T.C.
SÜLEYMAN DEMİREL ÜNİVERSİTESİ
FEN BİLİMLERİ ÜNİVERSİTESİ

BİLGİ GÜVENLİĞİ STANDARTLARI VE KAMU KURUMLARI BİLGİ GÜVENLİĞİ İÇİN BİR MODEL ÖNERİSİ

Tuğba HAKLI

Danışman: Yrd. Doç. Dr. Ecir Uğur KÜÇÜKSİLLE

YÜKSEK LİSANS TEZİ
ELEKTRONİK BİLGİSAYAR EĞİTİMİ ANABİLİM DALI
ISPARTA-2012

TEZ ONAYI

Tuğba HAKLI tarafından hazırlanan "Bilgi Güvenliği Standartları ve Kamu Kurumları Bilgi Güvenliği İçin Bir Model Önerisi" adlı tez çalışması aşağıdaki jüri tarafından oy birliği / oy çokluğu ile Süleyman Demirel Üniversitesi Elektronik Bilgisayar Eğitimi Anabilim Dalı'nda **YÜKSEK LİSANS TEZİ** olarak kabul edilmiştir.

Danışman : Yrd. Doç. Dr. Ecir Uğur KÜÇÜLSİLLE (İmza)

Süleyman Demirel Üniversitesi Bilgisayar Mühendisliği Anabilim Dalı

Jüri Üyeleri :

Yrd. Doç. Dr. Yrd. Doç. Dr. İsmail Serkan ÜNCÜ (İmza)

Süleyman Demirel Üniversitesi Elektronik Bilgisayar Eğitimi Anabilim Dalı

Yrd. Doç. Dr. Okan BİNGÖL (İmza)

Süleyman Demirel Üniversitesi Elektrik-Elektronik Mühendisliği Anabilim Dalı

Prof. Dr. Mehmet Cengiz KAYACAN

Enstitü Müdürü

Not: Bu tezde kullanılan özgün ve başka kaynaktan yapılan bildirilerin, çizelge, şekil ve fotoğrafların kaynak gösterilmeden kullanımı, 5846 sayılı Fikir ve Sanat Eserleri Kanunundaki hükümlere tabidir.

İÇİNDEKİLER

Sayfa

ÖZET i
ABSTRACT ii
TEŞEKKÜR iii
ŞEKİLLER DİZİNİ iv
ÇİZELGELER DİZİNİ v
SİMGELER VE KISALTMALAR DİZİNİ vi
1. GİRİŞ 1
2. KAYNAK ÖZETLERİ 3
3. MATERYAL VE YÖNTEM 5
3.1. Bilgi Güvenliği ve Bilgi Güvenliği Standartları 5
3.2. Proses Yaklaşımı 6
3.3. Diğer Yönetim Sistemleriyle Uyumluluk 9
3.4. Kapsam 10
3.5. Uygulama 10
3.6. Terimler ve Tarifler 10
3.6.1. Varlık 10
3.6.2. Kullanılabilirlik 11
3.6.3. Gizlilik 11
3.6.4. Bilgi güvenliği 11
3.6.5. Bilgi güvenliği olayı 12
3.6.6. Bilgi güvenliği ihlal olayı 12
3.6.7. Bilgi güvenliği yönetim sistemi (BGYS) 12
3.6.8. Bütünlük 12
3.6.9. Risk 13
3.6.10. Artık risk 13
3.6.11. Riskin kabulü 13
3.6.12. Risk analizi 13
3.6.13. Risk değerlendirme 13
3.6.14. Risk derecelendirme 13
3.6.15. Risk yöntemi 14

3.6.16. Risk işleme 14
3.7. Uygulanabilirlik Bildirgesi 14
3.8. Bilgi Güvenliği Standartları 14
3.8.1. ISO 27001 standardı 18
3.8.2. ISO 27002 standardı 20
3.8.3. ISO 27003 standardı 20
3.8.4. ISO 27004 standardı 21
3.8.5. ISO 27005 standardı 21
3.8.6. ISO 27006 standardı 22
3.9. TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) 23
3.9.1. Genel gereksinimler (Madde.4.1.) 24
3.9.2. BGYS'nin kurulması ve yönetilmesi (Madde.4.2.) 24
3.9.3. Dokümantasyon gereksinimleri (Madde.4.3.) 28
3.9.4. Yönetim sorumluluğu (Madde.5.) 29
3.9.5. BGYS iç denetimleri (Madde.6) 31
3.9.6. BGYS'yi Yönetimin Gözden Geçirmesi (Madde.7.) 31
3.9.7. BGYS iyileştirme (Madde.8.) 32
4. ARAŞTIRMA BULGULARI 34
4.1. Bilgi Güvenliği Probleminin Ortaya Konulması 34
4.2. Bilgi Güvenliği İçin İç Tetkik Uygulamalarının Yapılması 34
4.3. Geliştirilen Yazılımın Tanıtılması 35
4.4.Veri Tabanı Yönetim Sistemleri 35
4.5. Veri Tabanı Yöneticiliği 37
4.5.1. İlişkisel veri tabanı sistemleri 37
4.5.2. Veri tabanı dilleri 38
4.6. Veri Tabanı Sistemi "MySQL" 38
4.6.1. MySQL'in güçlü yanları 39
4.6.2. MySQL komutları 39
4.7. Programlama Dili "PHP" 40
4.7.1. PHP avantajları 41
4.8. Veri Tabanı Yazılım Geliştirme 43
4.8.1. Planlama aşaması 44

4.8.2. Riskleri tanımlama aşaması 47
4.8.3. Riskleri çözümleme ve değerlendirme aşaması 52
4.8.4. Uygulanabilirlik bildirgesi (EkA) uygulama aşaması 55
4.8.5. Risk yönetim süreci (kontrol et aşaması) 57
4.8.6. Önlem al aşaması 61
5. TARTIŞMA VE SONUÇ 63
6. KAYNAKLAR 65
EKLER 69
ÖZGEÇMİŞ 89

ÖZET

Yüksek Lisans Tezi

BİLGİ GÜVENLİĞİ STANDARTLARI VE KAMU KURUMLARI BİLGİ GÜVENLİĞİ İÇİN BİR MODEL ÖNERİSİ

Tuğba HAKLI

Süleyman Demirel Üniversitesi
Fen Bilimleri Enstitüsü
Elektronik-Bilgisayar Eğitimi Anabilim Dalı

Danışman: **Yrd. Doç. Dr. Ecir Uğur KÜÇÜKSİLLE**

Bilgi güvenliği yeni bir kavram olmamakla beraber, teknolojinin gelişmesi ile birlikte son yıllarda popülerliği ve bilinirliliği artmış durumdadır. Kuruluşların günümüzde en büyük zorluklarından ve aynı zamanda zorunluluklarından en önemlisi sahip olduğu bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlayabilmektir.

Bu tezde, Bilgi Güvenliğinin tanımı yapılmış, Bilgi Güvenliği Standartları incelenmiştir. Kamu kurumlarına, Bilgi Güvenliği Standartları uygulanması için bir model tasarlanmış ve tasarlanan model anlatılmıştır. Bu model önerisi için bir yazılım geliştirilmiştir. Bilgi Güvenliği Yönetim Sistemi'ni (ISO/IEC 27001 BGYS) kurup yönetirken yapılması gereken tüm adımlar sırasıyla yazılımda belirtilmiş ve açıklanmıştır. Kullanılan program doğrultusunda örnek çalışmalar yapılmıştır. Bu yazılım ile kamu kurumları ve şirketlere ISO/IEC 27001 BGYS'nin uygulanması için yol gösterici olunmuştur. Ayrıca bu tez çalışması ile ilk defa çalışmaların bilgisayar ortamında kayıt altına alınması imkanı yaratılmıştır.

Tez konusu ile ilgili literatür taramasına ek olarak, danışmanlık şirketi ziyaret edilerek gerekli bilgiler toplanmış ve ISO/IEC 27001 BGYS eğitimine katılım sağlanmıştır.

Anahtar Kelimeler: Bilgi güvenliği, ISO/IEC 27001 BGYS (Bilgi güvenliği yönetim sistemi)

2012, 89 sayfa

ABSTRACT

M.Sc. Thesis

INFORMATION SECURITY STANDARDS AND A NEW MODEL FOR PUBLIC INSTITUTIONS OF INFORMATION SECURITY

Tuğba HAKLI

Süleyman Demirel University
Graduate School of Applied and Natural Sciences
Electronic and Computer Education Department

Supervisor: Yrd. Doç. Dr. Ecir Uğur KÜÇÜKSİLLE

Information security concept, in fact, isn't so new but in recent years with the development of the technology it has increased its popularity and the recognition. One of the biggest difficulties and the neccessilies of business organizations is to provide secrecy, integrity and accesibility of business information and data.

In this thesis, information security is defined, the information security standards were examined. Guiding the implementation of information security standards for public institutions designed model, a model designed and explained. The model is a software developed for the propasal. Information Security Management System (ISO / IEC 27001 ISMS), respectively, set up and manage the software and explained all the steps to be done. Representative studies, performed using the program. With this software in public institutions and companies, ISO / IEC 27001 ISMS been carried out to provide guidance to the implementation. Also in this thesis will be recorded with the computer environment, enabling works for the first time.

In addition to literature review related to the study, collected the necessary information by visiting the consulting firm and ISO / IEC 27001 ISMS participated in the training.

Key Words: Information Security, ISO/IEC 27001 ISMS (Information Security Management System)

2012, 89 pages

TEŞEKKÜR

Tez çalışmam süresince tecrübe, bilgi ve yardımlarını esirgemeyen Danışmanım Sayın Yrd. Doç. Dr. Ecir Uğur KÜÇÜKSİLLE'ye sonsuz teşekkürlerimi ve saygılarımı sunarım.

Çalışmalarım sırasında bilgisine başvurduğum Sayın Uzman Sertaç Selim SARICA'ya teşekkür ederim.

2649-YL-11 No`lu Proje ile tezimi maddi olarak destekleyen Süleyman Demirel Üniversitesi Bilimsel Araştırma Projeleri Yönetim Birimi Başkanlığı'na teşekkür ederim.

Tez çalışmalarım esnasında manevi desteklerini hissettiğim aileme, her zaman yanımda olan, desteğini benden hiç esirgemeyen değerli eşim Zafer HAKLI'ya, motivasyon kaynağı oğlum Yağız HAKLI'ya sabır ve anlayışları için teşekkür ederim.

Tuğba HAKLI
ISPARTA, 2012

ŞEKİLLER DİZİNİ

Şekil 3.1. BGYS proseslerine uygulanan PUKÖ modeli 8
Şekil 3.2. PÜKO döngüsü ve BGYS adımları 18
Şekil 3.3. ISO 27001 döngüsünün planlanması aşamasında ISO 27002 kontrollerinin seçilmesi 19
Şekil 3.4. ISO 27001 döngüsü ve ISO 27002 kontrolleri 20
Şekil 3.5. ISO 27001 sürecinin aşamaları 24
Şekil 4.1. MySQL-istemci ilişkisi 39
Şekil 4.2. PHP-sunucu ilişkisi 41
Şekil 4.3. PHP ve java script karşılaştırılması 42
Şekil 4.4 Program menülerinin gösterimi 43
Şekil 4.5. Programın genel görüntüsü 44
Şekil 4.6. Bölüm girişi formu 44
Şekil 4.7. Personel girişi formu 45
Şekil 4.8. Kontrol görev girişi formu 45
Şekil 4.9. Kontrol görevi atama formu 46
Şekil 4.10. BGYS kapsam dokümanı formu 47
Şekil 4.11. Risk değerlendirme formu 48
Şekil 4.12. BGYS varlık envanteri formu 49
Şekil 4.13. Varlıkların kullanım politikası formu 51
Şekil 4.14. Tehdit ve açık tablosu formu 52
Şekil 4.15. Risk değerlendirme ve derecelendirme formu 53
Şekil 4.16. Kontrol ve amaçlarını belirleme formu 55
Şekil 4.17. Uygulanabilirlik bildirgesi (EkA) formu 57
Şekil 4.18. Risk yönetim süreci formu 59
Şekil 4.19. Kontrol etkinlikleri ölçülmesi formu 60
Şekil 4.20. Politika formu 60
Şekil 4.21. Prosedür formu 61
Şekil 4.22. Kişisel risk belirleme formu 61
Şekil 4.23. BGYS etkinlik ve performansı etkileyecek olayları kaydetme formu 62

ÇİZELGELER DİZİNİ

Çizelge 3.1. BGYS proseslerine uygulanan PUKÖ modelinin açıklanması..... 9
Çizelge 3.2. Risk kavramları ve tanımları..... 22

SİMGELER VE KISALTMALAR DİZİNİ

BGYS	Bilgi güvenliği yönetim sistemi
BSI	British standards institute
COBIT	Control objectives for information and related technology
DBMS	DataBase management system
DoD	US department of defense
IBM	International business machines
IEC	International electrotechnical commission
ISACF	System audit and control foundation
ISMS	Information security management system
ISO	International standarts organization
ITIL	Information technology infrastructure library
KYS	Kalite yönetim sistemi
MySQL	My structured query language
OECD	Organisation for economic co-operation and development
PUKÖ	Planla- uygula- kontrol Et- önlem Al
PHP	Hypertext preprocessor
RDBMS	Relational dataBase management system
TCSEC	Trusted computer system evaluation criteria
TPEP	Trusted product evaluation program
TSE	Türk standartları enstitüsü

1. GİRİŞ

Günümüzde kamu kurumları ve şirketler çalışmalarını devam ettirebilmek için bilgi kullanımına önem vermişlerdir. Zaman ilerledikçe bilginin kullanımı artmış, aynı zamanda bilginin bir yerden başka bir yere gönderilme ihtiyacı ortaya çıkmıştır. Bu sebepten bilginin güvenli bir şekilde korunmasna önem verilmeye başlanmıştır. Bilgiyi açıklarsak; kurum ve şirket için anlamı olan tüm verilerdir. Bilgi güvenliği ise, bilginin bütünlüğü, ulaşabilirliği ve gizliliğinin korunmasıdır.

