygulama sorumluluğunun tespit edilmesi dahil olmak üzere gerekli olarak tanımlanan risk yanıtlarının uygulanması amaçlı kontrol faaliyetler tüm seviyelerde önceliklendirilerek planlanmalıdır. Önerilen faaliyetler için onay ve arta kalan tüm riskler için kabul istenmelidir, yapılan faaliyetlerin, etkilenen süreç sahibi (sahipleri) tarafından sahiplenmesi sağlanmalıdır. Planların yerine getirilmesi takip edilerek tüm sapmalar üst düzey yönetime raporlanmalıdır.

4.2.1.10 PO10 Projeleri Yönetme

PO10.1 Program Yönetim Çerçevesi
PO10.2 Proje Yönetim Çerçevesi
PO10.3 Proje Yönetim Yaklaşımı
PO10.4 Paydaş Bağlılığı
PO10.5 Proje Kapsam Beyanı
PO10.6 Proje Aşamasının Başlatılması
PO10.7 Entegre Proje Planı
PO10.8 Proje Kaynakları
PO10.9 Proje Risk Yönetimi
PO10.10 Proje Kalite Planı
PO10.11 Proje Değişiklik Kontrolü
PO10.12 Güvence Yöntemlerinin Proje Planlaması
PO10.13 Proje Performansının Ölçülmesi, Raporlanması ve Takibi
PO10.14 Proje Kapanışı

PO10.1 Program Yönetim Çerçevesi

Projeler tespit edilmelidir, tanımlanmalıdır, değerlendirmelidir, önceliklendirilmelidir, seçilmelidir, başlatılmalıdır, yönetilmelidir ve kontrol edilmelidir. BT-etkili yatırım programlarının portföyüyle ilgili projelerin programını tutulmalıdır. Projelerin, program hedeflerini desteklemesi sağlanmalıdır. Çoklu projelerin faaliyet ve birbirine bağlılığını koordine edilmelidir, program içindeki tüm projelerin beklenen sonuçlara katkısını yönetilmelidir ve kaynak ihtiyaçları ile anlaşmazlıkları çözülmelidir.

PO10.2 Proje Yönetim Çerçevesi

Projeleri yönetmenin kapsamı ve sınırlarını, ayrıca da üstlenilen her projede benimsenen ve uygulanan yöntem sistemlerini tanımlayan bir proje yönetim çerçevesi kurularak sürdürülmelidir. Yöntem sistemleri minimum olarak projelerin başlangıç, planlama, yürütme, kontrol ve kapanış aşamaları, ayrıca da kontrol noktaları ve onayları kapsamalıdır. Çerçeve ve destek niteliğindeki yöntem sistemleri, işletme portföy yönetimi ve program yönetim süreçleriyle entegre edilmelidir.

PO10.3 Proje Yönetim Yaklaşımı

Her projenin boyut, karmaşıklık ve yönetmenlik gereksinimleriyle orantılı birer proje yönetim yaklaşımı oluşturulmalıdır. Proje yönetim yapısı program sponsorunun rol, sorumluluk ve hesap verebilirlikleri, proje sponsorları, yürütme komitesi, proje bürosu ile proje müdürü ve bunların söz konusu sorumlulukları (raporlama ve aşamaların gözden geçirilmesi gibi) yerine getirebilecekleri mekanizmaları içermelidir. Tüm BT projelerinin, stratejik programın tamamı boyunca projenin yürütülmesini sahiplenmek için yeterli yetkiye sahip sponsorların bulunmasına dikkat edilmelidir.

PO10.4 Paydaş Bağlılığı

Projenin, BT-etkili yatırım programının tamamı bağlamı dahilinde tanımlanmalıdır ve yürütülmesinden etkilenen paydaşların bağlılık ve katılımı sağlanmalıdır.

PO10.5 Proje Kapsam Beyanı

Paydaşlar arasında projenin ve, BT-etkili yatırım programının tamamı içerisindeki diğer projelerle nasıl bağlantılı olduğunun genel olarak anlaşılmasını sağlamak ve bu anlayışı geliştirmek amacıyla projenin özellik ve kapsamı tanımlanarak belgelenmelidir. Proje başlatılmadan önce söz konusu proje sponsorlar tarafından resmi olarak onaylanmalıdır.

PO10.6 Proje Aşamasının Başlatılması

Ana proje aşamalarının başlatılmasının resmi olarak onaylanarak tüm paydaşlara bildirilmesi sağlanmalıdır. Başlangıç aşamasının onaylanması, program yönetimi kararlarına bağlı olmalıdır. Sonraki aşamaların onayı bir önceki aşamada elde edilenlerin gözden geçirilerek kabul edilmesi ve programın bir sonraki büyük gözden geçirilişinde güncellenmiş iş olurluk incelemesinin onaylanmasına bağlı olmalıdır. Proje aşamalarının üst üste binmesi (örtüşmesi) durumunda onay noktası, projenin ilerlemesinin onaylanması için program ve proje sponsorları tarafından tespit edilmelidir.

PO10.7 Entegre Proje Planı

Proje ömrü boyunca projenin yürütülmesi ve proje kontrolüne kılavuzluk etmek üzere (iş ve bilişim sistemleri kaynaklarını kapsayan) resmi, onaylı ve entegre bir proje planı oluşturulmalıdır. Çoklu projelerin program içindeki faaliyet ve birbirine bağlılıkları anlaşılmalı ve belgelenmelidir. Proje planı, projenin ömrü boyunca sürdürülmelidir. Proje planı ve ona yapılan değişiklikler, program ve proje yönetim çerçevesine uygun olarak onaylanmalıdır.

PO10.8 Proje Kaynakları

Proje takım üyelerinin sorumluluk, ilişki, yetkiler ve performans kriterleri tanımlanmalıdır ve projede yetkin personelin ve/veya sözleşmeli elemanların alınarak görevlendirilmesi için temel tanımlanmalıdır. Her proje için gerekli ürün ve hizmetlerin istihsali, müessesenin istihsal uygulamalarını kullanarak proje hedeflerine ulaşmak için planlanmalıdır ve yönetilmelidir.

PO10.9 Proje Risk Yönetimi

İstenmeyen değişikliklere neden olma potansiyeli bulunan alan yada olaylar için sistematik bir planlama, tanımlama, analiz, yanıt, takip ve kontrol süreciyle ayrı projelerle ilgili spesifik riskler ortadan kaldırılmalıdır yada en aza indirgenmelidir. Proje yönetim süreci ve projeden elde edilenlerin maruz kaldığı riskler tespit edilmeli ve kesinlikle kayda geçirilmelidir.

PO10.10 Proje Kalite Planı

Proje kalite sistemi ve bu sistemin nasıl uygulanacağını tanımlayan bir kalite yönetim planı hazırlanmalıdır. Plan, ilgili tüm taraflarca resmi olarak gözden geçirilerek kararlaştırılmalı ve daha sonra entegre proje planına alınmalıdır.

PO10.11 Proje Değişiklik Kontrolü

Projenin ana kısmına (örn. maliyet, program, kapsam ve kalite) yapılan tüm değişiklikler gerektiği şekilde gözden geçirilmelidir, onaylanmalıdır ve entegre proje planına program ve proje yönetim çerçevesine uygun olarak konulması için her proje için değişiklik kontrol sistemi oluşturulmalıdır.

PO10.12 Güvence Yöntemlerinin Proje Planlaması

Proje planlama sırasında yeni yada değiştirilen sistemlerin akreditasyonu (tanınmasını) desteklemek için gerekli güvence görevlerini tespit ederek bunları entegre proje planı kapsamına alınmalıdır. Görevler, iç kontrol ve güvenlik özelliklerinin tanımlanan şartlara uygun olduğunun güvencesini sağlamalıdır.

PO10.13 Proje Performansının Ölçülmesi, Raporlanması ve Takibi

Proje performansı ana proje kriterlerine (örn. kapsam, program, kalite, maliyet ve risk) göre ölçülmelidir; gerçekleşen tüm plandan saplamaları tespit edilmelidir; bunların proje ve program geneline olan etkisini değerlendirilmelidir; sonuçları ana paydaşlara bildirilmelidir; ve gerektiğinde program ve proje yönetim çerçevesine uygun olarak sorun giderme faaliyetleri önerilmelidir, uygulanmalıdır ve takibini yapılmalıdır.

PO10.14 Proje Kapanışı

Her projenin sonunda proje paydaşlarının, projenin planlanan sonuç ve faydaları sağlayıp sağlamadığını tespit etmeleri talep edilmelidir. Projenin planlanan sonuçları ve programın faydalarını elde etmek için gerekli, eksik kalmış tüm faaliyetler tespit edilerek bildirilmelidir ve gelecekteki proje ve programlarda kullanılmak üzere alınan tüm ders ve çıkarımlar tespit edilerek belgelenmelidir.

4.2.2 Tedarik ve Uygulama

Tedarik ve Uygulama alanı BT gereksinimlerini belirleme, teknolojiyi satınalma ve kurumun mevcut iş süreçlerine uyarlama için kurumun stratejilerini adreslemektedir. Bu alan aynı zamanda bilgi teknolojileri sisteminin ve parçalarının hayatını sürdürebilmesi için kurumun kabulleneceği bir bakım planı geliştirilmesini içermektedir.

Tedarik ve Uygulama alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır:

- *AI1 Otomatize Edilmiş Çözümleri Tanımlama*
- *AI2 Uygulama Yazılımını Temin Ederek Bulundurma*

- *AI3 Teknoloji Altyapısını Temin Ederek Sürdürme*
- *AI4 Çalışma ve Kullanımı Etkinleştirme*
- *AI5 BT Kaynaklarını Elde Etme*
- *AI6 Değişiklikleri Yönetme*
- *AI7 Çözüm ve Değişikliklerin Kurulması ve Akreditasyonu*

4.2.2.1 AI1 Otomatize Edilmiş Çözümleri Tanımlama

AI1.1 İşletmenin İşlevsel ve Teknik Şartlarının Tanımlanarak Sürdürülmesi
AI1.2 Risk Analiz Raporu
AI1.3 Fizibilite Araştırması ve Alternatif Faaliyet Yollarının Oluşturulması
AI1.4 Şartlar ve Fizibilite Kararı ile Onayı

AI1.1 İşletmenin İşlevsel ve Teknik Şartlarının Tanımlanarak Sürdürülmesi

BT-etkili yatırım programının beklenen sonuçlarını elde etmek için gerekli tüm inisiyatiflerin tam kapsamını dahil eden, işletmenin işlevsel ve teknik şartları tanımlanmalıdır, önceliklendirilmelidir, belirtilmelidir ve kararlaştırılmalıdır. Şartların kabulü için kriterler tanımlanmalıdır. İşletmenin iş, iş süreçleri, insan yetenek ve yetkinlikleri, organizasyon yapısı ve işi kolaylaştıran teknolojisi için gerekli tüm değişiklikler bu inisiyatiflerin kapsamında olmalıdır. İşin işlevsel ihtiyaçları, işletmenin teknolojik yönü, performans, maliyet, güvenilirlik, uyumluluk, denetlenebilirlik, güvenlik, kullanılabilirlik ve süreklilik, ergonomi, kullanım kolaylığı, emniyet ve yasalar ihtiyaçlarda dikkate alınmalıdır. Süregelen sistem tedarik ve geliştirmesinin kontrolü için temel olarak iş ihtiyaçlarının bütünlük, doğruluk ve cariliğini sağlama ve yönetme amaçlı süreçleri oluşturmalıdır. Bu ihtiyaçlar iş sponsoru tarafından sahiplenmelidir.

AI1.2 Risk Analiz Raporu

Müessesenin ihtiyaç geliştirme sürecinin bir parçası olarak iş süreçleriyle ilgili riskler tespit edilmelidir, belgelenmelidir ve analiz edilmelidir. Veri bütünlüğü, güvenliği, kullanılabilirliği, gizliliğine ve yasa ile yönetmenliklere uyuma karşı tehditler riskler arasındadır. Gerekli iç kontrol önlemleri ve denetim izleri bu ihtiyaçların bir parçası olarak tespit edilmelidir.

AI1.3 Fizibilite Araştırması ve Alternatif Faaliyet Yollarının Oluşturulması

İhtiyaçların uygulanabilirliğini inceleyen bir fizibilite araştırması geliştirilmelidir. Araştırma, yazılım, donanım, hizmet ve yetenekler için, işletmenin tespit edilen işlevsel ve teknik ihtiyaçlarını karşılayan alternatif faaliyet yolları tanımlamalıdır ve tanımlanan her faaliyet yolunun, BT-etkili yatırım programı bağlamında teknolojik ve ekonomik fizibilitesini (potansiyel maliyet ve fayda analizi) değerlendirmelidir. İş süreçlerine yapılan değişiklikler, teknoloji ve yetenekler gibi faktörlerin etkileri değerlendirildikçe fizibilite araştırmasının geliştirilmesinde çok sayıda yineleme gerçekleşebilir. BT işleviyle desteklenen iş yönetimi fizibilite ve alternatif faaliyet yollarını değerlendirmeli ve iş sponsoruna öneride bulunmalıdır.

AI1.4 Şartlar ve Fizibilite Kararı ile Onayı

Önceden tespit edilen önemli aşamalarda iş sponsoru işletmenin işlevsel ve teknik ihtiyaçları onaylanmalıdır teyit edilmelidir. Her teyit, kalite incelemelerinin başarılı bir şekilde geçmesi sonrası gerçekleşir. Çözüm ve tedarik yaklaşımı kararıyla ilgili nihai karar hakkı iş sponsoruna aittir.

4.2.2.2 AI2 Uygulama Yazılımını Temin Ederek Bulundurma

AI2.1 Üst Düzey Tasarım
AI2.2 Ayrıntılı Tasarım
AI2.3 Uygulama Kontrolü ve Denetlenebilirliği
AI2.4 Uygulama Güvenliği ve Kullanılabilirliği
AI2.5 Tedarik Edilen Uygulama Yazılımının Konfigürasyon (Yapılandırma) ve Uygulanması
AI2.6 Mevcut Sistemler için Ana Upgrade'ler (Yükseltimler)
AI2.7 Uygulama Yazılımının Geliştirilmesi
AI2.8 Yazılım Kalite Güvencesi
AI2.9 Uygulama İhtiyaçlarının Yönetimi
AI2.10 Uygulama Yazılımının Sürdürülmesi

AI2.1 Üst Düzey Tasarım

Müessesenin teknolojik yönü ve bilgi mimarisini dikkate alarak iş ihtiyaçları yazılım geliştirme için üst düzey tasarım spesifikasyonuna çevrilmelidir ve üst düzey tasarımının ihtiyaçlara cevap vermesini sağlamak için tasarım spesifikasyonları onaylanmalıdır.

AI2.2 Ayrıntılı Tasarım

Ayrıntılı yasarım ve teknik yazılım uygulama ihtiyaçları hazırlanmalıdır. İhtiyaçların kabulü için kriterler belirlenmelidir. Üst düzey tasarıma uygun olmalarını sağlamak için ihtiyaçlar onaylanmalıdır. Sınırlama konulmaksızın kapsama alınacaklar arasında giriş şartı tanımlaması ve belgeleri, arabirim tanımı, kullanıcı arabirimi, kaynak verilerini toplama tasarımı, program spesifikasyonu, dosya ihtiyaçlarının tanımı ve belgeleri, süreç ihtiyaçları, çıkış şartının tanımı, kontrol ve denetlenebilirlik, güvenlik ve kullanılabilirlik ve testler bulunmaktadır. Geliştirme yada sürdürme sırasında önemli teknik yada mantıksal tutarsızlıkların ortaya çıkması halinde değerlendirme yeniden yapılmalıdır.

AI2.3 Uygulama Kontrolü ve Denetlenebilirliği

İş kontrollerinin, sürecin doğru, tam, zamanlı, yetkili ve denetlenebilir olacağı şekilde, gerektiği gibi uygulama kontrollerine çevrilmesi sağlanmalıdır. Özellikle ele alınacak konular yetkilendirme mekanizmaları, bilgi bütünlüğü, erişim kontrolü, yedekleme ve denetim izlerinin tasarımı konuları olmalıdır.

AI2.4 Uygulama Güvenliği ve Kullanılabilirliği

Tespit edilen risklere cevap ve veri sınıflandırılması, müessesenin bilgi güvenliği mimarisi ve risk profiline uygun olarak uygulama güvenliği ve kullanılabilirliği ele alınmalıdır. Ele alınacak konular arasında erişim hakları ve imtiyazların yönetimi, tüm aşamalarda hassas bilginin korunması, doğrulama ve işlem bütünlüğü ve otomatik kurtarma bulunmalıdır.

AI2.5 Tedarik Edilen Uygulama Yazılımının Konfigürasyon (Yapılandırma) ve Uygulanması

Yapılandırma, kabul ve test prosedürlerini kullanarak iktisat edilen otomatize işlevselliği uyarlanarak uygulanmalıdır. Ele alınarak konular arasında sözleşme şartlarına göre doğrulama, müessesenin bilgi mimarisi, mevcut uygulamalar, mevcut uygulama ve veritabanı sistemleriyle karşılıklı çalışabilirlik, sistem performans verimi, belgeler ve kullanım kılavuzları, entegrasyon ve sistem test planları bulunmalıdır.

AI2.6 Mevcut Sistemler için Ana Upgrade'ler (Yükseltimler)

Mevcut tasarımlar ve/veya işlevsellikte ciddi değişikliklere sebebiyet veren, mevcut sistemler ve büyük değişiklikler durumunda, yeni sistemlerin geliştirilmesine benzer geliştirme süreci izlenmelidir. Ele alınacak konular arasında etki analizi, maliyet/fayda doğrulaması ve ihtiyaçların yönetilmesi bulunmalıdır.

AI2.7 Uygulama Yazılımının Geliştirilmesi

Otomatize işlevselliğin tasarım spesifikasyonlarının, geliştirme ve belge standartları ve kalite şartlarına göre geliştirilmesi sağlanmalıdır. İşlevsellik, performans ve kalite incelemelerinin başarılı bir şekilde yapılmasından sonra uygulama yazılımını geliştirme sürecinin her ana aşamasına onay verilerek teyit edilmelidir. Ele alınacak konular arasında tasarım spesifikasyonlarının iş, işlevsellik ve teknik ihtiyaçlarına uygun olduğuna dair onay; değişiklik taleplerinin onaylanması; ve uygulama yazılımının üretime uygun olup göç için hazır olduğu teyidi bulunmalıdır. Bunun yanı sıra, tüm yasal ve sözleşme ile ilgili unsurların tanımlanarak üçüncü taraflarca geliştirilen uygulama yazılımlarıyla ilgili olarak ele alınması sağlanmalıdır.

AI2.8 Yazılım Kalite Güvencesi

İhtiyaçlar tanımı ve müessesenin kalite politika ve prosedürlerinde belirtilen kaliteyi elde etmek için bir kalite güvence planı geliştirilmelidir ve plan için kaynak tahsis ederek plan uygulanmalıdır. Kalite güvencesi planında ele alınacak konular arasında kalite kriterleri belirtilmelidir ve, inceleme, deneme ve testler dahil, doğrulama ve kontrol süreçleri bulunmalıdır.

AI2.9 Uygulama İhtiyaçlarının Yönetimi

Tasarım, geliştirme ve uygulama sırasında ayrı ihtiyaçların (reddedilen tüm ihtiyaçlar dahil olmak üzere) durumu takip edilmelidir ve ihtiyaçlara yapılan değişikliklerin kurulu bir değişiklik yönetim süreci ile onaylanması sağlanmalıdır.

AI2.10 Uygulama Yazılımının Sürdürülmesi

Yazılım uygulamalarının sürdürülmesi ve onaylanması için strateji ve plan geliştirilmelidir. Ele alınacak konular arasında onay planlama ve kontrolü, kaynak planlama, küçük hata giderimi ve hataların düzeltilmesi, küçük iyileştirmeler, belgelerin bulundurulması, acil durum değişiklikleri, diğer uygulama ve altyapı ile karşılıklı bağlılık, yükseltme stratejileri,

destek konuları ve yükseltmeler gibi sözleşme şartları, iş ihtiyaçlarına göre periyodik gözden geçirme, riskler ve güvenlik şartları bulunmalıdır.

4.2.2.3 AI3 Teknoloji Altyapısını Temin Ederek Sürdürme

AI3.1 Teknoloji Altyapısı Tedarik Planı
AI3.2 Altyapı Kaynaklarının Korunması ve Kullanılabilirliği
AI3.3 Altyapının Bakımı (Sürdürülmesi)
AI3.4 Fizibilite Testi Ortamı

AI3.1 Teknoloji Altyapısı Tedarik Planı

İşletmenin kurulu işlevsel ve teknik ihtiyaçlarını karşılayan ve müessesenin teknoloji yönüne uygun olan teknoloji altyapısının tedarik, uygulama ve sürdürülmesi için bir plan geliştirilmelidir. Planda, gelecekteki kapasite eklentileri için esneklik, geçiş masrafları, teknik riskler ve teknoloji yükseltmeleri (upgrades) için yatırımın ömrü dikkate alınmalıdır. Yeni teknik kapasite eklenirken karmaşıklık maliyetleri ve satıcı ile ürünün ticari olarak ayakta kalma şansı (finansal kapasitesini) değerlendirilmelidir.

AI3.2 Altyapı Kaynaklarının Korunması ve Kullanılabilirliği

Kaynakları korumak ve kullanılabilirlik ile bütünlüğü sağlamak için donanım ve altyapısal yazılımın yapılandırma, entegrasyon ve bakımı (sürdürülmesi) sırasında iç kontrol, güvenlik ve denetlenebilirlik önlemleri uygulanmalıdır. Hassas altyapı bileşenlerinin kullanımıyla ilgili sorumluluklar net bir şekilde tanımlanmalıdır ve altyapı bileşenlerini geliştiren ve entegre edenler tarafından anlaşılmalıdır. Bunların kullanımı takip edilmelidir ve değerlendirilmelidir.

AI3.3 Altyapının Bakımı (Sürdürülmesi)

Altyapının sürdürülmesi için bir strateji ve plan geliştirilmelidir ve değişikliklerin, müessesenin değişiklik yönetim prosedürüne göre kontrol edilmesi sağlanmalıdır. İş ihtiyaçlarına göre periyodik gözden geçirme, yama yönetimi ve yükseltme (upgrade) stratejileri, riskler ve güvenlik ihtiyaçları kapsam dahiline alınmalıdır.

AI3.4 Fizibilite Testi Ortamı

Tedarik ve geliştirme sürecinin erken aşamalarında uygulama ve altyapının etkili ve verimli fizibilite ve entegrasyon testini desteklemek amacıyla geliştirme ve test ortamları

oluşturulmalıdır. İşlevsellik, donanım ve yazılım konfigürasyonu, entegrasyon ve performans testi, ortamlar arasında göç, versiyon kontrolü, test araçları ve güvenliği ele alınmalıdır.

4.2.2.4 AI4 Çalışma ve Kullanımı Etkinleştirme

AI4.1 İşlemsel Çözümleri için Planlama
AI4.2 İşletme Yönetimine Bilgi Transferi
AI4.3 Son Kullanıcılara Bilgi Transferi
AI4.4 İşlemler ve Destek Personeline Bilgi Transferi

AI4.1 İşletimsel Çözümler için Planlama

Otomatize sistemler yada altyapının kullanıma alınması yada yükseltilmesi (upgrade) sonucunda tüm paydaşların yönetim, kullanıcı ve işlem prosedürlerinin üretilmesinde zamanında sorumluluk alabileceği şekilde tüm teknik unsurlar, işlemsel kapasite ve gerekli hizmet seviyelerini tanımlamak ve belgelemek amacıyla bir plan geliştirilmelidir.

AI4.2 İşletme Yönetimine Bilgi Transferi

Sistem ve verileri sahiplenmeleri ve hizmetlerin sunulması ile kalite, iç kontrol ve yönetim süreçlerinin uygulanmasından kaynaklanan sorumluluğu icra etmelerine izin vermek için işletme yönetimine bilgi transfer edilmelidir. Bilgi transferi erişim onayı, imtiyaz yönetimi, görevlerin ayrıştırılması, otomatik iş kontrolleri, yedekleme/kurtarma, fiziksel güvenlik ve kaynak belgelerin arşivlenmesini kapsamalıdır.

AI4.3 Son Kullanıcılara Bilgi Transferi

Son kullanıcılara, iş süreçlerini desteklemek amacıyla, uygulama sistemini etkili ve verimli bir şekilde kullanmalarına izin vermek için bilgi ve yetenek transferi gerçekleştirilmelidir. Bilgi transferi, başlangıçtaki ve devam eden eğitim ve yetenek gelişimi, eğitim materyalleri, kullanım kılavuzları, prosedür kılavuzları, çevrimiçi yardım, hizmet masası desteği, ana kullanıcının tanımlanması ve değerlendirilmesi konularını ele almak için bir Eğitim Prosedür'ünün geliştirilmesini kapsamalıdır.

AI4.4 İşlemler ve Destek Personeline Bilgi Transferi

İşlemler ve destek personelinin uygulama sistemi ve ilgili altyapıyı gerekli hizmet seviyelerine göre etkili ve verimli sağlama, destekleme ve sürdürmesine izin vermek için bilgi

ve yetenek transferi gerçekleştirilmelidir. Bilgi transferi başlangıçtaki ve devam eden eğitim ve yeteneklerin gelişimi, eğitim materyalleri, çalışma kılavuzları, prosedür kılavuzları ve hizmet masası senaryolarını içermelidir.

4.2.2.5 AI5 BT Kaynaklarını Elde Etme

AI5.1 Tedarik Kontrolü
AI5.2 Tedarikçi Sözleşmesinin Yönetimi
AI5.3 Tedarikçi Seçimi
AI5.4 Yazılım Tedariği
AI5.5 Geliştirme Kaynaklarının Tedariği
AI5.6 Altyapı, Tesis ve İlgili Hizmetlerin Tedariği

AI5.1 Tedarik Kontrolü

BT ile ilgili altyapı, tesis, donanım, yazılım ve hizmetlerin iş ihtiyaçlarını karşılamasını sağlanmak için iş müessesinin genel istihsal süreci ve tedarik stratejisine uygun bir takım prosedür ve standartlar geliştirilerek bunlar izlenmelidir.

AI5.2 Tedarikçi Sözleşmesinin Yönetimi

Tüm tedarikçilerle sözleşmelerin akdedilmesi, değiştirilmesi ve feshi için bir prosedür oluşturulmalıdır. Prosedür minimum olarak, yasal konular, mali konular, organizasyon konuları, belge konuları, performans, güvenlik, güvenlik, fikri mülkiyet ve fesih sorumluluklar ve yükümlülüklerini (ceza hükümleri dahil) kapsamalıdır. Tüm sözleşme ve sözleşme değişiklikleri hukuk danışmanları tarafından incelenmelidir.

AI5.3 Tedarikçi Seçimi

Potansiyel tedarikçilerden alınan bilgi ile geliştirilmiş ve müşteri ile tedarikçi(ler) arasında kararlaştırılmış şartlar bazında sürdürülebilir en uygun alternatifi sağlamak için tedarikçiler adil ve resmi bir uygulamaya göre seçilmelidir.

AI5.4 Yazılım Tedariği

Tedarik ile ilgili tüm taahhüt sözleşmelerinde müessesenin çıkarlarının korunması sağlanmalıdır. Tedarik konusu yazılımın devam eden kullanımı için sözleşme şartlarına tüm

tarafların hak ve sorumlulukları dahil edilerek icra edilmelidir. Bu hak ve sorumluluklar arasında fikri mülkiyetin mülkiyet hakları ve lisanslanması, bakım, garantiler, mahkeme prosedürleri, yükseltme (upgrade) şartları ve güvenlik, emanet ve erişim hakları dahil olmak üzere amacına uygunluk bulunmalıdır.

