T.C

HALİÇ ÜNİVERSİTESİ

FEN BİLİMLERİ ENSTİTÜSÜ

YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI

ITIL (Information Technology Infrastracture Library) Güvenlik Yönetimi Süreçlerinin Orta/Büyük Şirketlerde Uygulanması

YÜKSEK LİSANS TEZİ

Hazırlayan

BÜLENT NACİ ALPAY

Tez Danışmanı

Prof. Dr. Ali OKATAN

Ocak 2008

İSTANBUL

İÇİNDEKİLER

ÖNSÖZ

Yüksek lisans eğitimimiz boyunca desteklerini esirgemeyen Sayın Prof. Dr. Ali OKATAN, lisans ve yüksek lisans eğitimimi beraber tamamladığım ve her aşamada yardımını aldığım Cem TOPKAYA, tez hazırlama safhasında görüş ve eleştirileri ile yol gösterici olan Sayın Y. Muh. Teoman ALPAY'a ve her alanda olduğu gibi bu dönemde de manen ve madden verdikleri destek ve gösterdikleri anlayış için aileme teşekkürü bir borç bilirim.

KISALTMALAR

IT	Bilişim Teknolojileri
ITIL	IT Infrastructure Library - Bilişim Teknolojileri Altyapı Kütüphanesi
ISO 20000	ISO IT Service Managment System Standard
ISO 27000	ISO Information Security Standard
CCTA	Central Coputer and Telecommunications Agency-Merkezi Bilgisayar ve Telekomünikasyon Ajansı
CI	Configuration Item - Konfigürasyon Bileşeni
SLA	Service Level Agreement - Servis Seviye Anlaşması
OLA	Operational Level Agreements - Operasyonel Seviye Anlaşması
SBYS	Servis Bilgi Yönetim Sistemi
CMBD	Configuration Management DataBase - Konfigurasyon Yönetimi Veritabanı
CMS	Change Management System - Değişim Yönetim Sistemi
SKMS	Service Knowledge Management System - Servis Bilgi Yönetim Sistemi
ITSM	IT Service Management - Bilişim Teknolojileri Servis Yönetimi
SLR	Service Level Requirement - Servis Seviye Anlaşması
BS 7799	British Standards7799 - Bilgi Güvenliği Yönetimi Nizamnamesi
EDP	Electronic Data Processing - Elektronik Veri işlemesi
RFC	Request for Change - Degişim Talebi

ŞEKİL TABLOSU

ÖZET

Bilgi İşlem servislerinin, iş ile çok daha yakından entegre olmaları ile ITIL (Information Technology Infrastructure Library), Bilgi İşlem'in bir iş gibi yönetilmesi için Bilgi İşlem Servis Yönetimine bir iş yönetim yaklaşımı ve disiplini getirmiştir. Servis Yönetimi, müşterilere, servisler formunda değer katmayı hedefleyen bir dizi özelleşmiş organizasyonel becerilerdir. Servis Yönetimi'nin temelinde kaynakları değerli servislere dönüştürmek yatar. ITIL Servis Yönetimi ISO/IEC 20000 üzerine kurulmuştur.

Bilgi Güvenliği, Güvenlik Yönetimi'nin temel bir konusudur. Bilgi Güvenliği'nin birincil hedefi bilginin güvenliğini garanti altına almaktır. Bilgi korunurken aslında korunması gereken bilginin değeridir. ITIL Güvenlik Yönetimi ISO/IEC 27000 üzerine kurulmuştur.

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

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

Bu tezde, ITIL'ın Bilgi İşlem Servis Yönetimi konseptinden yola çıkarak ana konularından biri olan Servis Tasarımı dahilinde Bilgi Güvenliği Yönetimi süreci üzerinde özelleşerek şirketlerde olası uygulama esasları ve yöntemleri hakkında açıklayıcı ve yol gösterici çizgide bir tarz benimsenmiştir. Ayrıca, farklı iş kollarında benzer Bilgi İşlem servislerinin hepsi için "en iyi uygulama" yaratmada göz önüne alınması gereken hususlar tarif edilmiş ve bunların gerçek ortamda hayata geçirilebilmesi için takip edilecek teorik bir yol çizilmiştir.

SUMMARY

As IT services become more closely aligned and integrated with the business, ITIL assists in establishing a business management approach and discipline to IT Service Management, stressing the complementary aspects of running IT like a business. Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services. The core of Service Management is transforming resources into valuable services. ITIL Service Management is based on the ISO/IEC 20000.

A basic concept of Security Management is the information security. The primary goal of information security is to guarantee safety of information. When protecting information it is the value of the information that has to be protected. ITIL Security Management is based on the ISO/IEC 27000.

The ITIL Security Management Process describes the structured fitting of security in the management organization and thus by this process, not only a basic level of security but also the determination of the security requirements defined in the SLA and other external requirements can be achieved.

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

Within this thesis, an illustrative and mentoring way was followed for describing the appliance bases and methods while concentrating on Information Security Management process where exists in Service Design which is one of the five core volumes of ITIL as setting out from the ITIL'S IT Service Management concept. Besides, mandatory steps to be accomplished have been described for all same type IT services in different business departments and generate a virtual path to be followed in the real infrastructure.

1 GİRİŞ

1.1 ITIL

Artan karmaşıklık ve bilgi teknolojisine bağımlılık yüzünden IT “en iyi uygulamalar” konsepti daha da önemli hale gelmiştir. Birçok yönetimsel yapı, bugünkü IT profesyonellerine IT proseslerinde teknolojiyi kullanmada ve yönetiminde yardım etmektedir. Bunlardan biri olan ITIL (Information Technology Infrastructure Library®), servis yönetimi uygulamalarında en yaygın kabul görenidir.

Orijinal olarak, İngiliz Birleşik Krallık Central Computer and Telecommunications Agency (CCTA) tarafından 1990’ların başında yaratılmış olan ITIL, en iyi iş yönetimi sonuçlarını almak üzere, karışık bir IT yapılanmasında nasıl organize olmayı ve yönetmeyi içeren sektör liderlerinden toplanmış görüşleri temsil eden bir dizi kitabın kütüphanesidir.

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

“En iyi uygulamalar” ismi itibariyle bir miktar hatalı bir tanımlama olabilmektedir, çünkü “en iyi uygulama” denilen zamanla değişmektedir. COBIT (Control Objectives for Information Technology) ve enhanced Telecom Operations Map (eTOM) gibi diğer yapılarda, güvenilir bir rehberlik sağlarlar. Bazı durumlarda ITIL dışındaki bazı yapılar belirli iş yönetimlerine daha iyi karşılık verebilmektedir. Birçok durumda, tüm uygun model ve yapılar ele alınıp iş yönetim hedeflerine en uygun olanının adapte edilmesiyle çok daha iyi hizmet edilmiş olunur.

2007 yazında, ITIL’ın üçüncü versiyonu çıkartılmıştır. Bu, 10 yazar ve 23 adet ITIL danışmanı endüstri uzmanı tarafından tarif edildiği üzere oluşturulmuş önder uygulamaları yansıtan kayda değer bir ilerlemedir. ITIL’ın üçüncü sürümü,

servis yönetimi hayat döngüsü üzerine yeni bir odaklanma sağlarken kabul görmüş uygulamaların öneminin altını çizmektedir...

ITIL üçüncü versiyonunun ne kadar önemli olduğu, şirketlere göre değişkenlik gösterir. Spesifik iş yönetimi hedefleri ve fırsatları, birincil olarak göz önüne alınmalıdır. Ancak daha sonra, anlık iş yönetimi hedeflerini sağlayacak en iyi yaklaşımı belirlemek üzere ITIL ve benzeri yapılar değerlendirmeye alınmalıdır.

ITIL kütüphanesi, servis yönetimi optimizasyonu ile ilgilenen şirketler için piyasada en fazla dikkate alınan, en iyi bilinen ve en büyük ölçüde uygulanmış yapılar içinde ona gösterilen belirgin saygıdan yararlanır. ITIL, ücretsiz bulunabilen, hiçbir kimse tarafından kontrol edilemeyen ve sahiplenemeyen en iyi uygulamaların açık koleksiyonudur. “Açık Kaynak” değildir fakat geniş kabul görmüş bir uygulamalar bütünüdür.

ITIL, her tür servis yönetimi iyileştirme çalışmasında iyi bir başlangıç noktası olabilecek şekilde hizmet veren değerli bir rehberler setidir. En iyi uygulamalar üzerine bir kütüphane olmasının yanında, birçok iş yönetimi bu ek yardımı gerekli görür. Birçok organizasyon, değerlendirme, planlama, tasarım ve uygulanma safhalarında, iş yönetimi nesne oryantalli yaklaşımlara nereden başlanacağına pratik olarak rehberlik etmesinden faydalanır.

1.2 Güvenlik Yönetimi

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

Hükümetler, askeriye, finansal enstitüler, hastaneler ve özel işletmeler işçileri, müşterileri, ürünleri, araştırmaları ve finansal statüleri hakkında büyük miktarda veri biriktirirler. Bu bilginin büyük bir kısmı artık bilgisayarlarda

toplanmış, biriktirilmiş ve ağ boyunca diğer bilgisayarlarla paylaşılabilir haldedir. Bir işletmenin müşterileri veya finansal değerleri veya yeni bir ürün hakkındaki bilgilerin rakiplerin eline düşmesi halinde, böyle bir güvenlik aşımı, iş kaybına, davalara ve hatta işletmenin batmasına yol açabilir. Gizli kalması gereken bilgiyi korumak bir iş yönetimi gerekliliğidir ve birçok anlamda etik ve yasal zorunluluktur.

Çalışanlar, bilgi işlem kaynaklarının uygun ve uygun olmayan kullanımı arasındaki farklılıkları bilmelidir. Bu her zaman önemli olmuştur ve şimdi de politika bazlı bir vurgu haline gelmektedir. Buna ek olarak, bir güvenlik sorunu olduğunda ne yapmak gerektiğini bilmek her zaman önemlidir fakat yakın zamana kadar çalışanların ve yönetimin bir kriz sırasında elekronik postalarını okumaya, acil toplantılar düzenlemeye ve ne yapılması gerektiğini bulmaya vakti olacağına inanılırdı. Talihsiz bir gerçektir ki günümüzün bilgisayarlaşmış toplumunda, güvenlik tedbirlerini de göz önüne alırsak plan yapmakta başarısız olursanız, başarısız olmayı planlarsınız.