Her birey bilgi sistemleri üzerinden hizmet alırken veya hizmet sunarken kurumsal bilgi varlıklarını kullanmaktadır. Bu hizmetler kurumsal anlamda bir hizmet alımı olabileceği gibi, bankacılık işlemleri veya bir kurum içerisinde yapılan bireysel işlemler de olabilir. Burada kişilerin bilgi güvenliği önem arz ederken, bundan daha önemlisi, kişilerin güvenliğini doğrudan etkileyen kurumsal bilgi güvenliğidir. (Vural, 2007).

Bu tez çalışmasında, etkin bir bilgi güvenliği oluşturabilmek için gerekli olan, güvenlik süreçleri ve kamu kurumları için fayda sağlayacak Bilgi Güvenliği standartları incelenerek, incelenen standartların neden kullanılması gerektiği belirtilecektir. Kamu kurumlarının bilgi güvenliği için neler yapması gerektiği, hangi programları kullanması gerektiği tavsiye edilecek ve kamu kurumlarında bilişim teknolojileri güvenlik sistemi kurulması için hareket planı önerilecektir.

Ayrıca, en uygun güvenliği sağlamak için Bilgi Güvenliği standartları çerçevesinde kamu kurumları için model önerisi yapılmaya çalışılacaktır. Kamu kurumları model önerisini kolayca uygulayarak zamandan tasarruf sağlayabileceklerdir.

Yapılan model önerisi ile, kuruluşun sahip olduğu bilgi varlıklarının ve değerlerinin farkına varabilmesi hedeflenmiştir. Kuruluş, oluşturacağı ISO 27001 Bilgi Güvenliği Yönetim Sisteminin kontrolleri ve koruma metodlarını belirleyerek ve uygulayarak, sahip olduğu bilgi varlıklarının, sistemli bir şekilde korunmasını sağlayacaktır. Bu sayede; çalışanlarının motivasyonunu yükselterek, başta tedarikçileri olmak üzere,

hizmet verdiği kurum ve kuruluşların güvenini kazanarak, verimlilik ve saygınlık artışını sağlayacaktır.

Günümüzde, yapılan çalışmaların tüm aşama ve bölümlerini gösteren Türkçe kaynak çok az olmakla beraber, Bilgi Güvenliği Yönetim Sistemi bilgileri ve uygulamaları sadece danışmanlık şirketleri tarafından ücretler karşılığı verilmektedir. Yapılan bu program sayesinde Bilgi Güvenliği Yönetim Sistemini kurarken ve bu sitemi geliştirirken kamu kurum ve şirketlerin zaman ve kaynak ihtiyaçlarını düşüreceği hedeflenmektedir.

2. KAYNAK ÖZETLERİ

Erkan (2006) tarafından yapılan çalışmada, Bilgi Güvenliği Yönetim Sistemi süreçlerinin otomasyonunu konu alır. ISO/IEC 27001:2005 ve ISO/IEC 17799:2005 standartlarına uygun olarak dokümante edilmiş bir BGYS için gerekli faaliyetlerin mümkün olduğunca otomatikleştirilmesi kurumlara yardım olacağı düşünülmüştür.

Çetinkaya (2008) tarafından yapılan çalışmada, kurumların bilgi güvenliğini hangi başarılılıkta uyguladıklarını saptamak için, ISO/IEC 27001:2007 Bilgi Güvenliği Yönetim Sistemi prensiplerinin kullanıldığı web tabanlı bir test aracı geliştirilmiştir. Bu test aracı, kurumlardaki bilgi güvenliği altyapısının zaman içindeki durumlarının izlenmesi amacıyla da kullanılabilir. Test aracı, popüler bir açık kaynak programlama dili olan PHP ile geliştirilmiş; veri tabanı yönetim sistemi olarak ise yine açık kaynak mimarisine sahip MySQL kullanılmıştır.

Mete (2010) tarafından yapılan çalışmada, araştırma problemi; kuruluşları bünyesinde bilgi güvenliği kültürünü oluşturacak ISO/IEC 27001 BGYS Standardını, kurmak ve yönetmek isteyen Bilgi İşlem Merkezi Yöneticileri'ne Türkçe bir rehber hazırlamak olarak ifade edilebilir. Bu faaliyetlerin tüm aşamalarını ulaşılabilir manada tek bir belgelerin az olması ve kuruluşların BGYS kurmak ve işletmek için zaman ve kaynak ihtiyaçlarını düşüreceği amaçlanan çalışmada sistemi kurup yönetirken yapılması gereken tüm adımlar sırasıyla anlatılmıştır.

Bingöl (2010) tarafından yapılan çalışmada, sözkonusu BGYS faaliyetini tamamen Açık Kaynak Kodlu yazılımları tekrar BGYS kapsamında düzenleyerek BGYS sürecinin denetimini çok düşük maliyetle sağlanabileceğini belirtmiştir. BGYS kurmak ve yönetmek isteyen bir işletmenin sürecin yönetimi esnasında ne tür bir sisteme ihtiyaç duyduğunu dikkate almıştır.

Tok (2010) tarafından yapılan çalışmada, “Kamu Kurumları İçin Bir Bilgi Güvenliği Yönetişim Modeli” adındaki bu çalışmada; Türkiye için kamu kurum ve kuruluşlarında kullanılacak yeni Bilgi Güvenliği Yönetişimi Modeli önerilmiştir. Öncelikle tek bir kamu kuruluşunda bu modelin nasıl uygulanacağı açıklanmıştır. Ayrıca modelin tek bir kurum ya da kuruluşun da kullanılması için tasarlanmasının yeterli olmayacağı düşüncesinden hareketle, önerilen modelde kurum ve kuruluşların birbirleriyle etkileşimini de içeren yeni bir yapı ortaya konulmuştur. Bu sistemin işleyebilmesi için de tüm kamu kurum ve kuruluşları ile birlikte özel şirketleri de içeren bir Bilgi Güvenliği Stratejisi Kurulu (BGSK)’nun kurulmasının gerekliliğine vurgu yapılarak, bilgi güvenliği konusunun yasal dayanaklarla desteklenmesi önerilmiştir.

Tan (2011) tarafından yapılan çalışmada, kurum ve kuruluşların bilgi sistemi güvenliği konusu ele alınmıştır. Internet kullanımı ve bilgi sistemlerine dayalı iş modellerinin artışı ile bilgi sistemi güvenliği önemli bir hale gelmiştir. Temel güvenlik kavramları ile kurumsal bilgi sistemleri güvenliği konuları ele alınmıştır. Bir güvenlik mimarisi önerebilmek için bir uygulama geliştirilmiştir.

Kandemirli (2011) tarafından yapılan çalışmada, bilgi teknolojileri güvenlik yönetimi konusunda dünyada en yaygın uygulama alanı bulan üç standart incelenmiştir. Bu üç standarttan birincisi olan ISO 27001 standardı, ISO 27002 en iyi uygulama standardı çerçevesinde, bilgi teknolojileri güvenlik yönetimi için çok iyi sınıflandırılmış, taktik ve operasyonel seviyede işleyen ve kolay uygulanabilen bir standart iken, CobIT standardının bilgi teknolojileri yönetimine stratejik açıdan bakan ve temelini yönetim kararları, yönetilebilirlik ve denetlenebilirlik üzerine kuran geniş kapsamlı bir yapısı vardır ve bilgi güvenliğini CobIT Security Baseline yani CobIT Güvenlik Temel Çizgisi çerçevesinde desteklenmiştir.

3. MATERYAL VE YÖNTEM

Tez çalışmasında, bilgi güvenliği standartları kullanılacaktır. Bilgi güvenliği standartları rapor haline getirilecek ve bu standartlar çerçevesinde bir model önerisi sunulacaktır. Model önerisi, geliştirilecek bir uygulama yazılımı ile desteklenecektir.

3.1. Bilgi Güvenliği ve Bilgi Güvenliği Standartları

Bilgi güvenliği; bilginin bir varlık olarak hasarlardan korunması, doğru teknolojinin, doğru amaçla ve doğru şekilde kullanılarak bilginin her türlü ortamda, istenmeyen kişiler tarafından elde edilmesini önlemektir. Başka bir tanımla bilgi güvenliği; elektronik ortamlarda verilerin veya bilgilerin saklanması ve taşınması esnasında bilgilerin bütünlüğü bozulmadan, izinsiz erişimlerden korunması için, güvenli bir bilgi işleme platformu oluşturma çabalarının tümüdür. Bunun sağlanması için, uygun güvenlik politikasının belirlenmesi ve uygulanması gereklidir. Bu politikalar; faaliyetlerin sorgulanması, erişimlerin izlenmesi, kayıtlardaki değişikliklerin tutulup değerlendirilmesi ve silme işlemlerinin sınırlandırılması olarak belirlenebilir (http://tr.wikipedia.org).

Ayrıca, bilginin güvenli olmasını sağlamak için ulaşılması gereken amaçlar genel olarak, korunmakta olan bilginin gizliliği, bütünlüğü, ve ulaşılabilirliği olarak ifade edilebilir (Schlienger, Teufel, 2001).

Bilgi Güvenliği uygulamasında, bilgisayarda şifre korumalı ekran koruyucu kullanılması, bilgisayar başından uzun süreliğine ayrı kalındığında sistemden çıkılması, kullanılan şifrelerin tahmininin zor olacak şekilde belirlenmesi, bu şifrelerin gizli tutulması ve belirli aralıklarla değiştirilmesi, virüs koruma programlarının kurulu olması, bu programların ve işletim sistemi hizmet paketlerinin ve hata düzeltme ve güncellemelerinin düzenli aralıklarla yapılması, disk paylaşımlarında dikkatli olunması, internet üzerinden indirilen veya e-posta ile gelen dosyalara dikkat edilmesi, önemli belgelerin şifreli olarak saklanması, gizli veya

önemli bilgilerin e-posta, güvenlik sertifikasız siteler gibi güvenli olmayan yollarla gönderilmemesi, kullanılmadığı zaman internet erişiminin kapatılması, önemli bilgi ve belgelerin düzenli aralıklarla yedeklerinin alınması kişisel bilgisayar güvenliği için önemli olan ve yapılması gereken önlemlerden bazılarıdır (http://tr.wikipedia.org).

Bilgi Güvenliği standardı, bir Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) (Information Security Management System - ISMS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır (Tan, 2011).

Bir kuruluş için BGYS'nin benimsenmesi stratejik bir karar olmalıdır. Bir kuruluşun BGYS tasarımı ve gerçekleştirmesi, ihtiyaçları ve amaçları, güvenlik gereksinimleri, kullanılan prosesler ve kuruluşun büyüklüğü ve yapısından etkilenir. Bunların ve destekleyici sistemlerinin zaman içinde değişmesi beklenir. Bir BGYS gerçekleştirmesinin kuruluşun ihtiyaçlarına göre ölçeklenmesi beklenir (Örneğin, basit durumlar basit BGYS çözümleri gerektirir.). Bu standart, uyumluluğu değerlendirmek için ilgili iç ve dış taraflarca kullanılabilir (www.iso.org).

3.2. Proses Yaklaşımı

Bu standart, bir kuruluşun Bilgi Güvenliği Yönetim Sistemi'ni kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir proses yaklaşımını benimser. Bir kuruluşun, etkin bir şekilde işlev görmek için, birçok faaliyetini tanımlaması ve yönetmesi gerekir. Kaynakları kullanan ve girdilerin çıktılara dönüştürülebilmesi için yönetilen her faaliyet, bir proses olarak düşünebilir. Çoğunlukla bir prosesin çıktısı doğrudan bunu izleyen diğer prosesin girdisini oluşturur (TS ISO/IEC 27001, 2006, s.2.).