AI5.5 Geliştirme Kaynaklarının Tedariği

Tedarik ile ilgili tüm taahhüt sözleşmelerinde müessesenin çıkarlarının korunması sağlanmalıdır. Tedarik konusu geliştirme kaynaklarının dağıtımı için sözleşme şartlarına tüm tarafların hak ve sorumlulukları dahil edilerek icra edilmelidir. Bu hak ve sorumluluklar arasında fikri mülkiyetin mülkiyet hakları ve lisanslanması, geliştirme yöntem sistemleri, diller, test, istenilen performans kriterleri, performansın incelenmesi, ödeme temeli, garantiler, mahkeme prosedürleri, insan kaynakları yönetimi ve müessesenin politikalarına uyum dahil kalite yönetim süreçleri bulunmalıdır.

AI5.6 Altyapı, Tesis ve İlgili Hizmetlerin Tedariği

Altyapı, tesis ve ilgili hizmetlerin tedariği için kabul kriterleri dahil olmak üzere sözleşme şartlarına tüm tarafların hak ve sorumlulukları dahil edilerek icra edilmelidir. Bu hak ve sorumluluklar arasında hizmet seviyeleri, bakım prosedürleri, erişim kontrolleri, güvenlik, performans incelemesi, ödeme temeli ve mahkeme prosedürleri bulunmalıdır.

4.2.2.6 AI6 Değişiklikleri Yönetme

AI6.1 Standart ve Prosedürleri Değiştiriniz
AI6.2 Etki Değerlendirmesi, Önceliklendirme ve Yetkilendirme
AI6.3 Acil Durum Değişiklikleri
AI6.4 Değişiklik Durumunun İzlenmesi ve Raporlanması
AI6.5 Değişikliğin Kapanışı ve Belgelenmesi

AI6.1 Standart ve Prosedürleri Değiştiriniz

Uygulama, prosedür, süreç, sistem ve hizmet parametreleri ile temelinde bulunan platformlara yapılan değişikliklerle ilgili tüm talepleri (bakım ve yamalar dahil) standartlaştırılmış bir şekilde işlemden geçirmek için resmi değişiklik yönetimin prosedürleri oluşturulmalıdır.

AI6.2 Etki Değerlendirmesi, Önceliklendirme ve Yetkilendirme

Tüm değişiklik taleplerinin, işletim sistemi ve onun işlevselliği üzerindeki etkiler bakımından yapılandırılmış bir şekilde değerlendirilmesi sağlanmalıdır. Bu değerlendirme değişikliklerin kategorilere ayrılması ve önceliklendirilmesini içermelidir. Üretime geçişten önce değişiklikler için ilgili paydaş tarafından onay verilmelidir.

AI6.3 Acil Durum Değişiklikleri

Kurulu değişiklik sürecini izlemeyen acil durum değişikliklerin tanımlanması, geliştirilmesi, değerlendirilmesi ve onaylanması için bir süreç oluşturulmalıdır. Belgeleme ve testler muhtemelen, acil durum değişikliği yapıldıktan sonra yapılır.

AI6.4 Değişiklik Durumunun İzlenmesi ve Raporları

Raporlama sistemi oluşturulmalıdır.

AI6.5 Değişikliğin Kapanışı ve Belgelenmesi

Sistem değişiklikleri her uygulandığında ilgili sistem ve kullanıcı belgeleri ile prosedürleri ona göre güncellenmelidir. Değişikliklerin eksiksiz olarak uygulanmasını sağlamak için gözden geçirme süreci oluşturulmalıdır.

4.2.2.7 AI7 Çözüm ve Değişikliklerin Kurulması ve Akreditasyonu

AI7.1 Eğitim
AI7.2 Test Planı
AI7.3 Uygulama Planı
AI7.4 Test Ortamı
AI7.5 Sistem ve Veri Dönüşümü
AI7.6 Değişikliklerin Test Edilmesi
AI7.7 Son Kabul Testi
AI7.8 Üretim Promosyonu
AI7.9 Yazılım Sürümü
AI7.10 Sistem Dağıtımı
AI7.11 Değişikliklerin Kaydı ve İzlenmesi

AI7.1 Eğitim

Her enformasyon sistemi gelişiminin, uygulama veya modifikasyon projesinin bir parçası olarak, tanımlanan eğitim ve uygulama planı ve yardımcı materyaller ile birlikte BT fonksiyonu operasyon ve etkilenen kullanıcı bölümleri kadrosunun eğitimi sağlanmalıdır.

AI7.2 Test Planı

Bir test planı hazırlanması ve ilgili taraflardan onay alınmasıdır. Test planı kurum genelindeki standartlara dayanmalıdır ve rolleri, sorumlulukları ve başarı kriterleri tanımlanmalıdır. Plan hazırlanırken test hazırlığı (site hazırlığı dahil), eğitim gereklilikleri, tanımlanan test ortamının kurulması veya güncellenmesi, test vakalarının planlanması/ gerçekleştirilmesi/ belgelenmesi/ elde tutulması, hata işlemleri ve düzeltmeler, ve resmi onay dikkate alınmalıdır. Sistem başarısızlığı risk değerlendirmesi ve uygulama hatalarına dayanarak, plan performans, stres, kullanışlılık, pilot ve güvenlik testi için gereklikleri içermelidir.

AI7.3 Uygulama Planı

Bir uygulama planı oluşturulmalıdır ve ilgili taraflardan onay alınmalıdır. Plan, sürüm tasarımını, sürüm paketlerinin oluşturulmasını, ürünün yeni pazarlara girişi prosedürlerini/kurulumunu, olay işlemlerini, dağıtım kontrollerini (araçlar dahil), yazılım saklanmasını, sürüm revizyonunu ve değişikliklerin belgelenmesini tanımlar.

AI7.4 Test Ortamı

Test için ayrı bir test ortamı hazırlanmalıdır. Bu ortam sağlam testler için gelecek operasyonlar ortamını (örn. Benzer güvenlik, iç kontroller ve iş yükleri) yansıtmalıdır. Test ortamında kullanılan prosedürlerin üretim ortamında kullanılacak verilerin (gerekirse temizlenmiş) temsilcisi olmasını sağlamak için prosedürler yerinde olmalıdır. Hassas test verilerinin açıklanmasını önlemek için yeterli önlemler alınmalıdır. Belgelendirilmiş test sonuçları elde tutulmalıdır

AI7.5 Sistem ve Veri Dönüşümü

Kurumun gelişme metotlarının tüm gelişme, uygulama veya modifikasyon projelerinin, donanım, yazılım, işlem verileri, veri dosyaları, yedekleme ve arşivler, diğer sistemlerle ara yüzler, prosedürler, sistem dokümantasyonu gibi tüm gerekli unsurların eski sistemden yenisine önceden belirlenmiş bir plana göre dönüştürmesi sağlanmalıdır. Dönüşüm öncesi ve sonrası sonuçlarının bir denetim raporu hazırlanmalıdır ve korunmalıdır. Yeni sistemin ilk

sürecinin detaylı bir doğrulaması başarılı geçişi konfirme etmek için sistem sahipleri tarafından yapılmalıdır.

AI7.6 Değişikliklerin Test Edilmesi

Düzenli operasyonel ortamda kullanılmaya başlamadan değişikliklerin bağımsız (kuruculardan oluşan) bir test grubu tarafından ayrı bir test ortamında performans boyutunu içeren etki ve kaynak değerlendirmesine dayanan ve tanımlanan kabul planı ile uygun olarak test edilmesi sağlanmalıdır. Planın parçası olarak paralel veya pilot testi düşünülmelidir. Güvenlik kontrolleri, açılımdan önce test edilmeli ve değerlendirilmelidir, bu şekilde güvenlik etkinliği belgelenebilir. Geri çekme planları da üretim değişikliği promosyonundan önce geliştirilmelidir ve test edilmelidir.

AI7.7 Son Kabul Testi

Yeni veya modifiye edilmiş enformasyon sistemlerinin kalite güvence testi veya nihai kabulünün bir parçası olarak, prosedürler, etkilenen kullanıcı bölümleri ve BT fonksiyon yönetimi tarafından test sonuçlarının resmi değerlendirmesini ve onayını sağlamalıdır. Testler enformasyon sisteminin tüm unsurlarını (örn. Uygulama yazılımı, tesisler, teknoloji ve kullanıcı prosedürleri) kapsamalı ve tüm unsurların enformasyon güvenlik gerekliliklerini karşılaması sağlanmalıdır. Test verileri denetim ve gelecekteki testler için saklanmalıdır.

AI7.8 Üretime Promosyon

Uygulama planı ile paralel olarak gelişmeden operasyonların test aşamasına kadar sistemin devir teslimini kontrol etmek için resmi prosedürler uygulanmalıdır. Yönetim gereğince sistem sahibi yetkisinin yeni bir sistemin üretime geçmesinden ve eski sistemin iptalinden önce alınmalıdır. Yeni sistemin günlük, aylık, üç aylık ve yıl-sonu üretim devrelerinde çalışması kontrol edilmelidir.

AI7.9 Yazılım Sürümü

Yazılım sürümünde oturumu kapatma, paketleme, regresyon testi, dağıtım, devir teslim, statü izleme, yedekleme prosedürleri ve kullanıcı bildirisi resmi prosedürleri izlenmelidir.

AI7.10 Sistem Dağıtımı

Zamanında ve doğru dağıtımın sağlanması ve onaylanan konfigürasyon ürünlerinin güncellenmesi için kontrol prosedürleri belirlenmelidir. Bunlar arasında entegre kontrolleri,

yapan, test eden ve işletenler arasındaki görev ayrımı; ve tüm eylemlerin uygun denetim raporları olmalıdır.

AI7.11 Değişikliklerin Kaydı ve İzlenmesi

Uygulamalar, prosedürler, süreçler, sistem ve hizmet parametreleri ve altta yatan platformlar için yapılan değişikliklerin kaydı ve izlenmesini desteklemek ve uygulama sistem değişikliklerini izlemek için otomatik sistem kullanılmalıdır.

4.2.3 Hizmet Sunumu ve Destek

Hizmet Sunumu ve Destek alanı bilgi teknolojilerinin teslim yönüne odaklanmaktadır. Bu alan bilgi teknolojileri sistemindeki uygulamaların hayata geçirilmesi ve sonuçları ile bu BT sistemlerinin etkin ve elverişli uyarlanmasını sağlayan destek süreçlerini de kapsamaktadır. Bu destek süreçleri güvenlik konuları ve eğitimini içermektedir.

Hizmet Sunumu ve Destek alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır:

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

4.2.3.1 DS1 Servis Düzeyi Yönetimi

DS1.1 Hizmet Düzeyi Yönetimi Çerçevesi
DS1.2 Hizmetlerin Tanımı
DS1.3 Hizmet Düzeyi Anlaşmaları
DS1.4 İşletim Düzeyi Anlaşmaları
DS1.5 Hizmet Düzeyi Başarılarının İzlenmesi ve Raporlanması
DS1.6 Hizmet Düzeyi Anlaşmaları ve Sözleşmelerinin Revizyonu

DS1.1 Hizmet (Düzeyi) Yönetimi Çerçevesi

Müşteri ve hizmet sağlayıcı arasında resmi hizmet düzey yönetim süreci sağlayan bir çerçeve tanımlanmalıdır. Bu çerçeve iş gereklilikleri ve öncelikleri için sürekli bir sıralama sağlamalı ve müşteri ve tedarikçi(ler) arasında ortak anlayışı kolaylaştırmalıdır. Çerçeve hizmet gerekliliklerinin oluşturulması, hizmet tanımları, hizmet düzeyi anlaşmaları (SLA ler), işletim düzeyi anlaşmaları (OLA ler) ve fon kaynakları için süreçleri içermelidir. Bu yaklaşımlar hizmet kataloğunda organize edilmelidir. Çerçeve iç ve dış hizmet sağlayıcılarının ve müşterilerin rollerini, görev ve sorumluluklarını kapsayan, hizmet düzeyi yönetimi için kurumsal yapıyı tanımlamalıdır.

DS1.2 Hizmetlerin Tanımı

Hizmet kataloğu/portfolyo yaklaşımı uygulaması üzerinden merkezi olarak organize edilen ve saklanan, hizmet özellikleri ve işletme gereklilikleri hakkında BT hizmetlerinin temel tanımlanmalıdır.

DS1.3 Hizmet (Düzeyi) Sözleşmeleri

Müşteri gereklilikleri ve BT kapasitelerine dayanan tüm kritik BT hizmetleri için hizmet düzeyi anlaşmaları tanımlanmalı ve kabül prosedürleri belirlenmelidir. Bu, müşteri taahhütlerini, hizmet destek gerekliliklerini, hissedarlar tarafından sonlandırılan hizmet ölçümü için nicel ve nitel metrikleri, varsa fon ve ticari anlaşmaları, ve SLA gözetimi dahil rol ve sorumlulukları kapsamalıdır. Dikkate alınacak konular, bulunabilirlik, güvenilirlik, performans, büyüme kapasitesi, destek düzeyleri, süreklilik planlaması, güvenlik ve talep sınırları olmalıdır.

DS1.4 Operasyonel Hizmet (Düzeyi) Sözleşmeleri

İşletim düzeyi anlaşmaları optimal tarzda SLA(lar)yı desteklemek için teknik olarak hizmetlerin nasıl dağıtılacağını açıklamalıdır. OLA' lar hizmet sağlayıcıya anlamlı olarak teknik süreçleri belirtmeli ve çeşitli SLA'ları desteklemelidir.

DS1.5 Hizmet (Düzeyi) Başarılarının İzlenmesi ve Raporlanması

Belirtilen hizmet düzeyi performans kriterleri sürekli olarak izlenmelidir. Hizmet düzeyi başarıları hakkında müşteriye anlamlı bir formatta raporlar sunulmalıdır. İzleme istatistikleri analiz edilmeli ve toplam hizmetler için olduğu gibi bireysel hizmetler için de negatif ve pozitif trendlerin tanımlanması için bunlar kullanılmalıdır.

DS1.6 Hizmet (Düzeyi) Anlaşmaları ve Sözleşmelerinin Revizyonu

Hizmet anlaşmaları ve bağlı sözleşmelerin etkin, güncel olmasını ve gerekli değişikliklerin yapılmasını sağlamak için bunlar iç ve dış hizmet sağlayıcıları ile düzenli revize edilmelidir.

4.2.3.2 DS2 Üçüncü Parti Hizmetlerin Yönetilmesi

DS2.1 Tüm Tedarikçi İlişkilerinin Tanımlanması
DS2.2 Tedarikçi İlişkisi Yönetimi
DS2.3 Tedarikçi Risk Yönetimi
DS2.4 Tedarikçi Performans Gözlemi

DS2.1 Tüm Tedarikçi İlişkilerinin Tanımlanması

Tüm tedarikçi hizmetler tanımlanmalı ve bunlar tedarikçi türü, önem ve kritikliğe göre kategorize edilmelidir. Bu tedarikçilerin temsilcilerinin rollerini ve sorumluluklarını, amaçlarını, beklenen teslimlerini ve onaylarını kapsayan teknik ve kurumsal ilişkilerin resmi dokümantasyonu sağlanmalıdır.

DS2.2 Tedarikçi İlişkisi Yönetimi

Her tedarikçi için tedarikçi ilişkisi yönetim süreci formalize edilmelidir. İlişki sahipleri müşteri ve tedarikçi konuları hakkında irtibat kurmalı ve güven ve şeffaflığa dayanarak (örn. Hizmet düzeyi anlaşmaları) ilişki kalitesi sağlanmalıdır.

DS2.3 Tedarikçi Risk Yönetimi

Sürekli temelde güvenli ve etkin bir tarzda hizmet teslimine devam etmek için tedarikçilerin yeteneği ile ilgili riskler tanımlanmalı ve hafifletilmelidir. Yasal ve mevzuat gerekliliklerine uygun olarak sözleşmelerin evrensel işletme standartlarına uygunluğu sağlanmalıdır. Risk yönetimi aynı zamanda gizli anlaşmalar, emanet sözleşmeler, sürekli tedarikçi finansal kapasitesi, güvenlik gerekleri ile uygunluk, para cezaları ve ödülleri de dikkate alınmalıdır.

DS2.4 Tedarikçi Performans Gözlemi

Tedarikçinin mevcut iş gerekliliklerini karşılamasını sağlamak ve sözleşme anlaşmalarına ve hizmet düzeyi anlaşmalarına bağlı kalmasını sağlamak ve performansın alternatif tedarikçiler ve Pazar koşulları ile rekabet etmesi için hizmet dağılımını gözleme süreci geliştirilmelidir.

4.2.3.3 DS3 Performans ve Kapasite Yönetimi

DS3.1 Performans ve Kapasite Planlama
DS3.2 Mevcut Kapasite ve Performans
DS3.3 Gelecekteki Kapasite ve Performans
DS3.4 IT Kaynakların Mevcudiyeti
DS3.5 Gözlem Ve Raporlama

DS3.1 Performans ve Kapasite Planlama

Hizmet anlaşmaları tarafından belirlenen şekilde anlaşılan iş yüklerini işleme koymak için düşük maliyetli kapasite ve performansın mevcut olmasını sağlamak amacıyla BT kaynaklarının performans ve kapasite revizyonu için bir planlama süreci oluşturulmalıdır. Kapasite ve performans planları, mevcut ve tahmin edilen performans modeli, kapasitesi üretmek ve BT kaynakları üretimi için uygun model tekniklerini içermelidir.

DS3.2 Mevcut Kapasite ve Performans

Hizmet düzeyindeki anlaşmaların yerine getirilmesi için yeterli kapasite ve performansın var olup olmadığını belirlemek için BT kaynaklarının performans ve kapasitesi revize edilmelidir.

DS3.3 Gelecekteki Kapasite ve Performans

Yetersiz kapasite veya performans degradasyonuna bağlı olarak hizmet bozukluklarının riskini minimuma indirmek için düzenli aralıklarda BT kaynaklarının performans ve kapasite

tahminleri yapılmalıdır. Performans ve kapasite planlarına girdi sağlamak için tahminler belirlenmeli ve iş yükü trendleri tanımlanmalıdır.

DS3.4 BT Kaynakların Mevcudiyeti

Normal iş yükleri, beklenmeyen olaylar, saklama gereklilikleri ve BT kaynağı yaşam devreleri gibi özellikler dikkate alınarak gereken kapasite ve performans sağlanmalıdır. Görev öncelikleri, hata tolerans mekanizmaları ve kaynak tahsis uygulamaları gibi performans ve kapasitenin istenen düzeye ulaşmadığı durumlarda genel hükümler yapılmalıdır. Yönetim beklenmeyen olay planlarının BT kaynaklarının mevcudiyeti, kapasitesi ve performansını uygun şekilde belirtmesini sağlamalıdır.

DS3.5 Gözlem ve Raporlama

BT kaynaklarının performans ve kapasitesinin sürekli gözlenmelidir. Elde edilen veriler iki amaca hizmet etmelidir:

• BT içindeki mevcut performansın korunması ve düzenlenmesi ve esneklik, beklenmeyen olaylar, mevcut ve projelendirilmiş iş yükleri, saklama planları ve kaynak edinimi gibi konuların belirtilmesi.

• SLA'lar tarafından gereken şekilde işletmeye sağlanan hizmet mevcudiyetinin rapor edilmesi. Düzeltme eylemleri için önerilerle birlikte tüm istisna raporlarının eklenmesi.

4.2.3.4 DS4 Sürekli Hizmetin Sağlanması

DS4.1 IT Süreklilik Çerçevesi
DS4.2 IT Süreklilik Planları
DS4.3 Kritik IT Kaynakları
DS4.4 IT Süreklilik Planının Korunması
DS4.5 IT Süreklilik Planı Testi
DS4.6 IT Süreklilik Planı Eğitimi
DS4.7 IT Süreklilik Planı Dağıtımı
DS4.8 IT Hizmetlerinin Kurtarılması ve Yeniden Başlatılması
DS4.9 Alan Dışı Yedekleme Belleği
DS4.10 Yeniden Başlatma Sonrasında Revizyon

DS4.1 BT Süreklilik Çerçevesi

Sürekli bir süreç ile kurum içinde iş sürekliliği yönetimini desteklemek için, BT sürekliliği, için bir çerçevenin geliştirilmelidir. Çerçevenin amacı, iç yapının istenen esnekliğinin belirlenmesine yardımcı olmak ve afet iyileştirme gelişimini ve BT beklenmeyen olay planlarını yönetmek olmalıdır. Çerçeve, süreklilik yönetimi için kurumsal yapıyı belirtmelidir, bu da iç ve dış hizmet sağlayıcılarının rollerini, görevlerini ve sorumluluklarını, bunların yönetimini ve müşterilerini, kuralları ve belge yapılarını, afet iyileştirme test ve yönetimini ve BT beklenmeyen olay planlarını kapsamalıdır. Plan aynı zamanda, kritik kaynakların tanımlanması, kritik kaynakların mevcudiyet gözlemi ve raporları, alternatif süreçler, alternatif işlemler ve yedekleme ve iyileştirme ilkeleri gibi konuları da belirtmelidir.

DS4.2 BT Süreklilik Planları

Anahtar iş fonksiyonları ve süreçlerdeki temel bozukluğun etkisini azaltmak için tasarlanan çerçeveye dayanan BT süreklilik planları geliştirilmelidir. Planlar esneklik gerekleri, alternatif süreçler ve tüm kritik BT hizmetlerinin iyileştirme kapasitesini belirtmelidir. Bunlar aynı zamanda kullanım kılavuzları, prosedürler, süreçler ve test yaklaşımlarını da kapsamalıdır.

DS4.3 Kritik BT Kaynakları

Esneklik oluşturmak için BT süreklilik planında en önemli olarak belirtilen konular üzerinde odaklanma ve iyileşme durumlarında öncelikler belirlenmelidir. Daha az önemli konuların iyileştirilmesinde dikkatin dağılması önlenmeli ve öncelikli iş ihtiyaçları ile paralel olarak yanıt ve iyileşme sağlanmalı ve maliyetlerin makul bir düzeyde tutulması ve mevzuat ve sözleşme gereklerine uyulması sağlanmalıdır. Farklı bağlayıcılar için esneklik, yanıt ve iyileşme gerekleri dikkate alınmaldır: Örnek; bir – dört saat, dört – 24 saat, 24 saatten fazla ve kritik iş operasyon periyotları.

DS4.4 BT Süreklilik Planının Korunması

BT yönetimi değişiklik kontrol prosedürlerini tanımlama ve yürütme konusu teşvik edilmelidir ve BT süreklilik planının güncel tutulması ve sürekli olarak fiili iş gerekliliklerinin yansıması sağlanmalıdır. Sorumluluklardaki değişiklikler zamanında bildirilmelidir.

DS4.5 BT Süreklilik Planı Testi

BT süreklilik planı düzenli temelde test edilerek, BT sistemlerinin etkin olarak iyileştirilmesi, kısa yolların belirtilmesi ve planın ilgili kalması sağlanmalıdır. Bu dikkatli hazırlık,

dokümantasyon, test sonuçlarının raporlanmasını ve sonuçlara göre, bir eylem planının uygulanmasını gerektirir. Tek uygulama iyileştirmeleri testi entegre test senaryoları ile ve bunlar da sonuç testleri ve entegre satıcı testleri ile karşılaştırılmalıdır.

DS4.6 BT Süreklilik Planı Eğitimi

Bir olay veya afet durumunda prosedürler ve rolleri ve sorumlulukları bakımından tüm ilgili tarafların düzenli eğitim programları alması sağlanmalıdır.

DS4.7 BT Süreklilik Planı Dağıtımı

Gerektiği zaman ve yerde uygun yetkili ilgili taraflara planların uygun ve güvenli dağıtımının ve hazır bulundurulmasının sağlanması için tanımlanan ve yönetilen bir dağıtım stratejisi bulundurulmalıdır. Tüm felaket senaryolarında planlar erişilebilir olmalıdır.

DS4.8 BT Hizmetlerinin Kurtarılması ve Yeniden Başlatılması

BT hizmetlerinin geri alınması ve yeniden başlatılması sürecinde uygulanacak eylemler planlanmalıdır. Bunlar arasında yedekleme sitelerinin aktivasyonu, alternatif işlemlerin başlatılması, müşteri ve hissedar iletişimi, yeniden başlatma prosedürleri olmalıdır. İşin geri alınması ve yeniden başlatılması gereksinimlerini desteklemek için işletmenin BT yeniden başlatma sürelerini ve gereken teknoloji yatırımlarını anlaması sağlanmalıdır.

DS4.9 Alan Dışı Yedekleme Belleği

BT kurtarma ve iş sürekliliği planları için alan dışında tüm kritik yedek medya, dokümantasyon ve diğer BT kaynaklarının saklanması gereklidir. Yedekleme belleğinin içeriği, iş süreci sahipleri ve BT personeli arasında işbirliği ile belirlenmelidir. Alan dışı saklama tesisinin yönetimi veri sınıflandırma politikasına ve kurumun medya depolama uygulamalarına yanıt vermelidir. BT yönetimi, alan dışı düzenlemelerin periyodik olarak, en azından yıllık olarak, içerik, çevresel korunma ve güvenlik bakımından değerlendirilmesini sağlamalıdır. Arşivlenen verilerin restore edilmesi için donanım ve yazılım uyumu sağlanmalı ve arşivlenen veriler periyodik olarak test edilmeli ve yenilenmelidir.

DS4.10 Yeniden Başlatma Sonrasında Revizyon

Bir felaketten sonra BT fonksiyonunun başarılı yeniden başlatılması için, BT yönetiminin plan uygunluğunu değerlendirmek için belirli prosedürleri olup olmadığı belirlenmeli ve buna göre plan güncellenmelidir.

4.2.3.5 DS5 Sistem Güvenliğinin Sağlanması

DS5.1 IT Güvenliği Yönetimi
DS5.2 IT Güvenlik Planı
DS5.3 Kimlik Yönetimi
DS5.4 Kullanıcı Hesabı Yönetimi
DS5.5 Güvenlik Testi, Gözetim ve Gözlem
DS5.6 Güvenlik Olay Tanımı
DS5.7 Güvenlik Teknolojisinin Korunması
DS5.8 Kriptografik Anahtar Yönetimi
DS5.9 Zararlı Yazılım Korunması, Tespiti ve Düzeltilmesi
DS5.10 Ağ Güvenliği
DS5.11 Hassas Verilerin Değişimi

DS5.1 BT Güvenliği Yönetimi

BT güvenliği uygun olan en yüksek kurumsal düzeyde yönetilmelidir ve güvenlik eylemleri yönetiminin iş gereklilikleri ile paralel olması sağlanmalıdır.

DS5.2 BT Güvenlik Planı

İş enformasyon gerekleri, BT konfigürasyonu, enformasyon riski eylem planları ve enformasyon güvenlik kültürü toplam BT güvenlik planına çevrilmelidir. Plan, hizmetler, personel, yazılım ve donanımda uygun yatırımlar ile birlikte güvenlik politikaları ve prosedürlerinde uygulanmalıdır. Güvenlik politikaları ve prosedürleri hissedarlara ve kullanıcılara bildirilmelidir.

DS5.3 Kimlik Yönetimi

Tüm kullanıcılar (iç, dış ve geçici) ve onların BT sistemlerindeki etkinlikleri (iş uygulaması, sistem operasyonu, geliştirme ve bakım) ayrı ayrı tanımlanabilir olmalıdır. Sistem ve verilere kullanıcı erişim hakları belli ve belgeli işletme gereksinimleri ve iş gereklilikleri ile paralel olmalıdır. Kullanıcı erişim hakları kullanıcı yönetimi tarafından talep edilmelidir, sistem sahibi tarafından onaylanmalıdır ve güvenlik sorumlusu tarafından uygulanmalıdır. Kullanıcı

kimlikleri ve erişim hakları merkez havuzda saklanmalıdır. Maliyet-etkili teknik ve prosedür önlemleri açıklanmalıdır ve kullanıcı tanımı belirlenmelidir, onay uygulaması ve erişim haklarının güçlendirilmesi için yürürlükte tutulmalıdır.