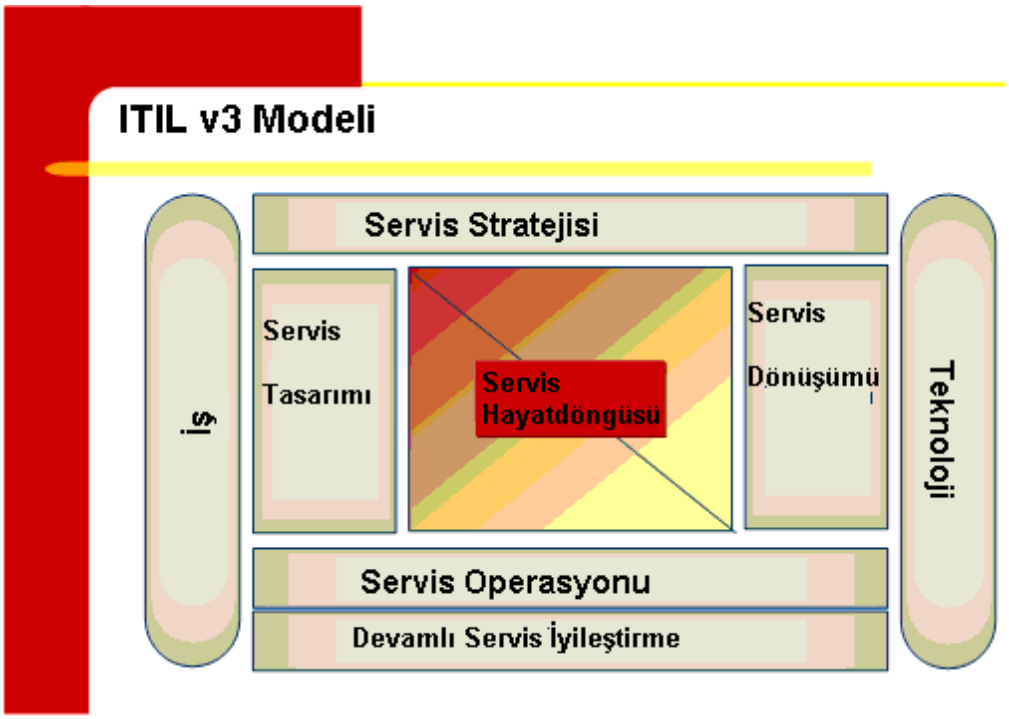
Bilgi güvenliği, son yıllarda büyümekte ve önemli ölçülerde gelişmektedir. Güvenlik, gizlilik ve iş yönetimi devamlılığı işletmeler küçülse bile ihtiyaç duydukları fonlama ve kaynakları elde edebilmektedir. Kariyer olarak bu alanda yer edinmenin birçok noktası bulunmaktadır. Bilgi Sistemleri Denetleme ve Yönetimi, Devamlılık Planlaması bunlara birer örnektir.

2 SERVİS HAYAT DÖNGÜSÜ

ITIL, günümüzde iş odaklı, maliyet etkin IT organizasyonlarını yönetmede fiili standarttır. ITIL yapısı yakın zaman önce süreç odaklı yaklaşımından servis yaşam döngüsü yaklaşımına doğru tekrar tasarlanmıştır. İş stratejisi ile IT' nin uçtan uca entegrasyonunu içeren bu görüş, ITIL'ın son versiyonunun temelindeki beş ana yayınında bulunmaktadır:

- Servis Stratejisi, IT stratejisinin, genel iş amaç ve beklentilerine eşlendiğinden emin olur.
- Servis Tasarımı, yeni veya değişmiş bir takım iş ihtiyaçları ile başlarken, dokümante edilmiş iş ihtiyaçları için bir çözüm geliştirilmesi ile sona erer.
- Servis Dönüşümü, değişim, risk ve kalite güvenceyle alakadar olup servis dizaynını hayata geçirir ve böylece servis operasyonunun, servis ve altyapıyı kontrollü bir tarzda yönetilebilinmesini sağlar.
- Servis Operasyonu: İş ile olağan aktiviteler kapsamında ilgilidir.
- Devamlı Servis İyileştirilmesi: Bütün diğer elementlerin genel bir görünümüne sahiptir, tüm sürecin ve servis provizyonunun iyileştirilmesi için yollar arar.

ITIL'ın yapısı bir servis yaşam döngüsü formatına olgunlaştırılmıştır. ITIL'ın kendisi bir servise dönmüştür ve onun "Servis Portföyü" de aşağıdaki şekil 2.1 de görülebilir:

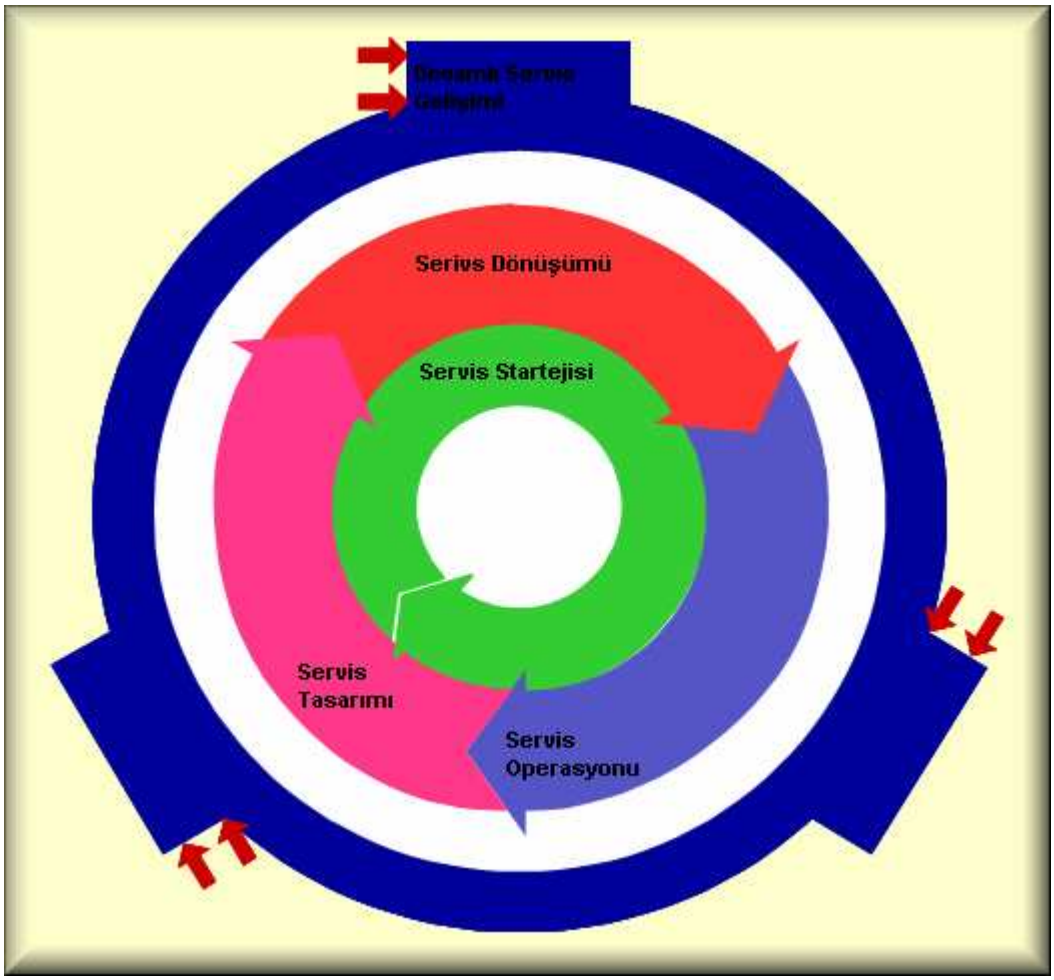


Şekil 0.1 ITIL V3 Modeli (ITSMF, 2007, http://itsmf.org)

Sürecin kalbinde, ITIL Servis Hayat Döngüsü etrafında dönen beş adet temel rehber bulunmaktadır. Hayat Döngüsü, Stratejiden başlayıp Dizayn, Dönüşüm, Operasyon ve Geliştirilmeye kadar mantıki bir akım olarak tasvir edilir fakat yapısının asıl güzelliği tamamen çok yönlü olmasıdır.

ITIL, hayat döngüsünün tüm alanlarında geri bilgilendirme sağlayan bir kapalı devre sistemi kullanır. Bu, bizlerin gerçek bilgi teknolojileri sistem yönetim dünyasına uyumludur. Yani hiçbir şey mutlak lineer değildir. Her ne kadar servis yönetimi döngü akışınının Kalite'nin Deming döngüsü (Planla-Yap-Kontrol Et-Harekete Geç) benzer olduğunu gözlemlesek de gerçek hayatta IT servis yönetimi nadiren tamamıyla lineerdir. Bu nedenle, ITIL mantıki bir akışı cesaretlendirecek şekilde tekrar tasarlanmış ve fakat servis yönetimi için tek başına lineer bir yol ile sınırlandırılmamıştır.

Servis hayat döngüsü, bir merkez-uç tasarımı içinde, uygulamanın kalbinde Strateji ve etrafında dönen bölümler olan Dizayn, Dönüşüm ve Operasyon şeklinde tasvir edilmiştir. Bu döngü, dahili diğer elemanlara nüfusunu yaymaya çalışan Devamlı Servis Gelişimi ile demirlenmiştir.



Şekil 0.2 Servis Hayat Döngüsü (PULTORAK, 2007, http://pultorak.com)

3 UYGULAMA OLARAK SERVİS YÖNETİMİ

Müşterilerine iş süreçlerini desteklemek amacıyla IT servisleri sunan tüm organizasyonlar, kalıtımsal bir yapıya ihtiyaç duyarlar. Yeni yaklaşımların meydana getirilmesine kadar bu yapı, fonksiyonlar ve teknik kabiliyetler üzerine kuruluyordu. Ancak teknolojideki hızlı değişim karşısında bu yaklaşım artık uygun olmamaktadır. Bu yüzden birçok IT organizasyonu alternatifler aramaktadırlar. Bunlar, organizasyonların ihtiyaçlarına tamamen bağlı olarak bir veya birden çok yapıdan oluşabilir. Birçok organizasyon için ITIL, servis sağlama yönetimini ve IT aktivitelerinin uçtan uca yönetilmesinin iyi bir yoludur.

3.1 En İyi ve İyi Uygulama

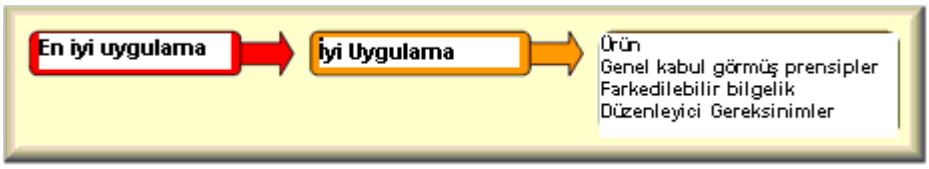
Bir endüstrideki bazı organizasyonlar, en iyi uygulamaları uyguladıkları veya bizzat geliştirdikleri için öne çıkarlar. Zamanla, endüstrideki diğerleri de aynı uygulamayı adapte ederler yada uygulamayıp piyasa dışına çıkarlar. Bir kere “ortak uygulama” yürürlülüğe girdi mi artık endüstri iyi uygulama vaziyetinde çalışır.

3.1.1 En iyi Uygulama

“En İyi Uygulama”, diğer teknik, yöntem, metot veya proseslerden daha efektif bir sonuç elde elden bir tekniğin, metodun, sürecin, aktivitenin, teşvikin veya ödülün mevcut olduğunu beyan eden yönetim fikridir. Buradaki düşünce, uygun süreçlerle, kontrollerle ve testlerle arzulanan sonucun daha az problemli ve daha az beklenmedik komplikasyonları olacağıdır. Bunun yanında en iyi uygulamalar, birçok insan için uzun bir zaman boyunca kendini onlara ispat etmiş olan tekrarlanmış prosedürlere dayanan en etkili ve verimli şekilde verilen bir görevi tamamlamanın yoludur.

3.1.2 Uygulama Gelişimi

Devamlı surette ilerleme için bir arayış bulunmaktadır. Şekil 3.9 da bu aşamada En İyi Uygulamaların İyi Uygulamalara ve onların da ticari ürünlere, genel kabul prensiplerine, algılanabilir bilgeliğe veya düzenleyici gereksinimlere dönüştüğü gösterilmektedir.