Bir kuruluş içerisinde, tanımları ve bunların etkileşimi ve yönetimleriyle birlikte proseslerin oluşturduğu bir sistem uygulaması "proses yaklaşımı" olarak

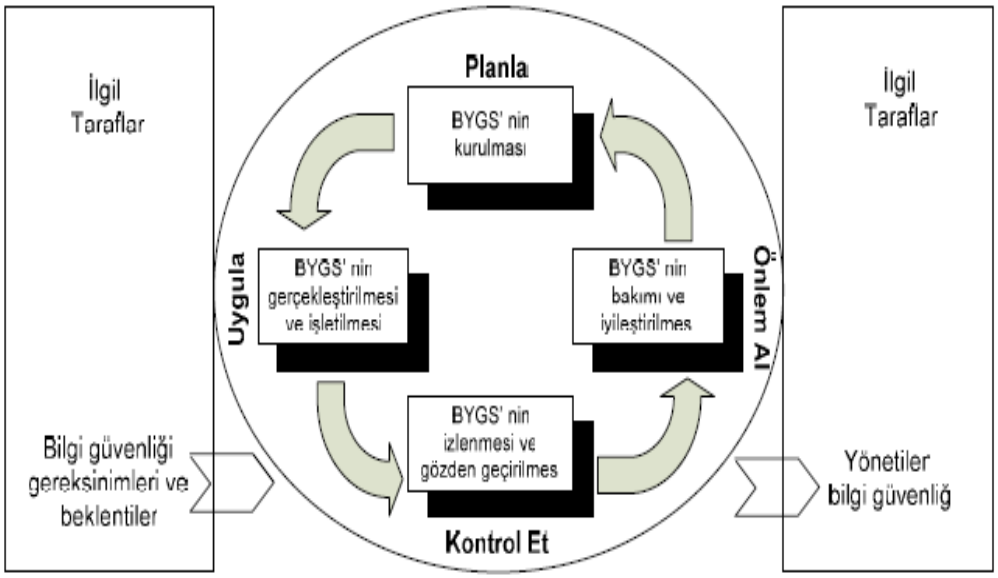
tanımlanabilir. Bu standartta sunulan bilgi güvenliği yönetimi proses yaklaşımı, kullanıcılarını aşağıdakilerin öneminin vurgulanmasına özendirir (OECD, 2002):

a) İş bilgi güvenliği gereksinimlerini ve bilgi güvenliği için, politika ve amaçların belirlenmesi ihtiyacını anlamak,
b) Kuruluşun tüm iş risklerini yönetmek bağlamında kuruluşun bilgi güvenliği risklerini yönetmek için kontrolleri gerçekleştirmek ve işletmek,
c) BGYS'nin performansı ve etkinliğini izlemek ve gözden geçirmek,
d) Nesnel ölçmeye dayalı olarak sürekli iyileştirmek (Doğantimur, 2008).

Bu standart, tüm BGS proseslerini yapılandırmaya uygulanan "Planla- Uygula- Kontrol Et- Önlem Al" (PUKÖ) modelini benimser. Şekil 3.1., bir BGYS'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve prosesler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını nasıl ürettiğini gösterir. Şekil 3.1 ayrıca, Madde4, Madde5, Madde6, Madde7, Madde8'de sunulan proseslerdeki bağlantıları da gösterir. PUKÖ modelinin benimsenmesi, bilgi sistemleri ve ağları güvenliğini yöneten OECD Kılavuzları'nda (OECD, 2002) belirlenmiş olan prensipleri de yansıtır. Bu standart, risk değerlendirme, güvenlik tasarımı ve gerçekleştirme, güvenlik yönetimi ve yeniden değerlendirmeyi yöneten bu kılavuzlardaki prensipleri gerçekleştirmek için sağlam bir model sağlar (Şekil 3.1.) (TS ISO/IEC 27001, 2006, s.2.).

*Örnek1:*Bir kuruluşta, bilgi güvenliği ihlallerinin ciddi finansal hasarlara neden olmaması veya kuruluşta rahatsızlığa yol açamaması bir gereksinim olabilir.

Örnek2: Ciddi bir durum oluştuğunda (örneğin, bir kuruluşun e-İş web sitesinin çökertilmesi) etkiyi en aza indirmek için, uygun proseslerde yeterli eğitime sahip kişilerin olmasının gerekliliği bir beklenti olabilir.



Şekil 3.1. BGYS proseslerine uygulanan PUKÖ modeli

Çizelge 3.1. BGYS proseslerine uygulanan PUKÖ modelinin açıklanması

Planla (BGYS'nin kurulması)	Sonuçları kuruluşun genel politikaları ve amaçlarına göre dağıtmak için, risklerin yönetimi ve bilgi güvenliğinin geliştirilmesiyle ilgili BGYS politikası, amaçlar, hedefler, prosesler ve prosedürlerin kurulması.
Uygula(BGYS'nin gerçekleştirilmesi ve işletilmesi)	BGYS politikası, kontroller, prosesler ve prosedürlerin gerçekleştirilip işletilmesi
Kontrol Et (BGYS'nin izlenmesi ve gözden geçirilmesi)	BGYS politikası, amaçlar ve kullanım deneyimlerine göre proses performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesi.
Önlem Al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi)	BGYS'nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici faaliyetlerinin gerçekleştirilmesi.

BGYS proseslerine uygulanan PUKÖ modeli ayrıntılarıyla anlatılmıştır (Çizelge 3.1) (TS ISO/IEC 27001, 2006, s.2.).

3.3. Diğer Yönetim Sistemleriyle Uyumluluk

Bu standart, ilgili yönetim standartlarıyla tutarlı ve tümleşik gerçekleştirme ve işletimi desteklemek için ISO 9001 ve ISO 14001 ile uyumludur. Bu nedenle, uygun şekilde tasarlanmış bir yönetim sistemi tüm bu standartların gereksinimlerini karşılayabilir. Bu standart, bir kuruluşun BGYS'sini ilgili yönetim sistemi gereksinimleriyle uyumlu yapabilmesi ya da bütünleştirebilmesi için tasarlanmıştır (TS ISO/IEC 27001, 2006, s.2.).

3.4. Kapsam

Bu standart, tüm kuruluş türlerini kapsar. Bu standart dokümante edilmiş bir BGYS'yi kuruluşun tüm ticari riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsar. Bağımsız kuruluşların ya da tarafların ihtiyaçlarına göre özelleştirilmiş güvenlik kontrollerinin gerçekleştirilmesi için gereksinimleri belirtir (Perendi, 2008).

BGYS, bilgi varlıklarını koruyan ve ilgili taraflara güven veren yeterli ve orantılı güvenlik kontrollerini sağlamak için tasarlanmıştır. Bu standartta "iş" terimi geniş anlamda kuruluşun varlık amaçlarının temeli olan etkinlikler anlamına gelmektedir. ISO/IEC 17999, kontroller tasarlanırken kullanabilecek gerçekleştirme kılavuzu sağlar (Perendi, 2008).

3.5. Uygulama

Bu standartla ortaya konulan gereksinimler geneldir ve türü, büyüklüğü ve doğasından bağımsız olarak tüm kuruluşlara uygulanabilir olması amaçlanmaktadır. Bir kuruluş bu standarda uyumluluk iddiasında bulunduğunda Madde4, Madde5, Madde6, Madde7, Madde8'de belirlenen herhangi bir gereksinimin dışarıda bırakılması kabul edilebilir değildir (TS ISO/IEC 27001, 2006, s.2.).

3.6. Terimler ve Tarifler

Bu standardın amacı bakımından aşağıdaki terimler ve tarifler uygulanır.

3.6.1. Varlık

Kuruluş için değeri olan herhangi bir şey varlık olarak ifade edilir (ISO/IEC 13335-1:2004).

3.6.2. Kullanılabilirlik

Yetkili bir varlık tarafından talep edildiğinde erişilebilir ve kullanılabilir olma özelliğidir (ISO/IEC 13335-1:2004).

Kullanılabilirlik demek, bilginin yetkili kişilerce erişilebilir olmasının yanında ulaşılabilir de olması demektir. Aynı zamanda bilgi, kullanıcılar tarafından zamanında ulaşılabilmeli, ve ulaşım sırasındaki kaynak paylaşımına izin verilen şekilde olmalıdır. Kullanılabilirliğe yönelik saldırı türleri engelleme veya değişiklik yapma ve üretim olabilir (Özkan, 2004).

3.6.3. Gizlilik

Bilginin yetkisiz kişiler, varlıklar ya da proseslere kullanılabilir yapılmama ya da açıklanmama özelliğidir (ISO/IEC 13335-1:2004).

Başa bir tanımla gizlilik, bilgiye sadece izni olan kişilerin, izin verilen yollarla erişimidir. Buradaki erişim, üzerinde değişiklik yapmaya değil sadece okumaya yönelik bir erişimdir. Bazı durumlarda bir bilginin varlığının bilgisi dahi kısıtlama altında olabilir. Yani yetkisi olmayan kişilerin herhangi bir bilginin varlığının bilgisine erişimleri dahi gizlilik amacının bir ihlali olabilir. Bu amacı ihlal etmeye yönelik saldırı türü izinsiz erişimdir (Özkan, 2004).

3.6.4. Bilgi güvenliği

Bilginin gizliliği, bütünlüğü, ulaşılabilirliği ve kullanılabilirliğinin korunmasıdır. Ek olarak, doğruluk, açıklanabilirlik, inkar edememe ve güvenirlik gibi diğer özellikleri de kapsar (ISO/IEC 17799:2005).

3.6.5. Bilgi güvenliği olayı

Olası bir bilgi güvenliği politikası açığı, koruyucuların başarısızlığı ya da güvenlikle ilgili olabilecek önceden bilinmeyen bir durumu belirten bir sistem, hizmet ya da ağ durumunun tanımlanan bir şekilde ortaya çıkışını ifade eder (ISO/IEC 18044:2004).

3.6.6. Bilgi güvenliği ihlal olayı

İş operasyonlarını tehlikeye atma ve bilgi güvenliğini tehdit etme olasılığı yüksek olan tek ya da bir dizi istenmeyen ya da beklenmeyen bilgi güvenliği olayını ifade eder (ISO/IEC 18044:2004).

3.6.7. Bilgi güvenliği yönetim sistemi (BGYS)

Bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası. Yönetim sistemi, kurumsal yapıyı, politikaları, planlama faaliyetlerini, sorumlulukları, uygulamaları, prosedürleri, prosesleri ve kaynakları içerir. (TS ISO/IEC 27001, 2006, s.2.)

3.6.8. Bütünlük

Varlıkların doğruluğunu ve tamlığını koruma özelliğidir (ISO/IEC 13335-1:2004).

Özel durumlar için bilginin bütünlüğü, özel şeyleri ifade etmek için kullanılabilir. Bütünlük ile anlatılmak istenen, bilginin her şeyden önce doğru ve kesin oluşudur. Bilgi aynı zamanda değiştirilemez olmalı, bir başka deyişle, sadece izin verilen yani yetkisi olan kişilerce ve sadece izin verilen yollarla değiştirilebilmelidir. Bilginin anlamlı ve tutarlı oluşu, kendi içinde çelişik olmaması da bilgi bütünlüğündeki amaçlar olarak sıralanabilir. Bilginin bütünlüğünü ihlale yönelik saldırı türleri zarar verme veya engelleme, değişiklik yapma ve üretim olabilir (Gökalp, 2003).

3.6.9. Risk

Olayların, tehlikelerin sonuçlarıdır. Başka bir tanımla; zarara ve kayba neden olacak bir olayın bilgi varlığı üzerinde gerçekleşme olasılığı olarak tarif edilebilir (Şahinaslan, Kandemir, Kantürk, 2011).

3.6.10. Artık risk

Risk işlemeden sonra kalan risktir (ISO/IEC Guide 73).

3.6.11. Riskin kabulü

Bir riski kabul etme kararıdır (ISO/IEC Guide 73).

3.6.12. Risk analizi

Kaynakları belirlemek ve riski tahmin etmek amacıyla bilginin sistematik kullanımıdır (ISO/IEC Guide 73).

3.6.13. Risk değerlendirme

Risk analizi ve risk derecelendirilmesini kapsayan tüm prosestir (ISO/IEC Guide 73).

Tanımlanan varlıklar için tehditler, açıklıklar ve risk değerleri ve hesaplamaların yapıldığı bölümdür (Şahinaslan, Kandemir, Kantürk, 2011).

3.6.14. Risk derecelendirme

Riskin önemini tayin etmek amacıyla tahmin edilen riskin, verilen risk kriterleri ile karşılaştırılması prosesidir (ISO/IEC Guide 73).

3.6.15. Risk yöntemi

Bir kuruluşun risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetleridir (ISO/IEC Guide 73).

Risk yönetim çerçevesi oluşturduktan sonra mevcut riskler tanımlanmalı ve tanımlanan risklere ilişkin aksiyon planları oluşturulmalı planların uygulanabilirliği ve sonuçları izlenmeli, değerlendirmelidir (Şahinaslan, Kandemir, Kantürk, 2011).

3.6.16. Risk işleme

Riski değiştirmek için alınması gereken önlemlerin seçilmesi ve uygulanması prosesidir (ISO/IEC Guide 73). Ayrıca var olan risklerin minimize edilmesi için oluşturulmuş prosesler bütünü olarak ifade edilir (Şahinaslan, Kandemir, Kantürk, 2011).