DS5.4 Kullanıcı Hesabı Yönetimi

Kullanıcı hesaplarının talep edilmesi, oluşturulması, çıkarılması, askıya alınması, modifiye edilmesi ve kapatılmasının kullanıcı hesabı yönetimi tarafından belirlenmesi sağlanmalıdır. Erişim ayrıcalıkları sağlayan veri veya sistem sahibini belirten onay prosedürü de dahil edilmelidir. Bu prosedürler, yöneticiler (ayrıcalıklı kullanıcılar), iç ve dış kullanıcılar, dahil olmak üzere tüm kullanıcılar için ve normal ve acil durumlar için uygulanmalıdır. Girişim sistemleri ve bilgiye erişim için ilgili haklar ve zorunluluklar tüm kullanıcı tipleri için sözleşmelerle düzenlenmelidir. Tüm hesaplar ve ilgili ayrıcalıkların düzenli yönetim revizyonu gerçekleştirilmelidir.

DS5.5 Güvenlik Testi, Gözetim ve Gözlem

BT güvenlik uygulamasının proaktif olarak test edilmesi ve gözlenmesi sağlanmalıdır. Onaylanan güvenlik düzeyinin sağlanması için BT güvenliği periyodik olarak yeniden akredite edilmelidir. Bir kayıt ve gözlem fonksiyonu belirlenmesi gereken olağan dışı veya anormal etkinliklerin erken tespiti sağlanmalıdır. Kayıt bilgilerine erişim, erişim hakları ve elde tutma gereklilikleri bakımından işletme gereklilikleri ile paralel olmalıdır.

DS5.6 Güvenlik Olay Tanımı

Potansiyel güvenlik olayları özelliklerinin açık olarak tanımlanması ve bildirilmesi sağlanmalıdır. Bu şekilde güvenlik olayları olay veya sorun yönetimi süreci tarafından uygun şekilde yönetilmelidir. Özellikler arasına güvenlik olayı ve etki derecesi olarak düşünülen şeylerin tanımı konmalıdır. Etki düzeylerinin sınırlı sayısı belirlenmelidir ve gereken her özel eylem için ve belirtilmesi gereken kişiler için tanımlanmalıdır.

DS5.7 Güvenlik Teknolojisinin Korunması

Önemli güvenlik teknolojisinin tehditlere karşı dirençli olması sağlanmalıdır ve güvenlik belgeleri gereksiz şekilde açıklanmamalıdır, örn. Düşük bir profile sahiptir. Ancak, sistemlerin güvenliğinin güvenlik spesifikasyonlarının gizliliğine bağlı olmaması sağlanmalıdır.

DS5.8 Kriptografik Anahtar Yönetimi

Modifikasyon ve yetkisiz açılmalara karşı anahtarların korunmasını sağlamak için kriptografik anahtarların yaratılmasının, değiştirilmesinin, iptalinin, bozulmasının, dağıtımının, sertifikasyonunun, saklanmasının, girişinin, kullanımının ve arşivlenmesinin düzenlenmesi için politika ve prosedürler yerinde olmalıdır.

DS5.9 Zararlı Yazılım Korunması, Tespiti ve Düzeltilmesi

Bilgi sistemlerinin ve teknolojisinin zararlı yazılımlardan korunması için (virüsler, solucanlar, casus yazılımlar, spam, içsel olarak geliştirilen tahrip edici yazılımlar, vb) koruyucu, tespit edici ve düzeltici önlemlerin yerinde olması sağlanmalıdır (özellikle güncel güvenlik yolları ve virus kontrolü).

DS5.10 Ağ Güvenliği

Güvenlik teknikleri ve ilgili yönetim prosedürlerinin (örn. Ateş duvarları, güvenlik uygulamaları, ağ segmentasyonu ve işgal tespiti) ağdan ağa bilgi akışını kontrol etmek ve erişimi yetkilendirmek için kullanılması sağlanmalıdır.

DS5.11 Hassas Verilerin Değişimi

Hassas işlem verilerinin içerik uyumu, sunum kanıtı, belge kanıtı ve kökenin reddedilmemesini sağlamak için sadece güvenli bir yoldan veya kontrollü olarak değişimi sağlanmalıdır.

4.2.3.6 DS6 Maliyetlerin Tanımlanması ve Dağıtımı

DS6.1 Hizmetlerin Tanımı
DS6.2 IT Muhasebesi
DS6.3 Maliyet Modelleri ve tarifeler
DS6.4 Maliyet Modeli Bakımı

DS6.1 Hizmetlerin Tanımı

Şeffaf bir maliyet modelini desteklemek için tüm BT maliyetler tanımlanmalıdır ve bunlar BT hizmetlerine bildirilmelidir. BT hizmetleri işletme süreçlerine bağlanmalıdır ve işletme ilgili hizmet fiyatlandırma düzeyleri tanımlanmalıdır.

DS6.2 BT Muhasebesi

Tanımlanan maliyet modeline göre fiili maliyetler tanımlanmalıdır ve dağıtılmalıdır. Tahminler ve fiili maliyetler arasındaki farklılıklar işletmenin finansal ölçme sistemlerine uygun olarak analiz edilmelidir ve raporlanmalıdır.

DS6.3 Maliyet Modelleri ve Tarifeler

Hizmet tanımına dayanarak, hizmetlerin direkt, indirekt, ve toplam maliyetlerini içeren bir maliyet modeli tanımlalıdır ve her hizmet için geri tarife oranlarının hesaplanması desteklenmelidir. Maliyet modeli işletmenin maliyet muhasebesi prosedürleri ile paralel olmalıdır. BT maliyet modeli hizmet tarifelerinin tanımlanabilir, ölçülebilir ve kaynakların uygun kullanımını teşvik etmek için kullanıcılar tarafından öngörülebilir olmasını sağlamalıdır. Kullanıcı yönetimi hizmetlerin fiili kullanımını ve hizmetlerin tarifesini doğrulamalıdır.

DS6.4 Maliyet Modeli Bakımı

Maliyet/tarife modelinin uygunluğu düzenli olarak revize edilmelidir, işaretlenmelidir ve gelişen işletme ve BT etkinliklerine uygunluğu ve ilgisi korunmalıdır.

4.2.3.7 DS7 Kullanıcıların Eğitimi ve Öğretimi

DS7.1 Eğitim ve Öğretim Gereksinimlerinin Tanımlanması
DS7.2 Eğitim ve Öğretimin Verilmesi
DS7.3 Alınan Eğitimin Değerlendirilmesi

DS7.1 Eğitim ve Öğretim Gereksinimlerinin Tanımlanması

Her çalışan hedef grubu için bir öğretim programı oluşturulmalıdır, düzenli olarak güncellenmelidir ve aşağıdaki konular dikkate alınmalıdır:

- Mevcut ve gelecekteki iş gerekleri ve stratejisi
- Kurumsal değerler (etik değerler, kontrol ve güvenlik kültürü, vb.)
- Mevcut beceriler, yetkinlik profilleri ve sertifikasyon ve/veya resmi onay gereksinimleri
- Teslim metotları (örn. Sınıf, web tabanlı), hedef grup boyutu, erişilebilirlik ve zamanlama

DS7.2 Eğitim ve Öğretimin Verilmesi

Tanımlanan eğitim ve öğretim gereksinimlerine dayanarak, hedef gruplar ve üyeleri, etkin teslim mekanizmaları, öğretmenler, belletmenler ve danışmanlar tanımlanmalıdır. Süreli temelde öğretmenler atanmalı ve eğitim programları düzenlenmelidir. Kayıtlar (ön gerekler dahil), devamlılık ve performans değerlendirmeleri kaydedilmelidir.

DS7.3 Alınan Eğitimin Değerlendirilmesi

Eğitim ve öğretim içeriği tamamlanmasından sonra ilgi, kalite, etkinlik, bilginin yakalanması ve tutulması, maliyet ve değer bakımından değerlendirilmelidir. Bu değerlendirme sonuçları gelecekteki müfredat programı tanımı ve eğitim programları için bir girdi olarak alınmalıdır.

4.2.3.8 DS8 Hizmet Masası ve Olaylar Yönetimi

DS8.1 Hizmet Masası
DS8.2 Müşteri Anketlerinin Kaydı
DS8.3 Olay Yükseltilmesi
DS8.4 Olay Kapatma
DS8.5 Trend Analizi

DS8.1 Hizmet Masası

BT ile kullanıcı ara yüzü olarak, tüm çağrıları, kayıtlı olayları, hizmet taleplerini ve bilgi taleplerini kaydetmek, iletmek, dağıtmak ve analiz etmek için bir hizmet masası fonksiyonu oluşturulmalıdır. Bir olay, hizmet talebi veya bilgi talebi olarak kaydedilen herhangi bir konunun sınıflandırmasını ve önceliğini sağlayan uygun SLA ile ilgili anlaşma sağlanan hizmet düzeylerine dayanan gözlem ve yükselme prosedürleri bulundurulmalıdır. Hizmet masası kalitesi ve BT hizmetleri ile son kullanıcı memnuniyeti ölçülmelidir.

DS8.2 Müşteri Anketlerinin Kaydı

Çağrıların, olayların, hizmet taleplerinin ve bilgi gereksinimlerinin kaydı ve izlenmesini sağlayan bir fonksiyon ve sistem oluşturulmalıdır. Olay yönetimi, problem yönetimi, değişiklik yönetimi, kapasite yönetimi ve mevcudiyet yönetimi gibi süreçlerle birlikte çalıştırılmalıdır. Olaylar iş ve hizmet önceliklerine göre sınıflandırılmalıdır ve uygun sorun yönetimi ekibine göre yönlendirilmelidir ve müşteriler anket durumu hakkında bilgilendirilmelidir.

DS8.3 Olay Yükseltilmesi

Hizmet masası prosedürleri oluşturulmalıdır, bu şekilde hemen çözülemeyen olaylar SLA' da tanımlanan sınırlara göre uygun şekilde yükseltilmelidir ve varsa, iş çevreleri sağlanmalıdır. Olay sahipliği ve yaşam devri gözleminin BT grubunun çözüm etkinlikleri hakkında çalışmasından bağımsız olarak kullanıcıya dayanan olaylar için hizmet masasında kalması sağlanmalıdır.

DS8.4 Olay Kapatma

Müşteri anketlerinin açıklanmasının zamanında gözlenmesi için prosedürleri oluşturulmalıdır. Olay çözüldüğünde, köken nedeni biliniyorsa hizmet masası tarafından kaydedilmelidir, ve uygulanan eylem müşteri tarafından onaylanmalıdır.

DS8.5 Trend Analizi

Hizmet performansını ve hizmet yanıt sürelerini ölçmek için ve trendleri ve tekrarlayan sorunları tanımlamak için yönetimi sağlamak üzere hizmet masası raporları üretilmelidir ve hizmet sürekli olarak geliştirilmelidir.

4.2.3.9 DS9 Konfigürasyon Yönetimi

DS9.1 Konfigürayon Havuzu ve Dayanak
DS9.2 Konfigürasyon Maddelerinin Tanımlanması ve Korunması
DS9.3 Konfigürasyon Entegrite Revizyonu

DS9.1 Konfigürasyon Havuzu ve Dayanak

Konfigürasyon maddeleri hakkında tüm ilgili bilgiyi içeren merkezi bir havuz oluşturulmalıdır. Bu havuzda donanım, uygulama yazılımı, orta yazılım, parametreler, dokümantasyon, prosedürler ve işletme araçları, sistemlerin ve hizmetlerin erişimi ve kullanımı bulundurulmalıdır. Dikkate alınacak ilgili bilgiler, isimlendirme, versiyon numaraları ve lisans detaylandırılmalıdır. Her sistem ve hizmet için değişikliklerden sonra dönülecek bir kontrol noktası olarak konfigürasyon maddelerinin dayanağı korunmalıdır.

DS9.2 Konfigürasyon Birimleri Tanımlanması ve Korunması

Aşağıdakiler için prosedürler uygulanmalıdır:

- Konfigürasyon birimleri ve özellikleri tanımlanmalıdır
- Yeni, modifiye edilmiş ve silinmiş konfigürasyon maddeleri kaydedilmelidir.
- Konfigürasyon havuzunda konfigürasyon birimleri arasında ilişkiler tanımlanmalıdır ve korunmalıdır
- Konfigürasyon havuzundaki mevcut konfigürasyon maddeleri güncellenmelidir
- Yetkisiz yazılım kullanılması önlenmelidir

Bu prosedürler konfigürasyon havuzundaki tüm eylemlerin uygun yetkilendirilmesini ve kayıtlarını sağlamalıdır ve değişiklik yönetimi ve sorun yönetimi prosedürleri ile uygun şekilde entegre edilmelidir.

DS9.3 Konfigürasyon Entegrite Revizyonu

Gerektiğinde, düzenli temelde, mevcut ve geçmişteki konfigürasyon verilerinin bütünlüğünün doğrulanması ve fiili durumlara karşı karşılaştırılması için uygun araçlar kullanılarak konfigürasyon maddelerinin statüsü revize edilmelidir ve doğrulanmalıdır. Mevcut lisans anlaşmalarının dışında herhangi bir yazılım veya lisanssız yazılım kullanılmasına karşı yazılım kullanımı politikaları periyodik olarak revize edilmelidir. Hatalar ve sapmalar rapor edilmelidir, müdahale edilmelidir ve düzeltilmelidir.

4.2.3.10 DS10 Sorun Yönetimi

DS10.1 Sorunların Tanımlanması ve Sınıflandırılması
DS10.2 Sorun İzleme Ve Çözüm
DS10.3 Sorun Kapatma
DS10.4 Değişiklik, Konfigürasyon ve Sorun Yönetimi Entegrasyonu

DS10.1 Sorunların Tanımlanması ve Sınıflandırılması

Olay yönetiminin parçası olarak tanımlanan sorunlar rapor edilmelidir ve sınıflandırılması için süreçler uygulanmalıdır. Sorun sınıflandırmada yer alan adımlar olay sınıflandırma adımları ile benzerdir; bunlar, kategori, etki, aciliyet ve önceliklerin belirlenmesidir. Sorunlar ilgili gruplar veya bölgelere uygun olarak kategorize edilmelidir (örn. Donanım, yazılım, destek yazılımı). Bu gruplar kurumsal sorumlulukları veya kullanıcı ve müşteri temelini birleştirir ve kadroyu desteklemek için sorunların tahsisinde temeldir.

DS10.2 Sorun İzleme Ve Çözüm

Sorun yönetimi sistemi, kaydedilen tüm sorunların köken nedenini izlemeyi, analizini ve belirlenmesini sağlayan uygun denetim raporu kolaylıkları sağlamalıdır ve şunları dikkate almalıdır:

- Tüm ilgili konfigürasyon birimleri
- Var olan sorunlar ve olayları
- Bilinen ve kuşku duyulan hataları

Belirlenen değişiklik yönetimi süreci üzerinden değişiklik talebi doğuran kök nedeni bildiren sürdürülebilir çözümler tanımlanmalıdır ve başlatılmalıdır. Çözüm süreci boyunca, sorun yönetimi, sorun ve hataların çözümünde varolan değişiklik yönetiminden düzenli raporlar alınmalıdır. Sorun çözümü sorunların devam eden etkilerini ve kullanıcı hizmetlerindeki bilinen hatalar gözlenmelidir. Bu etkinin şiddetli olması durumunda, sorun yönetimi sorunu yükseltilmelidir ve değişiklik talebi önceliğini arttırmak için yönetim kuruluna bildirilmelidir ve uygun acil değişiklik uygulanmalıdır. Sorun çözüm gelişimi SLA 'lere karşı gözlenmelidir.

DS10.3 Sorun Kapatma

Bilinen hatanın başarılı eliminasyonunun onayından sonra veya alternatif çözüm yollarının işletme ile belirlenmesinden sonra sorun kayıtlarını kapatmak için bir prosedür uygulanır.

DS10.4 Değişiklik, Konfigürasyon ve Sorun Yönetimi Entegrasyonu

Etkin sorun ve olay yönetimini sağlamak için, ilgili değişiklik süreçleri, konfigürasyon ve sorun yönetimi entegrasyonu uygulanmalıdır. İş gelişmesinin sağlanması yerine problemi, sorunu çözmek için ne kadar çaba gösterildiği ve gerekirse sorunları minimuma indirmek için ne yapılması gerektiği gözlenmelidir.

4.2.3.11 DS11 Veri Yönetimi

DS11.1 Veri Yönetimi için İşletme Gereklilikleri
DS11.2 Saklama ve Elde Tutma Düzenlemeleri
DS11.3 Medya Kütüphane Yönetimi Sistemi
DS11.4 Elden Çıkarma
DS11.5 Yedekleme ve Restorasyon
DS11.6 Veri Yönetimi için Güvenlik Gereklilikleri

DS11.1 Veri Yönetimi için İşletme Gereklilikleri

İşletmeden beklenen kaynak belgelerin teslim alınmasını sağlamak için düzenlemeler yapılmalıdır, işletmeden alınan tüm veriler işleme konulmalıdır, işletmenin gerektirdiği tüm çıktı hazırlanmalıdır ve teslim edilmelidir ve yeniden başlatma ve yeniden süreçlendirme gereksinimleri desteklenmelidir.

DS11.2 Saklama ve Elde Tutma Düzenlemeleri

Veri saklama ve arşivleme için prosedürler tanımlanmalıdır ve uygulanmalıdır, bu şekilde veriler erişilebilir ve kullanışlı kalacaktır. Prosedürler yeniden kullanma gerekleri, maliyet etkinliği, sürekli entegrite ve güvenlik gereklerini dikkate almalıdır. Kodlama ve onay için kullanılan veriler (anahtarlar, sertifikalar) gibi belgeler, veriler, arşivler, programlar, raporlar ve mesajlar (gelen ve giden) için yasal, mevzuat ve iş gereklerini karşılamak amacıyla saklama ve elde tutma düzenlemeleri yapılmalıdır.

DS11.3 Medya Kütüphane Yönetimi Sistemi

Onsite medya envanterinin sağlanması için prosedürler tanımlanmalıdır ve uygulanmalıdır ve kullanışlılıkları ve entegritesi sağlanmalıdır. Prosedürler uyuşmazlıklar hakkında zamanında revizyon ve takip sağlamalıdır.

DS11.4 Elden Çıkarma

Bir başka kullanıma aktarılacağı veya elden çıkarılacağı zaman ekirman ve medyadan hassas verilere ve yazılıma erişimi önlemek için prosedürler tanımlanmalıdır ve uygulanmalıdır. Bu prosedürler silinen veya atılan verilerin tekrar kullanılamayacağını sağlamalıdır.

DS11.5 Yedekleme ve Restorasyon

İş gerekleri ve süreklilik planı ile paralel olarak sistemlerin yedekleme ve restorasyonu, veri ve dokümantasyonu için prosedürler tanımlanmalıdır ve uygulanmalıdır. Yedekleme prosedürleri ile uygunluğu doğrulanmalıdır, ve başarılı ve tam restorasyon için yetenek ve zaman doğrulanmalıdır. Yedekleme medyası ve restorasyon süreci test edilmelidir.

DS11.6 Veri Yönetimi için Güvenlik Gereklilikleri

Makbuz, süreç, fiziksel depolama ve verilere ve hassas mesajlara uygulanan güvenlik gerekleri tanımlanmalıdır ve uygulanması için düzenlemeler yapılmalıdır. Bunlar fiziksel kayıtları, veri aktarımlarını ve site dışında saklanan verileri içermelidir.

4.2.3.12 DS12 Fiziksel Ortamların Yönetimi

DS12.1 Site Seçimi ve Planı
DS12.2 Fiziksel Güvenlik Önlemleri
DS12.3 Fiziksel Erişim
DS12.4 Çevresel Faktörlere Karşı Koruma
DS12.5 Fiziksel Tesis Yönetimi

DS12.1 Site Seçimi ve Planı

İş stratejisine bağlı olan teknoloji stratejisini desteklemek için BT ekipmanı için fiziksel siteler tanımlanmalıdır ve seçilmelidir. Bir site planının seçimi ve tasarımı, meslek sağlığı ve güvenlik mevzuatı gibi ilgili yasalar ve düzenlemeler ile birlikte doğal insan kaynaklı felaketlerle ilgili riski de dikkate almalıdır.

DS12.2 Fiziksel Güvenlik Önlemleri

İş gerekleri ile paralel olarak fiziksel güvenlik önlemleri tanımlanmalıdır ve uygulanmalıdır. Önlemler şunları içermelidir, ancak bunlarla sınırlı kalmamalıdır: Güvenlik perimetresi planı, güvenlik bölgeleri, kritik ekipmanın lokasyonu, ve sevkiyat ve teslim alanları. Özellikle, kritik ve önem arz eden Bilgi Teknolojileri operasyonlarının varlığı hakkında düşük bir profil tutulmalıdır. Gözlem sorumlulukları ve rapor prosedürleri ve fiziksel güvenlik olaylarının çözümü belirlenmelidir.

DS12.3 Fiziksel Erişim

Acil durumlar da dahil olmak üzere iş gereklerine göre arazilere, bina ve alanlara erişim verilmelidir, sınırlanması ve feshedilmesi için prosedürler tanımlanmalıdır ve uygulanmalıdır. Arazi, bina ve alan erişimleri değerlendirilmelidir, yetkilendirilmelidir, kaydedilmelidir ve gözlenmelidir. Bu, kadro, geçici kadro, müşteriler, satıcılar, ziyaretçiler veya diğer üçüncü taraflar dahil olmak üzere, arazilere giren tüm kişilere uygulanmalıdır.

DS12.4 Çevresel Faktörlere Karşı Koruma

Çevresel faktörlere karşı korunma için önlemler tasarlanmalıdır ve uygulanmalıdır. Çevre gözlemi ve kontrolü için uzmanlaşmış ekipman ve cihazlar kurulmalıdır.

DS12.5 Fiziksel Tesis Yönetimi

Yasa ve mevzuat, teknik ve iş gerekleri, satıcı spesifikasyonları ve sağlık ve güvenlik kılavuzları ile paralel olarak güç ve iletişim ekipmanı dahil, tesisler yönetilmelidir.

4.2.3.13 DS13 Operasyonların Yönetimi

DS13.1 Operasyonlar Prosedürleri ve Talimatları
DS13.2 İş Cetvelleri
DS13.3 IT İç Yapı Gözlemi
DS13.4 Hassas Belgeler ve Çıktı Cihazları
DS13.5 Donanım için Koruyucu Bakım

DS13.1 Operasyonlar Prosedürleri ve Talimatları

BT operasyonları için standart prosedürler tanımlanmalıdır, uygulanmalıdır ve korunması ve operasyon kadrosunun onlara verilen tüm operasyon görevleri hakkında bilgi sahibi olması sağlanmalıdır. Operasyonel prosedürler sürekli operasyonu sağlamak için vardiya devir teslimini kapsamalıdır.

DS13.2 İş Cetvelleri

İş gereklerini karşılamak için iş cetvelleri, süreçleri ve görevler en etkin sıraya göre düzenlenmelidir, üretim ve kullanışlılık maksimuma çıkarılmalıdır. Bu cetvel değişiklikleri ile birlikte ilk cetveller yetkilendirilmelidir. Standart iş cetvellerinden hareketleri tanımlamak, araştırmak ve onaylamak için prosedürler uygulanmalıdır.

DS13.3 BT Alt Yapı Gözlemi

BT alt yapısı ve ilgili olayları gözlemlemek için prosedürler tanımlanmalıdır ve uygulanmalıdır. Yeterli kronolojik bilginin operasyonlar kaydında saklanması sağlanmalıdır. Bu şekilde operasyonların zaman dizilerinin rekonstrüksiyonu, revizyonu ve değerlendirmesi ve operasyonları çevreleyen veya destekleyen diğer aktiviteler mümkün kılınır.

DS13.4 Hassas Belgeler ve Çıktı Cihazları

Özel formlar, görüşülen enstrümanlar, özel amaçlı yazıcılar veya güvenlik jetonları gibi hassas BT aktifleri üzerinde envanter yönetimi ve muhasebe uygulamaları ve uygun fiziksel güvenlik sağlanmalıdır.

DS13.5 Donanım için Koruyucu Bakım

Başarısızlık etkisi ve sıklığını veya performans düşüklüğünü azaltmak için içyapının zamanında korunmasını sağlamak amacıyla prosedürler tanımlanmalıdır ve uygulanmalıdır.

4.2.4 Gözlem ve Değerlendirme

Gözlem ve Değerlendirme alanı kurumun ihtiyaçlarını, mevcut BT sisteminin hedefleri karşılayıp karşılamadığını ve yasal gereksinimlerle uyumluluk için gerekli kontrolü tayin etmek için kurumun stratejilerini irdelemektedir. Gözlem ve Değerlendirme aynı zamanda bilgi teknolojileri sisteminin iş hedeflerini karşılamadaki etkinliği ile iç ve dış denetçilerce yapılan kurumun kontrol süreçlerinin bağımsız değerlendirmesi konularını kapsamaktadır.

Gözlem ve Değerlendirme alanındaki kontrol hedeflerini içeren liste aşağıda yer almaktadır:

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

4.2.4.1 ME1 IT Performansının Gözlemi ve Değerlendirmesi

ME1.1 Gözlem Yaklaşımı
ME1.2 Gözlem Verilerinin Tanımı ve Toplanması
ME1.3 Gözlem Metodu
ME1.4 Performans Değerlendirmesi
ME1.5 Yönetim Kadrosu ve Yönetici Raporlama
ME1.6 Çözüm Eylemleri

ME1.1 Gözlem Yaklaşımı

Yönetim, işletmenin portfolio yönetimi sonuçlarına ve program yönetimi süreçlerine ve Bilgi Teknolojileri kapasitesi ve hizmetlerinin teslimine özel süreçlere BT katkısının gözlenmesi için izlenecek kapsamı, metodolojiyi ve süreci tanımlayan genel bir gözlem çerçevesi ve yaklaşımı oluşturmalıdır. Çerçeve kurumsal performans yönetimi sistemi ile entegre edilmelidir.

ME1.2 Gözlem Verilerinin Tanımı ve Toplanması

İşletme ile çalışan Bilgi Teknolojileri yönetimi performans amaçları, önlemleri, hedefleri ve vurgularının dengeli bir setini tanımlamalıdır ve bunların işletme ve ilgili hissedarlar tarafından imzalanarak onaylanmasını sağlamalıdır. Performans göstergeleri şunları içermelidir:

- İşletme katkısı finansalları içeren ancak bunlarla sınırlı olmayan
- Stratejik iş ve BT planına karşı performans
- Mevzuat ile uyum ve risk
- İç ve dış kullanıcı tatmini
- Gelişme ve hizmet teslimini içeren anahtar BT süreçleri
- Geleceğe yönelik aktiviteler, örneğin, varolan teknoloji, tekrar kullanılabilen içyapı, iş ve BT personeli beceri setleri.

Hedef gelişmeleri hakkında raporlar için zamanında ve doğru verilerin toplanması amacıyla süreçler geliştirilmelidir.

ME1.3 Gözlem Metodu

Gözlem sürecinin kısa ve kapsamlı Bilgi Teknolojileri performansı gözlemi sağlayan bir metot açıklaması sağlanmalıdır (örn. Dengeli puan kartı) ve bu işletme gözlem sistemi ile uygun olmalıdır.