Şekil 0.1 Uygulama Evrimleri

3.2 Servis Nedir?

Servis, müşterilere, bir anlamda çok özel maliyet ve riskleri üstlenmeden elde etmek istedikleri sonuçlara ulaşmayı kolaylaştırmaktır.

Servis ile sağlanan kolaylıklar şunlardır:

- Kısıtlamaların etkisini azaltmak ve atanmış görevlerin performansını yükseltmek.
- Tasarlanan sonuçların alınma ihtimalini arttırmayı hedefler.

Servisin Etkileri ise aşağıdaki gibi sıralanabilir:

- Direkt olarak kaynaklar ve ilişkilendirildiği görev ve sınırlamalar üzerine olan etkiler
- Müşteri uygulamaları üzerindeki (örneğin iş uygulaması) etkiler

3.3 Servis Yönetimi Nedir?

Müşterilere, servis kapsamında değer sağlayan bir dizi uzmanlaşmış organizasyonel becerilerdir.

Organizasyonel beceriler ise, bir yaşam döngüsü üzerinden stratejide, tasarımda, dönüşümde, operasyonda ve devamlı geliştirmede özelleşen süreçler ve fonksiyonlar olarak bulunabilirler. Bunun yanında, bir aksiyon için servis organizasyonunun kapasitesini, güvenirliğini ve yeteneğini tasvir eder. Becerilerin şekillenmesi, üstesinden gelinmesi gereken zorluklar ile meydana gelir.

Bir servis organizasyonu, becerileri olmadan olsa olsa müşteriye gerçeğinden daha düşük değer sağlayan bir kaynak gruplaması olabilir. Servis yönetiminin temeli, kaynakları değerli servislere dönüştürmektir.

3.4 Servislerin Değer Teklifleri Nedir?

Servisler, müşteri varlıklarını arttırma ve müşteri organizasyonlarına değer yaratma potansiyeline sahiptir. Servislerin tasarımı, dönüşümü ve operasyonundaki iyileştirmeler müşteri performans potansiyelini yükseltir ve müşteri varlıkları üzerindeki değişim riskini azaltır.

Şekil 0.2 Servis Varlıkları

Şekil 3.2 de servislerin, servis varlıklarından nasıl meydana getirildiğini gösterilmektedir.

Servis oluşumunun evrelerinin etkileşimi aşağıda tanımlanmıştır:

- Servis potansiyeli müşterinin performans potansiyeline dönüştürülür.
- Sıklıkla performans potansiyelini arttırmak, ölçek veya kapsam anlamında servis için ek talepleri harekete geçirmektedir.
- Artan talep, servis varlıklarının daha yüksek miktarlarda kullanımına ve ilerleyen bakım ve güncelleme gerekçelerine çevrilir.
- Kullanılmayan kapasite azaltılır.
- Talebi karşılamak için yapılan masraflar müşteri onaylı maddeler ve şartlar ile geri alınır.

3.5 Fonksiyon Nedir?

Fonksiyon, Belirli bir metot, aktivite veya bunların bir kombinasyonunu tatbik eden ve otomatikleştirilmiş ölçümleri kaynak gösteren mantıki bir kavramdır.

Bir fonksiyon, gerekli kabiliyetlere ve kaynaklara sahip, kendine yeten ve belirli sonuçlar almaktan sorumlu özelleşmiş bir organizasyonel ünite olarak görülür.

Fonksiyonların karakteristik özellikleri:

- Kendi tecrübelerinden oluşmuş bir bilgi dağarcığına sahiptirler.
- Ürün üzerine odaklanarak kendi çalışma metotlarını optimize ederler.

Büyük organizasyonlarda bir fonksiyon bölünerek birçok bölüm, takım ve grup tarafından yürütülebilir veya bir tek organizasyonel ünite içinde şekillendirilebilir. Daha küçük organizasyonlarda bir kişi veya bir grup birçok fonksiyonu yürütebilmektedir.

Uygulama Modeli, farklı uygulama özelliklerini açıkça ifade etmeyi ve anlamayı sağlar, Uygulama modelleri çapraz fonksiyonel koordinasyon ve kontrolü kullanan fonksiyonel hiyerarşi ile bir organizasyonun başarısında kritik olan düzenleme ve geri bildirimin önündeki engelleri kaldırır.

3.6 Rol Nedir?

Rol, bir insan veya grubun spesifik bir bağlamda gerçekleştirdiği bir dizi bağlantılı tavır veya aksiyondur. Bu tanım, bizlere, özgün bir durumun beklenen davranış tarzını anlamamıza yardımcı olur. Rolün kapsamı veya tetikleyicisi ilişkili süreçler tarafından yönetimin onayı ile belirlenir.

Bir rol, ilgili süreçlere bağlı görevler gerçekleştiren bir takım, birim veya tekil bir insan olabilir. Bir departmandan, birden çok rolü birçok kez oynaması beklenebilir, örneğin teknik departmanın yürütebileceği roller:

- Vakaların asıl amaçlarını incelerken sorun yönetimi rolü

- Değişimlerin etkilerini değerlendirmek için değişim yönetimi rolü
- Kendi kontrolleri altındaki cihazların performansını yönetirken kapasite yönetimi rolü

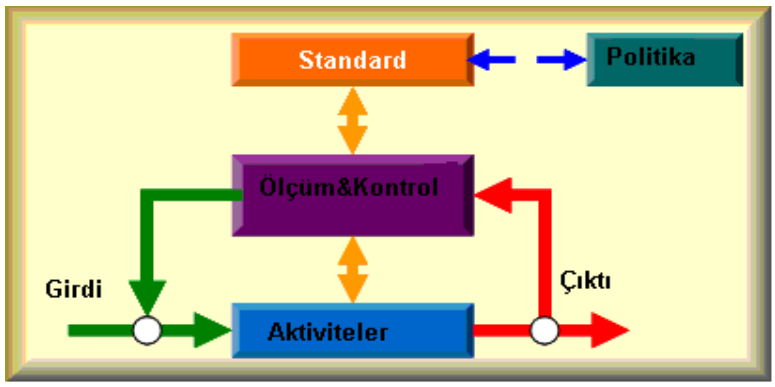
3.7 Süreç Nedir?

Süreç, bir müşteri için direkt veya endirekt değer yaratan bir ürün meydana getirmek üzere kaynak ve imkanları birleştirilmiş ve uygulanmış bir takım koordine edilmiş aktivitedir. Belirli bir amacı yerine getirebilmek için tasarlanan yapısal bir dizi aktivitedir

Sürecin karakteristikleri:

- Bir veya birçok girdi alarak bunları belirlenmiş çıktılara dönüştürür.
- Ürünleri, güvenilir şekilde teslim edebilmek için gerekli tüm rolleri, yükümlülükleri, araçları ve yönetim kontrollerini içerir.
- Gerekli görüldüğü takdirde, kuralları, standartları, rehberleri, aktiviteleri, süreçleri, prosedürleri ve çalışma direktiflerini tanımlayabilir veya revize edebilir.

Bir prosedür, mantıki olarak bağlantılı aktiviteler ve onların kimin tarafından yürütüldüğünün tarifidir. Bir prosedür farklı süreçlerin aşamalarını içerebilir. Bir prosedür kimin neyi yaptığını tanımlar ve organizasyona dayalı olarak değişkenlik gösterir. Bir grup çalışma talimatı, bir prosedür dahilinde bir veya daha çok aktivitenin nasıl yürütülmesi gerektiğini tanımlar.



Şekil 0.3 Süreç Döngüsü

3.8 Süreç Kontrolü

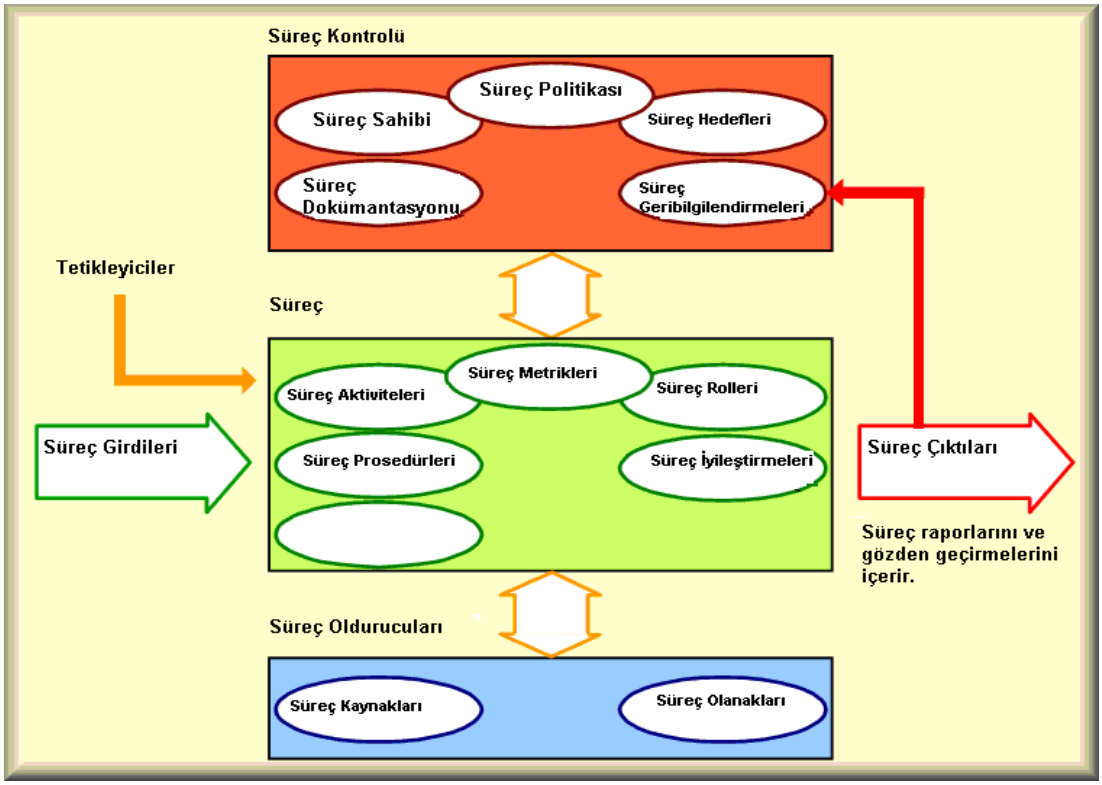
Kontrol, verimlilik, yeterlilik ve devamlılık anlamında bir süreci planlama ve regüle etme aktivitesidir.

Kontrolde önemli olan hususlar:

- Belirtilmiş süreçler dokümante ve kontrol edilmeli
- Kontrol edilmiş süreçler tekrarlanmalı ve yönetilebilir olmalı
- Kontrollü iyileştirme ve yöntem geliştirmek için yöntem ölçüm kapsamı tanımlanmalıdır.

3.9 Süreç Modeli

Süreç Modeli, farklı süreç özelliklerini anlamayı ve açıkça ifade etmeyi olanaklı kılar. Şekil 3.4'de bir Süreç Modeli tasviri bulunmaktadır.



Şekil 0.4 Süreç Modeli

Genel süreç elemanları Şekil 3.4 gösterildiği üzere gruplamak gerekirse:

- Girdiler
- İşlenmiş süreç
- Çıktılar
- Kontrol

Bu basit anlatım tüm süreç tanımlarını destekler. Bir süreç daima bir dizi hedef etrafında organize olmalı ve temel çıktıları, süreç metrikleri, raporlar ve gelişim tavsiyeleri tarafından yönlendirilmelidir.