3.7. Uygulanabilirlik Bildirgesi

Kuruluşun BGYS'si ile ilgili ve uygulanabilir kontrol amaçlarını ve kontrolleri açıklayan dokümante edilmiş bildirgedir (EkA).

Kontrol amaçları ve kontroller risk değerlendirme ve risk işleme proseslerinin sonuçları ve çıkarımlarını yasal ve düzenleyici gereksinimleri, anlaşma ve yükümlülüklerini ve kuruluşun bilgi güvenliği için iş gereksinimlerini temel alır (TS ISO/IEC 27001, 2006, s.2.)

3.8. Bilgi Güvenliği Standartları

Bilgi ve iletişimin büyük bir önem kazandığı dünyada şirketlerin verimliliklerini artırabilmeleri, pazarda etkin rol oynamaları, müşteri ve pazar paylarını artırmaları ve rekabet üstünlüğü sağlayabilmeleri için bilgi edinme ve bilgileri işleme konusunda gerekli teknolojileri kullanmaları, süreçlerini bilgi yönetimine göre

şekillendirmeleri ve insan kaynaklarını bu yönde yetiştirmeleri gerekmektedir. Geleneksel iş dünyasında IT sistemlerine gittikçe artan bağımlılık, bilişim dünyasının sunduğu olanaklar ve tüm bunların getirdiği iş fırsatları ve riskler ister istemez "bilgi" kavramının da yönetimsel bir yaklaşımla stratejik seviyede ele alınmasına ve kurumları bu alanda sistem yaklaşımları kurmaya zorlamıştır (Sevgi, 2008).

Bilgi Güvenliği Yönetim Sistemi (BGYS), kurumun/şirketin önemli bilgilerini yönetebilmek amacıyla benimsenen sistemli bir yaklaşımdır. Bu sistemin temel amacı hassas bilginin korunmasıdır. Bu sistem çalışanları, iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini kapsar (Önel, Dinçkan, 2007).

Tarihsel gelişimi içinde bilgi sistemlerinin güvenliği ve sonrasında Bilgi Güvenliği konusunda çok fazla akademik araştırma yapılmış, makaleler yayınlanmış ve ticari ürünler ortaya çıkartılmıştır (Çetinkaya, 2008).

Bilgisayar sistemlerinin güvenliği konusunda yapılan ilk çalışmaların IBM ve A.B.D. Savunma Bakanlığı (US Department of Defense –DoD-) kaynaklı olduğu görülmektedir. 1981 yılında Adalet Bakanlığı (Department of Defense, DoD) National Security Agency'e bilgisayar güvenliğinin sorumluluğunu vermiş ve DoD Computer Security Center kurulmuştur, daha sonra ismi değiştirilerek NCSC (National Computer Security Center) olmuştur. NCSC daha sonra "Orange Book" olarak da bilinen ilk DoD Trusted Computer System Evaluation Criteria (TCSEC) kriterini yayınlamıştır. 1985'te DoS Standart, DOD 5200.28-STD adı altında tekrar yayınlanarak TCSEC kriterinin temelini oluşturmuştur. TCSEC standardı güvenliğin devamlı arttığı bir sınıflandırma yapısına sahiptir. Her seviye, hem bir önceki seviyenin guvenlik seviyesine hemde bazı ek özelliklere sahiptir (DoD 5000.2-R, 2006).

Üreticilerin ürünleri bu TCSEC kriteri çerçevesinde Trusted Product Evaluation Program (TPEP) programıyla sınıflandırılır ve belli sınıf kodlarını alırlar. TPEP programıyla test edilen ve sonuçlanan ürünler EPL (Evaluation Product List)

listesinde yayınlanırlar. TPEP programının amacı güvenli bilgisayar ürününün geliştirilmesini teşvik etmektir (Çetinkaya, 2008).

DoD çalışmaları daha sonra Bilgi Güvenliği'nin daha fazla ön plana çıktığı 1990'larda, çeşitli firma temelli ya da uluslararası standartlar şekline gelmiştir (DoD 5200.1-I, 1995).

İngiltere Standartlar Enstitüsü'nün (British Standards Institute (BSI)) yaptığı çalışmalarla, "Bilgi Güvenliği Yönetim Sistemi" deyimi ilk kez 1998 yılında tarafından yayınlanan BS 7799-2 standardında kullanılmıştır. Daha sonra bu standart Uluslararası Standartlar Kurumu ISO tarafından kabul edilmiş ve ISO/IEC 27001:2005 olarak yayınlanmıştır. BSI tarafından yayınlanan bir diğer standart BS 7799-1 ise Bilgi Güvenliği'nin sağlanmasında kullanılacak kontrollerden bahsetmektedir. Bu da yine ISO tarafından kabul edilmiş ve ISO/IEC 27002:2005 olarak yayınlanmıstır. ISO/IEC 27002:2005 bu standardın Temmuz 2007'den itibaren kullanılan ismidir, bu tarihe kadar standart ISO/IEC 17799:2005 olarak adlandırılıyordu. Bilgi güvenliği yönetimi konusunda en yaygın olarak kullanılan standart, "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi için Uygulama Prensipleri" standardıdır. Bu standart, işletmeler içerisinde Bilgi Güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar. ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS'nin belgelendirmesi icin "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardı kullanılmaktadır. Bu standart, dökümante edilmiş bir BGYS'ni kurumun tüm iş riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsamaktadır. İş risklerini karşılamak amacıyla ISO/IEC 27002:2005'te ortaya konan kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği ISO/IEC 27001:2005'te belirlenmektedir (http://www.bsi-turkey.com/).

Her iki standardın Türkçe hali TSE tarafından sırasıyla TS ISO/IEC 17799:2005 ve TSISO/IEC 27001:2005 isimleri ile yayınlanmıştır. Söz konusu standardın

belgelendirmesi konusunda TSE tarafından "TS 13268-1 BGYS Belgelendirmesi için Gereksinimler ve Hazırlık Kılavuzu" yayınlanmıştır. ISO/IEC 27001 ve ISO/IEC 27002 standartları BGYS konusunda en temel başvuru kaynaklarıdır. Bu iki standart doğrudan Bilgi Güvenliği konusunu ele alırlar. Teknik ve teknoloji bağımlı standartlar değildirler. Belli bir ürün veya bilgi teknolojisi ile ilgilenmezler. Hatta bilgi teknolojileri güvenliği dahi bu standartların icerisinde yer almaz. Tek ilgi alanı vardır, o da Bilgi Güvenliği'dir. Diğer taraftan geliştirilmiş başka standart ve metodojilerde olmuştur. Bunlardan biri de "Control Objectives for Information and Related Technology – COBIT"dir. COBIT, bilgi teknolojileri süreçlerini iş süreçlerinin destekçisi olarak görür ve aralarındaki ilişkileri birebir ortaya koyar. Bu sayede bilgi teknolojileri kaynaklarının iş stratejileri doğrultusunda etkin biçimde kullanılmasına olanak sağlar (Çetinkaya, 2008).

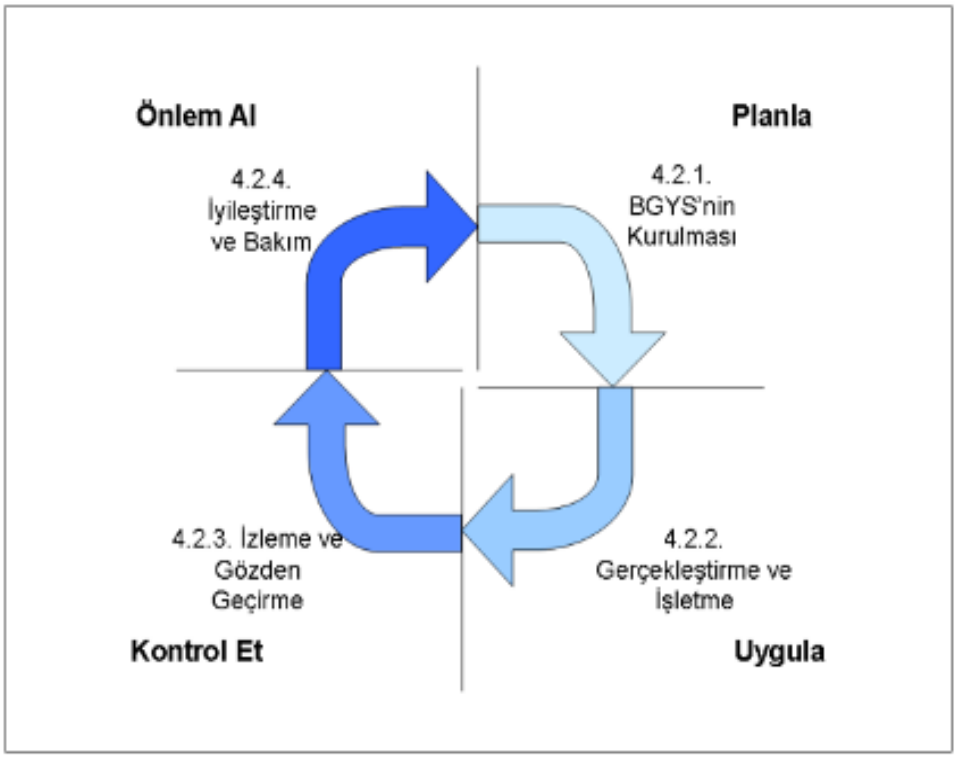
COBIT ilk olarak 1996 yılında Information System Audit and Control Foundation (ISACF) tarafından yayımlanmıştır. Bu metodoloji birçok standardı içinde barındırdığı ve diğer metodolojilerle uyum içinde olduğundan şirketlerin ilişki içinde oldukları iş ortakları, müşteri ve düzenleyici kurumlar tarafından talep edilen bilgi teknolojileri kontrol süreçleri sertifikasyonları denetimlerine hazır olmaya yardımcı olur ve böylece hızlı bir sertifikasyona olanak sağlar (http://www.cobit.org).

Bir diğer yönetim metodolojisi, "Information Technology Infrastructure Library-ITIL"dir. ITIL, BT servislerini eksiksiz ve en iyi kalitede yönetmek üzere geliştirilmiş servis yönetim metodolojisidir. ITIL, 1987'de İngiltere Ticaret Bakanlığı tarafından geliştirilmiştir. İş süreç yaklaşımı sayesinde ITIL, müşteri, tedarikçi, BT bölümü ve kullanıcıları arasında başarılı bir şekilde iletişim kurulmasını sağlamaktadır. "En iyi uygulamalar/deneyimler" üzerine yapılandırılmış olan ITIL, BT Servis Yönetimi ve dağıtımı süreçleri ile dünyada yaygın olarak kullanılmakta ve kabul görmüş bir standart olarak benimsenmektedir. ITIL, BT servislerini yönetmede ayrıntılı ve yapısal en iyi uygulama örnekleri serisidir. Bir başka standart olan ISO 20000 - BT Hizmet Yönetim Sistemi, hizmet kalitesinin artması, güvenilir kurumsal destek, hizmetler hakkında daha net veriler elde

edilmesi, çalışanların işteki başarısının doğru analiz edilmesi, müşteriler memnuniyeti, doğru hizmet sunulması, hizmet süreçlerinin güvenliğinin sağlanması ve sürekli erişim gibi birçok faydalar sağlayabilen bir sistemdir (http://www.iso27001security.com/).

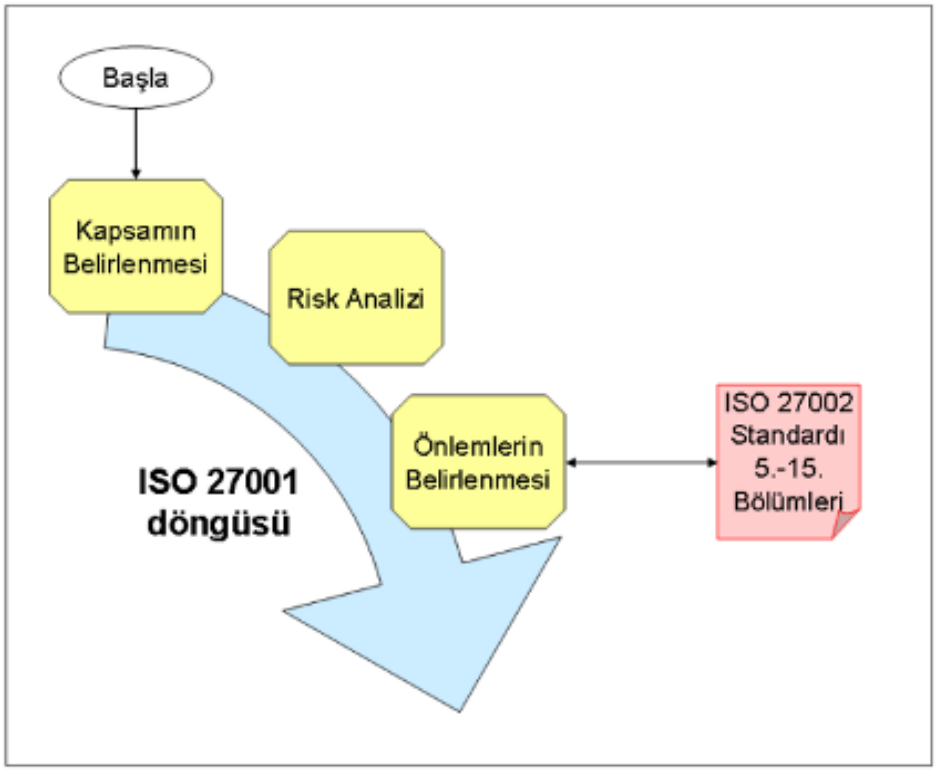
3.8.1. ISO 27001 standardı

ISO 27001 standardı yaşayan, dolayısı ile tehdit ve saldırılara reaksiyon gösteren ve kendini yenileyen bir bilgi güvenliği sisteminde yer alması gereken öğeleri tanımlamaktadır. ISO 27001'de tanımlanan yaklaşım uyarınca bilgi güvenliği bir süreç olarak ele alınması ve sürecin planlama, uygulama, kontrol etme ve önlem alma adımlarından oluşan bir döngü şeklinde çalıştırılması gerekmektedir. Yaşayan ve kendini yenileyen bir bilgi güvenliği sistemi ancak bu döngünün çalıştırılması ile mümkün olabilmektedir (Şekil 3.2.) (Ottekin, 2008).