ME1.4 Performans Değerlendirmesi

Periyodik olarak performans hedeflere karşı revize edilmelidir, köken neden analizi yapılmalıdır ve altta yatan nedenlerin belirlenmesi için çözüm eylemi başlatılmalıdır.

ME1.5 Yönetim Kadrosu ve Yönetici Raporlama

Kurum gelişmesi hakkında yüksek yönetim revizyonu için yönetim raporları sağlanmalıdır. Bu raporlarda tanımlanan amaçlar, özellikle BT yatırım programlarının işletme portfolyosu performansı ve bireysel programların hizmet düzeyleri ve BT katkısı belirtilmelidir. Statü raporları planlanan amaçların gerçekleştirilme derecesini, alınan teslimleri, karşılanan performans hedeflerini ve hafifletilen riskleri içermelidir. Revizyon üzerine, beklenen performanstan sapmalar tanımlanmalıdır ve uygun yönetim eylemi başlatılmalıdır ve rapor edilmelidir.

ME1.6 Çözüm Eylemleri

Performans gözlemi, değerlendirme ve raporlamaya dayanarak çözüm eylemleri tanımlanmalıdır ve başlatılmalıdır. Bu, tüm gözlem, raporlama ve değerlendirmelerin takibini içermelidir:

- Yönetim yanıtlarının revizyonu, müzakereleri ve oluşturulması
- Çözüm için sorumluluk atamaları
- Taahhüt edilen eylemlerin sonuçlarının izlenmesi

4.2.4.2 ME2 İç Kontrol Gözlemi ve Değerlendirmesi

ME2.1 İç Kontrol Çerçevesinin Gözlenmesi
ME2.2 Denetim Revizyonu
ME2.3 Kontrol İstisnaları
ME2.4 Kontrol Öz-değerlendirme
ME2.5 İç Kontrol Güvencesi
ME2.6 Üçüncü Taraflarda İç Kontrol
ME2.7 Çözüm Eylemleri

ME2.1 İç Kontrol Çerçevesinin Gözlenmesi

BT kontrol ortamı sürekli olarak gözlenmelidir ve çerçeve kontrol edilmelidir. BT kontrol ortamı ve kontrol çerçevesini geliştirmek için en iyi endüstri uygulamaları ve işaretlerinin kullanılarak değerlendirme yapılmalıdır.

ME2.2 Denetim Revizyonu

Denetim revizyonu ile BT üzerindeki iç kontrollerin etkinliği gözlenmelidir ve rapor edilmelidir: Örnek; politika ve standartlarla uygunluk, enformasyon güvenliği, kontrollerin değiştirilmesi ve hizmet düzeyi anlaşmalarında belirlenen kontroller.

ME2.3 Kontrol İstisnaları

Tüm kontrol istisnaları bakımından bilgiler kaydedilmelidir ve altta yatan neden analiz edilmelidir ve düzeltici eylem uygulanmalıdır. Fonksiyon için bireysel sorumluya iletilecek istisnalara yönetim karar vermelidir. Yönetim etkilenen tarafların bilgilendirilmesinden de sorumlu olmalıdır.

ME2.4 Kontrol Öz-değerlendirme

Sürekli bir kendi kendini değerlendirme programı ile BT süreçleri, politikaları ve sözleşmeleri üzerindeki yönetimin iç kontrollerinin bütünlüğü ve etkinliği değerlendirilmelidir.

ME2.5 İç Kontrol Güvencesi

Gereken şekilde üçüncü taraf revizyonları ile iç kontrollerin tamlık ve etkinliğinin güvencesi alınmalıdır. Bu revizyonlar kurumsal uygunluk fonksiyonu ile yönetilmelidir, veya yönetim talebi üzerine yapılmalıdır, iç denetim veya komisyonlu dış denetimciler ve danışmanlar veya sertifikasyon grupları tarafından yapılmalıdır. Denetimi yapan bireylerin kalifikasyonları sağlanmalıdır: Örnek; Sertifikalı Bilgi Sistemleri Auditor (CISA®) sertifikasyonu.

ME2.6 Üçüncü Taraflarda İç Kontrol

Her dış hizmet sağlayıcının iç kontrol statüsü değerlendirilmelidir. Dış hizmet sağlayıcıları yasal ve mevzuat gerekleri ve sözleşme zorunlulukları ile uyumlu davranmalıdır. Bu üçüncü taraf denetimi ile veya yönetimin iç denetim fonksiyonu ve denetim sonuçlarından sağlanmalıdır.

ME2.7 Çözüm Eylemleri

Kontrol değerlendirmeleri ve raporlara dayanarak çözüm eylemleri tanımlanmalı ve başlatılmalıdır. Raporlarda şunlar yer almalıdır:

- Yönetim yanıtlarının revizyonu, görüşmeleri ve oluşturulması
- Çözüm için sorumluluk atanması (risk kabulünü içerebilir)
- Taahhüt edilen eylem sonuçlarının izlenmesi.

4.2.4.3 ME3 Yönetmeliklere Uyumluluğun Sağlanması

ME3.1 BT üzerinde Potansiyel Etkisi Olan Yasa ve Yönetmeliklerin Tanımlanması
ME3.2 Yönetmelik Koşullarının Karşılanmasında Optimizasyonun Sağlanması
ME3.3 Yönetmelik Koşullarıyla Uyumluluğun Değerlendirilmesi
ME3.4 Uyumluluğun Olumlu Biçimde Sağlanması
ME3.5 Tümleşik Raporlama

ME3.1 BT üzerinde Potansiyel Etkisi Olan Yasa ve Yönetmeliklerin Tanımlanması

Bilgi, üçüncü taraf hizmetlerini de kapsayan bilgi hizmetleri teslimatı ve Bilgi Teknolojileri organizasyonu, süreçleri ve altyapısıyla ilgili yerel ve uluslar arası yasal koşulların, sözleşme, politika ve yönetmelik koşullarının zamanında tanımlanmasını sağlayacak bir süreç geliştirilmelidir. Elektronik ticaret, veri akışı, gizlilik, iç denetimler, finansal raporlama, sektörel yönetmelikler, fikri haklarla telif haklarının korunması ile sağlık ve güvenlik hakkındaki yasa ve yönetmelikler göz önüne alınmalıdır.

ME3.2 Yönetmelik Koşullarının Karşılanmasında Optimizasyonun Sağlanması

Yasa ve yönetmelikler tarafından belirlenen koşulların etkin biçimde kapsanmasını sağlamak amacıyla, Bilgi Teknolojileri politikalarını, standartlarını ve prosedürleri incelenerek, en iyi hale getirilmelidir.

ME3.3 Yönetmelik Koşullarıyla Uyumluluğun Değerlendirilmesi

Yasa ve yönetmeliklerde belirtilen koşullar da dahil olmak üzere, Bilgi Teknolojileri politikaları, standartlar ve prosedürler ile uyumluluğu, iş ve Bilgi Teknolojileri yönetiminin idaresinde ve iç denetim mekanizması da çalıştırılarak etkin biçimde değerlendirilmelidir.

ME3.4 Uyumluluğun Olumlu Biçimde Sağlanması

Uyumluluğun olumlu biçimde sağlanması ve raporlanması amacıyla, gerektiğinde sorumlu süreç sahibinin zamanında olası uyumluluk eksikliklerivle ilgili olarak düzeltici önlemleri almasını/uygulamasını sağlayan prosedürler tanımlanmalıdır ve uygulanmalıdır. Uyumluluk ilerleme ve mevcut durumu hakkındaki Bilgi Teknolojileri raporlaması, diğer iş fonksiyonlarından gelen benzer çıktılarla bütünleştirilmelidir.

ME3.5 Tümleşik Raporlama

Yasal gereklilikler hakkındaki Bilgi Teknolojileri raporlaması, diğer iş fonksiyonlarından gelen benzer çıktılarla bütünleştirilmelidir.

4.2.4.4 ME4 BT Yönetimi Sağlanması

ME4.1 BT Yönetimi Çerçevesinin Oluşturulması
ME4.2 Stratejik Uyum
ME4.3 Değer Yaratma
ME4.4 kaynak Yönetimi
ME4.5 Risk Yönetimi
ME4.6 Performas Ölçümü
ME4.7 Bağımsız Denetim/Güvence

ME4.1 BT Yönetimi Çerçevesinin Oluşturulması

Yönetim Kuruluyla birlikte çalışarak, kuruluşun BT 'nin etkinleştirildiği yatırım programlarının kendi stratejileriyle uyum içinde olmasını ve hedeflerine ulaşmasını sağlayacak liderlik, süreçler, roller ve sorumluluklar, bilgi gereksinimleri ve organizasyonel yapıları kapsayan BT yönetim çerçevesini tanımlanmalıdır ve oluşturulmalıdır. Söz konusu çerçeve; kuruluşun stratejisi, bu stratejiyi uygulayan BT 'nin etkinleştirildiği yatırım programları portföyü, bağımsız yatırım programları ile programları hazırlayan işletme ve BT projeleri arasında açık ve anlaşılır bir bağlantı sağlamalıdır. Çerçeve, iç denetimde ve idarede kopma yaşanmaması için sağlam/anlaşılır sorumluluklar ve uygulamalar sağlamalıdır. Çerçeve, kuruluşun genel denetim ortamıyla ve genel kabul gören denetim ilkeleriyle tutarlı olmalıdır ve BT sürecini ve denetim çerçevesini temel almalıdır.

ME4.2 Stratejik Uyum

BT 'nin rolü, teknolojik öngörüsü ve yetenekleri gibi BT konularında yönetim kurulunun ve yöneticilerin bilgi sahibi olması sağlanmalıdır. BT 'nin işletme stratejisine yapacağı olası katkı konusunda işletme ve BT arasında ortak bir anlayış geliştirilmelidir. BT 'nin etkinleştirildiği yatırımlar, işletmenin stratejilerine ulaşırken BT yeteneklerinden elde ettiği değeri en uygun hale getirmek için yapmak zorunda olduğu değişikliklerin tamamını içeren bir program portföyü olarak yönetildiğinde; değerin yalnızca BT 'den sağlandığı konusunun açıkça anlaşılması sağlanmalıdır. BT stratejik komitesi gibi yönetim organlarını tanımlayıp uygulamaya koyarken, BT ile ilgili yönetime strateji yön sağlamak amacıyla yönetim kuruluyla birlikte çalışarak, stratejilerin ve hedeflerin işletme birimlerine ve BT

fonksiyonlarına doğru yayılmasını ve işletme ile BT arasında güven oluşturulması sağlanmalıdır. Stratejik ve operasyonel açıdan BT 'nin işletmeden ayrılmasını sağlayarak, işletme ve BT 'yi stratejik karar alma ve BT 'nin etkinleştirildiği yatırımlardan yarar elde etme konusunda sorumluluğun paylaşılması cesaretlendirilmelidir.

ME4.3 Değer Yaratma

BT 'nin etkinleştirildiği yatırım programları ve BT varlıklarıyla hizmetleri, kuruluşun stratejisini ve hedeflerini desteklemede olası en yüksek değeri sağlayacak biçimde yönetilmelidir. BT 'nin etkinleştirildiği yatırımlardan ve bu sonuçları elde etmek için harcanması gereken çaba kapsamının tamamından beklenen iş sonuçlarının anlaşılması, kapsamlı ve tutarlı iş durumlarının oluşturulması ve paydaşlarca onaylanması, varlıkların ve yatırımların ekonomik ömür döngüsü içinde yönetilmesi ve yeni hizmetler, etkin kazançlar ve iyileştirilmiş müşteri talebi karşılama oranı gibi yararların elde edilmesinde aktif bir yönetim bulunması sağlanmalıdır. Portföy, program ve proje yönetiminde disiplinli bir yaklaşım uygulanmalıdır, işletmenin tüm BT 'nin etkinleştirildiği yatırımların sahipliğini üstlenmesinde ve BT 'nin de kendi olanaklarını ve hizmetlerini sunma maliyetlerini en uygun düzeye getirmesinde kararlı davranılmalıdır. Teknoloji yatırımlarının olası en yüksek oranda standartlaştırılmasını sağlanmalıdır ve teknik çözüm çeşitliliğinin yol açacağı artan maliyet ve karmaşıklıktan kaçınılmalıdır.

ME4.4 Kaynak Yönetimi

Yatırımı ve BT varlıklarının kullanımını düzenli değerlendirmelerle en iyi duruma getirilmelidir, BT 'nin şu anki ve gelecekteki stratejik hedeflere ulaşabilecek ve işletme taleplerini karşılayabilecek yeterli, güncel ve yetenekli kaynaklarının bulunması sağlanmalıdır.

Açıkça anlaşılır, tutarlı ve zorlayıcı insan kaynakları ve satın alma politikaları uygulayarak kaynak gereksinimlerinin etkin biçimde karşılanması ve yapısal politikalara ve standartlara uyulması sağlanmalıdır. BT altyapısı, olası her yerde standartlaştırılmasının ve gereken her yerde de birlikte çalışabilirlik özelliği taşımasının sağlanması amacıyla, düzenli olarak değerlendirilmelidir.

ME4.5 Risk Yönetimi

Kuruluştaki BT riskini tanımlamak amacıyla yönetim kuruluyla birlikte çalışılmalıdır. BT risk planını kuruluşa yayarak, bir risk planı üzerinde anlaşma sağlanmalıdır. Organizasyonda risk

yönetimi sorumlulukları belirleyerek, işletmenin ve BT ’nin düzenli olarak BT ile ilgili riskleri ve iş üzerindeki olası etkilerini düzenli olarak değerlendirilmesi ve raporlanması sağlanmalıdır. BT yönetiminin, iç denetimdeki ve yönetimdeki BT denetimi başarısızlıklarına ve zayıflıklarına ve bunların işletme üzerindeki gerçek ve olası etkilerine özellikle dikkat ederek risk oluşan yerlerin izlemesi sağlanmalıdır. Kuruluşun BT risk pozisyonu tüm paydaşlar tarafından izlenmelidir.

ME4.6 Performans Ölçümü

Portföy, program ve BT performansıyla ilgili bilgiler yönetim kuruluna ve yöneticilere zamanında ve eksiksiz biçimde bildirilmelidir. Yönetim raporları, üst yönetimin kuruluşun tanımlanan hedeflere doğru ilerleme durumunu inceleyebileceği biçimde sunulmalıdır. Durum raporları ise, hangi planlanan hedeflere ulaşıldığı, hangi çıktıların elde edildiği, karşılanan performans hedefleri ve giderilen riskler kapsamında tutulmalıdır. Diğer işletme fonksiyonlarından gelen benzer çıktıya sahip raporlar birleştirilmelidir. Performans ölçümleri büyük paydaşlar tarafından onaylanmalıdır. Yönetim kurulu ve üst yönetim bu raporları sorgulamalıdır ve BT yönetimine de olası sapmaları ve performans sorunlarını açıklama fırsatı verilmelidir.

ME4.7 Bağımsız Denetim/Güvence

Kuruluşun yeterli ve uygun sayıda personele sahip, BT ’nin politikalar, standartlar ve prosedürlerin yanı sıra genel kabul gören uygulamalar açısından da uyumluluğu hakkında zamanında yönetim kuruluna (büyük bir olasılıkla bir denetim kurulu aracılığıyla) bağımsız denetim bilgileri sunacak dış denetim hizmetlerini sağlayan bir fonksiyon kurması ve çalıştırması sağlanmalıdır.

COBIT denetim ilkeleri; anlamayı sağlama, kontrol değerlendirmesi, uyum değerlendirmesi ve teşvik riski olmak üzere dört unsurdan oluşur. COBIT yönetim ilkeleri; kritik başarı faktörleri, kilit hedef göstergeleri, kilit performans göstergeleri, vade modelleri olmak üzere dört unsurdan oluşur. COBIT bu süreçler sonucunda işletme hedeflerinin gerçekleştirilmesini amaçlar (Uzunay, 2007).

4.3 COBIT Olgunluk Modelleri

Bilgi teknolojilerinin iş hayatındaki önemi arttıkça, oldukça yüklü yatırım ve riskli proje yönetimlerini gerektiren bilgi teknolojileri süreçlerinin olgunluk seviyeleri hakkında güvence sağlayacak denetim metodolojilerine olan ihtiyaç da artmaktadır. Bu amaçla CobiT için

düzenlenmiş olan olgunluk seviyeleri kurumun bugün nerede olduğunu, endüstrideki durum ve karşılaştırmalarını ve kurumun ileride nerede olmak istediği sorularına cevap vermektedir. Son zamanlarda CobiT olgunluk seviyeleri hakkında bir sürü spekülasyonun ortaya atılması CobiT 4.1'in ortaya çıkması ile durmuştur. Ana hatları ile 0 ila 5 arasında puan verilerek sınıflandırılan CobiT Olgunluk Modellerinin hesaplaması Şekil 4.3 te gösterildiği gibidir (Artinyan, 2008):

	Anlayış ve Farkındalık	**Eğitim ve İletişimin**	**Süreç ve Uygulamalar**	**Teknoloji Kullanımı**	**Uygunluk**	**Uzmanlık**
0	Yok	yok	yok	yok	yok	yok
1	farkındalık var	ihtiyaç olduğunda münferit iletişim sağlanıyor	ihtiyaç olduğunda münferit dokümantasyon ve süreç yaklaşımı sağlanıyor	yok	yok	yok
2	ihtiyacın bilincine varılmış	genel konular ve ihtiyaçlar üzerine iletişim sağlanıyor	ortak / benzer ancak kişi insiyatifinde uygulamalar var	ortak / benzer araçlar kullanılmaya başlanmış	münferit durumlarda standard olmayan izleme yöntemleri kullanılıyor	yok
3	önlem alınması yönünde anlayış oluşmuş	kişisel girişimler ve bireysel eğitimler mevcut	prosedürler oluşturulmuş ve dokümante edilmiş, bunların iyileştirilmesine başlanmış	ortak yöntemlerin kullanılması için standard oluşturulmuş	standard olmayan izleme ve ölçme yöntemleri kullanılıyor; kurumsal karne uygulaması yapılan alanlar olabiliyor; kişiye bağlı sebep-sonuç ilişkileri gözlenebiliyor	iş süreçlerine teknoloji uzmanlarının da katılımı sağlanıyor
4	Tüm gereklilikler biliniyor	program yönetimi ve resmi eğitim var	süreç sahipliği ve sorumlulukları belirlenmiş, süreç olgunluğu sağlanmış, kurum içi en iyi uygulamalara geçilmiş	teknolojik olgunluğa ulaşılmış, standard yöntemlerin kullanılması sağlanmış	belirlenen süreçlerde kurumsal karne uygulaması yapılıyor, farklılıklar izleniyor ; sebep-sonuç analizi standard olarak uygulanıyor	konuyla ilgili tüm uzmanların katılımı sağlanıyor
5	üst düzey ve ileri görüşlü bir anlayış seviyesi var	iletişim ve eğitim konularında en iyi yöntemler uygulanıyor ve en yeni gelişmeler takip ediliyor	sektör ve konu ile ilgili en iyi yöntemler uygulanmakta	en gelişmiş teknolojiler uygulanmakta, teknoloji kullanımı optimize edilmiş	tüm süreçlerde kurumsal karne uygulaması yapılıyor, farklılıklar izleniyor ve iyileştirici önlemler alınıyor; sebep-sonuç analizi her durumda yapılıyor	yabancı uzmanların ve endüstri liderlerinin danışmanlığı alınıyor

Şekil 4.3 Cobit Olgunluk modelleri (Artinyan, 2008)

5. TEKNOLOJİ YÖNETİMİ

Teknoloji Yönetimi, "Bir organizasyonun stratejik ve taktik amaçlarının şekillendirilmesinde ve bunlara ulaşılmasında ihtiyaç duyulan teknolojik kapasitenin planlanması, geliştirilmesi ve uygulanmasıdır." Teknoloji Yönetimi kavramını biraz açarsak, teknoloji yönetimi yöneticilik ile teknik uzmanlık arasında bağlantıyı kurmak ve teknoloji transferi, teknoloji pazarlaması, teknolojik planlama, araştırma-geliştirme, tasarım, imalat, prototip oluşturma, test etme gibi teknoloji terimine ve teknoloji geliştirilmesine yönelik faaliyetlerin planlaması, örgütlenmesi, koordinasyonu ve kontrolü ile ilgili faaliyetlerin tümüdür. COBIT te de Teknoloji Yönetimi ile ilgili kavramlar AI Tedarik ve Uygulama bölümünde ele alınmaktadır.

Görüldüğü üzere, teknoloji yönetimi içinde yer alan faaliyetler farklı özelliklere sahip olduklarından bunların bir arada incelenmesi oldukça fazla çabayı gerektirmektedir. Mühendislik bilimleri, sosyal bilimler ve yönetim bilimi arasında bir köprü niteliği taşıyan Teknoloji Yönetimi farklı disiplinler arasında ara bir disiplin olarak, kendine has kavram, teknik ve bilimsel modelleri geliştirme yolunda 1970' li yıllardan bu yana emin adımlarla ilerlemektedir. İçinde yaşadığımız çağda teknolojik gelişmeler öyle hızlanmıştır ki, bu hız 21. yüzyılda artarak devam edecektir. Bu hızla gelişen teknolojiyi yönetmeyen ülkeler ve şirketler çağın gerisinde kalmaya mahkum oldukları gibi teknolojinin kendilerini yönetme tehlikesiyle karşı karşıya kalacaklardır.

5.1 Teknoloji Yönetiminde Yaklaşımlar

Teknoloji Yönetimi konusunda, farklı iki yaklaşım söz konusudur. Birinci yaklaşım, mikro yaklaşım olup, teknolojiyi firma bazında planlama, koordine etme ve yönlendirmeyi içerirken diğeri daha makro olup, ülke genelinde teknolojik tahmin, teknolojik planlama, bilim-teknoloji politikasının tespiti, uygulanması ve kontrolüyle ilgili faaliyetlerin tümünü inceler.

Mikro yaklaşımda, yani firma bazında ele alınan teknoloji yönetiminde esas hedef, firmanın karını ve üretimini maksimize etmeye dönük olarak, teknik imkanlarıyla insan gücü kaynaklarını en optimum şeklinde planlama, örgütleme ve koordine etmek suretiyle yönetim faaliyetini gerçekleştirmektir. Makro yaklaşımda ise, teknoloji yönetimi ülkenin sosyo-ekonomik kalkınma hedeflerine uygun olarak, bilim-teknoloji planlaması, politika tespiti, teknolojik yatırımlar ve teknolojik altyapıyla ilgili faaliyetlerin yürütülmesi konuları ele alınmaktadır. Teknoloji Yönetimi' nin kapsamı içindeki konular şunlardır:

- Teknolojik Tahmin
- Teknolojik Planlama
- Teknolojik Risk Analizleri
- Ar-Ge Yönetimi
- Teknolojik Yeniliklerin Yönetimi
- Teknolojik Rekabet Stratejileri
- Teknoloji Transferi
- Teknoloji Seçimi
- Teknolojinin Ticarileştirilmesi (Patent, Lisans Anlaşmaları, Copyrights, Ticari Markalar)
- Mühendislerin ve Bilim Adamlarının Yönetimi
- Teknoloji ve Organizasyonel Değişimler

Teknoloji Yönetimi 1970' lerdeki petrol krizinden sonra gelişmeye başlayan bir disiplin olması nedeniyle henüz çok yeni bir disiplindir. Kavramsal sistemi yeni gelişen bir bilim dalıdır ve teknoloji yönetimi tıp ve mühendislik bilim displinleri gibi "disiplinler arası" bir nitelik taşır. Teknoloji Yönetimi, endüstri mühendisliği, iktisat, işletme, sosyoloji, psikoloji, siyasi bilimler ve yönetim bilimi kavram ve ilkelerinden bilhassa Mühendislik Yönetimi (engineering management) kavramlarından önemli ölçüde istifade etmektedir.

Teknoloji Yönetimi, ekonomik üretim etmenleri ve daha genelde ülkenin ekonomik yapısı içinde yer alan teknolojik alt yapı ve teknolojik yenilik, teknolojik incelemelerde ekonomi biliminden de istifade eder. Ülkenin genel ekonomik yapısını bilmeden teknoloji seçimine ve teknolojiyle ilgili stratejilere karar vermek mümkün değildir. Üretim-istihdam ilişkileri, üretim yatırım ilişkileri, ithalat-ihracat dengesi gibi ekonomik konular teknoloji seçimini ve üretimini doğrudan etkilemektedir. Teknolojideki ilerlemelerin insan gücü kaynaklarının gelişmişliği ile eş anlamlı olduğu düşünüldüğünde bir ülkedeki insan gücünün eğitiminin, isthdamının ve sosyal ve kültürel yapının teknolojiyle yakından ilgili olduğu görülecektir. Ayrıca bir ülkenin sahip olduğu teknolojik gücün uluslararası sistemde o ülkenin yerini ve izleyeceği dış politikayı doğrudan etkileyeceği gerçeği inkar edilemez.

Gerek ülkeler, gerekse firmalar hızla değişen teknolojik, ekonomik ve siyasi şartlarda devam eden acımasız uluslararası rekabette güçlü olabilmek için en iyi stratejiyi tayin etmek ve uygulayabilmek durumundadırlar. Teknolojik gelişme ve teknolojik yeniliklere sahip olmak rekabette en güçlü silahtır. Ar-Ge ve teknoloji geliştirme yatırımları uzun vadede karlı ve kalifiye, yetişmiş insan gücü gerektiren yatırımlardır. Teknoloji temini için farklı seçenekler

söz konusudur:

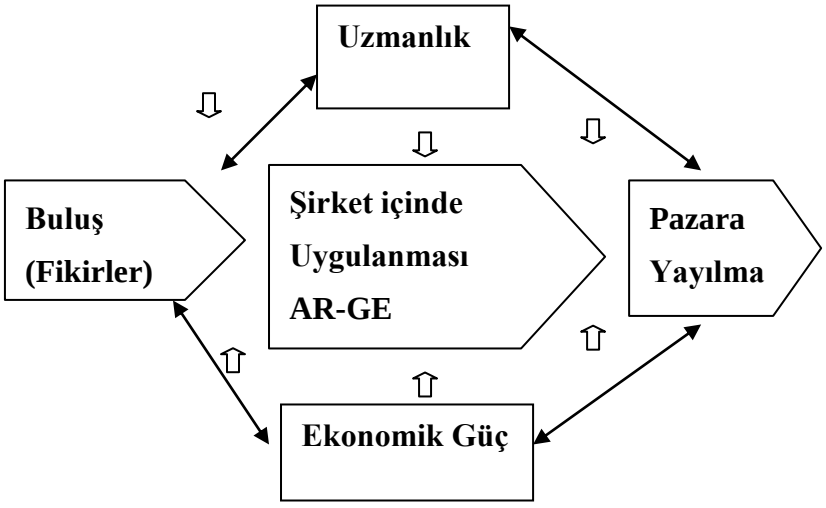
1. Firma içi Ar-Ge faaliyetleriyle ürün ve proses gelistirmek.
2. Teknolojiyi transfer etme (Lisans alma, Yabancı sermaye ortaklığı, Joint Venture vb.)
3. Mevcut teknolojiyi kullanmak

5.2 Teknoloji Yönetim Süreci

Teknolojik yenilik geliştirme süreci uzun bir süreci içerir. Buluş veya yeni bir fikir aşamasından başlayan bu süreç Ar-Ge faaliyetlerinin gerçekleştirilmesi ve Ar-Ge faaliyetleri sonucu ortaya çıkan yeni ürün ve hizmetlerin pazara ve müşterilere sunulmasına dek yapılan bütün faaliyetleri içerir. Bütün bu sürecin yönetimi esnasında verilen kararlar şirketin geleceği açısından son derece önemli kararlardır.