Bir sürecin, gelişimini garanti edebilmek üzere hedeflerine ulaştığını temin edecek bir sahibi olmalıdır. Bir süreç, organizasyonel ve coğrafik engellere sahip olabilir ve bunlar sıklıkla uygulamanın benzersiz dizayn ve şekillerini yaratan karmaşık farklılıklarda olur.

3.10 Süreç Karakteristikleri

Süreçler, çalışmayı organize etmeye yardımcı olur. Gerekmediği sürece değer değil ama aktivite ve sonuca göre sıralanmışlardır.

Süreçler stratejik değildir. Neyi elde etmek istediğinizi bilmeli veya müşterinin bildiğini farz etmelisiniz. Süreçlerin genel karakteristikleri aşağıda sıralanmıştır:

- Süreçler ölçülebilir, örneğin:
    - Süreçler performansa dayalı olduğundan, ilgili bir usulle ölçülebilir.
    - Yöneticiler ücret, kalite ve diğer değişkenleri ölçebilir
    - Uygulayıcılar süre ve üretkenlik ile değerleri ölçebilir
- Süreçlerin belirli sonuçları olmalıdır:

Bir sürecin var olma nedeni, tanımlandırılabilen ve ölçülebilen belirli bir sonucu veya sonuçları sağlamaktır. Örneğin, birkaç adet yardım masası çağrısı ölçülebilir bir durumdur (Yardım masası bir fonksiyondur).

- Süreçler müşterilere ulaştırılır:

Süreçlerin birincil sonuçları, organizasyon içi veya dışı olabilecek müşteriye teslim edilmelidir ancak süreç onların beklentilerini karşılamalıdır.

- Süreçler belirli bir olaya tepki vermelidir:

Bir süreç ister sürekli devam eden ister tekrarlanan olsun, belirli bir tetikleyici doğru takip edilebilir olmalıdır.

4 GENEL KAVRAM VE TANIMLAR

4.1 Servisin Değeri: Fayda ve Garanti

Müşterinin perspektifinden değeri etkileyen Fayda (amaca uygunluk) ve Garanti (kullanıma uygunluk) iki temel unsurdur.

4.1.1 Servisin Faydası

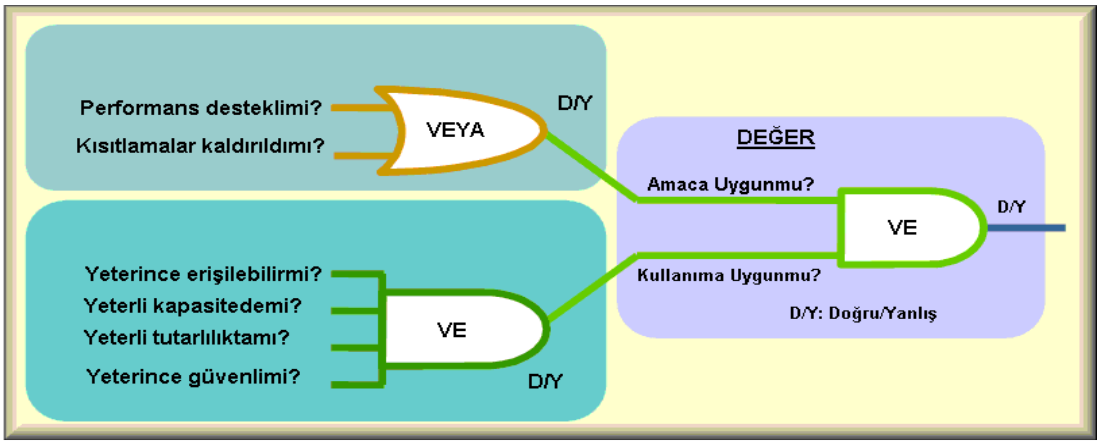
Fayda, müşterinin aldığı şeydir ve performans veya çıktılar üzerine pozitif etkisi olan servisin niteliklerinden türetilmiştir. Amaca uygunluk kapsamında performans üzerindeki bir kısıtlamayı kaldırmak ve rahatlatmak olumlu bir etki yaratabilir. Fayda, performansın averajını yükseltir.

4.1.2 Servisin Garantisi

Garanti, belli ürün ve servislerin sağlanacağı ve sağlanma yolunun kesin özellikleri karşılayacağına dair garantidir. Kullanıma uygunluk kapsamında ihtiyaç duyduğunda ulaşılabilirlik, yeterli kapasite ve değerde olma ve devamlılık ile güvenlik anlamında güvenilirlik sağlanmalıdır. Garanti, performans değişimini azaltır.

Servis çıktısındaki herhangi bir belirsizlik servislerin değeri hakkında şüphe yaratır, örneğin maliyet kesin olabilir ancak fayda çıktıdan çıktıya değişiyor olabilir. Bu tür endişeleri ortadan kaldırmak ve müşteriyi olası kazanım ve kayıplardan haberdar etmek için servisin değerinin fayda ve garanti anlamında tarif edilmesi gereklidir. Müşteriler, amaç için uygun ama kullanım için uygun olamayan (yada tersi) bir şeyden fayda elde edemezler.

Aşağıdaki şekilde, dizayn, tasarım ve geliştirme için fayda ve aracın mantığını ayırt eden bir illüstrasyon bulunmaktadır.



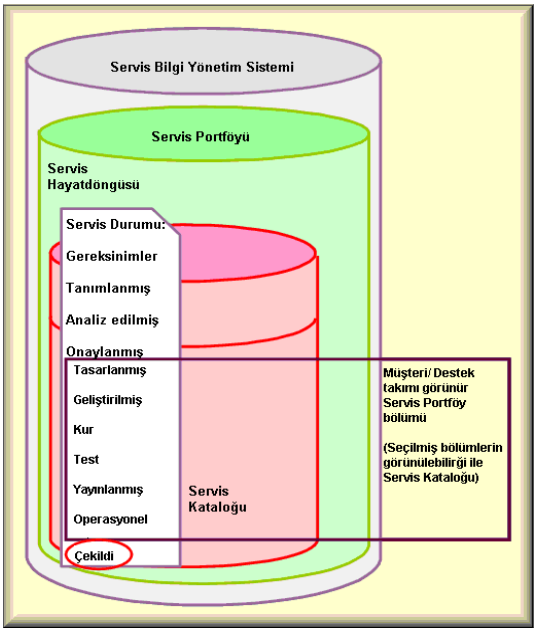
Şekil 0.1 Değer mantık şeması

4.1.3 Servis Portföyü

Servis portföyü, hayat döngüsünde nerde olduğu fark etmeksizin tüm servisleri içinde barındırır.

Portföy içeriği:

- Servis Ardışık düzeni içinde geliştirilen servisler
- Servis Kataloğunu oluşturur (Müşteri tarafından önerilmiş ve sarf edilmiş servisler).
- Görevden çekilen servisler (Servis Portföyü içinde kalmaya devam eder).

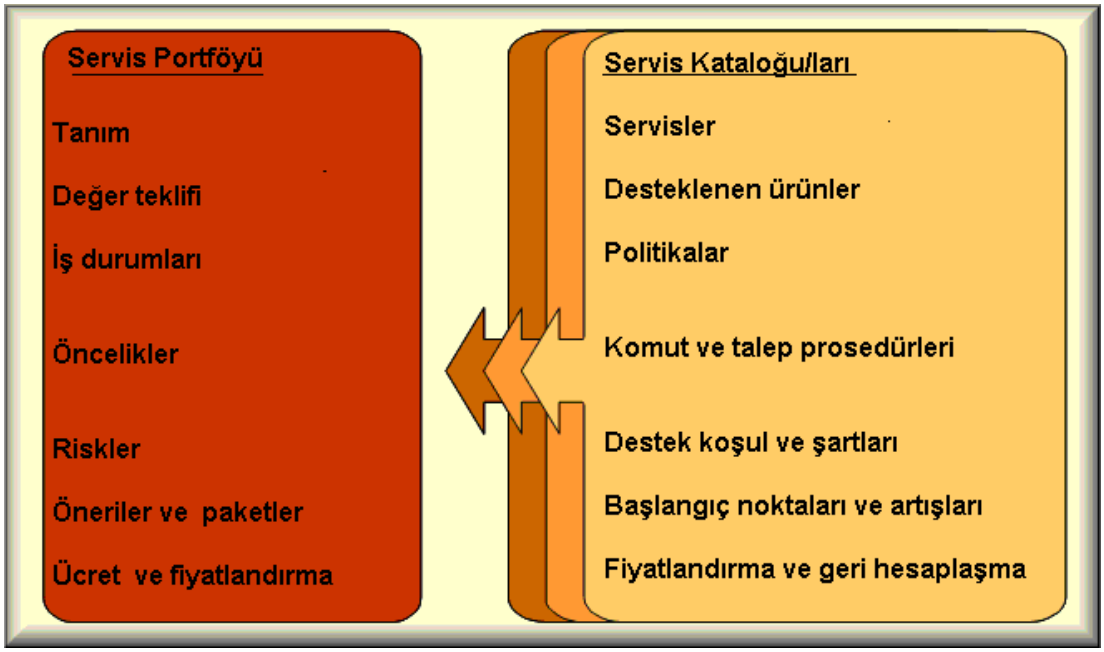


Şekil 0.2 Servis portföy şeması

4.1.4 Servis Kataloğu

Servis Katalogu, Servis Portföyü'nün müşterilere görünür olan bir alt kümesidir. Servis Operasyonu fazında hali hazırda aktif olan ve şimdiki veya olası müşterilere sunulması için onaylanmış servisleri içerir. Servis sağlayıcının mevcut ve hazırdaki becerilerine yapılan sanal bir projeksiyondur. Öğeler, servis kataloğuna ancak ilgili maliyet ve riskler üzerinde detaylı çalışıldıktan sonra girebilirler. Kaynaklar, aktif servislerin desteklenmesine angaje edilmiştir. Birçok müşteri sadece tedarikçinin ileride sağlayabileceğinden çok, sadece bugün ne vaat ettiği ile ilgilenirler.

Servis kataloğu, hangi servislerin Servis Portföy Yönetimi altına gireceğini ve her birinin ayrı ayrı amacını belirler.



Şekil 0.3 Servis portföyü ve Servis Katalogu arasındaki ilişki

Servis katalogunun iki ana konusu vardır:

- İş Servis Katalogu
- Teknik Servis Katalogu

4.1.4.1 İş Servis Katalogu'nun özellekleri:

Servis Kataloğu'nun müşteri açısından görülüşüdür.

Müşteriye sağlanan IT servislerinin detayını içerir.

IT servislerine dayanan iş süreçleri ve iş birimleri arasındaki ilişkiyi içerir.

İş Servis Yönetimi alanına daha çok şey geliştirmesine izin vererek, çok daha aktif hatta önleyici SLM sürecini geliştirmeye yardımcı olur.