Şekil 3.2. PÜKO döngüsü ve BGYS adımları

Bu sürecin planlama adımı içerisinde, kurumda bilgi güvenliği şemsiyesi altında bulunacak varlıkların korunması için risk analizi çalışmasının yapılması gerektiği kaydedilmektedir. Bu çalışmanın sonuçları göz önünde bulundurularak ISO 27002 standardında belirtilen önlemlerden kuruluşa en iyi hizmet edecek olanların seçilmesi ve uygulanması talep edilmektedir (Şekil 3.3.).



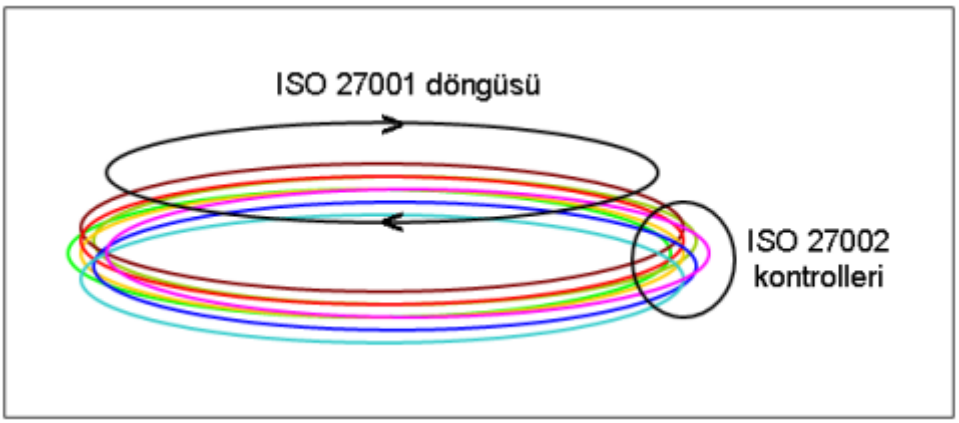
Şekil 3.3. ISO 27001 döngüsünün planlanması aşamasında ISO 27002 kontrollerinin seçilmesi

Böylece ISO 27001 ve ISO 27002 standartları arasındaki ilişki kurulmuş olmaktadır. Şöyle ki, ISO 27001 standardında tarif edilen döngü, ISO 27002 standardından seçilen önlemler için çalıştırılarak bilgi güvenliği süreci gerçekleştirilmeye ve yaşatılmaya çalışılmaktadır. Bilgi güvenliğinde esas olanın ISO 27001 süreci olduğu, bu süreç dışında, kayıtların oluşturulmadığı, gözden geçirme ve tetkiklerin yapılmadığı, önleyici ve düzeltici faaliyetlerin gerçekleştirilmediği bir sistemde önlemlerin kuruma hizmet etmeyeceği söylenebilir (Şekil 3.3.) (Ottekin, 2008).

3.8.2. ISO 27002 standardı

ISO 27002 standardı, bilgi güvenliği sürecinde işletilebilecek tedbirleri içeren bir önlem havuzudur (Ottekin, 2008). ISO 27002 standardının giriş bölümünde bilgi güvenliğinin seçilen önlemler aracılığı ile gerçekleştirileceği belirtilmekte, her önlem için uygulama, izleme ve iyileştirme çalışmalarının yapılması gerektiği belirtilerek ISO 27001 döngüsüne gönderme yapılmaktadır (Şekil 3.4.) (Ottekin, 2008)

.



Şekil 3.4. ISO 27001 döngüsü ve ISO 27002 kontrolleri

Burada önlemler ISO 27002 standardında, önlemlerin nasıl yaşatılacağı ise ISO 27001 standardında açıklanmaktadır.

3.8.3. ISO 27003 standardı

ISO 27003 standardı (Bilgi Teknolojileri - Güvenlik Teknikleri – Güvenliği Yönetim Sistemi için Uyarlama, gerçekleştirme Kılavuzu) Ocak 2010'da yayınlanmıştır ve kılavuz standarttır. Genel bir standart olup, zorunluluk yoktur. ISO 27001 standardına göre sistem kurarken veya sistemin sürekliliğini sağlarken; kapsam, terimler ve tanımlar, standardın yapısı, BGYS projesini uygulama, kabul etme ve onaylama, BGYS kapsam ve politikasını tanımlama, kurum analizi yapma, risk değerlendirme işleme planlarını yönetme, BGYS tasarımı işlemleri için genel bir çerçeve çizer ve yardımcı olur (Ottekin, 2008).

3.8.4. ISO 27004 standardı

ISO 27004 standardı (Bilgi Teknolojileri - Güvenlik Teknikleri – Güvenliği Yönetim Sistemi – Ölçekler, Raporlar Standardı) Aralık 2009'da yayınlanmıştır. Genel bir standart olup, zorunluluk yoktur.

ISO 27001 standardına göre sistem kurarken veya sistemin sürekliliğini sağlarken; BGYS ölçeklerine bakış, yönetim karşılıkları, ölçü ve ölçekleri geliştirme, ölçme işlemleri, veri analizi ve ölçüm sonuçlarının raporlanması, BGYS ölçüm programlarını değerlendirme ve iyileştirme işlemleri için genel bir çerçeve çizer ve yardımcı olur (http://www.iso27001security.com).

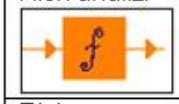
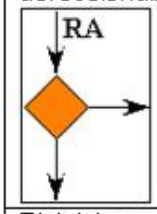
3.8.5. ISO 27005 standardı

ISO 27005 standardı (Bilgi Teknolojileri - Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemlerin Risk yönetimi Standardı) 2008'de yayınlanmıştır. Genel bir kapsamda hazırlanmıştır (Çizelge 3.2.) (Karabacak, 2009).

.

Özel, adlandırılmış, zorunlulukları belirlenmiş bir yaklaşıma sahip değildir. ISO 27001 standardın göre sistem kurarken risk değerlendirmelerinde ISO 27005 standardından yararlanılabilir (http://www.isokalitebelgesi.com).

Çizelge 3.2. Risk kavramları ve tanımları

Kavram	Tanım
Risk yönetimi	Risk yönetimi, bir kurumu "bilgi güvenliği riskleri" göz önünde bulundurarak yönetme ve kontrol etmeyi içeren koordineli aktivitelerdir. Risk yönetimi, bilgi güvenliği ile ilgili karşı önlemlerin seçilmesinde ve geliştirilmesinde temel karar verme mekanizmasıdır. İmkansız olan yüzde yüz güvenlik ile yanlış olan riski gözardı etmek arasında orta bir yol bulmaktır.
Risk değerlendirme	Risk analizi ve risk derecelendirme süreçlerinin bütününe risk değerlendirmesi denmektedir. Risk değerlendirmesi sonucunda aşağıdaki aktiviteler gerçekleştirilmiş olur: 1. riskler kritikliklerine göre sıralanır, 2. Kabul edilebilir risk seviyeleri belirlenir, 3. Hangi risk için ne yapılacağına karar verilir, 4. Azaltılacak risk kalemlerinin öncelikleri belirlenir.
Risk analizi 	Riski hesaplamak amacıyla yapılan sistematik çalışmalardır. Varlık, açıklık ve tehdit ile ilgili parametrik değerlerin girdi olarak alınıp, nitel veya nicel bir risk modeli sonucunda riskin ortaya konulduğu süreçtir.
Risk derecelendirme 	Risk analizi sonucunda hesaplanmış olan işlenmemiş risk değerlerinin kurum bünyesinde belirlenmiş olan kriterlere göre yorumlandığı ve yorumlama sonucunda risk işlemesi sürecine geçilmesine veya diğer risk kontrollerinin uygulanmasına karar verilen süreçtir. Kriter örnekleri: güvenlik ihtiyaçları, karşı önlemin maliyeti, karşı önlemin kullanılabilirliği ve kurumun bütçesi. Diğer risk kontrolü örnekleri: risk kabulü ve risk artırımı.
Risk işleme	Karşı önlemlerin uygulandığı süreçtir. Bu aşamada uygulanan her karşı önlemin bir dayanağı vardır. Bu dayanaklar risk değerlendirme sürecinin sonuçlarıdır.

3.8.6. ISO 27006 standardı

ISO 27006 standardı (Bilgi Teknolojisi - Güvenlik Teknikleri – Bilgi Güvenliği Yönetim Sistemlerin Denetim ve Belgelendirilmesi için Şartlar Standardı) genel olarak ISO 27001 standardına göre sistem kuran veya sürekliliğini sağlayan firmalar şirketlerin dışında ISO 27001 standardına göre akrediteli olarak Belgelendirme denetim gözetim hizmeti veren ISO 27001 Belgelendirme kuruluşlarını ilgilendiren ve kapsam belirleme, denetim, gün, vb. konuları içeren bir standarttır.

Bu konular ayrıca belgelendirme kapsamı, geçerli referanslar, terimler ve tanımlar, ilkeler, genel gereksinimler, yapısal gereksinimler, kaynak gereksinimleri, bilgi

gereksinimleri, süreç gereksinimleri, sertifikasyon kuruluşları için yönetim sistem gereksinimlerini kapsar (http://www.iso27001security.com/html/).

3.9. TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS)

BGYS, bilgi güvenliğini kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçası olarak adlandırılabilir (Önel, Dinçkan, 2007).

Bir işletme için BGYS'nin benimsenmesi stratejik bir karar olmalıdır. Bir kuruluşun BGYS tasarımı ve uygulaması, ticari ihtiyaçlar ve amaçlardan doğan güvenlik gereksinimlerinden, kullanılan proseslerden ve kuruluşun yapısı ve büyüklüğünden etkilenir. Bunların ve destekleyici sistemlerinin zaman içinde değişmesi beklenir. Basit durumların basit BGYS çözümlerinin olması beklenir (Tok, 2010).

İşletme etkin bir şekilde işlev görmesi için, birçok faaliyetini tanımlamalı ve yönetmek durumundadır. Kaynakları kullanan ve girdilerin çıktılara dönüştürülebilmesi için yönetilen her faaliyet, bir proses olarak düşünülebilir. Çoğunlukla, bir prosesin çıktısı doğrudan bunu izleyen diğer prosesin girdisini oluşturur. Kuruluş içerisinde, tanımları ve bunların etkileşimi ve yönetimleriyle birlikte proseslerin oluşturduğu bir sistem uygulaması "proses yaklaşımı" olarak tanımlanabilir. ISO 27001 standardı, bir kuruluşun BGYS'sini kurmak, gerçekleştirmek, işletmek, izlemek, bakımını yapmak ve etkinliğini arttırmak için bir proses yaklaşımının benimsenmesini özendirir. BGYS kurulumuna yönelik gereksinimleri, aşağıdaki toplam yedi başlık altında açıklanacaktır.

Bu başlıklar; genel gereksinimler, BGYS'nin kurulması ve yönetilmesi, dokümantasyon gereksinimleri, yönetim sorumluluğu, BGYS iç denetimleri, BGYS'yi yönetimin gözden geçirmesi, BGYS iyileştirme olacaktır.