Teknolojik Yenilik sürecinin yönetimindeki stratejik karar noktaları şunlardır:

- Stratejik Teknolojik Planlama
- Teknolojik Tahmin
- Araştırma ve Geliştirme
- Teknolojinin Ticarileştirilmesi
- Teknolojinin Pazarlanması



Sonuç olarak Teknoloji Yönetimi işletmeye, teknolojik alanda üretim teknolojisi, ürün teknolojisi ve yönetim teknolojisi konularında sürekli bir öğrenme, geliştirme ve gelişen teknolojileri takip edebilme yeteneği vermesinden dolayı oluşabilecek içsel veya dışsal herhangi bir soruna karşı daha duyarlı olmasını ve bu sorundan en az hasarla kurtulmasını sağlayacaktır. Çünkü Teknoloji Yönetimi uygulayan bir işletme teknoloji planlama, teknoloji

tahmini, araştırma ve geliştirme yönetimi gibi bileşenleriyle işletme içinde veya dışında ortaya çıkabilecek problemlerden en az kayıpla kurtulmasını sağlayacak çalışmaları yapabilecektir.

Teknolojik bazlı işletmeler Teknoloji Yönetimi'ni işletmelerinde kullanırlarsa teknolojik faktörlü her hangi bir krizi de önceden fark edebilirler, meydana gelen teknoloji faktörlü bir krizden işletmelerini en az hasarla çıkarmalarını ve işletmelerinin bu krizden fırsat yaratabilmesini de sağlarlar (Baraçlı, 2001).

5.3 Bankalarda Teknoloji Yönetimi ve Kontrolü

Rekabetin çok üst düzeylerde olduğu günümüz dünyasında teknoloji olmadan herhangi bir şey yapmak neredeyse imkansız hale gelmiştir. Teknolojiyi en iyi kullanan bankalar rakiplerine göre avantajlı olmakta, rekabette daha öne çıkmaktadırlar.

Teknolojinin önemini anlayamayan ya da teknolojiyi verimli bir şekilde kullanamayan bankalar ise zamanla küçülerek yok olma tehlikesi ile karşı karşıya kalabilmektedirler. Teknolojinin bu kadar önemli ve kritik bir hal alması, bankalar için beraberinde risklerini getirmektedir. Teknolojinin riski nedir? Nasıl ölçülür? Ne şekilde engellenebilir veya en aza indirilir? gibi soruların sorulması ve cevaplarına göre aksiyon alınması bankalar için gerekli hale gelmiştir. Çünkü teknolojide risk yoktur demek mümkün değildir. Önemli olan teknolojiyi kullanırken riskleri iyi belirlemek, hiçbir şekilde göz ardı etmemek veya küçümsememektir. Bankalar teknolojiyi bilinçsizce kullanmamalı, kısa vadeli ve dar açılı düşünmemeli, genişbir perspektifte gerekli tüm koşulları ile birlikte ele almalıdır. Bunu yapmanın yolu teknolojiyi iyi analiz etmek, işlemleri yaparken, projeleri geliştirirken kontrolleri ve riskleri düşünmek ve yapılması gerekenleri uygulamaktır. Yani teknolojinin kontrolü, risklerin en aza indirilmesinde en önemli araçlardan bir tanesidir.

Teknolojinin önemini benimsemiş bankaların, teknolojinin içerdiği riskleri de göz önüne alarak kararlar vermesi ve yatırımlar yapması en doğru olanıdır. Bu nedenle teknolojik risklerin neler olduğu, bu risklerin en aza indirilmesi için nelerin yapılması ve nasıl yapılmaları gerektiğinin belirlenmesi çok önemlidir.

Bilgi Teknolojilerinde teknoloji projeleri ve teknoloji operasyonları olmak üzere yönetim şekilleri ve kontrolleri ayrı iki ana unsur vardır. Teknoloji projeleri, belirli bir amacı gerçekleştirmek için, belirlenen zaman ve bütçe çerçevesinde, ortaya konan çalışmalardır. Proje yönetimi ise bir projenin öngörülen zaman diliminde, belirlenen bütçeyi aşmadan ve hedeflenen sonucu elde etmek için gerekli kaynakların yönetilmesidir. Teknoloji

Operasyonlarında dört ana işlev mevcuttur (Güvener, 2000).

1. Kesintisiz hizmet: Amaç, bankanın mevcut tüm sistemlerinin planlanan çalışma süreleri boyunca kesintisiz hizmet vermelerini sağlamaktır. Banka sistemlerinin servis dışı kalma süreleri yıllık olarak hedeflenen süreleri aşmamalıdır. Bankanın müşterisine "Sistemimiz çalışmıyor" şeklinde bir mazeret sunması hiçbir zaman kabul edilebilir bir durum olmamalıdır.

2. Güvenlik: Bankanın tüm sistemlerinin her türlü güvenliği sağlanmalıdır. Fiziksel güvenlik, bilgilerin güvenliği, girişkontrolü, virüs, yetkisiz erişim gibi tüm güvenlik sorunlarıbu gruptadır. Bankalar güvenlik unsurlarının hiç birinden, hiç bir durumda taviz verilmemelidir Çünkü bankalar için kurumsal bilgi en önemli varlıklar ıarasındadır ve bu nedenle çok iyi korunması gereklidir.

3. Destek ve Yardım Masası: Bankaların teknoloji operasyonlarında kullanıcıya (müşteriye yada banka içi kullanıcı) verilecek yardım ve destek çok önemli bir konudur. Destek olmadan sistemlerin sürekli ve verimli olarak hizmet vermeleri sağlanamaz. Kullanıcı desteği mutlaka yardım masası gibi yapılanmalar ile desteklenmelidir. Bunun sonucunda destek hizmetinin kalitesi artırılarak ve cevap verme süresi kısaltılarak iç müşteri memnuniyeti en üst düzeyegetirilmelidir.

4. Yedekleme: Yedekleme tüm teknoloji platformlarının operasyonları açısından çok önemlidir. Donanım, yazılım, işletim sistemleri ve data unsurlarının yedeklemelerinin sağlanmasıişin sürekliliği açısından şarttır. Bankalar mutlaka sistemlerini yedeklemeli, herhangi bir sorun meydana gelmesi durumunda data kaybına uğramamalıdır.

Bu dört ana işlevi eksiksiz yerine getirmek için takip edilmesi gerekli yöntemler 8 alt başlık altında ele alınabilir (Güvener, 2000)

5.3.1 Problem Yönetimi

Problem yönetimi banka içerisinde problemlerin tanımlanması, gruplandırılması, kayıt edilmesi, çözümlenmesi ve bir daha tekrar etmemesi için önlemlerin alınması konularını kapsar. Etkin bir problem yönetimi ile teknik aksaklıklar azaltılarak hizmet kalitesi artırılabilir. Bankada teknik anlamda aksayan ve zayıf yönler, etkin bir problem yönetimi ile kolayca tespit edilebilir ve gerekli önlemler alınabilir.

5.3.2 Değişim Yönetimi

Değişim yönetimi, bankalarda kullanılan sistemlerde yapılacak her türlü değişimin planlanması, test edilmesi ve uygulamaya alınmasınıkapsar. Burada ana amaç kullanımda olan tüm operasyonel sistemlerin güvenirliliğini sağlamak, yapılması gerekli değişiklik sırasında oluşabilecek riskleri en aza indirmektir. Çalışan sistemlere yapılacak her türlü değişiklik tabiatıgereği risk ihtiva etmektedir. Değişim yönetimi çok genişbir ölçekte ele alınmalıdır. Sistemdeki herhangi bir cihazın değişiminden, uygulama programlarındaki geliştirmelere kadar tüm değişiklikler bu kapsamda değerlendirilmelidir. Planlanan değişikliğin etkileri incelenmeli ve geri dönüşplanları da önceden mutlaka yapılmalıdır. Yapılacak her türlü değişim mutlaka ilgili yöneticiler tarafından onaylanmalıdır. Konunun önemine göre ana sistemlerde yapılan değişiklikler bir müddet izlenmeli ve herhangi bir olumsuz gelişme karşısında etkin olarak önlem alınmalıdır.

5.3.3 Bilgi Güvenliği

Bilgi güvenliği, değerli varlıkların kaybedilmesi, yanlış kullanılması, ifşa edilmesi ve zarar görmesini önlemekle ilgilidir. Değerli varlıklar; kaydedilen, işlenen, saklanan, paylaşılan, elektronik ortamda gönderilen bilgilerdir. Bu bilgiler tehditlere karşı korunmalıdır. Bilgi güvenliğinin amacı; bilgiyle ilgili olanları ve kullanılırlık, gizlilik, bütünlük unsurları ile ilgili başarısızlıklardan zarar görebilecek sistemleri bağlantıları korumaktadır.

İnternetin etkisi, internet üzerinden ekonominin büyümesi elektronik işlemlere güvenme ihtiyacını doğurmuştur. Ayrıca kurum veri tabanında oluşturulan her türlü bilgi o kurum için çok değerlidir ve çok özenle korunması gereklidir. Bu bilgilerin değiştirilmesi, açıklanması müşteri kaybına yol açacağı gibi yasal yaptırımlar da söz konusu olabilir. Bu nedenle tüm bu bilgilerin en üst düzeyde korunmalarının sağlanması taviz verilemeyecek bir zorunluluktur.

5.3.3.1 COBIT te Bilgi Güvenliği

Bilgi güvenliği, Bilgi teknolojisi yönetişiminin en önemli unsurudur ve bütün bilgi kullanıcıları için bunu anlamak ve uygulamak önemlidir. Bilgisayar sistemleri işten eve kadar hayatın her alanında yaygınlaştıkça, güvenlik riskleri de artmaktadır. İnternet, portatif bilgisayar gereçleri, mobil teknolojinin yaygın kullanımı artık tüm bilgilere daha çabuk ulaşmamızı sağlamaktadır. Ancak diğer taraftan bilgi teknolojisindeki bu gelişmeler, bilgi hırsızlığı, virüslerle kasıtlı saldırı, bilgisayar korsanlığı gibi bilgi teknolojisi ile ilgili problemlerin ortaya çıkmasına sebep olmaktadır. Bu riskler, dikkatsiz hatalar, ciddi finansal zararlara sebep olur. COBIT Güvenlik Dayanağı daha iyi güvenlik sağlama ihtiyacı üzerine

tasarlanmış ve bilgi kullanıcılarını risklerden korumak için önemli tavsiyeler ve pratik araçlar içeren bir modeldir.

COBIT Güvenlik Dayanağı, COBIT ’e dayandırılmaktadır. COBIT, bilgi kuruluşlarının Bilgi Teknolojisi yönetişimine ve kontrol çerçevelerine uyum sağlamaları için gerekli olan kapsamlı kaynakları içeren bir modeldir. COBIT, bilgi teknolojisi kullanımından doğan riskleri tespit eder. Bu model, bilgi teknolojisi güvenliğindeki önemli risklere karşı ana kullanıcıların, küçük ve orta ölçekli işletmelerin, idarecilerin ve büyük kuruluşların yönetim kurulu üyelerinin kolaylıkla uygulayıp, takip edilebilecekleri işlemlerin üzerinde yoğunlaşır.

COBIT Bilgi Güvenliği; arka planın başarıyla okunması, COBIT esaslı güvenlik dayanağı, teknolojik güvenlik risklerinin özetini içeren ek olmak üzere üç unsurdan oluşmaktadır.

Yüzde yüz güvenlik diye bir şey yoktur ama modeldeki tavsiyeleri takip ederek, güvenlikle ilgili riskler hakkında bilinci arttırarak çok etkili seviyede güvenlik sağlanabilir. Bilgi teknolojisi ortamı değişmeye devam etmektedir ve dolayısıyla yeni güvenlik riskleri ortaya çıkmaktadır. İyi bir güvenlik sağlamak büyük miktarlarda zaman ve para harcamakla gerçekleştirilmez. Bilgi teknolojisi kullan ılırken bilincin arttırılması, gerçekleşebilecek risklerin belirlenmesi ve hassas önlemlerin alınması çok az gayretle gerçekleştirilebilir. Bu model, kontrolün her safhasında ortaya çıkabilecek tüm riskleri teşhis etmez ama ne yapılması gerektiğini ve nasıl yapılması gerektiğini anlama yeteneğini geliştirir. İyi bir bilgi güvenliği sadece riskleri azaltmaz. İyi güvenlik, işletmenin bağlantıda bulunduğu diğer işletmeler üzerindeki itibarı, güveni de arttırır, zaman kaybını önleyerek ekinliği arttırır (Uzunay, 2007).

5.3.4 Beklenmedik Durum Planları

Bankaların müşterilerine vermekte olduğu hizmetlerin sürekliliğini sağlamak ve aksamalara engel olmak amacı ile beklenmedik durumlarda neler yapılacağının belirlendiği bir plan yapılması ereklidir (Başarır, 2006).

5.3.5 Kaynakların Yönetilmesi

Bankalarda teknoloji yönetiminde kaynakların bilinçli kullanımıson derece önemlidir. Hem teknolojik sistemler/platformlar hem de bunları kullanacak, destekleyecek elemanların etkin bir maliyet kontrolü ile en verimli şekilde kullanımı gerekmektedir. Banka düzeyinde işplanlarıve bunu destekleyen teknoloji planlarının yapılması gereklidir. Yıllık olarak yapılan planlara uyulmalıve değişiklikler ancak üst yönetimin onayıile yapılmalıdır. Mevcut sistemlerin performanslarısürekli olarak ölçülmeli, kapasite planlaması yapılmalıdır.

Sistemlerin bulunduğu ortamlar bankalar için hayati önem taşıyan alanlardır, bu nedenle çok iyi kontrol edilmelidir. Kaynakların yönetilmesi, PC yönetimi, network yönetimi, sistem yönetimi gibi başlıklarıda içerir. Bunlarla ilgili olarak detaylıprosedürler geliştirilmeli, tüm teknoloji personelinin bu kurallara uymalarısağlanmalıdır. Aynı şekilde teknoloji platformlarını kullanan personelin de kariyer planlarıyapılarak kurum içerisinde tutulmalarıve daha verimli çalışmaları sağlanmalıdır. Eğitim planlarıyıllık olarak yapılmalıve eğitimden tasarruf hiç bir durumda düşünülmemelidir, çünkü bu konuda yapılacak tasarruf gerçek anlamda bir tasarruf değil banka açısından bir risktir. Eğitim kaynakların verimli kullanımı için en önemli araçlardan bir tanesidir.

5.3.6 Uygulama Programlarının Geliştirilmesi

Uygulama program geliştirilmesi uzun süren ve yoğun bir çabayıgerektiren teknik bir iştir. Burada bankanın ihtiyaçlarıçerçevesinde, en ekonomik ve teknik anlamda en ileri seviyede ürünlerin geliştirilmesi söz konusudur. Mutlaka belirli standartlar çerçevesinde ve belirli yazılıprosedürlere uymak koşulu ile çalışmalar yapılmalıdır. Tüm uygulama program yazılımlarında projelerin başlatılması, tanımlamaların yapılması, tasarım ve test aşamaları ile uygulamaya alma konularında ilgili bölümler aktif olarak görev almalı ve projenin hedefine ulaşmasında çaba göstermelilerdir.

5.3.7 Uygulama Programlar Ve İşletim Sistemleri Alımı

Uygulama programlarını geliştirmek her zaman en uygun yöntem olmayabilir. Teknik olarak iyi düzeyde geliştirilmiş, maliyeti fazla olmayan ve bankanın ihtiyaçlarını karşılayacak uygulama programlarının piyasadan temin edilmesi de uygun bir çözüm olabilir. Bu durumda iyi bir araştırma yaparak bankanın ihtiyacını karşılayacak, ticari bir hazır paket çözümü yoluna gidilebilir. Burada dikkat edilmesi gereken en önemli nokta uyumluluktur. Alınan programların mevcut sistemler ile uyumlu olmaları hem destek hem de geliştirme açısından çok önemlidir (Güvener, 2000).

5.3.8 Dış Kaynak Kullanımı

Gerektiği durumlarda bazı hizmetlerin banka dışı kaynaklardan karşılanması düşünülebilir. Bu ancak maliyet, yüksek kalite, zaman kazanılması, uzmanlık gerektirmesi gibi nedenlerle olmalıdır. Muhasebe, teknoloji, halkla ilişkiler, reklam, piyasa araştırması, kontrol, güvenlik, temizlik, bina yönetimi, işe alma, çek/senet/nakit işlemleri gibi konularda dışkaynak kullanımına gidilebilir. Dışkaynak kullanımı mutlaka yazılı prosedürler ve yasal anlaşmalar

çerçevesinde bankanın varlıklarını ve iş yaşamını riske sokmayacak şekilde yapılmalıdır. Ayrıca alınan hizmetlerin denetlenmesi de oldukça önemlidir. Dışarıdan alınan hizmetler mutlaka bankanın kendi standartlarına uygun olmalı, banka hizmetlerinin bankanın vizyon ve misyonunu gerçekleştirmeye doğrudan veya dolaylı olarak katkısı olmalıdır.

Bilgi sistemlerinin ve bilişim teknolojisinin içerdiği risklerin, bankaların faaliyetlerinin kesintisiz yürütülmesi ve muhtemel zararların önlenmesi amacıyla, etkin olarak kontrolü şarttır. Genel kontrol ve incelemeler, veri yedekleme ve ilgili diğer işlemleri, kullanılan temel yazılımlardaki ve diğer yazılımlardaki gelişmeleri, bilgi erişim politikalarını ve bilgi erişimine ilişkin fiziki ve mantıksal güvenlik kontrollerini kapsar. Uygulamaya yönelik kontrol ve incelemeler, işlemlerin kaydının kontrolünü sağlayan ve yazılım uygulamalarının ve diğer el kitabı uygulama usullerinin içinde tanımlanan elektronik ortamdaki kontrol safhalarından oluşur. Uygulamaya yönelik kontrol ve incelemeler, mantıksal erişimler ile yazılımların özel kontrollerini ve benzeri diğer özel kontrol ve incelemeleri içerir.

Bankalarda teknoloji yönetimi, mutlaka teknoloji kontrolü ile desteklenmelidir. Teknoloji yönetim kadrolarından bağımsız bir birim, kurum içerisinde mutlaka oluşturulmalı ve yukarıda bahsedilen konuların belirli aralıklarla kontrolünü yapılarak ilgili birimlere rapor verilmelidir. Bu yaklaşım bankanın teknolojisinde aksayan yönleri, yani bankanın teknoloji risklerini açığa çıkaracağı gibi teknoloji işlevlerinin kalitesinin artırılmasına da yardımcı olur.

Teknoloji kontrol grubu, teknoloji yönetiminde kısaca vurgulanan tüm bu alt başlıklar için şablon kontrol noktaları belirlemeli, kontrol listeleri (check-list) hazırlamalı ve belirli aralıklarla bu konular da denetlemeler yapmalıdır. Aksayan yönler tespit edildikten sonra gerekli tedbirler alınarak bu sorunların giderilmesine çalışılmalı daha sonraki denetlemelerde bu konularda ki gelişmeler gözlemlenmelidir. Tespit edilen aksaklıkların kısa sürede giderilmesi çok önemlidir. Eğer bu takip edilmez ve aksamalar devam ederse, alışkanlık haline gelir ve mevcut risk daha da büyür. Bunun sonucunda da hem bankanın hiç öngörmediği risklerle karşılaşması mümkün olabilir. Belli başlı teknoloji kontrol noktaları şu şekilde olmalıdır (Güvener, 2000):

1. Logların kontrolü

2. Kontrol listelerinin (Checklist) denetlenmesi

3. Yedekleme işlemlerinin kontrolü

4. Gün sonu ve gün başı işlemlerinin kontrolü

5. Erişim haklarının denetlenmesi

6. Projelerin takibi, zamanında ve belirtilen bütçeler çerçevesinde gerçekleşip, gerçekleşmediklerinin tespiti, hedeflerin karşılanıp karşılanmadığının kontrolü

7. Değişim yönetimi kurallarına uyulup uyulmadığının kontrolü, gerekli onayların kontrolü

8.Problem yönetimi prosedürlerine uyulup uyulmadığının kontrolü, istatistiklerin değerlendirilip değerlendirilmediğinin incelenmesi

9. Virüs önleme mekanizması denetlenmeli aksamalar bildirilmesi

10. Dışkaynak kullanımında kurallara uyulup uyulmadığı, destek alınan firmanın kaliteli servis verip vermediği denetlenmesi

11. Beklenmedik durum planlarının yıllık olarak test edilmeleri kontrol edilmeli, testlerin kurallara uygun olarak ve gerçeği yansıtmaları sağlanması

12. Kaynak kullanımı ve sistemlerin performanslarının izlenip izlenmediği denetlenmesi

13. Kapasite planlamasının yapılması, teknoloji ve iş planlarının bulunup bulunmadığı kurum genelinde denetlenmesi

14. Kontrol prosedürlerinde standardizasyon sağlanması

15. Belirtilen bu kontroller hakkında detaylı şablonlar oluşturulmalı ve yazılı kontrol prosedürleri geliştirilmesi

6. RİSK ve YÖNETİMİ

6.1 Risk Kavramı

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

Riskin temel bileşenleri, oluşma olasılığı ve oluşması durumunda sonucu ne ölçüde etkileyeceğidir. Ancak riski, yalnızca olumsuz etkileri olan bir kavram olduğunu düşünmek büyük bir yanlış olur. Riske kazanç elde etme fırsatı olarak bakılmalı, fırsata dönüştürülmesi için sistematik bir çaba gösterilmelidir.

Belirsizlik Seviyesi	Özellikler	Örnekler
Seviye 0 **Belirsizlik yok (kesinlik)**	Sonuçlar tam olarak tahmin edilebilir.	Fizik yasaları, Doğa bilimleri
Seviye 1 **Objektif Belirsizlik**	Sonuçlar tanımlanmış ve olasılıklar bilinmektedir.	Şans oyunları (zar, iskambil)
Seviye 2 **Subjektif Belirsizlik**	Sonuçlar tanımlanmış ve olasılıklar bilinmemektedir.	Yangın, trafik kazaları, birçok yatırım
Seviye 3 **Sonsuz Belirsizlik**	Sonuçlar tam olarak tanımlanmamış ve olasılıklar bilinmemektedir.	Uzay keşifleri, genetik araştırma

Şekil 6.1Belirsizlik Seviyeleri örnek tablosu

Riskler birbiriyle etkileşim içerisinde olan 3 temel alanda ele alınır (Fikirkoca, 2003):

- Teknik risk, hedeflenen (tahmin edilen ve planlanan) performans değerine

ulaşamamanın bir ölçüsüdür. Teknik riskler, maliyet ve çizelge risklerinin temel nedenidir.

- Maliyet riski, tahmin edilen ve planlanan maliyet değerinin aşılması durumudur. Örneğin ekonomik koşullardaki belirsizlikler önemli maliyet risk kaynaklarından biridir.
- Çizelge riski ise bir işin tahmin edilen ve planlanan sürede gerçekleştirilememesinin bir ölçüsüdür.

6.2 Belirsizlik Kavramı

Belirsizlik; meydana gelecek sonuçların belirlenememesi ve bilinememesi olarak anımlanabilir. Belirsizlik sübjektif bir kavramdır, kişiye ve kurma göre değişir ve bu yüzden de kesin olarak ölçülemez. Bu nedenledir ki iki firma için de aynı riske sahip bir pazarda firmalar yeni ürünler üretmek için yatırım yapmayı düşünürken, bu firmaların sadece birisi yatırım kararı alabilir. Her iki firma için de risk aynı iken, yalnızca birinin yatırım kararı alması, belirsizliğin sübjektifliğini gösterir.

Belirsizlik yoksa kesinlik (belirlilik) vardır ve dolayısıyla meydana gelecek sonuçlarla ilgili şüphe yoktur. Geleceği öngörebilme yeteneği, öngörülmek istenilen olay ile ilgili bilgiye bağlıdır. Belirsizlik de sahip olunan bilgiye göre sınıflara ayrılabilir.

6.3 Risk Belirleme Süreci

Riski tanımak ve ölçmek mevcut durumu değiştirmediği gibi, yatırımın sonucunu da bilinir hale getirmez. Ayrıca bir yatırımın riski hesaplandıktan sonra yatırımın başarısız olabilme riski ortadan kalkmaz. Fakat kurumlar riski tanıyıp ve bildiklerinde yatırım konusunda daha bilinçli kararlar verebilecektir. Riski, mevcut durumu bulanık hale getirip yöneticileri yanlış kararlar vermeye sürükleyen bir tuzak olarak kabul edersek, ancak risk belirlenerek ve hesaplanarak bu belirsizlik ortadan kaldırılabilir (Arman, 1997). Risk ve belirsizlikle karşıkarşıya kalındığında öncelikle yapılması gereken riskin belirlenmesidir. Riskin belirlenebilmesi için aşağıda belirtilen sırada bir yaklaşım izlenebilir:

6.3.1 Riskin Tanımlanması

İlk aşamada riskli olduğu düşünülen önemli değişkenlerin gizli etki ve kimliği konusunda belirsizlik azaltılmaya çalışılmalıdır. Belirsizliğin azaltılmasına ve sorunun çözülmesinde yardımcı olabilecek bilginin işlevi daha iyi belirlenmelidir. Önemli değişkenler ve onların

belirsiz etkisini ortaya koymak için geleceğe yönelik planlama araçlarıkullanılabilir. Örneğin, gelecekteki işletme fırsatlarınıtanımak için en iyi, en olasıve en kötü biçimde geleceğe ilişkin senaryolar geliştirilir ve bu senaryolarla ilişkin çeşitli olaylar tanımlanır. Bu tür araçlar ve yöntemler, önemli değişkenlerin ve onların belirsiz etkilerinin yönetimce kavranmasını kolaylaştırabilir.

6.3.2 Riskin Ölçülmesi

Tek bir projenin ya da yatırımın riski ile toplam riskin ya da portföy riski birbirinden farklıdır. Bu nedenle riskin ölçülmesinin bir amacı da projelerin ya da yatırımların tek başlarına hangi risk sınıfına gireceğini belirlemek ve ona göre karar almaktır. Bu aşamada olaylara ilişkin öznel olasılık dağılımlarıbelirlenir. Bu dağılımlar, projenin ya da yatırımın riskini belirlemeye çalışan çözüm yöntemi olan risk simülasyonunun girdileridir. Kurulan model çözülerek ilgi duyulan değişkene/değişkenlere ilişkin olasılık dağılımı/dağılımları elde edilir. Bu çalışma, kurumu sadece projenin ya da yatırımın riskinin yüksek, orta ya da düşük olup olmadığıkonusunda aydınlatır; projenin üstlenilmesinin ya da yatırımın yapılmasının iyi ya da kötü olacağı konusunda hiçbir şey getirmez. Bu konudaki yargı, firmanın toplam riski ve diğer stratejik etmenlere dayanır.

6.3.3 Riskin Değerlendirilmesi

Yatırımın değerini yargılanırken yalnızca yukarıdaki belirtilen düşünce biçimi yeterli olmaz, ayrıca soyut ve ölçülemeyen etkenleri de göz önüne alınmalıdır. Ayrıca, hesaplamalarda kullanılan tüm varsayımların net şimdiki değere olan duyarlılığıda test edilmelidir.Bu aşamadan sonra yatırımın benimsenmesi söz konusu olabilir. Kurumun yatırımı benimserken soyut etmenlere karşı olası tutumu genellikle daha fazla önem kazanır. Bu etmenler, rekabete ilişkin ve örgütsel veya toplumsal niteliği olan stratejik etmenlerdir.