4.1.4.2 Teknik Servis Katalogu

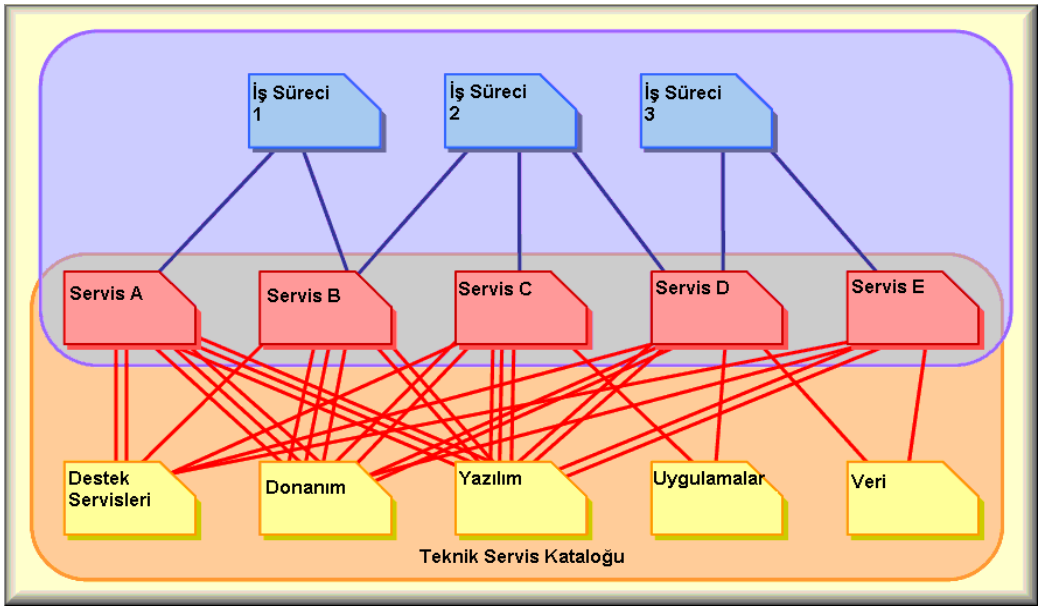
Teknik Servis Kataloğu, İş Servis Kataloğu'nu alttan desteklemeli ve müşteri görüşünün sadece bir bölümünü şekillendirmek yerine müşteriye verilen tüm IT servislerinin detayını içermelidir .

.İşe verilen servisin provizyonunu desteklemeye gerekli olan destek servisleri, paylaşımlı servisler, unsurlar ve CI'ların birbirleri ile olan ilişkilerini barındırır.

Bir servisi destekleyecek olan teknolojiyi ve unsurları destekleyen destek gruplarını belirleyerek, servisler, SLA'ler, OLA'lar, destekleyici anlaşmalar ve unsurları meydana getirirken faydalı olmaktadır.

Birtakım organizasyonlar ya bir İş Servis Kataloğu ya da bir Teknik Servis Katoloğu bulundururlar. Çok daha gelişmiş organizasyonlar her iki unsuru, Servis Yönetimi tarafından desteklenen tümüyle entegre edilmiş Servis Portföyü'nün parçası olarak tek bir Servis Kataloğu'nda bulundururlar. Bir İş Servis Kataloğu ile bir Teknik Servis Kataloğu'nun kombinasyonu, iş üzerindeki olayların ve değişikliklerin etkilerini çabukça değerlendirmek için paha biçilmezdir.

Şekil 4.4 de Servis Kataloğu'nun iki cephesi (İş Servisi Kataloğu & Teknik Servis Kataloğu) arasındaki ilişki tasvir edilmiştir.



Şekil 0.4 Servis Kataloğu'nun iki cephesi

4.1.5 İş Olurluk İncelemesi

Bir iş olurluk incelmesi, yöneticilerin, kalite gereksinimlerini ve ilgili teslim maliyetlerini daha iyi anlamasına olanak verir. Servis kalitesini sağlarken alternatif vasıtalarla maliyetleri düşürmeyi amaçlar.

Bir iş olurluk incelemesinin karakteristikleri:

- Servis yönetimine dayanan iş zorunluluklarını tanımlama amaçlıdır.
- Bir servisten ne amaçlandığının modelidir.
- Servis veya surecin iyileştirilmesinin ve bir hadisenin gelişiminin takip edilmesinin sebeplerini ispat edebilmek için veri ve delil sağlar.
- Maliyet ve arzulanan faydaları belirtmelidir.

4.1.6 Risk

Risk, ister olumsuz bir tehdit ister olumlu bir fırsat olsun, neticenin belirsizliği olarak tarif edilir.

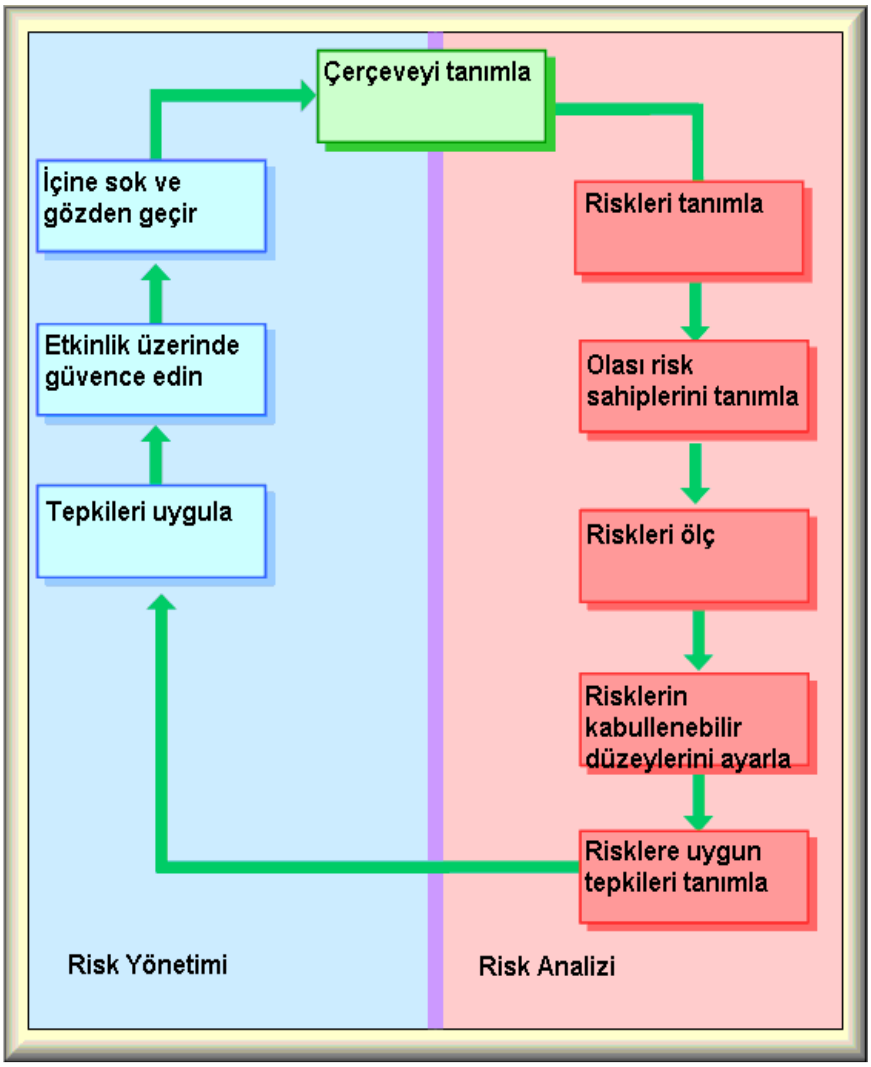
Riskleri yönetmek, bir amacın kazanımları üzerine etkisi olabilecek açıkların tanımlanmasını ve kontrolünü gerektirir.

4.1.6.1 Riskleri yönetmek

Bu yönetim, karar vermeye destek olacak şekilde görülebilir, tekrarlanabilir ve devamlı surette uygulanabilir olmalıdır. İyi tanımlanmış adımları olan risk yapıları maliyetin etkin kullanımını sağlar. Risklerin ve beklenen tesirlerin iyi anlaşılabilmesi daha iyi karar vermeyi, desteklemeyi amaçlar.

Riskleri yönetmenin iki farklı fazı vardır (Şekil 4.5):

- Risk Analizi
- Risk Yönetimi



Şekil 0.5 Risk Yönetimi ile Risk Analizi döngüsü

4.1.6.1.1 Risk Analizi

Organizasyonların daha uygun karar verebilmeleri ve riskleri daha tutarlı yönetebilmeleri için tehlike yaratabilecek riskler hakkında bilgi alma ile ilgilidir.

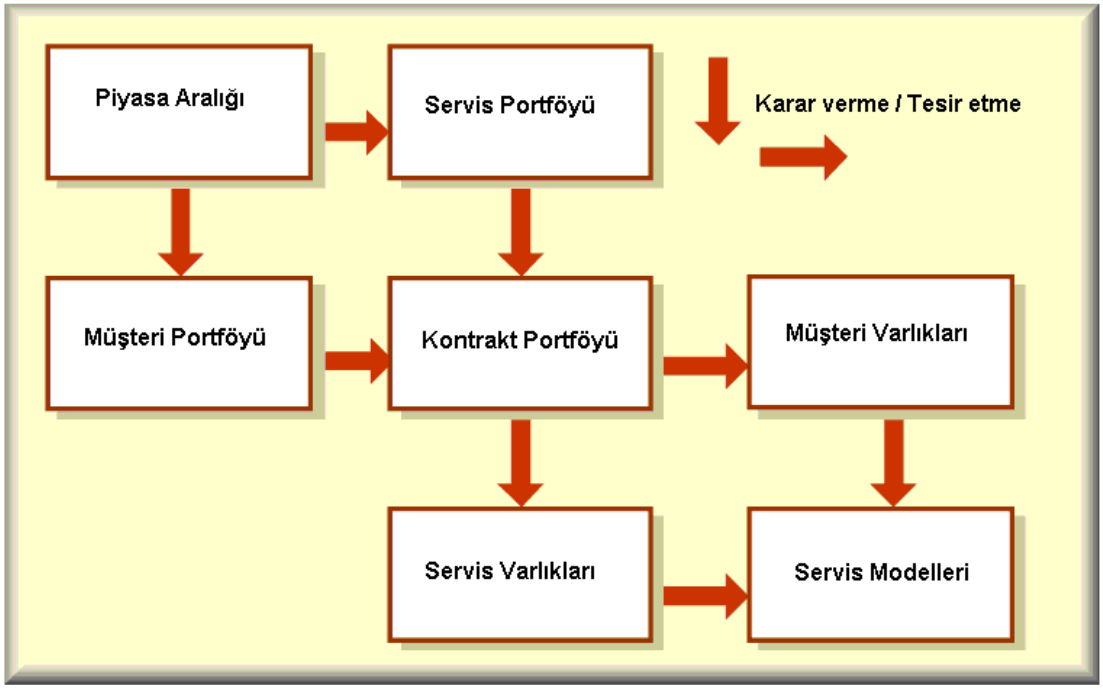
4.1.6.1.2 Risk Yönetimi

Risk Yönetiminde gözetilmesi gereken hususlar özetle:

- Riskleri gözetleyebilmek için süreçler içermeli, riskler hakkında güvenilir ve güncel bilgi erişimini sağlamalı.
- Riskleri çözümlerken mevcut olan kontrolün doğru ayarda olmasını sağlamalı.
- Bir risk analiz ve değerlendirme yapısı tarafından karar verici süreçlere sahip olunmasını sağlamalı.

4.1.7 Servis Modeli

Servis modelleri, değer yaratımı adına haberleşmek ve iş birliği yapmak üzere servis yönetim süreçleri ve fonksiyonlarının ipuçlarıdır.