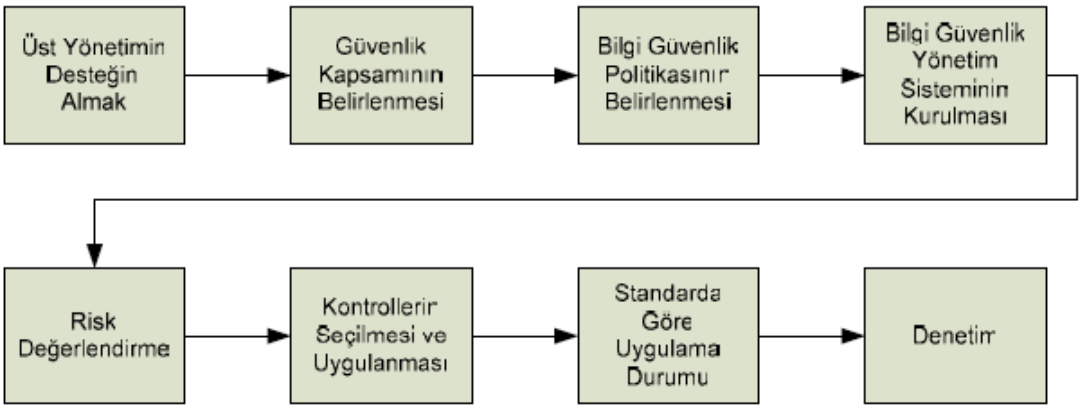
3.9.1. Genel gereksinimler (Madde.4.1.)

Kuruluş, yazılı hale getirilmiş bir BGYS'yi, kuruluşun tüm ticari faaliyetleri ve karşılaştığı riskleri bağlamında, geliştirir gerçekleştirir, sürdürür ve sürekli ilerletir. Bu standardın bir gereği olarak, kullanılan proses, PUKÖ modeline dayanır (TS ISO/IEC 27001, 2006, s.2.).

"Planla-Uygula-Kontrol Et-Önlem al" (PUKÖ) modeli olarak bilinen model, bu standart'ta benimsenen tüm BGYS proseslerine uygulanabilir. Şekil 2.1.'de bir BGYS'nin bilgi güvenlik gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve prosesler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını (örneğin, yönetilen bilgi güvenliği) nasıl ürettiğini gösterir.

3.9.2. BGYS'nin kurulması ve yönetilmesi (Madde.4.2.)

ISO 27001 standardına uygun olarak BGYS kurulması sürecinin aşamaları Şekil 3.5.'de gösterilmektedir (Carlson, 2001, s.11.). BGYS'nin kurulumuna ilişkin bu adımların detayları söz konusu standarda göre madde 4.2.1. numaralı başlık altında sunulmuştur.



Şekil 3.5. ISO 27001 sürecinin aşamaları

BGYS'nin Kurulması (Md.4.2.1.): İşletmeler, BGYS kurmak için temel olarak aşağıdaki faaliyetleri gerçekleştirmek durumundadırlar. Bunlar:

İşin, kuruluşun, yerleşim yerinin, varlıklarının ve teknolojisinin özelliklerine göre BGYS kapsamı ve sınırlarının tanımlanması gerekmektedir.

İşletme özelliklerine göre aşağıdaki özelliklere sahip bir BGYS politikası tanımlaması gereklidir. Bu politika oluşturulurken aşağıdaki hususlara dikkat edilmelidir (TS ISO/IEC 27001, 2006, s.2-10.):

BGYS politikası, amaçlarını ortaya koymak için bir çerçeve içeren ve bilgi güvenliğine ilişkin bir eylem için kapsamlı bir yön kavramı ve prensipleri içermeli, iş ve yasal ya da düzenleyici gereksinimleri ve sözleşmeye ilişkin güvenlik yükümlülüklerini dikkate almalı, BGYS kurulumu ve sürdürülmesinin yer alacağı stratejik kurumsal ve risk yönetimi bağlamını düzenlemeli, risk değerlendirme yapısının tanımlanacağı kriterleri kurmalı, yönetim tarafından kabul edilmiş olmalıdır. Ayrıca risk değerlendirmesine ilişkin sistematik bir yaklaşım tanımlanmalıdır (http://www.iso27001security.com).

İşletmeler, BGYS'ye ve tanımlanmış iş bilgisi güvenliğine, yasal ve düzenleyici gereksinimlere uygun bir risk değerlendirme yöntemini tanımlanmalıdır. Riskleri kabul edilebilir bir seviyeye indirmek için, BGYS politika ve amaçlarını ortaya koymalı ve kabul edilebilir riskler için seviye ve ölçütler belirlenmelidir.

Kuruluşlar tarafından riskler tanımlanmalıdır. Riskler için, BGYS kapsamındaki varlıkları ve bu varlıkların sorumluları, bu varlıklar için var olan tehditleri ayrıca gizlilik, bütünlük ve kullanılabilirlik kayıplarının varlıklar üzerinde olabilecek etkileri tanımlanmalı ve tehditlerin fayda sağlayabileceği açıklıklar belirlenmelidir.

Riskler çözümlenmeli ve derecelendirilmelidir. Risk değerlendirme yöntemleri göz önüne alınarak:

Varlıkların gizliliğine, bütünlüğüne ya da kullanılabilirliğine ilişkin oluşan kayıpların olası sonuçlarını dikkate alarak, bir güvenlik başarısızlığından kaynaklanabilecek iş

hasarlarını neler olabileceği belirlenmeli, mevcut tehditler, açıklıklar ve bu varlıklarla ilişkili tesirler ışığında oluşan bu ve benzeri güvenlik başarısızlıklarının gerçekçi olasılığını ve gerçekleştirilen mevcut kontroller değerlendirilmeli, risk seviyeleri tahmin edilmeli, riskin kabul edilebilir mi olduğunu yoksa risk değerlendirme maddesinde saptanan kriterler kullanılarak iyileştirme mi gerektirdiğine karar verilmesi gereklidir.

Risk iyileştirmesi için seçenekler tanımlanmalı ve değerlendirilmelidir. Olası eylemler; uygun kontrollerin uygulanmasını, kuruluşun politikasını ve risk kabul kriterlerini açıkça karşılaması şartıyla, bilerek ve nesnel olarak risklerin kabul edilmesini, risklerden kaçınmayı, bağlı iş risklerini diğer taraflara, örneğin, sigorta şirketlerine, tedarikçilere aktarmayı içermektedir.

Risk iyileştirmesi için kontrol amaçları ve kontroller seçilmelidir. Uygun kontrol amaçları ve kontroller, risk değerlendirme ve risk iyileştirme proseslerinde tanımlanan gereksinimleri karşılamak için seçilmeli ve gerçekleştirilmelidir.

Sunulan artık risklere ilişkin yönetim onayı alınmalıdır. BGYS'yi gerçekleştirmek ve işletmek için yönetim yetkilendirmesi alınmalıdır. Uygulanabilirlik Bildirgesi hazırlanmalıdır. Seçilen kontrol amaçları ve kontroller ve bunların seçilme nedenleri Uygulanabilirlik Bildirgesi dokümanında yer almalıdır. Aynı şekilde seçilmeyen kontrollere ilişkin seçilmeme nedenlerine de yer verilmelidir (TS ISO/IEC 27001, 2006, s.2-10.).

BGYS'nin Gerçekleştirilmesi ve İşletilmesi (Madde.4.2.2.): Kuruluşların, BGYS'yi gerçekleştirebilmek ve işletebilmek için gerekli faaliyetleri şu şekilde sıralanabilir:

Bilgi güvenlik risklerini yönetmek için uygun yönetim eylem, sorumluluklar ve öncelikleri tanımlayan bir risk iyileştirme planı hazırlamalı, finansman değerlendirmesi, roller ve sorumlulukların tahsisini içeren, tanımlanan kontrol amaçlarına ulaşmak için risk iyileştirme planı uygulanmalı, kontrol amaçlarını karşılamak için seçilen kontroller uygulanmalı, seçilen kontrollerin etkinliğinin nasıl

ölçüleceği ve daha sonra bu ölçüm sonuçlarının nasıl kullanılacağı tanımlanmalı, eğitim ve farkında olma programları gerçekleştirilmeli, BGYS'nin işleyişini yönetmeli, BGYS'nin kaynaklarını yönetmeli, güvenlik olaylarını anında saptayabilme ve yanıt verebilme kabiliyetine sahip prosedür ve kontroller gerçekleştirilmelidir (TS ISO/IEC 27001, 2006, s.2-10.).

BGYS'nin İzlenmesi ve Gözden Geçirilmesi (Madde.4.2.3.): Kuruluşlar BGYS'ni izlenmesi ve gözden geçirilmesi için aşağıdakileri gerçekleştirmek durumundadır:

İzleme prosedürlerini ve diğer kontrolleri aşağıda belirtilen amaçlara ulaşmak için yürütülmelidir. Bu amaçlar; işleme sonuçlarındaki hataları anında saptamak, denenen ve başarılı olan güvenlik kırılmalarını ve ihlal olaylarını anında tanımlamak, yönetimin, kişilere devredilen ya da bilgi teknolojisince gerçekleştirilen güvenlik faaliyetlerinin beklenen biçimde çalışıp çalışmadığını belirleyebilmesini sağlamak, güvenlik olaylarını saptama ve belirteçler kullanarak güvenlik ihlal olaylarını engellemeye yardım etmek, bir güvenlik kırılmasını çözmek için alınan önlemlerin etkili olup olmadığını karar vermektir (TS ISO/IEC 27001, 2006, s.2-10.).

Güvenlik denetimlerinin, olaylarının, önerilerinin sonuçlarını ve tüm ilgili taraflardan geri bildirimleri dikkate alarak BGYS'nin (güvenlik politikaları ve amaçlarını karşılama, ve güvenlik kontrollerini gözden geçirme dahil) etkinliği düzenli olarak gözden geçirilmelidir. Güvenlik gereksinimlerinin karşılandığını doğrulamak için kontrollerin etkinliğini ölçülmelidir. Oluşacak değişiklikleri dikkate alarak, artık risklerin ve kabul edilebilir risklerin seviyesi gözden geçirilmelidir. Planlanan aralıklarda iç BGYS denetimleri gerçekleştirilmelidir. BGYS'nin yönetim tarafından düzenli olarak gözden geçirilmesi üstlenilmelidir. İzleme ve gözden geçirme faaliyetlerindeki bulgular dikkate alınarak güvenlik planları güncelleştirilmelidir. BGYS etkinliğinde ya da performansında bir etkisi olabilecek eylemleri ve olayları kaydedilmelidir.

BGYS'nin Sürekliliği ve İyileştirilmesi (Madde.4.2.4.): İşletmeler, süreklilik sağlama ve iyileştirme amacı ile belirli aralıklarla bazı faaliyetleri yapmak durumundadırlar. İşletmelerin yapacağı faaliyetlerden bazıları şunlardır:

BGYS'deki tanımlanan gelişmeleri gerçekleştirmelidirler. Uygun düzeltici ve engelleyici önlemler alınmalıdır. Diğer kuruluşların ve kendisine ait güvenlik deneyimlerinden alınan dersler uygulanmalıdır. Sonuçları ve eylemleri bildirilmeli ve ilgili tüm taraflarla mutabık kalınmalıdır. İyileştirmelerin tasarlanan amaçlara ulaşması sağlanmalıdır (TS ISO/IEC 27001, 2006, s.2-10.).

3.9.3. Dokümantasyon gereksinimleri (Madde.4.3.)

Dokümantasyon yönetim kararlarının kayıtlarını içermeli, eylemlerin yönetim kararları ve politikalarına izlenebilir olmasını ve kaydedilen sonuçların yeniden üretilebilir olması sağlanmalıdır. Tüm dokümantasyon BGYS politikası gereğince kullanılabilir yapılmalıdır.

BGYS dokümantasyonu, BGYS politikası ve kontrol amaçlarının dokümante edilmiş ifadeleri, BGYS kapsamını, BGYS'yi destekleyici prosedür ve kontrolleri, risk değerlendirme metodolojisinin bir tanımını, risk değerlendirme raporunu, risk iyileştirme planını, kuruluş tarafından, bilgi güvenliği proseslerinin etkin planlanmasını, işlemesini ve kontrolünü sağlamak için gereksinim duyulan dokümante edilmiş prosedürleri, ihtiyaç duyulan kayıtları, Uygulanabilirlik Bildirgesini kapsamalıdır.

Dökümanların Kontrolü (Madde 4.3.2): BGYS tarafından talep edilen dokümanlar korunur ve kontrol edilir. Dokümante edilmiş bir prosedür, ihtiyaç duyan yönetim eylemlerini belirlemek için kurulmalıdır.

Bu yönetim eylemleri, yayınlanmadan önce dokümanları uygunluk açısından onaylamayı, gerektiğinde dokümanları gözden geçirme, güncelleme ve tekrar onaylamayı, doküman değişikliklerinin ve mevcut revizyon durumunun tanınmasını

sağlamayı, ilgili dokümanların en son sürümlerinin kullanım noktalarında kullanılabilir olmasını sağlamayı, dokümanların okunaklı ve hazır olarak tanınabilir olmasını, dış kaynaklı dokümanların tanınmasını, doküman dağıtımının kontrol edilmesini sağlamayı, yürürlükte olmayan dokümanların istenmeden kullanımını engellemeyi, eğer herhangi bir amaç için tutuluyorsa, bu dokümanlara uygun bir kimlik uygulanmasını kapsar (TS ISO/IEC 27001, 2006, s.2-10.).