6.3.4 Riskin Yargılanması

Yönetimin kararı firmanın toplam riski konusunda bir yargıyı içermelidir. Bu nedenle bir projenin ya da yatırımın toplam riske ya da portföy riskine etkisi göz önüne alınmalıdır. Firmanın amacı sermayedarlarının servetini arttırmaksa; yönetimin, getirisi (verimi) sermaye piyasasında beklenen getiriyi aşan projelere yatırım yapması gerekir. Sermaye piyasasında getiri, risk primlerini içerir. Yüksek riskli yatırımlar, sermaye piyasasındaki fırsatlara bağlıolarak yüksek getiri sağlamalıdır. Bu nedenle benzer yatırımlar, tabi olduğu riske göre sınıflandırılmalı ve bu risk sınıfına giren projeler için riske göre ayarlanmış uygun ıskonto

(verim) oranları çıkarılmalıdır. Yönetim, böylece riske göre ayarlanmış oranlar kullanarak yatırımın, firmanın pazar değerine olası net etkisini kestiren net şimdiki değer rakamlarınıbelirleyebilir. Yönetim, bu yolla firma değerinin artacağınıbekleyebilir. Çünkü bu yaklaşım, tek bir yatırımla firmanın portföy riski arasındaki ilişkileri göz önüne almaktadır (Atan, 2002).

Bu sürecin çıktısı, firmanın pazar değerine yatırımın olasıetkisini gösteren yatırımın net şimdiki değer rakamıdır. Bu aşamada kurum yatırım konusunda değerleme yapmalıve sonuç olarak kabul ya da ret konusunda bir karara ulaşmalıdır.

6.4 Risk Yönetimi

Risk Yönetimi, proaktif ve hızlı kararlar ve faaliyetler ile sürekli olarak risklerin belirlendiği, hangi risklerin öncelikle çözümlenmesi gerektiğinin değerlendirildiği, risklerle başa çıkmak için stratejiler ve planların geliştirilerek uygulandığıbir sistematiktir. Başka bir deyişle, risk yönetimi belirsizlikleri ve belirsizliğin yaratacağı olumsuz etkileri daha kabul edilebilir düzeye indirgemeyi hedefleyen bir disiplindir. Risklerin probleme ya da tehlikeye dönüşmeden belirlenmesi ve en aza indirgenmesi faaliyetlerinin planlanması ve yürütülmesini kapsar. Farkında olmasalar da ekonominin içinde yer alan bütün aktörler, özellikle de finansal kuruluşlar aslında risk yönetimine odaklanmışlardır. Ancak, sadece son on-yirmi yıldır bu amaçla yürütülen faaliyetler "risk yönetimi" diye adlandırılmış ve bütünlükçü bir yaklaşımla "sistem" haline getirilmiştir. Bu sistemin geliştirilmesine yönelik çabalar, piyasaların (ülkelerin) gelişmişlik düzeylerine göre farklı boyutlarda fakat hemen aynı hızla devam etmektedir. Günümüzün modern işletme teorisinin ulaştığı en kapsamlıçözümlerden bir tanesi risk yönetimidir. Çünkü risk yönetimi getiri, sermaye ve riski ilişkilendiren; bunların arasında optimum dengeyi kuran bir yaklaşım, bir yönetim tekniği, bir yönetim anlayışıdır. Risk yönetimi tüm işletmeler için önemli bir iştir. Ancak risk yönetimi bankalar için özel bir öneme sahiptir. Çünkü bankacılık sektöründe ortaya çıkabilecek olan yeni bir risk, sadece o sektörü değil, ekonomik sistemin tamamını peşinden sürükleyebilmektedir (Başarır, 2006).

Risk yönetiminin en temel amacı, firmalara taşıdıkları risklerle uyumlu sermaye tahsisi sağlamak ve riske göre düzeltilmiş sermaye getirisini en üst düzeye çıkartarak yaratılan katma değeri artırmaktır. Risk yönetiminin bir diğer önemli hedefi ise, karar verme mekanizmaları için riskleri görünür ve ölçülebilir hale getirmek, sübjektifliği azaltmak ve firmaların yapacakları yatırımın sonuçlarını görerek hareket etmelerini sağlamaktır.

Günümüz dünyasında, artan küreselleşme ile sermayenin serbest dolaşımı üzerindeki engeller

giderek azalmakta, piyasaların entegrasyonu ve teknoloji sayesinde ise finansal hareketlilik artmaktadır. Bu nedenle finansal kuruluşlar, eskiden maruz olduklarırisklere ilaveten uluslar arası piyasalarda faaliyet göstermekten kaynaklanan global risklere de açık hale gelmişlerdir. Teknolojik ilerleme ve küreselleşme olguları, bankaların faaliyetlerindeki belirsizliğini ve maruz kaldıkları risklerin çeşitliliğini artırmıştır. Son yıllarda finans piyasalarında ortaya çıkan krizlerin çoğunda etkin bir risk yönetimi bulunmayışının neden olarak gösterilmesi daha karmaşık risk yönetimi tekniklerine olan ihtiyacı artırmıştır. Geleceğin belirsizliklerle dolu olmasından dolayı; geleceğe yönelen her kararda risk unsuru hesaba katılmalıdır. Günümüzde kuruluşları en çok zorlayan ekonomik konulardan biri de finansal riskin etkin yönetimidir. Son zamanlarda dünyada yaşanan krizler, global bazda otoritelerin, yatırım bankalarının ve şirket müdürlerinin risk yönetimi kavramını yöneticinin birincil ihtiyatlılık sorumluluklarından biri olarak görmelerine sebep olmuştur (Mandacı, 2003). Genellikle finansal risklerin şirket bilançoları ve gelir tablolarında kendilerini anlaşılması güç ve lineer olmayan bir şekilde göstermeleri, dikkatleri piyasa değerlerindeki dalgalanmaların istatistiksel anlamda ölçülmesinde yoğunlaştırmıştır. Çoğu güncel risk yönetim sistemleri ve protokollerinin altında yatan, riskin istatistiksel elde edilmiş değer hesaplamalarıdır.

6.4.1 Bilgi Teknolojilerinde Risk Yönetimi

Risk yönetiminde esas olan, riskin tümüyle engellenmesi değil, sorunlara sistematik ve dikkatli bir şekilde yaklaşılması ve almaya karar verilen risklerin dikkatli yönetimi yoluyla gereksiz kayıpların engellenmesidir. Başarılı bir risk yönetimi için, kurumun varlıklarına ve hedeflerine yönelik riskleri belirlemek, analiz etmek, denetim altında tutmak ve izlemek gereklidir.

Riski yönetmenin en doğru yolu, gerçekleşmesi ve vereceği zarar en yüksek olma olasılığı bulunan riskleri azaltacak resmi bir BT risk yönetim sürecinin oluşturulmasıdır. Risk yönetim sürecinin oluşturulması kararı sonrası yapılması gereken ilk iş bir risk yönetimi lideri atanmasıdır. Bu liderin kim olacağı veya işi nasıl yürüteceği, kurumun büyüklüğüne ve gereksinimlere göre değişecektir. Büyük kurumlarda risk yönetimi için ayrı bir bölümün oluşturulması da söz konusu olabilmektedir. Bu birim anahtar bilgiyi toplayacak ve kararlar verecektir. Aynı zamanda risk yönetim politikalarını ve kılavuzlarını/dokümanlarını oluşturacak ve belki de özel amaçlı risk yönetim sistemlerini devreye alacaktır. Daha küçük çaplı kurumlarda, mevcut birimlerden bir yönetici risk yönetimi çalışmalarının liderliğini yürütebilir. Buradaki önemli nokta, bu işlerin tek bir kişinin görevi olmadığının ve kurum içi ortak bir çalışma gerektiğinin bilincine varılması gerekliliğidir.

Önemli diğer bir nokta iletişim kanallarının düzgün oluşturulmasıdır. BT risk yönetimi hedeflerini oluştururken öncelikle üst yönetimle iyi bir iletişim kurulması gereklidir. Risk yönetimi çalışmalarının, mümkün olan en üst düzey yöneticiyle birlikte planlanması risk yönetiminin başarı şansını artıracaktır. Başarı şansını artıracak bir konu da, risk yönetiminin iş hedefleriyle uyumudur. Üst yönetimden iş hedeflerinin net bir şekilde ortaya konması istenmelidir. BT risk yönetiminden sorumlu yönetici, yürüteceği çalışmanın amaçlarını belirlerken diğer birimlerin risk yöneticilerini de sürece dahil etmeli ve zaman içinde risk değerlendirme bulgularını kurumsal risk çerçevesi içine koymalıdır.

Risk yönetimi ile ilgili destek sağlandıktan sonra işleyiş yöntemlerinin oluşturulması gerekecektir. Bunun için öncelikle kurumun uzun vadeli hedefleri üzerinde çalışılmalıdır. Daha sonra bu hedefleri tehlikeye atacak risklerin tanımlanması ve bu riskler için denetimlerin oluşturulması gerekecektir. Her kurumun bir risk yönetim planı olmalı ve bu plan daima güncel tutulmalıdır.

Risk yönetimi hedefleri, kayıp öncesi ve kayıp sonrası olmak üzere iki kategoride ele alınabilir: Kayıp öncesi hedefler, risklerin gerçekleşmesi beklenmeden alınması gereken önlemleri ve denetimleri (etkin çalışma ortamının sağlanması, belirsizliklerin ortadan kaldırılması, yasal ve diğer resmi düzenlemelere uyum, etik yaklaşımların sağlanması gibi) tarif edecektir. Üretim ortamındaki verilerin bütünlüğünün korunması kayıp öncesi hedeflere iyi bir örnektir. Bu hem yasal ve resmi düzenlemelere uyumu sağlayacak, hem de bu verileri kullanan iş birimlerinin risklerini azaltacaktır. Bu örnek hedefin gerçekleştirilebilmesi amacıyla, üretim ortamlarında değişiklik yönetimi uygulaması devreye alınmalıdır. Bu yöntem verinin keyfi bir şekilde değiştirilmesini engelleyecek, dolayısıyla da olası bir risk faktörünü ortadan kaldıracaktır.

Kayıp sonrası hedefler ise, işletimin hatadan kurtarılması ve devamlılığının sağlanması çerçevesinde değerlendirilmektedir. Soruna müdahale, iş devamlılığının sağlanması ve olağanüstü durumdan kurtulma yöntemleri bu kapsamda oluşturulmalı ve sorun anında gecikmeksizin uygulanmalıdır.

Burada önemle üzerinde durulması gereken konu etkinliktir. Risklerin ortadan kaldırılması veya azaltılması için denetimlerin oluşturulması gereklidir, ancak çok fazla denetim sebebiyle iş yapılamaz duruma gelinmesi de kurumlar için bir risk faktörü olabilmektedir. Risk yönetimi işleyiş yöntemleri oluşturulurken getiriler ve etkinlik iyi değerlendirilmelidir.

Risk yönetimi kapsamında kurumdaki tüm çalışanların bir rolü bulunmaktadır. BT risk yönetimindeki roller de bu genel çerçeve içinde değerlendirilmektedir. Bu bölümde, kurum içinde risk yönetiminde değişik grupların üstlenebilecekleri sorumluluklar ve roller incelenmektedir.

Üst yönetimin sorumlulukları:

- Risk yönetiminin kurum stratejilerine entegrasyonu
- Risk yönetiminin yakından izlenip gerekli desteğin sağlanması.
- Risk yönetim çalışmalarının etkililiğinin sorgulanması.
- Risk yönetimi eğitimlerinin sağlanması.
- Risk yönetiminin daha sistematik hale getirilmesi için gerekli yatırımların yapılması

Birim Yönetimlerinin sorumlulukları:

- Risk yönetim stratejilerinin kurum içinde uygulanmasının sağlanması
- Risklerin önceliklendirilmesi
- Risk yönetiminin performansının değerlendirilmesi
- Risk yönetimi prensiplerinin karar verme sürecinin bir parçası haline getirilmesi
- Risk yönetiminde yeterli planlama, gerçekleştirme, eğitim, kontrol, izleme ve dokümantasyon çalışmasının yapılması

Risk Yönetimi Uzmanlarının sorumlulukları:

- Risk yönetimi ile ilgili öneri, yönlendirme ve yardımların tüm kurumun risk politikalarıyla ve üst yönetimin hedefleri doğrultusunda yapılması
- Birimlerin riskleri belirlemelerine ve risk değerlendirmesi yapmalarına yardımcı olunması
- Birimlere, daha etkili bir risk yönetimi için yardımcı araçlar sağlanması veya bu tür araçların tasarım ve gerçekleştirimine yardımcı olunması

İç Denetim ve Kontrol uzmanlarının sorumlulukları:

- Risk Yönetimi kuralları çerçevesinde üst yönetime birimlerin performansı konusunda raporlama yapılması

Tüm çalışanların sorumlulukları:

- Risk yönetimi konularına karşı ilgili ve bilgili olunması
- İşlerin risk değerlendirmesi çerçevesinde yürütülmesi
- Bilgi ve doküman sağlanması

6.4.1.1 COBIT te Risk Yönetimi

BT Riskleri ile ilgili kavramlar COBIT te, *PO9 BT Risklerini Değerlendirerek Yönetme* bölümünde ifade edilmiştir. Buna göre COBIT Risk Yönetimim için aşağıdaki maddeleri

öngörür:

- BT yönetimi, risk yönetimi ve kontrol çerçevesini müessesenin (işletmenin) risk yönetimi çerçevesiyle entegre edilmelidir. Bu, müessesenin risk alınabilirlik ve riske tahammül seviyesiyle uyumlaştırmayı da kapsamaktadır.

- Uygun sonuçları sağlamak için risk değerlendirme çerçevesinin uygulandığı içerik tespit edilmelidir. Her risk değerlendirmesinin iç ve dış bağlamının tespiti, değerlendirmenin amacı ve riskler değerlendirilirken kullanılacak kriterler bu kapsam dahil edilmelidir.

- İş, yönetmenlik, yasa, teknoloji, ticari ortak, insan kaynakları ve işlevsel unsurlar dahil olmak üzere, işletmenin hedeflerine potansiyel bir etkiye sahip olan tüm olaylar tanımlanmalıdır. Olumlu yada olumsuz olmak üzere etkinin özelliği de tespit edilerek bu bilgiler sürdürülmelidir.
- Tekrarlanabilirlik bazında nicel ve nitel yöntemler kullanarak tanımlanmış tüm risklerin ihtimal ve etkisi değerlendirilmelidir. İçsel ve arta kalan riskle ilgili ihtimal ve etki ayrı-ayrı olarak, kategoriye göre portföy bazında tespit edilmelidir.

- Risk sahibi ile etkilenen süreç sahipleri tespit edilmelidir, uygun maliyetli kontrol ve güvenlik önlemlerinin sürekli olarak risklere karşı savunmasızlığı hafifletmesini sağlamak için risk yanıtı geliştirilerek sürdürülmelidir. Risk yanıtı, önleme, azaltma, paylaştırma yada kabul şeklinde risk stratejilerini tanımlamalıdır. Yanıtı geliştirirken maliyet ve faydaları dikkate alınız ve arta kalan riskleri belirli risk tahammül sınırları içerisinde tutan yanıtlar tercih edilmelidir.

- Maliyet, fayda ve uygulama sorumluluğunun tespit edilmesi dahil olmak üzere gerekli olarak tanımlanan risk yanıtlarının uygulanması amaçlı kontrol faaliyetler tüm seviyelerde önceliklendirilerek planlanmalıdır. Önerilen faaliyetler için onay ve arta kalan tüm riskler için kabul istenmelidir, yapılan faaliyetlerin, etkilenen süreç sahibi (sahipleri) tarafından sahiplenmesi sağlanmalıdır. Planların yerine getirilmesi takip edilerek tüm sapmalar üst düzey yönetime raporlanmalıdır.

7. COBIT VE DİĞER BT DENETİMİ KONTROL VE UYGULAMA YÖNTEMLERİ

7.1 COBIT ve Diğer Denetim Modelleri

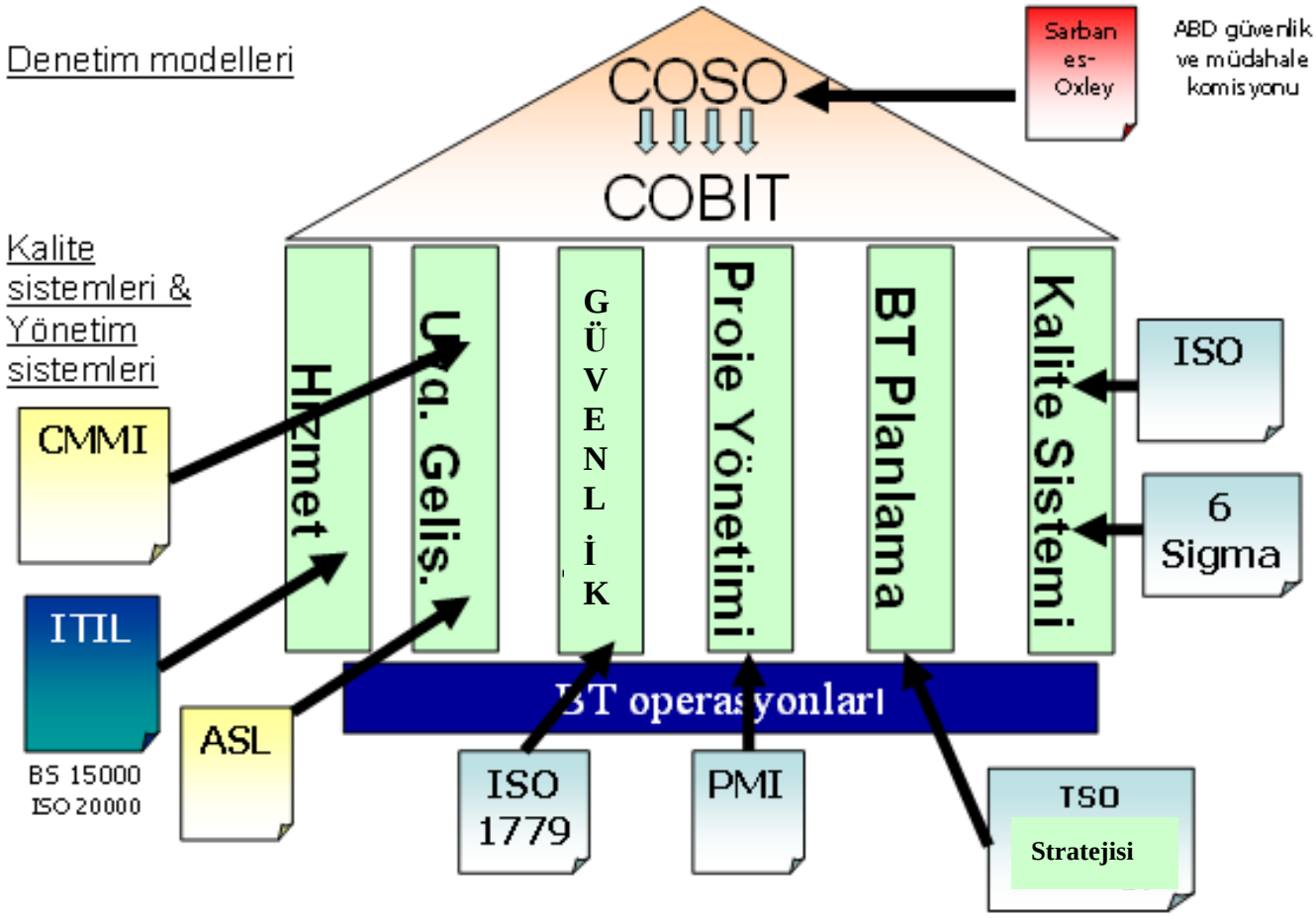
Şekil 7.1 de BT denetimi ile ilgili model ve metodlara yer verilmiştir.

Bunlardan;

ITIL: Kısaca bilgi teknolojileri BT Hizmet Yönetimi ile ilgili en iyi dokümanları içerir.

CMMI: Yazılım geliştirme süreç olgunluğunun ölçülmesi ve belli olgunluk seviyelerinin tanımlanarak hedeflenmesine olanak tanıyan bir rehberdir.

ISO/IEC 17799: Bilgi güvenliği ile ilgili yaygın kabul gören uygulamalar rehberidir.



Şekil 7.1 COBIT ile diğer denetim araçları arasındaki ilişkiyi gösteren örnek çizim

Temel olarak COBIT, ISO/IEC 17799 ve ITIL karşılaştırıldığında;

COBIT içerdiği süreçler ve kontrol hedefleri için işin detayda nasıl yapılacağını anlatmamış ve süreçleri bir düzen içinde sıralamamıştır. Süreçleri sınıflandırırken konusal bir sınıflandırma çalışması yapmıştır. Bu nedenle COBIT' e uygun hale gelmek için bahsi geçen süreçleri hayata geçirmek amacıyla diğer kaynaklardan yararlanmak gereklidir. Bu kaynaklar başta ITIL olmak üzere CMMI, PMI ve Prince2 gibi kaynaklardır. Bunlar içerdikleri süreçler için nasıl yapılması gerektiğini somut örneklerle anlatan süreç modelleridir. Bu modellere bakıldığında her birinin endüstri mühendisliğindeki süreç yaklaşımı ve kalite iyileştirme çalışmalarının Bilgi Teknolojileri süreçlerine somut olarak uyarlanmış halleri olduğu görülebilir. COBIT de hangi süreçlerin ITIL, CMMI, PMI ve Prince2 da hangi alt süreçlere/konulara denk geldiğini gösteren haritalar mevcuttur.

7.1.1 BS7799 / ISO17799 / TS 17799 Güvenlik Standartı

ISO 17799, bilgi güvenliği yönetimi için uygulama prensiplerinin ortaya konulduğu dünyada kabul görmüş bir standarttır. ISO 17799 standardı bir kurumda bulunması gereken güvenlik önlemlerine yer vererek temel bir güvenlik çerçevesi çizer.

ISO 17799 standardının temeli BS 7799 standardına dayanmaktadır. BS 7799 bir İngiliz standardıdır. İlk olarak 1995 senesinde yayınlanmıştır. 1999 senesinde günün ihtiyaçlarına göre büyük ölçüde değişikliğe uğramıştır. BS 7799 standardı 2000 senesinde ISO standardı olarak yayınlanmış ve tüm dünyada ISO 17799 olarak kabul görmüştür.

2002 senesinde çıkartılan BS 7799-2 (Bölüm 2) standardı ile ortaya konan kullanım kılavuzu ile kurumların ISO 17799 sertifikasyonu alması hedeflenmiştir. TSE, ISO 17799'u 2002 senesinde BS 7799-2'yi ise Şubat 2005'te Türkçe olarak yayınlamıştır.

BS7799 standartı kurumlar bünyesinde bilgi güvenliği yönetimi sürecini başlatan, gerçekleştiren ve sürekliliğini sağlayan kişilerin kullanımı için, bilgi güvenliği yönetimi ile ilgili tavsiyeleri kapsar. Bu bağlamda aşağıda belirtilen üç temel prensip çok önemlidir.

- **Gizlilik**: Bilginin sadece erişim yetkisi verilmiş kişilerce erişilebilir olduğunun garanti edilmesi.
- **Bütünlük**: Bilginin ve işleme yöntemlerinin doğruluğunun ve bütünlüğünün temin edilmesi.
- **Elverişlilik**: Yetkilendirilmiş kullanıcıların, gerek duyulduğunda bilgiye ve ilişkili kaynaklara erişime sahip olabileceklerinin garanti edilmesi.

7.1.1.1 COBIT ve ISO17799 İlişkisi

COBIT ve ISO 17799 içeriklerinin karşılaştırıldığı ilişki aşağıdaki Çizelge 7-1 de görülmektedir.

Çizelge 7-1 COBIT & ISO17799 ilişkisi

COBIT	**ISO 17799**
Kurumsal Yönetişim	Bilgi Güvenliği Odaklı
İş Strateji ve Süreçlerinin Değerlendirilmesi	Bilgi Güvenliği Standardı
Ölçüm Yöntemi	Güvenlik Kontrollerinin Değerlendirilmesi

7.1.2 Sarbanes Oxley

Sarbanes-Oxley Yasası, 30 Temmuz 2002'de yürürlüğe girmiş olan, Özel Şirketler Muhasebe Yeniden Düzenlemesi ve Yatırımcının Korunması Yasası olarak da bilinen (genel olarak SOX ya da SarbOX diye adlandırılan) bir ABD federal yasasıdır.

Yasanın içeriğinde Özel Şirket Muhasebe Gözetim Kurulu'nun kurulması, denetçinin bağımsızlığı, şirkete ait sorumluluk ve gelişmiş finansal açıklamalar gibi konular yer almaktadır. Sarbanes Oxley, kanuni denetim gereksinimlerini incelemek üzere planlanmış bir yasa olup 1930'lardan beri Amerika güvenlik yasalarında yapılan en büyük değişiklik olarak görülmektedir. Bu yasa SEC diye bilinen Amerika Menkul Kıymetler ve Borsa Kurulu'na ilave yetkiler ve sorumluluklar vermektedir.

Yasa, aralarında Enron, Tyco International, Worldcom (MCI) gibi firmalarında etkilendiği bir seri finansal skandalın patlak vermesiyle birlikte doğmuştur. Senatör Paul Sarbanes ve Vekil Michael G. Oxley'in adlarından oluşmaktadır.

Hükümler

Sarbanes-Oxley Yasasının başlıca hükümleri aşağıda belirtilmektedir.

11. Finansal raporların Genel Müdür ve Finans Müdürü tarafından tasdik edilmesi
12. Tüm Yönetici ve Müdürlere kişisel kredinin yasaklanması
13. İçeriden alınan bilgilerle hisse senedi alışverişinde bulunanların hızlandırılmış raporlanması

14. Emeklilik fonlarını karartma zamanlarında içeriden alınan bilgilerle hisse senedi alışverişinde bulunmanın yasaklanması
15. Genel Müdür ve Finans Müdürü'nün tazminat ve karlarının halka açıklanması
16. İlave açıklamalar yapılması
17. Denetim bağımsızlığı; bazı tür işlerden tamamen men edilmesi ve denetime tabii olmayan tüm işlerin Denetim Komitesi tarafından önceden tasdiklenmesi
18. Menkul Kıymetler Yasasının çiğnenmesi için kriminal ve medeni cezalar verilmesi
19. Bilerek ve isteyerek finansal tablolarını farklı gösteren şirket yöneticileri için çok daha uzun hapis cezaları ve büyük tazminat bedelleri uygulanması
20. Müşterilerine hukuksal ve ya danışmanlık gibi denetim işleriyle ilgisi olamayan ekstra 'katma değerli' hizmetler sunan denetim firmalarının yasaklanması
21. Halka açık firmaların finansal raporlama ile ilgili iç denetimlerinin varlığı ve durumuyla ilgili yıllık bağımsız raporlar vermeleri gereksinimi

PCAOB (Özel Şirketler Muhasebe Gözetim Kurulu) 'un Gereksinimleri

- Finansal tablolardaki belli başlı hesaplar ve açıklamalarla ilgili uygun teyitlerin kontrolünün planlanması
- Belli başlı hareketlerin nasıl başladığı, yetkilendirildiği, desteklendiği, yürütüldüğü ve raporlandığı hakkında bilgi
- Yanlışlık ya da kasıtlı olarak oluşmuş yanlış beyanların yerlerinin saptanması için hareketlerin akışıyla ilgili yeterli bilgi
- Sahtekarlığı önlemek ve saptamak için gerekli kontrollerin oluşturulması (kontrollerin kimin tarafından yapıldığı ve düzenlenmiş görev ayrımlarını da içeren)
- Dönem-sonu finansal raporlama işlevinin kontrolü
- Mal varlıklarının korunmasının kontrolü
- Yönetimin testlerinin ve değerlendirmesinin sonuçları

7.1.2.1 COBIT ve Sarbanes Oxley İlişkisi

Bugünün iş çevresinde, kurumlarının çoğunun finansal raporlama süreçleri bilgi teknolojileri sistemlerinden alınmaktadır. Sadece az miktarda kurum verilerini elle yönetmektedir. Kurumların pek çoğu verinin, dokümanların ve anahtar operasyonel süreçlerin elektronik yönetimine geçmiştir. Bundan dolayı, iç denetimde bilgi teknolojilerinin hayati bir rol oynadığı görülmektedir. PCAOB şöyle demektedir:

"Bir kurumun bilgi sistemleri içinde bilgi teknolojilerini kullanma şekli, içeriği ve özellikleri kurumun finansal raporlama üzerindeki iç kontrolünü etkilemektedir."