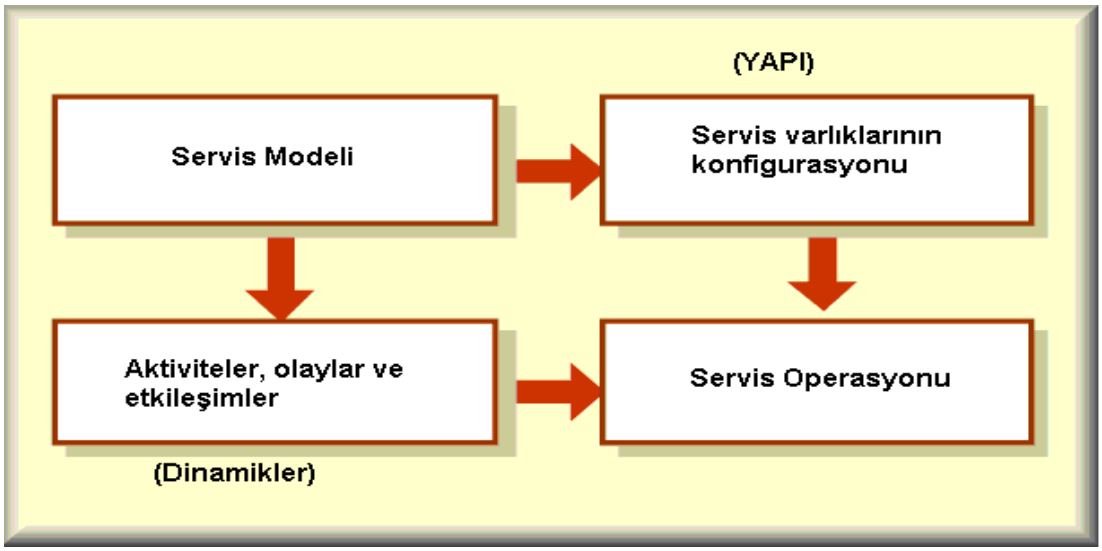


Şekil 0.6 Servis Modeli

Servis Model'leri, müşteri ve servis sağlayıcı varlıklarının belirli bir portföy üzerinde etkileşimidir. Etkileşim, hizmet verme kapasitesi ile talebin bağlantısıdır.

Servis anlaşmaları, her iki taraf için taahhütleri ve beklentileri oluşturan etkileşimin koşulları ve şartlarını belirtir. Müşterilere sağlanan araçlar ve garantiye dayanan sonuçlar, müşteri için yaratılmış değeri tanımlar. Müşterilere sağlanan araç ve garantilerin etkilediği servis modelleri, servislerin yapı ve dinamiklerini derler.

4.1.7.1 Servis Yapı ve Dinamikleri



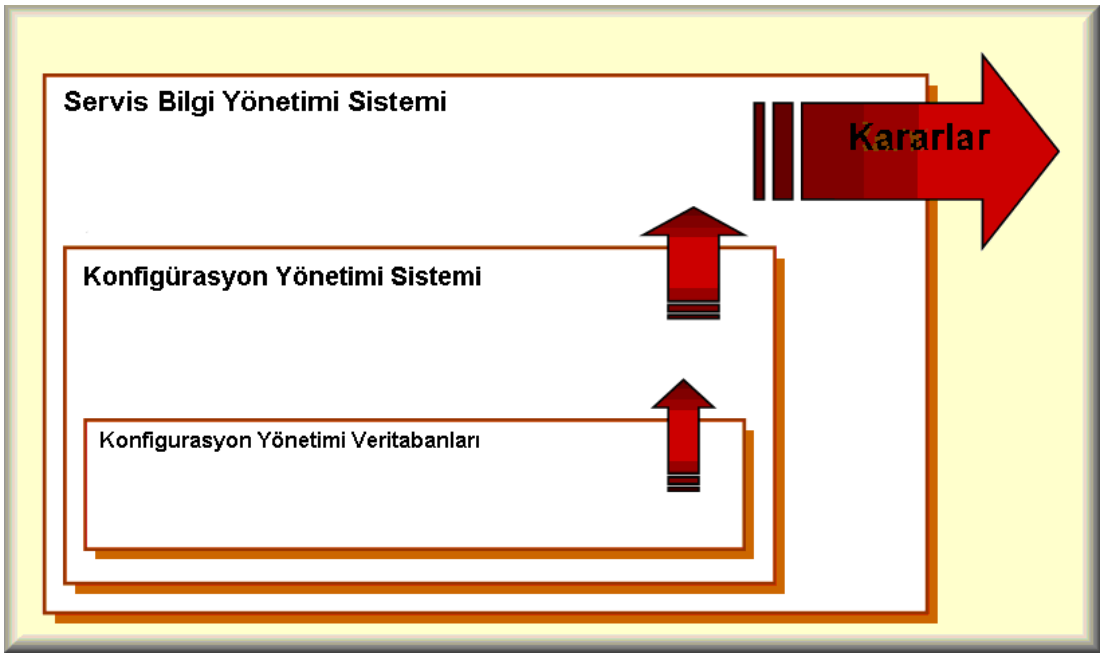
Şekil 0.7 Servis Yapı ve Dinamikleri

Servis Yapısı, ihtiyaç olunan belirli servis varlıkları ve konfigure edildikleri şablonlar cinsinden belirtilmiştir

Servisin Dinamikleri, iş eylem şablonları, talep şablonları ve varyasyonlarını, aktiviteleri, kaynakların akışını, koordinasyonu ve etkileşimleri içerir.

4.1.8 Servis Bilgi Yönetim Sistemi

Bilgi Yönetimi, IT Servis Yönetimi dâhilinde SBYS (Servis Bilgi Yönetim Sistemi) üzerine odaklanır. SBYS, mantıksal bir havuzda veya Konfigrasyon Yönetim Sistemi ve Konfigurasyan Yönetim Veritabanı içinde tutulan veri tarafından desteklenir.



Şekil 0.8 Servis Bilgi Yönetimi'nde Karar Akışı

Sistem dahilinde karar süreci adımları:

- Birinci aşamada CMBD dâhilinde veri akışı
- İkinci aşamada CMS yoluyla SKMS'yi besleme
- Üçüncü aşamada bilgilendirilen karar verici süreçlerin desteklenmesi

SKMS, daha geniş bir bilgi üssünü içine alan ileri bir kavramdır.

Örneğin:

- Personel için tecrübe
- Çevresel meseleler hakkındaki kayıtlar (örn: kullanıcı sayı ve davranışları, organizasyonun performans göstergeleri)
- Tedarikçi ve ortakların ihtiyaçları, kabiliyetleri ve beklentileri
- Tipik ve beklenen kullanıcı beceri seviyeleri

5 SERVİS TASARIMI

Servis Tasarımı, uygun ve yenilikçi IT altyapısı servis çözümlerinin ve süreçlerinin dizaynı için IT kurallarının, mimarisinin ve dokümanlarının üretilmesi ve idamesi üzerinde rehberlik sağlar.

Servis Tasarımı, işe efektif servis verebilmeyi, büyüme ve değişim için talepleri karşılayabilmeyi sağlar. Geliştirme için gerekli olan bütçe ve kaynaklar, oluşturma için gerekli olandan bir kaç kat fazladır, bu yüzden tüm hayat döngüsü için tasarıma çok büyük önem verilmelidir. Bir kere üretim ortamına geçtikten sonra her koşul veya zaman için bir servisin veya ürünün tekrar mühendisliği yapılamayabilir. Bir kere çalışmaya başladıktan sonra tasarıma yaklaşabilmek mümkün olabilse de geri dönmek imkânsız olacaktır. Servisin tekrardan uyarlanması zor ve maliyetli olduğu gibi en başında tasarımın düzgün olması durumunda kazanılacak faydayı sağlamayacaktır.

IT servis tasarımı toplam iş değişim sürecinin bir parçasıdır. Bir kere işin değişen gereksinimlerine uygun olacak şekilde ihtiyaç duyulan ve onaylanan şey hakkında doğru bilgi edinildiği takdirde, karşılanacak ihtiyaç için servis planı uygulanabilir.

Servis Tasarımı'nın tüm iş değişim süreci üzerindeki rolünü "Uygun ve yenilikçi IT servislerinin tasarımını, mimarisini, süreçlerini, kurallarını ve dokümantasyonunu içerecek şekilde şu an ve ilerideki iş gereksinimlerini karşılamalıdır" şeklinde tanımlayabiliriz.

Doğru ara yüzlerin ve bunların tasarım aktivitelerine bağlantılarının olması önemlidir. Yeni veya değişmiş servislerin tasarımında servis hayat döngüsünün, tamamının ve ITSM süreçlerinin başlangıçta dâhil edilmiş olması hayati önem taşır. Genelde sorunlar yeni tasarlanmış servislerin aktif ortamlara aktarıldığı ilk zamanlarda ortaya çıkar. Bir servis tasarımını devreye alırken işin ihtiyaçlarının karşılandığından emin olmak için alınması gereken önlemler aşağıdaki gibi sıralanabilir:

- Yeni servis çözümü, toplam Servis Portföyü'ne konsept aşamasından eklenmeli ve Servis Portföyü tüm artan veya ötelenen güncellemeleri yansıtacak şekilde güncellenmelidir. Bu, özellikle finansal açıdan olmak üzere tüm alanlar açısından tasarım sırasında yararlı olacaktır.

- Kapasite Yönetimi, SLR’ dan edindiği bilgiler dâhilinde hâlihazırdaki yapının yeni servisi destekleyip destekleyemeyeceğine karar verir. Yeterli zaman olduğu takdirde modelleme aktiviteleri Kapasite Planı dâhiline alınabilir.
- Eğer yeni servis için yeni bir alt yapı gereksinimi veya aktif yapının genişletilmesi gerekiyorsa Finansal Yönetim, bütçeyi ayarlaması için duruma dâhil edilir.
- Yardım Masası, yeni servislerini, gerçek zamanlı operasyonda hazırlıklı olunması için Yardım Masası çalışanlarını ve olası IT müşteri çalışanlarını eğiterek ve hazırlayarak haberdar eder.
- Servis Dönüşümü, uygulamayı planlamaya ve ileriye yönelik zamanlamaya başlayabilir.
- Tedarik Yönetimi, yeni servis için ek tedarik yapılması gerekiyorsa devreye girebilir.

5.1 Aktiviteler

Tasarım süreç aktivitelerini aşağıdaki sıralamada gösterebiliriz:

- İş ihtiyaçlarının açık şekilde dokümante edildiği ve üzerinde anlaşıldığından emin olacak şekilde ihtiyaçlar listesi, analiz ve mühendisliğin yapılması
- İş ihtiyaçlarının karşılanması için uygun servislerin, teknolojinin, süreçlerin, bilginin ve süreç önlemlerinin tasarlanması
- Tasarım, planlama, mimari ve kuralların Servis Tasarımı dâhilindeki tüm süreçlerin ve dokümanların yeniden gözden geçirilmesi ve revizyonu
- Tüm diğer tasarım ve planlama aktiviteleri ve rolleri ile irtibata geçilmesi (örneğin çözüm tasarımı)
- Tasarımları, planları, mimarileri ve kuralları içeren IT kuralları ve tasarım dokümanlarının oluşturulması ve muhafazası

- Yol haritaları, programlar ve proje planlarını kullanan IT stratejilerinin uygulanması ve yaygınlaştırılması için tasarım dokümantasyonunun ve planlamanın revizyonu
- Tüm tasarım süreçlerinin ve çıktıların risk tanımlanması ve yönetilmesi
- Tüm şirket ve IT stratejileri ve kuralları ile düzgün hizalama

5.2 Güvenlik Yönetimi

Bilgi Güvenliği Yönetimi, bilginin provizyonu ve bilginin izinsiz kullanımını engellemeyi amaçlayan önemli bir aktivitedir. Uzun bir süre Bilgi Güvenliği göz ardı edilmiştir, ancak bu zamanla değişmektedir. Günümüze gelindiğinde güvenlik şu anda üzerinden gelinmesi gereken en temel yönetim unsurlardan biridir.