Kayıtların Kontrolü (Madde.4.3.3.): Kayıtlar, gereksinimlere uygun olduğuna ve BGYS'nin etkin işlediğine dair kanıtlar sağlamak için kurulmalı ve sürdürülmelidir. Kayıtlar korunmalı ve kontrol edilmelidir. BGYS, ilgili her yasal gereksinimi dikkate alır. Kayıtlar, okunabilir, hazır olarak tanınabilir ve geri alınabilir halde tutulur. Kayıtların tanınması, saklanması, korunması, geri alınması, tutulma ve düzenleme zamanları için gereken kontroller yazılı hale getirilmelidir. Kayıtlar, proses performansına ve BGYS ile ilgili tüm güvenlik ihlal olaylarının oluşumlarına ilişkin tutulmalıdır. Kayıtlara ilişkin örnek olarak, ziyaretçi defterleri, denetim kayıtları ve erişim yetkilendirme formları verilebilir (TS ISO/IEC 27001, 2006, s.2-10.).

3.9.4. Yönetim sorumluluğu (Madde.5.)

Yönetim desteği bilgi güvenliği programının olmazsa olmaz unsurudur. Güvenlik mesajlarının etkili olabilmeleri için en yukarıdan desteklenmeleri gereklidir. Pek çok yönetici bu tür çalışmalar konusunda desteğini dile getirse de, desteğin gerçekleşmesini söylemek kadar kolay olmamaktadır. Bu durum yöneticilerin kendi iş ve sorumluluklarının bulunmasından kaynaklanmaktadır (Emiral, 2006).

BGYS kurulumunda yönetim sorumluluğu, yönetimin bağlılığı ve kaynak yönetim başlıkları altında açıklanmaya çalışılacaktır.

Yönetimin Bağlılığı (Madde.5.1.): Yönetim BGYS'nin kurulumuna, gerçekleştirilmesine, işletimine, izlenmesine, gözden geçirilmesine, sürdürülebilirliğine ve iyileştirilmesine olan bağlılığını bazı faaliyetleri gerçekleştirerek kanıtlamalıdır.

Bu faaliyetler; bir bilgi güvenlik politikası kurmak, bilgi güvenlik amaçlarının ve planlarının kurulmasını sağlamak, bilgi güvenliği için rolleri ve sorumlulukları kurmak, kuruluşa, bilgi güvenlik amaçlarını karşılamanın ve bilgi güvenlik politikalarına uyumun önemini, yasaya karşı sorumluluklarını ve sürekli iyileştirmeye olan gereksinimi bildirmek, BGYS'yi geliştirmek, gerçekleştirmek, işletmek ve bakımını yapmak için yeterli kaynak sağlamak, kabul edilebilir risk seviyesini belirlemek, iç BGYS denetimlerini sağlamak, yönetimin BGYS incelemelerini yürütmektir.

Kaynak Yönetimi (Madde.5.2.): BGYS gerçekleştirmede yönetim sorumluluğu kapsamında yer alan kaynak yönetim kapsamını, kaynakların belirlenmesi, sağlanması ve uygun yeterlilikte personel için gereken faaliyetleri içermektedir. Bu faaliyetleri sırası ile aşağıdaki gibidir (Emiral, 2006):

Kaynakların Sağlanması (Md.5.2.1.): Kuruluş, BGYS faaliyetlerinin planlandığı şekilde sürdürülmesine yönelik bazı faaliyetler için gereken kaynaklara karar vermeli ve bunları yürütmelidir.

Bu faaliyetler; bir BGYS kurmak, gerçekleştirmek, işletmek, sürdürmek ve iyileştirmek, bilgi güvenlik prosedürlerinin iş gereksinimlerini desteklemesini sağlamak, yasal ve düzenleyici gereksinimleri ve sözleşmeden doğan güvenlik yükümlülüklerini tanımlamak ve ifade etmek, gerçekleştirilen tüm kontrollerin doğru uygulamalarıyla, uygun güvenliği sürdürmek, gerektiğinde incelemeleri yürütmek ve bu gözden geçirme sonuçlarına uygun olarak hareket etmek, ihtiyaç olduğunda, BGYS etkinliğini geliştirmektir.

Eğitim, Farkında Olma ve Yeterlilik (Md.5.2.2.): İşletmeler, ilgili tüm personelin bilgi güvenliği faaliyetlerinin yarar ve öneminin ve BGYS amaçlarına ulaşılmasına nasıl katkı sağlayacağının farkında olmasını sağlamalıdır.

Bu amaçla kuruluşlar; BGYS'yi etkileyecek işleri gerçekleştiren personel için gerekli yeterlilikleri belirlemeli, yeterli eğitimi sağlama ve gerekirse, bu ihtiyaçları karşılamak üzere yeterli personel istihdam etmeli, alınan önlemlerin etkinliğini değerlendirmeli, eğitime, öğretime, becerilere, deneyime ve niteliklere ilişkin kayıtları tutmalıdır (Erkan, 2006).

3.9.5. BGYS iç denetimleri (Madde.6)

Kuruluş, BGYS kontrol amaçlarının, kontrollerinin ve prosedürlerinin standardın gereklerine, tanımlanan bilgi güvenliği gereksinmelerine uyup uymadığını belirlemek için, planlanan aralıklarla iç denetimler yürütmelidir.

Bir denetleme programı, bir önceki denetim sonuçlarının yanı sıra denetlenecek proseslerin ve alanların durumu ve önemi dikkate alınarak planlanmalıdır. Denetim kriterleri, kapsamı, sıklık ve yöntemler tanımlanmalıdır. Denetmenlerin seçiminde ve denetimlerin gerçekleştirilmesinde, denetim prosesinin nesnel ve tarafsız olarak işlemesi sağlanmalıdır. Denetmenler kendi çalışmalarını denetlememelidirler.

Denetimlerin planlanması ve yürütülmesinde ki ve sonuçların raporlanması ve kayıtların tutulmasında ki sorumluluklar ve gereksinimler, yazılı hale getirilmiş bir prosedür içinde tanımlanır. Denetlenen alandan sorumlu olan yönetim, saptanan uygunsuzlukların ve bunların nedenlerinin giderilmesi için, gereksiz gecikmeler olmaksızın önlemlerin alınmasını sağlamalıdır. İzleme faaliyetleri, alınan önlemlerin doğrulanmasını ve doğrulama sonuçlarının raporlanmasını içermelidir (TS ISO/IEC 27001, 2006, s.2-10.).

3.9.6. BGYS'yi Yönetimin Gözden Geçirmesi (Madde.7.)

Yönetim, kuruluşun BGYS'sini planlanan aralıklarla, sürekli uygunluğunu, doğruluğunu ve etkinliğini sağlamak için gözden geçirmelidir. Bu gözden geçirme, güvenlik politikası ve güvenlik amaçları dahil BGYS'nin iyileştirilmesi ve gereken değişikliklerin yapılması için fırsatların değerlendirilmesini de içermelidir. Gözden

geçirme sonuçları açıkça yazılı hale getirilmeli ve kayıtlar tutulup saklanmalıdır. Bu nedenden dolayı, gözden geçirme faaliyetlerinin kapsamı gözden geçirme girdisi ve gözden geçirme çıktısı başlıkları altında incelenecektir.

Gözden Geçirme Girdisi (Madde.7.2.): BGYS kapsamında gerçekleştirilecek yönetimin gözden geçirme faaliyetleri için gerekli girdiler, BGYS denetimleri ve gözden geçirmelerinin sonuçlarını, ilgili taraflardan edinilen geri bildirimleri, kuruluşta BGYS'nin performansını ve etkinliği artırmak için kullanılabilecek teknikler, ürünler ya da prosedürleri, önleyici ve düzeltici faaliyetlerin durumunu, etkinlik ölçümlerinin sonuçlarını, önceki risk değerlendirilmesinde uygun olarak ifade edilmeyen açıklıklar ya da tehditleri, önceki yönetim gözden geçirmelerinden izleme eylemlerini, BGYS'yi etkileyebilecek herhangi bir değişikliği, iyileştirme için öneri içermelidir.

Gözden Geçirme Çıktısı (Madde.7.3.): Bir BGYS yönetim gözden geçirme çıktıları, BGYS etkinliğini iyileştirmek, risk değerlendirme ve risk işleme planını güncelleştirmek, gerektiğinde, BGYS üzerinde etkisi olabilecek iç ya da dış olaylara karşılık vermek için bilgi güvenliğini etkileyen prosedür ve kontrol değişiklikleri, kaynak ihtiyaçları, kontrollerin etkinliğinin ölçümünde iyileşme faaliyetleri ile ilgili her kararı ve eylemi içermelidir (TS ISO/IEC 27001, 2006, s.2-10.).

3.9.7. BGYS iyileştirme (Madde.8.)

BGYS proseslerine uygulanan PUKÖ modelinin "Önlem Al" kapsamında, BGYS'nin sürekli iyileştirilmesini sağlamak için, yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve önleyici eylemlerin gerçekleştirilmesi gerekmektedir.

Sürekli İyileştirme (Madde.8.1.): Kuruluş, bilgi güvenlik politikasını, güvenlik amaçların, denetim sonuçlarını, izlenen olayların analizini, düzeltici ve önleyici faaliyetleri ve yönetim gözden geçirmelerini kullanarak BGYS etkinliğini sürekli iyileştirmelidir.

Düzeltici Faaliyetler (Madde.8.2.): Kuruluş tekrarları engellemek için, BGYS gereksinimleriyle uygunsuzlukların nedenlerini gidermek üzere önlemler almalıdır.

İşletmeler, düzeltici faaliyetlerde yazılı hale getirilmiş prosedür için; uygunsuzlukları tanımlama, uygunsuzlukların nedenlerini belirleme, uygunsuzlukların tekrarlanmamasını sağlamak için ihtiyaç duyulan faaliyetleri değerlendirme, gereken düzeltici faaliyetleri belirlemek ve gerçekleştirme, gerçekleştirilen faaliyetlerin sonuçlarını kaydetme, gerçekleştirilen düzeltici faaliyetleri gözden geçirme için gerekli gereksinimleri tanımlamalıdır.

Önleyici Faaliyetler (Madde.8.3.): Kuruluş tekrar ortaya çıkmalarını önlemek için, BGYS gereksinimleriyle olası uygunsuzlukların nedenlerini gidermek üzere alınacak önlemleri belirlemelidir. Gerçekleştirilen önleyici faaliyetler, olası sorunların yapacağı etkiye uygun olmalıdır. Önleyici faaliyetlerin önceliği, risk değerlendirme sonuçlarına bağlı olarak belirlenir.

İşletmeler, önleyici faaliyetlerde yazılı hale getirilmiş prosedür için, olası uyumsuzlukları ve bunların nedenlerini belirlemek, ihtiyaç duyulan önleyici faaliyetleri belirlemek ve gerçekleştirmek, gerçekleştirilen faaliyetlerin sonuçlarını kaydetmek, gerçekleştirilen önleyici faaliyetleri gözden geçirmek, değişen riskleri tanımlamak ve dikkatin önemli derecede değişen riskler üzerinde yoğunlaştıracak önleyici faaliyet gereksinimlerini, kapsamalıdır (TS ISO/IEC 27001, 2006, s.2-10.).

4. ARAŞTIRMA BULGULARI

Günümüzde, Kamu kuruluşların Bilgi güvenliği yönetim sistemi (BGYS) kurmak ve işletmek için zaman ve kaynak ihtiyaçlarını düşüreceği amaçlanan çalışmada sistemi kurup yönetirken yapılması gereken tüm adımlar sırasıyla programda belirtilmiş ve açıklanmıştır. Ayrıca kamu kurumları için yapılan model önerisi (ISO 27001 BGYS yol gösterici program) yapılırken kullanılan veri tabanı ve programlama dilleri anlatılmıştır. Yapılan yazılım Süleyman Demirel Üniversitesi Bilgi İşlem Daire Başkanlığı'nın bazı bölümlerine uygulanmış, yapılan uygulama ve uygulama sonucunda erişilen bulgulara yer verilmiştir.

4.1. Bilgi Güvenliği Probleminin Ortaya Konulması

Bu tez çalışmasında, bilgi güvenliğine yönelik saldırıların önlenmesinde zaman içinde hem sayı hem de çeşitlilik açısından arttığı bir ortamda etkin bir bilgi güvenliği oluşturabilmek için gerekli olan, güvenlik süreçleri ve bilgi güvenliği standartlarını incelemek, incelenen standartların neden kullanılması gerektiğini belirtmektir. Bilgi güvenliği standartları çerçevesinde kamu kurumları için bilgi güvenliği model önerisi yapmaktır. Ayrıca kamu kurumlarının bilgi güvenliği için neler yapması gerektiği, hangi programları kullanması gerektiği tavsiye edilerek ve kamu kurumlarında bilişim teknolojileri güvenlik sistemi kurulması için hareket planı önerilmiştir.

Bu çalışmada Bilgi Güvenliği açısından en çok ihtiyaç duyulan Bilgi İşlem Merkezi örnek alınarak uygulama yapılmıştır.