Tüm bunları göz önüne alan Sarbanes Oxley finansal veri üretimi ile ilişkisi bulunan BT süreçlerinin COBIT te olduğu gibi denetlenmesini ve kontrol altında tutulmasını öngörmektedir.

7.1.3 Basel II

Basel Sermaye Uyumu adı verilen Basel II, ikinci Basel Anlaşmadır ve bankanın sermayesinin kifayetini ölçen uluslararası standartları gözden geçirmek için Bankacılık Denetimi üzerine kurulan 13 ülkeden merkez bankacıların oluşturduğu Basel Komiteyi temsil etmektedir. Basel II Basel II, operasyonel risklerin tanımlanması, değerlendirilmesi ve ölçülmesi için geliştirilmiş bir kurallar bütünüdür. Basel II, bankaların ve bankacılık düzenleyicilerinin ulusal sınırlar arasında risk yönetimine yaklaşım yöntemlerindeki tutarlılığı yükseltmek için yaratılmıştır. Yüksek standartlara sahip olan Basel II'ye uyum sağlamak için bankaların pek çok gerekliliği yerine getirmesi gerekmektedir.

7.1.3.1 COBIT ve Basel II ilişkisi

Aşağıdaki tabloda Basel II olay çeşitlerinin COBIT kontrol hedeflerinden hangilerine karşışl geldiği görülmektedir. BDDK' nın bilgi sistemleri denetim metodolojisi olarak COBIT seçmesinin nedenlerinden biriside bu uyumdur.

Çizelge 7-2 COBIT & Basel II ilişkisi

Basel II Olay Çeşitleri	**BT ile ilgili alanlar**	**COBIT Kontrol Hedefleri**
İç Dolandırıcılık	• Programların kasıtlı değiştirilmesi • Değişiklik fonksiyonlarının yetkisiz kullanımı • Sistem yönergelerinin kasıtlı değiştirilmesi • Donanımın kasıtlı değiştirilmesi • Sistemin ve uygulama verilerinin Hackleme yoluyla kasıtlı değiştirilmesi • Lisansız yazılım kullanımı/kopyalanması • Erişim haklarının içeriden değiştirilmesi	• PO6 (Yönetimin amaçlarının ve talimatlarının iletilmesi) • DS5 (Sistem güvenliğinin sağlanması) • DS9 (Konfigürasyon yönetimi)
Dış Dolandırıcılık	• Sistemin ve uygulama verilerinin Hackleme yoluyla kasıtlı değiştirilmesi	• DS5 (Sistem güvenliğinin sağlanması)

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

7.1.4 COSO (Treadway Komisyonunu Destekleyen Kuruluşlar Komitesi)

Bir iç kontrol modeli olan COSO tezin 1.1.3 başlığında ele alınmıştır.

7.1.4.1 COBIT & COSO İlişkisi

COSO' nun geliştirmiş olduğu denetim standartları ile COBIT standartları arasındaki ilişki aşağıdaki Çizelge 7-3 te görülmektedir.

Çizelge 7-3 COBIT & COSO ilişkisi

	COBIT	**COSO**
Birincil Takipçiler	Yönetim, kullanıcılar ve BS denetçileri	Yönetim
(Bütünleşme Konsorsiyumu) BK gözüyle	Politikaları, süreçleri, uygulamaları ve organizasyonel yapıları içeren süreçler kümesi	Süreç
BK hedefleri - Organizasyonel	Etkin & Verimli operasyonlar, Gizlilik, Bilginin Uyumluluğu ve Ulaşılabilirliği, Kanun ve düzenlemelerle uyumlu güvenilir finansal raporlama	Etkin&Verimli operasyonlar, Kanun ve düzenlemelerle uyumlu güvenilir finansal raporlama
Bileşenler ve Alanlar	**Alanlar:** Planlama ve Organizasyon Tedarik ve Uygulama Hizmet Sunumu ve Destek İzleme ve Değerlendirme	**Bileşenler:** Kontrol ortamı Risk yönetimi Kontrol eylemleri Bilgi ve haberleşme takibi
Ana Alan	Bilişim Teknolojisi	Sektörün tamamı

7.1.5 ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi)

Bilgi Teknolojileri Altyapı Kütüphanesi olarak adlandırılan ITIL, tez çalışmasının 3 numaralı başlığında detaylı olarak ele alınmıştır.

7.1.5.1 COBIT ve ITIL İlişkisi

BT Altyapı Kütüphanesi ITIL ile COBIT kontrol hedefleri karşılaştırma tablosuna aşağıda yer verilmiştir.

Çizelge 7-4 COBIT & ITIL ilişkisi

ITIL Süreci	**Süreç Kontrol**	**Detay**	**COBIT Süreci**
Hizmet (Seviye) Yönetimi	DS 1	DS 1.0	Hizmet seviyelerini tanımla ve yönet
Hizmet Yönetimi Süreci	DS 1	DS 1.1	SLA çerçevesi
Sürecin Planlanması	DS 1	DS 1.2	SLA lerin görüşleri
Sürecin Uygulanması	DS 1	DS 1.2	SLA ve sözleşmelerin gözden geçirilmesi
Sürecin Devamı	DS 1	DS 1.5	SLA lerin görüşleri
Müşteri Hizmet Anlaşmalarının (SLA) içerik ve hedefleri	DS 1	DS 1.2	SLA lerin görüşleri
Hizmet Yönetimi etkinlik ve verimliliği için Anahtar Performans Göstergeleri (KPI) ve metrikler	DS1	DS 1.4	İzleme ve raporlama
BT hizmetleri için Finansal Yönetim	PO 5	PO 5.0	BT yatırımlarını yönet
Bütçeleme	PO 5	PO 5.1	Yıllık BT yürütüm bütçesi
BT Muhasebe sistemini geliştirme	PO 5	PO 5.1	Yıllık BT yürütüm bütçesi
Sorumluluk yükleme sistemi geliştirme	DS 6	DS 6.2	Maliyetlendirme prosedürleri
BT muhasebe ve yüklemeleri için planlama yapma	DS 6	DS 6.1	Yüklenebilecek bileşenler
Uygulama	DS 6	DS 6.0	Maliyetleri tanımlama ve dağıtma
Süregiden yönetim ve operasyon	DS 6	DS 6.3	Kullanıcı faturalandırma ve geri ödemeleri
Kapasite Yönetimi	DS 2	DS 2.0	3. Parti hizmetleri yönet
Kapasite Yönetim süreci	DS 3	DS 3.0	Performans ve kapasiteyi yönet
Kapasite yönetiminde aktiviteler	DS 3	DS 3.7	Kaynak kapasite yönetimi
Maliyet, fayda ve olası problemler	DS 3	DS 3.7	Kaynak kapasite yönetimi

7.1.6 COBIT ve Diğer BT Denetimi Kontrol ve Uygulama Yöntemlerinin Kıyaslanması

Tüm BT standart ve yöntemlerinin COBIT kontrol hedeflerinde var olan karşılıklarının dağılım sıklığını aşağıdaki tabloda gösterilmiştir.

Çizelge 7-5 COBIT &Diğer BT standartları karşılaştırma tablosu

	COBIT Proseslerinin Diğer Standartlardaki Karsılıkları												
CobiT Process	COSO	ITIL	ISO/IEC 17799	FIPS PUB 200	ISO/IEC TR 13335	ISO/IEC 15408	PRINCE2	PMBOK	TickIT	CMMI	TOGAF 8.1	IT BPM	NIST 800-14
PO 1	+	-	-	-	-	-	-	-	-	-	-	-	-
PO 2	+	-	+	+	+	-	-	-	-	-	+	-	+
PO 3	+	+	+	+	+	-	-	-	-	-	+	+	+
PO 4	+	+	+	+	+	-	-	-	-	-	+	-	+
PO 5	+	+	-	-	-	-	+	+	-	-	-	-	-
PO 6	+	-	+	+	+	-	-	-	-	-	-	+	+
PO 7	+	-	+	+	-	-	-	-	-	-	-	-	+
PO 8	-	-	-	-	-	+	+	+	+	+	-	-	-
PO 9	+	-	+	+	+	-	+	+	-	+	-	-	+
PO 10	-	-	-	-	-	-	+	+	-	+	-	-	-
AI 1	+	-	-	-	+	-	-	-	+	-	+	-	+
AI 2	+	-	+	+	-	+	-	-	+	+	-	-	+
AI 3	+	-	+	+	-	+	-	-	+	-	-	+	+
AI 4	+	+	+	+	-	+	-	-	+	-	-	-	+
AI 5	-	-	-	-	-	-	-	+	+	-	-	-	-
AI 6	+	+	+	+	+	-	-	-	+	+	-	-	+
AI 7	+	+	+	+	+	-	-	-	+	+	-	-	+
DS 1	+	+	-	-	-	-	-	-	-	-	+	-	-
DS 2	-	+	+	+	-	-	-	-	-	-	-	-	+
DS 3	+	+	+	+	-	-	-	-	-	-	-	-	+
DS 4	+	+	+	+	+	-	-	-	-	-	-	+	+
DS 5	+	+	+	+	+	+	-	-	-	-	-	+	+
DS 6	-	+	-	-	-	-	-	-	-	-	-	-	-
DS 7	+	-	+	+	+	-	-	-	-	+	-	-	+
DS 8	-	+	+	+	-	-	-	-	-	-	-	-	+
DS 9	+	+	+	+	-	-	+	-	-	+	-	-	+
DS 10	-	+	-	+	-	-	-	-	-	+	-	-	+
DS 11	+	+	+	+	+	+	-	-	-	+	-	+	+
DS 12	+	-	+	+	+	+	-	-	-	-	-	+	+
DS 13	-	-	+	-	-	-	-	-	-	-	-	-	+
ME 1	-	-	+	-	-	-	-	-	+	+	-	-	+
ME 2	-	-	+	+	+	+	-	-	+	-	-	+	+
ME 3	+	-	-	-	-	-	-	-	-	-	-	-	-
ME 4	+	-	+	+	-	-	-	-	-	-	-	-	+

(+) Sıkça adreslenen

(-) Seyrek / hiç adreslenmeyen

8. UYGULAMA

8.1 Giriş

Uygulama olarak Halkbank'da hali hazırda COBIT ve ITIL uyumluluğu için çalışan Kalite Yönetimi Ekibinin belirlediği metodoloji ile ITSM (Information Technology Service Management – Bilgi Teknolojileri Hizmet Yönetimi) süreçlerinin COBIT ve ITIL uygunluk analizi yapılmıştır. Bulunan eksiklikler yönetime raporlanmış ve gerekli iyileştirme çalışmalar için süreç sahiplerine sorumluluk atanmıştır.

Halkbankası ITIL Süreçlerinin COBIT kontrol hedeflerindeki karşılıkları Çizelge 8-1 de gösterildiği gibi şöyledir:

Çizelge 8-1 Halkbankası ITIL Süreçlerinin COBIT kontrol hedeflerindeki karşılıkları

	COBIT KONTROL HEDEFLERİ							
ITIL SÜREÇLERİ	AI6 Değişiklikleri Yön@	DS1 Servis Seviyeleri Tanımla ve Yön@	DS3 Performans ve Kapasiteyi Yön@	DS9 Konfigürasyonu Yön@	AI3 Teknoloji Altyapısını Tedarik Et ve Bakımını Yap	DS8 Yardım Masası ve Çağrıları Yön@	DS10 Problemleri Yön@	DS9 Konfigürasyonu Yön@
Değişiklik Yönetimi Süreci	X							
Hizmet Yönetimi Süreci		X						
Kapasite ve Performans Yönetimi Süreci			X					
Konfigürasyon Yönetimi Süreci				X				
Kullanılabilirlik Yönetimi Süreci					X			
Olay Yönetimi Süreci						X		
Problem Yönetimi Süreci							X	
Varlık Yönetimi Süreci								X

ITSM kapsamında Halkbank da yer alan süreçler şöyledir:

1. Değişiklik Yönetimi Süreci
2. Hizmet Yönetimi Süreci

3. Kapasite ve Performans Yönetimi Süreci
4. Konfigürasyon Yönetimi Süreci
5. Kullanılabilirlik Yönetimi Süreci
6. Olay Yönetimi Süreci
7. Problem Yönetimi Süreci
8. Varlık Yönetimi Süreci

Süreç değerlendirme çalışmaları yapılmadan önce her çalışma için bir plan yapılarak süreç sahipleri ile mutabakat sağlamış ardından yönetim onayı alınarak çalışmalar yapılmıştır. Çalışmanın adımlarını anlatan iş akışı aşağıdaki gibidir.

Şekil 8.1 Halkbank BT - Kalite Yönetimi Süreç Değerlendirme Metodolojisi

Kurum bilgileri göz önüne alınarak bu uygulamada yukarıda bahsi geçen tüm sürelere dair bilgiler verilemeyecek olup örnek bir kaç süreç ve sonucunda tüm süreçlerin dahil olduğu genel değerlendirme yapılacaktır.

8.2 Ele Alınan Halkbank BT Yönetim Süreçleri

Uygulamada sırası ile aşağıdaki iki süreç ele alınmıştır.

1. Değişiklik Yönetimi Süreci
2. Olay Yönetimi Süreci

8.2.1 Değişiklik Yönetimi Süreci

Halkbankta Değişiklik Yönetimi sürecinin tarifi aşağıdaki gibidir.

"Değişiklik yönetimi, BT altyapısında ortak kullanılan tüm bileşenlerdeki (yazılım, donanım, servis, doküman vs…) herhangi bir değişikliğin gerçekleştirilmesi adımlarını yönetir. Değişikliklerin yol açabileceği sorunları en aza indirmek amacıyla, etkili planlama ve kontrolü esas alır."

"Değişikliklerin hızlı bir şekilde hayata geçirilmesi için standartlaştırılmış yöntem ve işleyişlerin kullanılmasını sağlayan teknik destek sürecidir. Bu şekilde, değişiklik gereksinimi ile değişikliklerin olası zararlı etkileri arasında doğru denge kurulabilir."

Uygulama kapsmanda süreç ITIL ve COBIT isterlerine göre değerlendirilmiştir.

8.2.1.1 Değişiklik Yönetimi Süreci Gözden Geçirme Planı Ve Raporu

DEĞİŞİKLİK YÖNETİMİ SÜRECİ GÖZDEN GEÇİRME PLANI	
SÜREÇ SAHİBİ	Süreç Sahibi (Gizlilik çerçevesinde isimler paylaşılmamıştır)
KALİTE EKİBİ	Kalite Ekibi Üyeleri (Gizlilik çerçevesinde isimler paylaşılmamıştır)
GÖZDEN GEÇİRME AMACI/ KAPSAMI	ITSM projesi kapsamında hayata geçen Değişiklik Yönetimi sürecinin amaçlarının, kontrollerinin, aktivitelerinin ve metriklerinin COBIT standartlarına uygunluğunun kontrol edilmesi ve değerlendirilmesi. Değerlendirme neticesinde varsa güncellemelerin ve eksikliklerin ve bunların giderilmesi için yapılması gerekenlerin belirlenmesi.
GÖZDEN GEÇİRME KRİTERLERİ	Gözden geçirme kriterimiz süreç için hazırlanmış olan dokümanlardır. Bu dokümanlarda yer alan sürece dair amaçlar, kontroller, aktiviteler ve metrikler gibi konuların COBIT standartlarına uygun mu sorusuna bu gözden geçirme ile cevap aranmaktadır.
SÜREÇ GÖZDEN GEÇİRME KODU	**2010_02_GG_004**

ÖNCEKİ GÖZDEN GEÇİRME KODU/ TARİHİ	**2009_06_GG_002**				
BAŞLANGIÇ TARİHİ	**02. 02. 2010**	**BİTİŞ TARİHİ (*PLANLANAN*)**	**22. 02. 2010**	**BİTİŞ TARİHİ *(GERÇEKLEŞEN)***	**04.02.2010**
KALİTE EKİBİ LİDERİ		**SÜREÇ SAHİBİ**			
Ekip Lideri		Süreç Sahibi			

İNCELENEN KONULAR	
Değişiklik Yönetimi Süreci Amaçları	
COBIT Amaçları	**Halkbank Mevcut Amaçlar**
❖ BT Amaçları ✓ İş ihtiyaçlarına iş stratejilerine uyumlu bir şekilde cevap vermek ✓ Çözüm ve hizmet sunum hatalarını azaltmak ✓ BT hizmet kesintilerinden veya değişikliklerinden kaynaklanan olayların işe etkisinin minimum olmasını sağlamak ✓ İş fonksiyonları ve kontrol ihtiyaçlarının efektif ve etkin otomatik çözümlere nasıl dönüştürüleceğinin tanımlanması ✓ Bilgi ve bilgi işleme alt yapısı bütünlüğünün sağlanması ve sürdürülmesi ❖ Süreç Amaçları ✓ BT alt yapı ve uygulamaları için	❖ Yönetilebilirlik ✓ <Bu kısımda Halkbank Değişiklik yönetimi süreci amacı yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay ilgi verilememektedir.> ❖ Optimum Bürokrasi ✓ <Bu kısımda Halkbank Değişiklik yönetimi süreci amacı yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay ilgi verilememektedir.> ❖ Son Kullanıcı Verimliliğinin artırılması ✓ <Bu kısımda Halkbank Değişiklik yönetimi süreci amacı yer

değişikliklerin yetkilendirilmesi ✓ BT alt yapı, uygulamaları ve teknik çözümler için değişikliklerin etkilerinin değerlendirilmesi ✓ Anahtar paydaşlar için değişiklik durumlarının izlenmesi ve raporlanması ✓ Eksik talep özelliklerinden kaynaklanan hataların minimize edilmesi	almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay ilgi verilememektedir.> ❖ Maliyet tasarrufuna yardımcı olmak ✓ <Bu kısımda Halkbank Değişiklik yönetimi süreci amacı yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay ilgi verilememktedir.>
Değerlendirme Sonucu	
COBIT' de yer alan sürece spesifik amaçlar yerine Halkbank Değişiklik Yönetimi süreci kapsamında belirlenen amaçlar BT ve İş tarafı için daha genel amaçlardır. Ancak genel olarak ifade edilen bu amaçlar COBIT amaçlarını kapsamaktadır.	

Değişiklik Yönetimi Süreci Kontrolleri	
COBIT Kontrolleri ve Amaçları	**Halkbank Mevcut Durum**
❖ Değişiklik Standartları ve Prosedürleri ✓ Yazılımlar, prosedürler, süreçler, sistemler ve sistem parametreleri ile temel platformlarda ki tüm değişiklik taleplerinin standart bir yapı ile yönetilmesi için genel değişiklik yönetimi prosedürlerinin düzenlenmesi.	❖ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
❖ Etki Değerlendirme, Önceliklendirme ve Yetkilendirme ✓ Tüm değişiklik talepleri, operasyonel sistem ve fonksiyonlarına olan etkisini	❖ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>

belirlemek için oluşturulmuş bir yapı ile değerlendirilmeli. Böylelikle değişikliklerin kategorisi, önceliği ve yetkilendirilmesinden emin olunur.	
❖ Acil Değişiklikler ✓ Acil değişikliklerin değişiklik sürecini takip etmemesini sağlamak için tanımlama, uygulama, test, dokümantasyon, değerlendirme ve yetkilendirme içeren bir süreç oluşturulması.	❖ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
❖ Değişiklik Durum İzleme ve Raporlama ✓ Red edilmiş değişiklikler, onaylanmış ve uygulamada olan değişikliklerin durum iletişimleri ve tamamlanmış değişikliklerin dokümantasyonu için bir izleme ve raporlama sisteminin oluşturulması. Onaylanmış değişikliklerin planlandığı gibi uygulandığından emin olmak.	❖ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
❖ Değişiklik Kapatma ve Dokümantasyon ✓ Değişiklikler uygulandığında, buna göre ilgili sistemler, kullanıcı dokümanları ve prosedürlerin güncellenmesi.	❖ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
Değerlendirme Sonucu	
COBIT' de yer alan kontrol amaçlarını yerine getirmek için gerekli kontrollerin	

Halkbank Değişiklik Yönetimi süreci içerisinde tanımlanmış olduğu görülmektedir.

Değişiklik Yönetimi Süreci Aktiviteleri	
COBIT Aktiviteleri	**Halkbank Mevcut Durum**
❖ Değişiklik taleplerinin kaydı, değerlendirilmesi ve önceliklendirilmesi için sürekli bir sürecin geliştirilmesi ve uygulanması.	❖ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
❖ Değişikliklerin iş ihtiyaçlarına göre önceliklendirilmesi ve etkilerinin değerlendirilmesi.	❖ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
❖ Tüm acil ve kritik değişikliklerin onaylanmış süreci takip etmesinin sağlanması.	❖ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
❖ Değişikliklerin yetkilendirilmesi	❖ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
❖ Değişiklikler konusunda ilgili bilgilerin	❖ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>

yönetilmesi ve iletilmesi	
Değerlendirme Sonucu	
COBIT' de yer alan kontrol aktivitelerin Halkbank Değişiklik Yönetimi süreci içerisinde tanımlanmış ve mevcutta tanımlandığı gibi yürümekte olduğu görülmektedir.	

Değişiklik Yönetimi Süreci Metrikleri	
COBIT Metrikleri	**Halkbank Mevcut Metrikleri**
❖ BT Metrikleri ✓ Hatalı spesifikasyonlardan veya eksik etki değerlendirmesinden kaynaklanan hizmet kesilmesi veya veri hatası sayısı ❖ Süreç Metrikleri ✓ Eksik değişiklik spesifikasyonlarından kaynaklanan yeniden yapılan uygulama toplamı ✓ Değişikliklerin yapılması için gerekli efor ve zamanın azaltılması ✓ Acil değişiklik yüzdesi ✓ Eksik değişiklik spesifikasyonlar dolayısıyla başarısız olan değişiklikler yüzdesi ✓ Formal olmayan izleme, raporlama veya yetkilendirme gerçekleştirilen değişikliklerin sayısı ✓ Bekleyen değişiklik talepleri sayısı	❖ Başlangıç ve Kayıt ✓ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.> ❖ Ön Değerlendirme ve Yetkilendirme ✓ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.> ❖ Planlama/Onaylama ✓ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>

	❖ Gerçekleştirme ✓ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.> ❖ Tamamlama ve Kapatma ✓ <Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
Değerlendirme Sonucu	
COBIT' de yer alan metriklerin Halkbank Değişiklik Yönetimi süreci içerisinde tanımlanmış olduğu görülmektedir.	

DEĞİŞİKLİK YÖNETİMİ SÜRECİ GÖZDEN GEÇİRME SONUÇ RAPORU	
SÜREÇ SAHİBİ	Süreç Sahibi (Gizlilik çerçevesinde isimler paylaşılmamıştır)
KALİTE EKİBİ	Kalite Ekibi (Gizlilik çerçevesinde isimler paylaşılmamıştır)
GÖZDEN GEÇİRME AMACI/ KAPSAMI	ITSM projesi kapsamında hayata geçen Değişiklik Yönetimi sürecinin amaçlarının, kontrollerinin, aktivitelerinin ve metriklerinin COBIT standartlarına uygunluğunun kontrol edilmesi ve değerlendirilmesi. Değerlendirme neticesinde varsa güncellemelerin ve eksikliklerin ve bunların giderilmesi için yapılması gerekenlerin belirlenmesi.
SÜREÇ GÖZDEN GEÇİRME KODU	**2010_02_GG_004**
ÖNCEKİ GÖZDEN GEÇİRME KODU/TARİHİ	**2009_06_GG_002**

BAŞLANGIÇ TARİHİ	**02. 02. 2010**	**BİTİŞ TARİHİ (*PLANLANAN*)**	**22. 02. 2010**	**BİTİŞ TARİHİ (*GERÇEKLEŞEN*)**	**04.02.2010**

GÖZDEN GEÇİRME SONUCU
Halkbank Değişiklik Yönetimi süreci kapsamında tanımlanan amaçların, kontrollerin, aktivitelerin ve metriklerin COBIT Değişiklik Yönetimi süreci kapsamında belirtilen amaçlar, kontroller, aktiviteler ve metrikler ile karşılaştırılması sonucu sürecin COBIT'e uygun olduğu görülmüştür.

HAZIRLAYAN:	**Kalite Yönetimi Ekibi**	**ONAYLAYAN:**	**Onaylayan Yetkili**

No.	SÜREÇ GÖZDEN GEÇİRME ETKİNLİĞİ KAPSAMINDA YAPILAN ÇALIŞMALAR
1.	COBIT kaynağından Değişiklik Yönetimi sürecinin amaçları, kontrolleri, aktiviteleri ve metrikleri çıkarılmıştır.
2.	Halkbank Değişiklik Yönetimi süreci kapsamında hazırlanan tüm dokümanlar süreç ekibinden temin edilerek incelenmiştir.
3.	Halkbank Değişiklik Yönetimi süreci kapsamında tanımlanan amaçlar, kontroller, aktiviteler ve metrikler COBIT Değişiklik Yönetimi süreci kapsamında belirtilen amaçlar, kontroller, aktiviteler ve metrikler ile karşılaştırılmıştır.
4.	Halkbank Değişiklik Yönetimi süreci kapsamında tanımlanan amaçlar, kontroller, aktiviteler ve metrikler COBIT Değişiklik Yönetimi süreci kapsamında belirtilen amaçlar, kontroller, aktiviteler ve metrikler ile karşılaştırmaları Değişiklik Yönetimi Süreci Gözden Geçirme Planında dokümante edilmiştir.
5.	Değişiklik Yönetimi Süreci Gözden Geçirme Planı, Değişiklik Yönetimi Süreci ekibi ile paylaşılarak onaylarına sunulmuştur.
6.	Değişiklik Yönetimi Süreci Gözden Geçirme Planı doğrultusunda Değişiklik Yönetimi Süreç Gözden Geçirme Sonuç Raporu hazırlanmıştır.

8.2.2 Olay Yönetimi Süreci

Olay Yönetimi süreci Halkbankası'nda aşağıdaki gibi tanımlanmıştır.

"Olay,

Sağlanan bir hizmette meydana gelen, hizmette kesintiye yol açan veya hizmet kalitesinde azalmaya neden olan, standart operasyonun bir parçası olmayan her durum 'Olay' olarak tanımlanır."

"Olay Yönetimi,

İş ortamında en az olumsuz etki oluşturmak üzere, normal hizmet operasyonunu mümkün olduğunca hızlı bir şekilde eski haline getirmek, böylece erişilebilirlik ve hizmet seviyesinin en iyi düzeyde korunmasını garantilemek için yapılan çalışmaların tümüdür."