Bu disipline gösterilen ilgi, internet ve elektronik ticaretin artan kullanımı ile artmaktadır. Birçok işletme işlerine elektronik çıkış yollarını konumlandırmaktadır. Bu sızma riskini ortaya çıkarmaktadır.

İşletmelerin üst yönetimleri güvenlik konusunda karar almalı ve fakat bu kararların sadece bir risk analizi ile alındığı takdirde uygulanabilir olduğunun farkında olunmalıdır. Yapılan analiz, Güvenlik Yönetimine güvenlik gereksinimlerini belirlemek için girdi sağlamalıdır.

Bu tür gereksinimler IT servis sağlayıcılarını etkilediğinden ve Servis Seviye Anlaşmalar ile koşullara bağlanmalıdırlar. Güvenlik Yönetimi, servislerin güvenlik durumlarının tüm zamanlarda müşteri ile üzerinde anlaşılmış düzeylerde sağlanmasını amaçlar. Güvenlik, günümüzde yönetimin zaruri kalite gereksinimlerindendir. Güvenlik Yönetimi, IT organizasyonunda servis sağlayıcının bakış açısıyla güvenliği entegre eder.

Bilgi Güvenliği Yönetimi Nizamnamesi (ISO 27000), güvenlik önlemlerinin geliştirilmesi, tanıtımı ve değerlendirmesine rehberlik eder.

5.2.1 Temel Kavramlar

Bilginin güvenliğini sağlamayı amaçlayan Güvenlik Yönetimi, Bilgi Güvenliği'nin şemsiyesinin altına girer. Güvenlik, bilinen risklere ve bilinmeyen

risklere karşı mümkün olduğunca açık olmamaktır. Bunu sağlayacak araç güvenliktir. Amaç bilginin değerini korumaktır. Bu değer, güvenilirlik, bütünlük ve ulaşılabilirliğe dayanmaktadır.

5.2.2 Tanım olarak güvenlik kapsamında yer alan olgular:

- Güvenilirlik: Bilgiyi izinsiz kullanım ve erişimden korumak
- Bütünlük: Bilginin tutarlılığı, eksiksizlik ve zamanlılığı
- Erişilebilirlik: Üzerinde anlaşılan herhangi bir zamanda bilgi, her an ulaşılabilir olmalı

Güvenlik Yönetimi, bilgi işleme sistemleri tarafından sağlanan devamlılığa dayanır. İkincil durumlar ise gizlilik, kimliksizlik ve doğrulanabilirliği içermektedir.

5.2.3 Hedefler

Yakın yıllarda, hemen hemen tüm işyerleri bilgi sistemlerine daha da bağımlı hale gelmiştir. Bilgisayar ağlarının kullanımı sadece iş yerlerinde değil iş yeri ile dışarıdaki dünya ile arasında da büyümüştür.

IT altyapısının artan karmaşıklığı ile işletmeler şimdilerde teknik sorunlara yol açabilecek risklere, insan hatasına, hacker ve crackerlara, bilgisayar virüslerine daha da açıktır.

Büyüyen bu karmaşıklık, konsolide yönetim yaklaşımını gerektirir. Güvenlik Yönetimi diğer süreçlerle önemli bağlar barındırır. Diğer ITIL süreçleri Güvenlik Yönetimi denetiminde bazı güvenlik aktivitelerini yürütebilir.

Güvenlik Yönetimin iki temel hedefi:

- SLA’lerin ve diğer harici kontratların, mevzuatların ve dışarıdan dayatılmış kuralların güvenlik gereksinimlerini karşılamak
- Temel seviyede güvenlik seviyesini sağlamak üzere, diğer harici gereksinimlerden bağımsız olarak Güvenlik Yönetimi, IT organizasyonunun müdahalesiz operasyonunu sağlamayı amaçlamak

Güvenlik Yönetimi ayrıca Bilgi Güvenliği Servis Seviye Yönetimini basitleştirmeye yardımcı olur ki, büyük sayılarda SLA'yi yönetmek limitli sayıda olandan çok daha zordur.

Süreç girdisi, kurallar dokümanından ve diğer harici gereksinimden edinilmiş olabilecek SLA'ler tarafından sağlanır. Süreç ayrıca diğer süreçlerdeki ilgili güvenlik meselelerinden (örn güvenlik olayları) bilgi alır. Sonuç, beklenti raporları ve rutin güvenlik planlamalarını içeren, uygulaması tamamlanmış SLA'ler hakkında bilgi içerir.

Bu zamanda, birçok organizasyon Bilgi Güvenliği ile stratejik bir düzeyde, bilgi kuralları ve bilgi planları dâhilinde araç ve diğer güvenlik ürünleri alarak uğraşır. Güvenlik Yönetimi'nin aktif yönetimine, devamlı analiz ve kuralların teknik opsiyonlara aktarımı ve güvenlik önlemlerinin gereksinimlerin ve şartların değişimleri durumda efektif olmasına yeterli özen gösterilmelidir. Olabilecek eksik bir bağlantının handikabı, taktik yönetim düzeyinde, büyük yatırımların yeni ve daha etkili önlemlerin alınması gerektiği bir zamanda artık ilgisiz olan alanlara yapılmasıdır. Güvenlik Yönetimi, stratejik, taktiksel ve operasyonel seviyelerde Güvenlik Yönetimi önlemlerinin alındığını temin etmeyi amaçlar.

5.2.4 Kazanımlar

Bilgi Teknolojisi tek başına bir hedef değildir; işin veya organizasyonun çıkarlarını korumayı amaçlar. Birtakım bilgi ve bilgi sistemleri organizasyonda diğerlerinden daha önemli olacaktır. Bilgi Güvenliği bilginin güvenliğine uygun olmalıdır. Güvenlik önlemleri, bilginin değeri ve süreçsel ortam tehditleri arasında dengeyi sağlayarak iyi oluşturulmuş bir güvenliği geliştirir.

Efektif bir bilgi kaynağı, yeterli Bilgi Güvenliği ile birlikte bir organizasyonda iki nedenden dolayı önemlidir:

- İçsel nedenler: Bir organizasyon ancak doğru ve tamamlanmış bilgi istenildiğinde erişilebiliniyorsa efektif çalışabilir. Bilgi Güvenliğinin düzeyi buna uygun olmalıdır.
- Dışsal nedenler: Bir organizasyondaki süreçler, belirli amaçları karşılamak üzere piyasaya veya topluma sunulan ürün veya servisleri

üretirler. Yetersiz bilgi tedariki, standart dışı ürünler ve servislere yol açarken, hedefleri karşılamada kullanılamaz ve organizasyonun devamını tehdit eder. Yeterli Bilgi Güvenliği, yeterli bilgi tedarikine sahip olmak için önemlidir. Bu nedenle Bilgi Güvenliği'nin harici önemi kısmen dâhili önemi tarafından belirlenir. Güvenlik, bilgi sistemine önemli değerler katar. Efektif güvenlik, organizasyonun devamlılığına katkıda bulunur ve hedeflerine ulaşmada yardımcı olur.

5.2.5 Süreçler

Organizasyonların onların bilgi sistemleri değişken bir yapıdır. Kontrol listeleri, statik olup IT deki hızlı değişimleri adreslemede yetersiz kalırlar. Bu yüzden, devamlı surette Güvenlik Yönetim aktivitelerin etkinlikleri gözden geçirilmelidir. Güvenlik Yönetimi, hiç bitmeyen planla, yap, kontrol et ve harekete geç döngüsüne yol açar. Servis Seviye Anlaşmaların güvenlik bölümü, bu gereksinimleri güvenlik servisleri ve sağlanacak güvenlik seviyesi anlamında ifade eder.

Servis sağlayıcı kendi organizasyonu ile bu anlaşmaları, bir güvenlik standardı veya Operasyonel Seviye Anlaşması ile bir Güvenlik Planı dâhilinde haberleştirir. Öncelikle bu plan uygulanmalı ve uygulama değerlendirilmelidir. Plan ve değerlendirme daha sonra güncellenir. Servis Seviye Antlaşması bu aktiviteler ve müşteriler hakkında raporlama yapar. Böylece, müşteri ve servis sağlayıcı birlikte bir tamamlanmış dönemsel süreci oluştururlar. Müşteri, raporlar dâhilinde kendi gereksinimlerini değiştirebilir ve servis sağlayıcı bu değerlendirmeleri veya SLA de tanımlanmış hususları değiştirmek amacıyla planı veya uygulamasını bunlara uyarlar.

5.2.6 Aktiviteler

Bilgi Güvenliği Yönetimi aktivitelerinin incelendiği alt başlıklar:

- Kontrol
- Kurallar
- Bilgi Güvenliği Organizasyonu
- Planlama

5.2.6.1 Kontrol – Bilgi Güvenliği kuralları ve organizasyonları

Kontrol aktivitesi, Güvenlik Yönetimi'nin ilk aktivesi olup sürecin organizasyonu ve yönetimi ile alakalıdır. Bu, Bilgi Güvenliği Yönetimi'nin kavramsal çatısını içerir. Bu yapı alt süreçleri tanımlar, bu süreçler; güvenlik planlarının açıklanması, uygulamaları, uygulamaların değerlendirilmeleri ve yıllık güvenlik planlarında (aksiyon planları) uygulamaya geçişidir. Müşteriye, Servis Seviye Yönetim tarafından sağlanan raporlar ayrıca adreslenir. Bu aktivite alt süreçleri, güvenlik fonksiyonlarını, rolleri ve sorumluluklarını belirler. Ayrıca organizasyonel yapıyı, raporlama düzenlemelerini ve kontrol sırasını (kimin kime, kimin neyi ve nasıl uygulandığının raporlaması) tarif eder.

5.2.6.2 Kurallar (Uygulamadaki kuralların yapısal özelliklerinin tarifi):

- Kural tanımlaması ve uygulanması diğer kurallar ile bağ kurmak
- Hedefleri, genel prensipleri ve önemi içermek
- Alt süreçlerin tarifini barındırmak
- Alt süreçler için fonksiyonlar ve sorumlulukların tahsis edilmesini üstlenmek
- Diğer IITL süreçlerine ve onların yönetimleriyle bağlanmak
- Personelin genel sorumluluklarının belirtmek
- Güvenlik meseleleri ile uğraşmak

5.2.6.3 Bilgi Güvenliği organizasyonu (Organizasyonel yapı unsurları):

- Yönetim yapısı
- Sorunlulukların daha detaylı dağılımı
- Bilgi Güvenlik İcra Komitesi'nin kurulması
- Bilgi Güvenliği koordinasyonu
- Katılım araçları (örneğin risk analizi ve farkındalığın iyileştirilmesi)
- IT hizmetlerinin yetkilendirilmesinin müşteri ile müzakere edilerek tarifi
- Uzman tavsiyesi
- Organizasyonlar arasında işbirliği, iç ve dış iletişimler.

- Bağımsız EDP denetlemesi
- Üçüncü kişilerin erişimleri için güvenlik prensipleri
- Üçüncü kişiler ile anlaşmalar dâhilinde Bilgi Güvenliği

5.2.6.4 Planlama

Planlama aktivitesi, SLA'in güvenlik bölümünün tarifini, Servis Seviye Yönetimi ve güvenlikle alakadar Destekleyici Anlaşmalar ile konsültasyon dahilinde yapar. SLA'in genel mevzular içinde belirtilmiş hedefleri, detaylandırılmış ve bir Operasyonel Servis Anlaşması formunda yer verilmiştir. Bir OLA, servis sağlayıcısının organizasyonel ünitesi ve örneğin her bir IT platformu, uygulaması ve ağı için özel bir güvenlik planı olarak değerlendirilir. Planlama aktivitesi sadece SLA den girdi almaz ayrıca servis sağlayıcının kural prensiplerinden de (Kontrol aktivitesi) alır.