8.2.2.1 Olay Yönetimi Süreci Gözden Geçirme Planı Ve Raporu

OLAY YÖNETİMİ SÜRECİ GÖZDEN GEÇİRME PLANI	
SÜREÇ SAHİBİ	Olay Yönetimi Süreç Sahibi
KALİTE EKİBİ	Kalite Ekibi
GÖZDEN GEÇİRME AMACI/KAPSAMI	ITSM projesi kapsamında hayata geçen Olay Yönetimi sürecinin ITIL ve COBIT standartlarına uygun işlerliğinin kontrol edilmesi ve değerlendirilmesi. Değerlendirme neticesinde varsa güncellemelerin ve eksikliklerin ve bunların giderilmesi için yapılması gerekenlerin belirlenmesi.
GÖZDEN GEÇİRME KRİTERLERİ	Gözden geçirme kriterimiz süreç için hazırlanmış olan prosedürlerdir. Bu prosedürler ITIL ve COBIT standartlarına uygun mu? Süreç tanımlanmış prosedürler doğrultusunda işliyor mu? Gibi sorulara bu gözden geçirme ile cevap aranmaktadır.
SÜREÇ GÖZDEN GEÇİRME KODU	**2010_05_GG_005**
ÖNCEKİ GÖZDEN GEÇİRME KODU/TARİHİ	-

BAŞLANGIÇ TARİHİ	**18.05.2010**	**BİTİŞ TARİHİ (*PLANLANAN*)**	**31. 05. 2010**	**BİTİŞ TARİHİ *(GERÇEKLEŞEN)***	**26.05.2010**

KALİTE EKİBİ LİDERİ	**SÜREÇ SAHİBİ**
Ekip Lideri	Olay Yönetimi Süreç Sahibi

İNCELENEN KONULAR	İNCELEME SONUCU
1. Süreç prosedürleri tanımlanmış mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
2. Süreç prosedürleri, BSTH prosedür şablonuna uygun olarak hazırlanmış mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
3. Prosedürler güncel işleyişe uygun mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
4. Olay yönetimi sürecinin amaç ve hedefleri tanımlanmış mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
5. Olay yönetimi sürecinin kapsamı tanımlanmış mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
6. Olay yönetiminin politikaları, ilkeleri ve ana kavramları tanımlanmış mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
7. Olay yönetimi süreçlerinin modelleri ve iş akışları tanımlanmış mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
8. Süreç işleyişi tanımlanan modeller ve iş akışları doğrultusunda yürütülüyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
9. Organizasyon tanımlı mı? Nerede tanımlı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
10. Roller ve sorumluluklar tanımlı mı? Nerede tanımlı? Bu tanımlara	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>

İNCELENEN KONULAR	İNCELEME SONUCU
nasıl ulaşılmaktadır?	
11. Roller ve sorumluklar tanımlandığı şekilde yerine getiriliyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
12. Girdiler, çıktılar ve süreçler arası arayüzler tanımlanmış mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
13. Sürecin diğer süreçler ile bulunduğu bilgi alış verişleri tanımlanmış mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
14. Sürecin diğer süreçler ile bulunduğu bilgi alış verişleri tanımlandığı gibi yapılıyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
15. Süreçten iyi yararlanabilmek için bir tool kullanılıyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
16. Süreç ile ortak, düzenli gözden geçirme aktiviteleri var mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
17. KPI' lar ve/veya metrikler tanımlanmış mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
18. KPI' lar ve/veya metrikler ölçülüyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
19. Raporlama yapılıyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
20. Süreç ile ilgili kayıtlar hangi ortamda tutuluyor?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
21. Süreç ile ilgili kayıtlara nasıl ulaşılıyor? Yetkilendirme nasıl yapılıyor?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
22. Süreç işletilirken bir problem	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla

İNCELENEN KONULAR	İNCELEME SONUCU
olduğunda bu problem nasıl giderilmektedir? İlgili kayıtlar nasıl tutulmaktadır? Güncelleme yapılıyor mu?	detay bilgi verilememektedir.>
23. BT çalışanları arasında bu sürecin anlaşılırlık oranı yüksek mi?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
24. Olayların oluştukları zamanlar kayıt altında tutuluyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
25. Olaylara bir sınıflandırma dahilin de kod veriliyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
26. Son kullanıcılarda oluşan olay sayısını azaltmanın genel anlamda verimliliği arttıracağı yönünde bir düşünce var mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
27. Olaylarının kayıt altına alınmasını sağlayan araçlar ve tüm olay azaltma faaliyetleri için ayrılmış bir bütçe var mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
28. Olaylar kapatıldığı zaman kök nedeni belirlenip bu kök nedene özel bir kod veriliyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
29. Olay çözümüne başlamadan önce bu olayın daha önce olup olmadığına bakılıyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
30. Bu alandaki çalışanları eğitmek için gerekli zaman ve bütçe bulunuyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
31. Olay çözümlerinin memnuniyet	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla

İNCELENEN KONULAR	İNCELEME SONUCU
derecesini belirlemeye yarayan prosedürler var mı?	detay bilgi verilememektedir.>
32. Hangi olayların hangi destek seviyesinde çözüldüğüne ait raporlar hazırlanıp üst yönetimle paylaşılıyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
33. Bu süreçteki proseslerin performanslarını gösteren önemli performans göstergeleri var mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
34. Tüm olaylar kaydediliyor mu veya bu olayların kaydedilmeden geçilebilmesi mümkün mü?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
35. Olay yönetimi sürecinden problem yönetimi sürecine kaliteli bilgi akışı sağlanıyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
36. Olaylar kayıt altına alınırken farklı şekilde değerlendirilecek yüksek öncelikli bir kullanıcı listesi var mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
37. Yüksek etkili olaylarla ilgilenilirken kullanılacak bir prosedür var mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
38. Her olay benzersiz bir numara ile kayıt altına alınıyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
39. Organizasyonunuzda bir yardım masası bulunuyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
40. Yeni çalışanlar yardım masasına nasıl ulaşacakları ve hangi	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>

İNCELENEN KONULAR	İNCELEME SONUCU
konularda yardım alacakarı konusunda bilgilendiriyorlar mı?	
41. Yardım masası tüm BT problemleri için bilinen iletişim noktası mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
42. Yardım Masası ile yapılan telefon görüşmeleri kayıt altına alınıyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
43. Yardım Masası beklenen hizmet kesintileri konusunda son kullanıcıları uyarıyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
44. Organizasyon genel olarak yardım masasını yararlı bir yatırım olarak görüyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
45. Alınan çağrılara ve bu çağrıların çeşitlerine yönelik kolayca alınabilecek raporlar mevcut mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
46. Yardım masası proaktif olarak kullanıcılara çağrılarının durumları hakkında belirli zamanlar geçildikten sonra bildirimde bulunuyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
47. Bir kullanıcı memnuniyeti belirleme araştırması yapılıyor mu? Bu otomatik olarak her sorundan sonra olabilir, çeyrek veya yıllık araştırmalar olabilir.	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
48. Yardım masası çalışanları en yoğun zamanlarda değişmeli	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>

İNCELENEN KONULAR	İNCELEME SONUCU
çalışıyorlar mı?	
49. Yardım masası çalışanları otomasyon araçların kullanımları, telefonda hitap teknikleri ve genel müşteri destek yetenekleri konusunda yeterli eğitim alıyorlar mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
50. İlk olarak kullanıcı yardım masası ile görüştükten sonra çözümlenemeyen çağrılar için bir atama süreci mevcut mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
51. Yardım Masası performansının temel performansının gösterildiği düzenli bir yardım masası gözden geçirmesi var mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
52. Yardım Masası otomasyonları Yardım Masası çalışanlarının aktivitelerinin seviyelerine uygun olarak seçilmiş midir?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
53. İşyerinizde yardım masasında çalışmak çok gereksinimi olan bir iş mi, sorun çözmede ve insanları yönetmede uzman yetenekler gerektiriyor mu?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>
54. Yardım masası çalışanları trend belirleme çalışmaları yapıyorlar mı ve müşteri memnuniyeti raporları oluşturuyorlar mı?	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>

OLAY YÖNETİMİ SÜREÇ GÖZDEN GEÇİRME SONUÇ RAPORU	
SÜREÇ SAHİBİ	Olay Yönetimi Süreç Sahibi
KALİTE EKİBİ	Kalite Ekibi
GÖZDEN GEÇİRME AMACI/ KAPSAMI	ITSM projesi kapsamında hayata geçen Olay Yönetimi sürecinin ITIL ve COBIT standartlarına uygun işlerliğinin kontrol edilmesi ve değerlendirilmesi. Değerlendirme neticesinde varsa güncellemelerin ve eksikliklerin ve bunların giderilmesi için yapılması gerekenlerin belirlenmesi.
SÜREÇ GÖZDEN GEÇİRME KODU	**2010_05_GG_005**
ÖNCEKİ GÖZDEN GEÇİRME KODU/ TARİHİ	-

BAŞLANGIÇ TARİHİ	**18.05.2010**	**BİTİŞ TARİHİ (*PLANLANAN*)**	**31. 05. 2010**	**BİTİŞ TARİHİ (*GERÇEKLEŞEN*)**	**26.05.2010**

GÖZDEN GEÇİRME SONUCU

Süreç için hazırlanması gereken tüm dokümanlar hazırlanmış ve Süreç Modeli'nde yayınlanmıştır. Hazırlanan dokümanların ITIL ve COBIT standartlarına uygun olduğu tespit edilmiştir.

<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>

Sürecin gözden geçirilmesi sonucunda "SÜREÇ GÖZDEN GEÇİRME ETKİNLİĞİ KAPSAMINDA YAPILAN ÇALIŞMALAR" ve "SÜREÇ GÖZDEN GEÇİRME SONUCUNDA ORTAYA ÇIKAN BULGULAR" adı altında aşağıda yer alan iki tablo oluşturulmuştur.

GÖZDEN GEÇİRME SONUCU			
Süreç sahibi ile yapılan değerlendirmede, eksikliklerin giderilmesi için çalışmaların planlanmış olduğu bulgular için planlanan çalışmalar aşağıdaki tabloda düzeltici faaliyetler olarak belirtilmiştir. Planlanan çalışma olmayan bulgu/bulgular için süreç ekibi tarafından ilgili Düzeltici Faaliyetler, İyileştirme Planları oluşturularak uygulanmalıdır.			
HAZIRLAYAN:	**Hazırlayan**	**ONAYLAYAN:**	**Onaylayan Yetkili**

No.	SÜREÇ GÖZDEN GEÇİRME ETKİNLİĞİ KAPSAMINDA YAPILAN ÇALIŞMALAR
1.	ITIL ve COBIT kaynakları incelenerek, sürecin kurgu ve işleyiş bakımından gereklilikleri tespit edilmiştir.
2.	Sürecin gerekliliklerinin tanımlanıp, tanımlandığı gibi uygulanıp uygulanmadığının kontrolünü sağlamak için soru seti hazırlanmış ve Olay Yönetimi Süreç Gözden Geçirme Planı oluşturulmuştur.
3.	Süreç ekibi ile toplantı düzenlenerek hazırlanan sorular yöneltilmiş ve cevapları alınmıştır.
4.	Verilen cevaplar doğrultusunda Olay Yönetimi Süreç Gözden Geçirme Planı güncellenmiş, süreç yöneticisi ve süreç ekibi ile paylaşılmıştır.
5.	Süreç ekibinden gelen geri bildirimler doğrultusunda Olay Yönetimi Süreç Gözden Geçirme Planı güncellenmiştir.
6.	Süreç Gözden Geçirme Planı değerlendirilerek süreçte ortaya çıkan bulgular tespit edilmiştir.
7.	Olay Yönetimi Süreç Gözden Geçirme Sonuç Raporu oluşturulmuştur.

SÜREÇ GÖZDEN GEÇİRME SONUCUNDA ORTAYA ÇIKAN BULGULAR			
NO	**BULGU**	**DÜZELTİCİ FAALİYET**	**İYİLEŞTİRME PLANI (Sorumlu / Tarih)**
1.	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	Olay Yönetimi Süreç Sahibi / Sürecin organizasyonel dönüşüm oranı istenilen seviyeye ulaşıncaya kadar.
2.	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	Olay Yönetimi Süreç Sahibi / 31.09.2010
3.	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	Olay Yönetimi Süreç Sahibi / İstenilen oranda doğru ve güvenilir olay kayıt verisine ulaşıncaya kadar.

8.3 ITSM Programı Genel Değerlendirme Sonucu

YÖN@ PROGRAMI SÜREÇ DEĞERLENDİRMELERİ SONUÇ RAPORU	
ÇALIŞMANIN AMACI	Yön@ Programı kapsamında hayata geçen ve geçmesi planlanan süreçlerin ITIL ve COBIT standartlarına uygun tasarlanıp tasarlanmadığının ve işlerliğinin kontrol edilmesi ve değerlendirilmesi. Değerlendirme neticesinde varsa güncellemelerin ve eksikliklerin tespit edilerek, bunların giderilmesi için yapılması gerekenlerin belirlenmesi.
DEĞERLENDİRİLEN SÜREÇLER	Değişiklik Yönetimi Hizmet Yönetimi Konfigürasyon Yönetimi Varlık Yönetimi Kullanılabilirlik Yönetimi Problem Yönetimi Olay Yönetimi Kapasite ve Performans Yönetimi
ÇALIŞMA EKİBİ	(Gizlilik çerçevesinde isimler paylaşılmamıştır)
SÜREÇ DEĞERLENDİRMELERİ SONUCU	

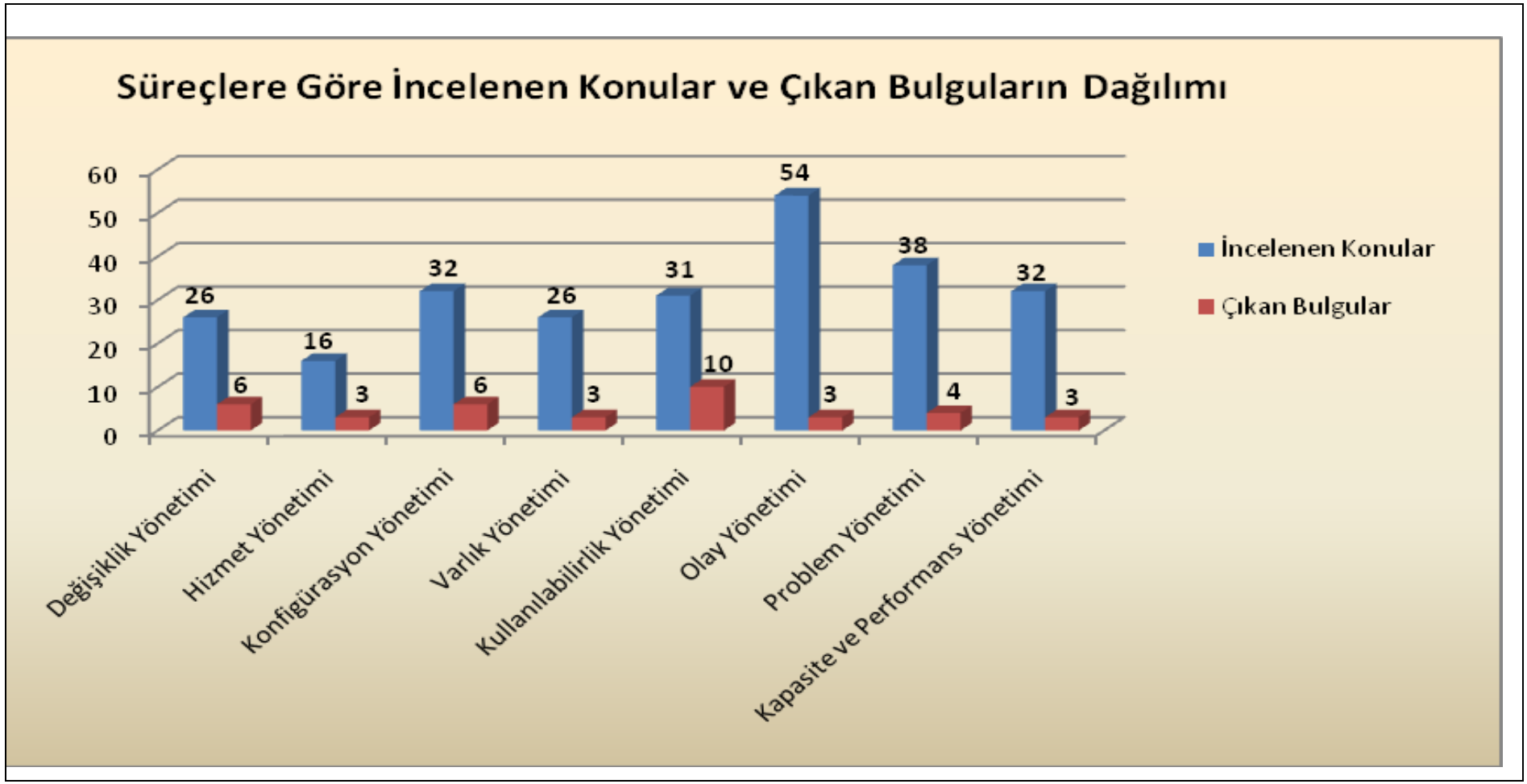
Yön@ Programı kapsamında gerçekleştirilen süreç gözden geçirme çalışmalarında hayata geçen veya henüz hayata geçmemiş olan tüm süreçlerin ITIL ve COBIT standartlarına göre doğru tasarlanıp tasarlanmadığı ve hayata geçen süreçlerin ise tasarlandığı şekilde uygulanıp uygulanmadığı kontrol edilmiştir.

<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>

Yapılan çalışmalar süreçlerin dışarıdan bir gözle değerlendirilmesini, COBIT ve ITIL uyumluluğu baz alınarak süreç aktivitelerindeki eksik ve/veya zayıf noktaların ortaya çıkmasını sağlamıştır. Bu şekilde henüz hayata geçmemiş süreçlerin daha tasarım aşamasında iken eksiklikleri belirlenmiş ve tamamlanması için planlamalar yapılması sağlanmışken, hayata geçen süreçlerin ise COBIT ve ITIL uyumlu olarak yürütülüp yürütülmediği ve işlerliğinin uygunluğu değerlendirilmiş, tespit edilen eksikliklerin giderilmesi için gerekli çalışmalar planlanmıştır.

Yön@ Programı süreç gözden geçirme çalışmaları aşağıdaki grafik ile özetlenmiştir.

Aşağıdaki grafik; süreç gözden geçirme çalışmaları kapsamında süreçler bazında incelenen konuların ve bu konular kapsamında ortaya çıkan bulguların sayılarını göstermektedir.



Şekil 8.2 Örnek bulgu grafiği[1]

[1] Burada yer alan sayılar Halkbank Bilgi Güvenliği Politikası uyarınca değiştirilmiştir. Yukarıda yer alan sayılar gerçek değerleri yansıtmamaktadır.

ÇALIŞMALAR SONUCU SÜREÇLERDE ORTAYA ÇIKAN ÖNEMLİ BULGULAR/EKSİKLİKLER			
SÜREÇ	**BULGU**	**DÜZELTİCİ FAALİYET**	**İYİLEŞTİRME PLANI (Sorumlu / Tarih)**
Değişiklik Yönetimi	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	Değişiklik Yönetimi Süreç Sahibi / Üst yönetim kararı sonrası belli olacaktır.
Hizmet Yönetimi	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	Hizmet Yönetimi Süreç Sahibi / Asset Management, CMDB Discovery ve SIM süreçleri tamamlandıktan sonra gerçekleştirilebilecektir.
Konfigürasyon Yönetimi	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	Konfigürasyon Yönetimi Ekibi / 31.12.2010
Varlık Yönetimi	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	Varlık Yönetimi Ekibi / Net bir tarih bildirilmemiştir. Süreç entegrasyon çalışmalarının (1. faz) tamamlanmasının ardından geçilecek 2. fazda konu ele alınacaktır.

Kullanılabilirlik Yönetimi	< Bu kısımda bankaya özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için daha fazla detay verilememektedir.>	< Bu kısımda bankaya özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için daha fazla detay verilememektedir.>	Kullanılabilirlik Yönetimi Süreç Sahibi / SIM kurulumu yapıldıktan sonra konu ele alınacaktır.
Olay Yönetimi	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	Olay Yönetimi Süreç Sahibi / İstenilen oranda doğru ve güvenilir olay kayıt verisine ulaşıncaya kadar çalışma devam edecektir.
Problem Yönetimi	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	Problem Yönetimi Süreç Sahibi / Sürecin organizasyonel dönüşüm oranı istenilen seviyeye ulaşıncaya kadar çalışma devam edecektir.
Kapasite ve Performans Yönetimi	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	<Bu kısımda Halkbanka özel bilgiler yer almaktadır. Ancak Kuruma özel bilgi olduğu için burada daha fazla detay bilgi verilememektedir.>	Kapasite ve Performans Yönetimi Ekibi / Üst yönetim kararı sonrası belli olacaktır.

8.4 Uygulama Sonucu

Uygulama kapsamında öncelikle Halkbank'da kullanılmakta olan ITSM (Information Technology Service Management – Bilgi Teknolojileri Hizmet Yönetimi) süreçlerinden Değişiklik Yönetimi ve Olay Yönetimi süreçleri için; Kalite ekibi tarafından yapılan gözden geçirme etkinliklerinin bir kısmına çalışmada yer verilmiştir. Gözden geçirme faaliyetleri sonrası ortaya çıkan bulgular kuruma özel bilgiler çerçevesinde tezde paylaşılamamıştır.

Son olarak Halkbank ITSM projesi olan Yön@ kapsamındaki tüm süreçler için gözden geçirme raporunun bir örneğine çalışmada yer verilmiştir ve yapılan çıkarımları temsilen bulgu dağılımları gösterilmiştir. Kalite ekibi süreçler bazında bu dağılımları yorumlamakta ve gerekli aksiyonların alınması için önceliklendirmeye tabi tutmaktadır.

9. SONUÇLAR ve ÖNERİLER

Kurumların güvenilir olması, müşterilerine ve devlete karşı olan sorumluluklarını eksiksiz yerine getirebilmesi için hizmet kalitesini arttırmaya yönelik stratejiler geliştirmesi kaçınılmazdır. Ancak günümüz rekabet ortamında bu stratejiler zorunlu olsa da zaman zaman ortaya çıkan skandallar kurumların iç denetimlerinin yanında bağımsız kuruluşlarca denetlenmesini de zorunlu kılmıştır. Denetime tabi olan kuruluşların başında da finansal kuruluşlar olan bankalar gelmektedir.

Çalışmada Denetim Kavramı ile başlayan anlatım kapsamında BT denetimi, denetimin sınıflandırılması, denetim süreçleri, denetim alanları detaylandırılmıştır. Sonraki bölümde ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi) ile ilgili genel bilgiler verilmiş ve ardından BDDK tarafından yayınlanan tebliğler ile bankalar için zorunlu hale gelen BT Denetim yöntemi olan COBIT e geniş bir şekilde yer verilmiştir.

COBIT, ISACA (Bilgi Sistemleri Denetim Kontrol Birliği)' nın bir alt kuruluşu olan ITGI (Bilgi Teknolojileri Yönetişim Enstitüsü) tarafından yaratılmış bilgi sistemleri Yönetimi için bir çerçevedir. COBIT BT yöneticileri, denetçiler ve BT kullanıcıları için bir kurumda bilgi teknolojileri kullanımının ve uygun BT yönetişiminin geliştirilmesi ve kontrol edilmesinin faydalarını artırmak için genel olarak kabul edilmiş bilgi teknolojileri kontrol hedef setleri sunmaktadır. Çalışma kapsamında bu kontrol hedefleri tek tek anlatılmıştır.

Bir sonraki bölümde COBIT ile uluslar arası diğer denetim ve kontrol yöntemleri karşılaştırılmıştır.

Çalışmada COBIT in son versiyonu olan 4.1 detayları ile anlatılmıştır. Yakın zamanda yayınlanacak yeni versiyon ve sonrasında denetimlerden edinilen bilgi ve istatistiklere göre gerekli konularda güncellemelere gidilmesi ve gerçek hayattaki tecrübelerin yansıtılması önemli olacaktır.

Son olarak Türkiye Halkbankası ITSM projesi olan Yön@ kapsamındaki Bilgi Teknolojileri Yönetim süreçlerinden iki tanesi için COBIT ve ITIL uyumluluğu ile çalışan Kalite ekibinin gerçekleştirdiği iç denetim tez uygulaması olarak sunulmuştur. Halkbankasında olduğu gibi büyük küçük her kuruluş bu konulara önem vermeli ve uygulamalarının güncelliğini yakından takip etmelidir.

KAYNAKLAR

Arman, T., (1997), Risk Analizine Giriş, Alfa Kitabevi, İstanbul.

Artinyan, E.N., (2008), "COBIT Çerçevesi", Deloitte Kurumsal Risk Hizmetleri, 1-6.

Atan, M., (2002), Risk Yönetimi Ve Türk Bankacılık Sektöründe Bir Uygulama, Doktora Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Baraçlı, H., (2001), "Kriz ve Teknoloji Yönetimi", İstanbul: Yıldız Teknik Üniversitesi 3Gen Dergisi

Başarır, M., (2006), Bankalarda Teknoloji Riski Ve Yönetimi, Yüksek Lisans Tezi, Marmara Üniversitesi Bankacılık ve Sigortacılık Enstitüsü, İstanbul.

BDDK, (2006), "Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik", Ankara.

Birengel, S., (2006), "Başarılı Bilgi İşlem Merkezi Modeli-5. Çalışma Grubu" Türkiye Bilişim Derneği Kamu Bilgi İşlem Yöneticileri Birliği-Kamu Bilişim Platformu VIII, İstanbul

Fikirkoca, M., (2003), Bütünsel Risk Yönetimi, Kalder Yayınevi, Ankara

Güvener, E., (2000), "Teknoloji Yönetimi Ve Teknoloji Kontrolü" Active Bankacılık ve Finans Dergisi, Şubat-Mart (11)

Heschl, J., (2006), COBIT Mapping: Overvıew Of Internatıonal IT Guıdance 2nd Edition, Illinois, USA

Johnson, B., (2007), Hizmet Yönetimi Süreç Haritaları, Paloma Yayınevi, İstanbul

Mandacı, P.E., (2003), "Türk Bankacılık Sektörünün Taşıdığı Riskler ve Finansal Kriz Aşmada Kullanılan Risk Ölçüm Teknikleri", İzmir: 9 Eylül Üniversitesi SBE Dergisi, 5(1): 67-84.

Pekel, A., (2008), "Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (COBIT)" Türkiye Bilişim Derneği Kamu Bilgi İşlem Yöneticileri Birliği-Kamu Bilişim Platformu X, İstanbul

Uzunay, V., (2007), "CobiT (Control Objectives for Information and related Technology)", İç Kontrol Merkezi Uyumlaştırma Dairesi, Ankara

Yazıcı, A., (2006), "Bilişim Teknolojilerinde Risk Yönetimi-2. Çalışma Grubu ", Türkiye Bilişim Derneği Kamu Bilgi İşlem Yöneticileri Birliği-Kamu Bilişim Platformu VIII, İstanbul

İNTERNET KAYNAKLARI

[1] http://www.isaca.org

[2] www.itsmf.com

[3] www.itgi.org

[4] www.pmi.org

[5] http://www.denetimnet.net/

[6] http://www.bddk.org.tr

[7] http://www.iso.org

[8] www.itil-officialsite.comhttp://en.wikipedia.org/wiki/ITIL

[9] http://en.wikipedia.org/wiki/IT_Governance

[10] http://en.wikipedia.org/wiki/Risk_management

[11] http://en.wikipedia.org/wiki/IT_Service_Management

ÖZGEÇMİŞ

Doğum Tarihi:		20.11.1985
Doğum Yeri:		Safranbolu
Lise:	2001–2004	Safranbolu Anadolu Lisesi
Lisans:	2004–2008	Yıldız Teknik Üniversitesi Makine Fak. Endüstri Mühendisliği
Yüksek Lisans:	2008-	Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Endüstri Mühendisliği Ana Bilim Dalı, Sistem Mühendisliği Programı

Çalıştığı Kurumlar:

2008-2009	Denizbank Bilgi İşlem – Intertech
2009-	Türkiye Halk Bankası Bilgi Teknolojileri