Bu prensiplerin içerdiklerini örnek olarak:

- "Her kullanıcı eşsiz olarak tanımlanabilmeli"
- "Tüm müşterilere her zaman için temel bir güvenlik seviyesi sağlanmalı"

Bilgi Güvenliği için Operasyonel Seviye Anlaşmaları (spesifik güvenlik planları), normal prosedürler kullanılarak taslaklaştırılmış ve uygulanmıştır. Bu, ihtiyaç duyulan aktivitelerin diğer süreçlerle bir koordinasyon içinde bulunmalarını zorunlu kılar. Güvenlik Yönetimi tarafından sağlanan girdiyi kullanan Değişimi Yönetimi, IT alt yapısına gerekli değişiklikleri yapar. Değişim Yöneticisi, Değişim Yönetimi sürecinden sorumludur. Planlama aktivitesi, SLA'in güvenlik bölümünün ifade edilmesini, güncellemesini ve uyumlu olmasını için Servis Seviye Yönetimi ile tartışılmaktadır.

Servis Seviye Yöneticisi bu koordinasyondan sorumludur. SLA, güvenlik gereksinimlerini mümkün olduğu alanlarda ölçülebilir koşullarda tanımlamalıdır. Müşterinin güvenlik gereksinimleri ve standartları doğrulanabilmeli, gerçekçi ve ulaşılabilir olmalıdır.

Uygulama alt süreci, planlarda belirlendiği üzere tüm önlemleri uygulamayı amaçlar. Aşağıdaki kontroller ile bu aktiviteyi destekleyebilir:

5.2.6.4.1 IT Kaynaklarının Sınıflandırılması ve Yönetimi Esasları

- CMDB deki CI'ların bulundurulması için girdi sağlar.
- IT kaynaklarının, üzerinde anlaşılmış rehber uyarınca sınıflandırılması.

5.2.6.4.2 Personel Güvenliği Esasları

- İş tanımlarında görevlerin ve sorumlulukların tanımlanması
- Eleme
- Personel için gizlilik anlaşması
- Eğitim
- Personele güvenlik olayları ve saptamada güvenlik zayıflıkları konusunda rehberlerin oluşturulması
- Disiplin önlemleri
- Güvenlik farkındalığını arttırmak

5.2.6.4.3 Güvenlik Yönetimi Esasları

- Sorumlulukların ve iş ayrımının uygulanması
- Yazılı çalışma talimatlarının oluşturulması
- İçsel regülâsyonun elenmesi
- Güvenlik tüm hayat döngüsünü kapsamalı; sistemin oluşturulması, testi, benimsenmesi, operasyonları, bakımı ve ortadan kaldırması ile ilgili güvenlik talimatnameleri bulunmalıdır.
- Geliştirme ve test ortamlarının üretim ortamlarından ayrılması.
- Olaylar ile uğraşabilmek için gerekli prosedürler (Olay Yönetimi kapsamında)
- Geri dönüş olanaklarının geliştirilmesi
- Değişim Yönetimi için girdi sağlama
- Virüs koruma önlemlerinin uygulanması
- Bilgisayarlar, uygulamalar, ağlar ve ağ servisleri için yönetim tedbirlerinin uygulanması.
- Veri medyası için güvenliğin sağlanması

5.2.6.4.4 Erişim Kontrolü

- Erişim ve erişim kontrol kurallarının uygulanması
- Bilgisayarlara, uygulamalara, ağ servislerine ve ağlara kullanıcı ve uygulama erişim seviyelerinin bulundurulması
- Ağ güvenlik bariyerlerinin bulundurulması (güvenlik duvarı, anahtarlar, yönlendiriciler, modem servisleri)
- Bilgisayar sistemlerinin ve ağdaki bilgisayarların tanımlanması ve onayı için önlemlerin uygulanması.

5.2.6.4.5 Değerlendirme

Uygulamanın planlanmış önlemlerinin bağımsız bir denetimden geçmesi zaruridir. Bu denetim, performansı ölçmek ve aynı zamanda müşteriler ve üçüncül şahıslar için gereklidir. Değerlendirme aktivitesinin sonuçları, müşterilerle konsültasyon çerçevesinde onaylanmış önlemlerin güncellenmesi ve ayrıca onların uygulanmasında da kullanılabilir. Değerlendirme sonuçları değişiklikler önerebilir, öyle ki bir RFC tanımlanabilir ve Değişim Yönetim sürecine gönderilebilir.

Değerlendirmenin üç formu bulunur:

- Kişisel-Değerlendirmeler: Esasen sürecin emir-kumanda organizasyonu tarafından uygulanır
- İç denetimler: Dâhili EDP denetçiler tarafından yapılır
- Dış denetimler: Harici EDP denetçiler tarafından yapılır.

Kişisel değerlendirmelerin aksine, diğer alt süreçlerde bulunan personel denetlemelerde bulunmaz. Bu sorumlulukların ayrılması prensibinin uygulandığını garanti etmek içindir. Değerlendirmeler ayrıca güvenlik olaylarına karşılık olarak yürütülür.

Temel aktiviteler:

- Uyumluluğun güvenlik kuralı ile doğrulanması ve güvenlik planlarının uygulanması
- IT sistemleri üzerinde güvenlik denetimlerinde bulunması
- IT kaynaklarının uygunsuz kullanımlarının belirlenmesi
- Diğer EDP denetlemelerinin güvenlik yönlerinin dikkate alınması

5.2.6.4.6 Bakım

IT alt yapısında, organizasyonunda ve iş süreçlerindeki değişimler ile riskler de değiştiği için güvenlik bakıma gereksinim duyar. Güvenlik bakımı, SLA'in güvenlik bölümünü ve detaylı güvenlik planlarının bakımını içerir.

Bakım, Değerlendirme aktivitesinin sonuçlarına ve risklerdeki değişimin değerlendirmesine dayanarak yürütülür. Bu öneriler, Planlama aktivitesinin içine tanıtılabilir veya SLA içinde bir bütün dâhilinde tanıtılabilir. Her iki durumda da, öneriler, yıllık güvenlik planındaki dâhil etme aktivitelerinde sonuçlanır. Tüm değişimler normal Değişim Yönetimi sürecine konu olur.

5.2.6.4.7 Raporlama

Raporlama bir aktivite değildir, fakat diğer alt süreçlerin bir ürünüdür. Raporlar, elde edilen güvenlik performansı hakkında bilgi sağlamak ve müşterileri güvenlik meseleleri hakkında bilgilendirmektir. Bu raporlara çoğunlukla müşteri ile yapılan anlaşmalar altında gereksinim duyulur.

Raporlama hem müşteri hem de servis sağlayıcı için önemlidir. Müşteri, eforların etkinliği ve aktif güvenlik önlemleri hakkında doğru bilgilendirilmelidir. Müşteri ayrıca tüm güvenlik olayları hakkında bilgilendirilir.

Örnek raporlar ve raporlanabilir olaylar:

- Planlama Aktivitesi:
  - SLA ile uyumluluk kapsamı ve onaylanmış güvenlik Temel Performans Göstergeleri hakkındaki raporlar
  - Destekleyici Kontratlar ve onlarla ilgili problemler
  - Operasyonel Seviye Anlaşmaları (iç güvenlik planı) ve servis sağlayıcısının kendi güvenlik prensipleri hakkındaki raporlar.
  - Yıllık güvenlik planları ve aksiyon planları hakkındaki raporlar.
- Uygulama aktivitesi:
  - Bilgi Güvenliği uygulamaları hakkındaki raporlar.

- Güvenlik olayları, bu olaylara gösterilen tepkiler ve opsiyonel olarak bir önceki raporlama periyodu ile karşılaştırmayı içeren bir liste
- Olay eğilimleri hakkında tanımlama
- Farkındalık programının durumu

SLA' de tanımlanmış olaylar hakkında müşteriye direkt bağlantı yapabilecek bir yetkilinin servis sağlayıcı tarafından atanması gereklidir. Bu Servis Seviye Yöneticisi, Olay Yöneticisi veya Güvenlik Yönetici aracılığı ile olabilir ki genelde bu görevli Güvenlik Yöneticisi olmaktadır. Aynı zamanda özel durumlarda haberleşmenin de bir prosedürle tanımlanması gereklidir.

Özel durumlardaki istisnalardan ayrı olarak, raporlar Servis Seviye Yönetimi aracılığı ile bildirilir.

SONUÇ

Küçük ve orta çaplı şirketlerden büyük organizasyonlara IT'nin yeri ve gelişimi zamanla ayrıca yönetilmesi gereken iş süreçlerine benzer bir önem arz etmeye başlamıştır. Yönetim tarzında benimsenecek prensipler zamanla piyasadaki aktörlerin edindikleri tecrübeler ile şekillenmiş ve farklı yönetim oluşumları meydana çıkmıştır. Bu çalışmada detaylandırmaya gayret edilen ITIL, bu oluşumların en çok rağbet edileni ve piyasada en itibar görenidir. Yirmi yılı bulan uygulanma tarihi boyunca üç kez sürüm değişikliği geçirmiş ve son haliyle en iyi uygulama olma yönünde bir ileri adım atmıştır.

ITIL'ın bu denli kabul görmesi ve yaygınca uygulanmasının en önemli nedenlerinden biri, geliştirilmesinde ve adaptasyonunda bağımsız grupların aktif olması ve marka veya ürün tercihi üzerinden bir düzenleme sunuyor olmamasıdır. Son sürümü ile günümüzün ve ilerisinin ihtiyaçlarını da kapsayabilecek olmayı hedefleyen ITIL, gelişmeye açık, standardizasyon ile uyuşumlu bir uygulamalar bütünüdür.

Bilgi Güvenliği Yönetimi'ni bir önceki sürümünden farklı olarak Servis Tasarımı ana bölümünde ele alınan ITIL, bu sayede tüm diğer yönetim esaslarıyla etkileşimli olan Bilgi Güvenliği Yönetim Sistemi'ni bir fonksiyon olarak ele değerlendirmektense bir süreç olarak kullanmayı tercih etmiştir.

Ülkemizde, işletmelerde ITIL adaptasyonunun, zaman içinde bilgi yönetimi ve güvenliğinin değer kazanmasıyla yükselen bir eğilim olacağını ve ancak bu safhanın geçilmesiyle verilen servisin sağladığı değerin arzulanan ölçülerde doğru şekilde ölçülebilir, kontrol edebilir, denetlenebilir ve maliyetlendirilebilir olacağından bahsedilebilir olacağı bir gerçektir.

KAYNAKÇA

1. Office of Government Commerce, (2007). "*ITIL Service Design"*.
2. Office of Government Commerce, (2007). "*The Offical Introduction To Service Life Cycle"*.
3. Office of Government Commerce, (2007). "*http://www.ogc.gov.uk/"*.
4. ITSMF, (2007). "*http://www.itsmf.net"*.
5. IBM, (2007). "*http://www.ibm.com"*.
6. HP, (2007). "*http://www.hp.com"*.
7. OGC, (2007). "*Service Design"*.
8. PULTORAK, (2007). "*http://pultorak.com*"