4.2. Bilgi Güvenliği İçin İç Tetkik Uygulamalarının Yapılması

Yapılan yazılım ile aşamalar belirtilmiştir. İlk adım olan Planlama aşaması oluşturulmuş, daha sonra riskler belirlenmiş, riskler için varlık envanterleri oluşturulmuştur. Riskler çözümlenmiş ve değerlendirilmiştir. Her kurumun kendi

için oluşturacağı EkA aşaması ana hatlarıyla kaydedilmiştir. Ayrıca, kontrol et aşaması olan risk yönetim süreci oluşturulmuştur. Bu bilgiler oluşturulduktan sonra yazılımda bilgi güvenliğinin devamı için kontrol sağlanacak uygulamalar eklenmiştir.

4.3. Geliştirilen Yazılımın Tanıtılması

Çalışmada planlama, riskleri tanımlama, riskleri çözümleme ve değerlendirme, uygulanabilirlik bildirgesi (EkA), risk yönetim süreci, önlem al aşamalarının tanımlanabildiği bir yazılım geliştirilmiştir. Yazılım PHP programlama dili kullanılarak geliştirilmiştir. Bilgilerin saklandığı ortam için ise My SQL veritabanı kullanılmıştır.

4.4.Veri Tabanı Yönetim Sistemleri

Veri tabanı özetle, çeşitli bilgilerin bir arada tutulduğu depo olarak tanımlanabilir. Bu tanımı biraz daha açar ve incelersek; çeşitli amaçlara yönelik olarak hazırlanmış tablolardan oluşan bilgi depolarıdır. Bu tablolarda tutulan bilgiler ve bunların birbiriyle ilişkilerinin düzenlendiği, bilgiye hızlı bir biçimde erişme yöntemlerinin sağlandığı bir sistemdir. Örnek olarak bir ürünü üreten şirketi ele alacak olursak; bu şirketin ürettiği ürünler, bu ürünleri üretmek için kullanması gereken malzemeler, bu malzemeleri aldığı diğer şirketler, üretilen malzemeleri satın alanlar, şirkette çalışanlar, şirketin makine parkı, iş yaptığı diğer şirketlerle olan mali alışverişleri gibi bilgiler değişik tablolarda tutulmaktadır. Saymaya çalıştığım bu evrelerin her birinde ayrı ayrı veri tabanları kullanılacağı gibi tek bir veri tabanı altında da toplanabilir. Diğer şirketlerin veri tabanlarıyla gerçekleştirilecek olan bağlantılarla bilgi alışverişinde de bulunulmaktadır (http://www.bilgisite.com).

Daha basit anlatımla insan beynide bir veri tabanı olarak nitelendirilebilinir. Hayatımız boyunca çeşitli kaynaklardan alınan ve öğrenilen bilgiler beyinde toplanmakta ve istenilen zamanda kullanılmaktadır. O halde en gelişmiş veri tabanı 'İnsan Beynidir'. Beyinde çeşitli başlıklar altında tutulan bilgiler istendiğinde tek

olarak veya diğer bilgilerle birleştirilerek kullanıma sunulur. Renkler tablosunda bildiğimiz ve tanıdığımız renkler tutulur. Kişiler tablosunda tanıdığımız kişilerin isimleri, adresleri, telefon bilgileri yer alır. Hatta bu kişiler tablosunda görsel olarak bu kişilerin yüzlerinin resimleri de yer almaktadır. Tatlar tablosunda ise acı, tatlı, ekşi gibi bilgiler yer alır. İşte ayrı ayrı tablolarda tutulan bu bilgileri tek başına kullandığımız gibi diğer tablolardaki bilgilerle birleştirerek daha da zenginleştirmek mümkündür (http://www.bilgisite.com).

Oluşan bir veya birden fazla veri tabanı yönetilmesine yönelik olarak çeşitli yazılımlar mevcuttur ve bunlara DBMS (DataBase Management System) denmektedir. Ayrıca veri tabanlarının birbirleriyle olan ilişkilendirilmesine RDBMS (Relational DataBase Management System) şeklinde tanımlanmaktadır. Günümüzde en basitinden en karmaşığına kadar bir yığın Veri tabanları mevcuttur. En basiti Microsoft'un Access programı altında veya Paradox, Foxpro altında oluşturulan tablolara da veri tabanı denilebilinir. Ayrıca Microsoft'un SQL veya ORACLE, PROGRESS, SYBASE bilinen veri tabanlarıdır. Aynı şekilde IBM AS/400 veya main frame sistemlerinde kullanılan DB2'da bir veri tabanıdır. Gelişen teknoloji ile veri tabanlarının kullanım alanlarının gelişmesi sonucu içinde görsel bilgileri (resim, ses, video vb.) tutar hale gelmiştir. İnternetin yaygınlaşması sonucu ve veri tabanlarının işlevleri de geliştirilmiş ve WEB uyumlu hale gelmiştir (Çetinkaya, 2008).

Kurulacak olan veri tabanı üzerinde bilgi girişi veya sorgulama yapacak olunması bu sistemin iyi analiz edilmesini gerektirmektedir. Bu veri tabanının hangi ortamlarda çalışacağı yani Local Network'lerde mi yoksa daha geniş uzak alanlarda) mı çalışacağı, işletim sistemine, ana makinenin performansına (disk, memory, işlemci bazında), veri tabanı üzerinde çalışacak olan programlama diline bağlıdır. Bir ana makine (server) üzerinde kurulmuş olan veri tabanını oluşturan tabloları, bağlı kullanıcıları ve bunların tablolar üzerindeki haklarını, işletim sistemiyle olan bağlantıları yani gereken disk alanı, gerekli bellek ve işlemci hızlarını ayarlayan sistem Veri tabanı Yönetim Sistemi (DBMS DataBase Management System) olarak adlandırılır.

Veri tabanı tasarımı aynı program tasarımı gibidir. Neyi, nerede ve nasıl tutulacağı düşünülerek tablolar oluşturulur ve içleri çeşitli alanlara ayrılarak bilgiler yerleştirilir. Amaç; aynı türden bilgilerin bir tablo altında toplanması, tekrarlanmaması (değişik tablolarda da yer almaması), bu bilginin birlikte kullanılabileceği diğer bilgilerin yer aldığı tablolarla sağlam bağlantılarının oluşturulmasıdır. Bir Tablo (Table) içinde, birden fazla sayıda ve tipte yani karakter, sayısal, görsel vb. Alan (Field) bulunmaktadır. Bu tablonun alanlarına satır satır girilen bilgilerde (Record) Kayıttır (http://www.bilgisite.com).

4.5. Veri Tabanı Yöneticiliği

Günümüzde veri tabanı sistemleri, bankacılıktan otomotiv sanayisine, sağlık bilgi sistemlerinden şirket yönetimine, telekomünikasyon sistemlerinden hava taşımacılığına, çok geniş alanlarda kullanılan bilgisayar sistemlerinin alt yapısını oluşturmaktadır. Veri tabanı fiziksel olarak bilgileri tutarken mantıksal bir sisteme de sahiptir. Veri tabanı sistemlerinin kurulumu, konfigürasyonu, dizaynı, sorgulaması, güvenliği ve denetiminin karmaşık bir hal alması veri tabanı yöneticiliği kavramının oluşmasına neden olmuştur. Bir veri tabanı yöneticisi mantıksal data modelleme, fiziksel veri tabanı tasarımı çıkarma, fiziksel olarak veri tabanı oluşturma, sorgu yazma, kurulum ve ayarları, güvenlik yönetimi ve ayarları, veri tabanı yönetimi ve bakımı, veri tabanı denetleme ve küçültme işlerini üstlenir.

4.5.1. İlişkisel veri tabanı sistemleri

- MySQL
- MsSQL
- PostgreSQL
- Oracle
- Sybase
- Berkeley
- Firebird
- Ms access

4.5.2. Veri tabanı dilleri

- SQL
- PL/SQL
- OQL

4.6. Veri Tabanı Sistemi "MySQL"

MySQL, çok hızlı ve çok sağlam bir ilişkisel veri tabanı yönetim sistemidir. Bunlara literatürde RDBMS (Relational Database Management System) denir. MySQL çok kullanıcılı, çok kanallı bir sunucudur (Şekil 4.1.) (Torun, 2011)

.

Dünya çapında standart kabul edilen veri tabanı sorgulama dili olan SQL'i (Stractured Query Language) kullanır. Dünyanın en popüler açık kaynak kodlu veri tabanı sistemidir (Bingöl, 2010).

Php ile kullanılan en yaygın veri tabanı türü olan Mysql yapılan güncellemeler ile çok hızlı çalışır duruma getirilmiştir (www.phpkodlari.com).

Veri tabanı içinde bilgiler tablo adı verilen gruplar halinde bulunur. Benzetmek gerekirse Microsoft Excel sayfasındaki tablolar gibi düşünülebilir, fakat Mysql içinde görünebilir bir satır çizgisi olmaz. bilgiler yığın halindedir. Verilen komuta göre Mysql uygulaması tarafından yine grup halinde bilgiler alınabilir.

Özellikle kategori ve liste halindeki bilgileri depolamak için veri tabanı en uygun ortamdır. Örneğin: öğrenci listesi, ürün listesi, fiyatlar vb. sayılabilir.

Şekil 4.1. MySQL-istemci ilişkisi

4.6.1. MySQL'in güçlü yanları

MySQL'in başlıca rakipleri PostgreSQL, Microsoft SQL Server ve Oracle'dır. Ancak MySQL; yüksek performans, düşük maliyet, yapılandırma ve öğrenim kolaylığı, taşınabilirlik, açık kaynak gibi özellikleriyle daha güçlüdür (Ayan, 2010).

4.6.2. MySQL komutları

Mysql Komutları temel seviyede aşağıdaki gibi sayılabilir. Ama daha kapsamlı uygulamalar için bunların parametrelerini ve diğer mysql komutlarını kullanmak gerekir.

Create Database: Yeni bir veri tabanı üretir.
Create table: Yeni bir tablo üretir.
Insert into: Veri tabanına yeni kayıt ekler.
Select from: Veri tabanından bilgi okumaya yarar.
Where: Yapılan işlemin etkileyeceği sütunları belirtir.
Order by: Seçim işleminde sıralama veya tersten sıralama yapar.
Update set: Veri tabanında değişiklik yapar.
Delete from: Bilgi siler.
Show table: Tabloların listesini verir.

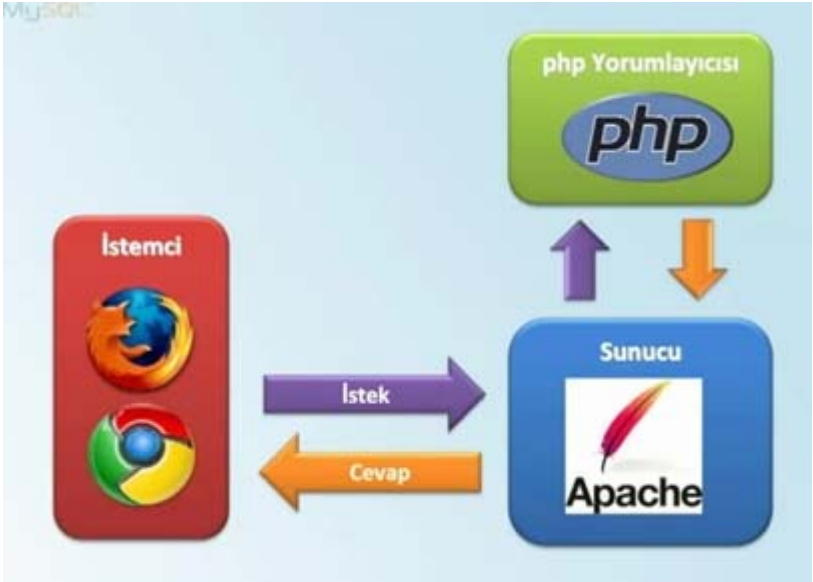
Describe: Tablo sütunlarının adını yazar.
Drop database: Veri tabanını toptan siler.
Drop table: Tabloyu toptan siler.
Drop index: Belirtilen indexi siler.
Truncate table: Tablodaki bilgileri siler, tablo ayarlarını sıfırlar.
Alter database: Veri tabanının öz niteliklerini değiştirir.
Alter table: Tabloya alan ekleme, tablodaki alanı düzenleme ve silme işlemlerini yapar.
Alter view: Görünüm değiştirmede kullanılır.
Create index: Yeni bir index oluşturur.
Delete: Belirtilen tablodan yeri where deyimi ile saptanan satırı siler.
Rename table: Var olan tablonun adını değiştirir.
Select: Veri tabanındaki tablonun tamamını ya da where ile belirtilen alanı gösterir (www.phpkodlari.com).

4.7. Programlama Dili "PHP"

PHP, server tabanlı HTML gömülü bir script dilidir. Özellikle web geliştiricileri için dinamik sayfalar oluşturmayı amaç gütmektedir (Şekil 4.2.) (Torun, 2011).

Bu sebepten geliştiricilere yabancı olmadıkları bir syntax yapısı imkanı vermektedir. Syntax yapısı olarak ise C, Java ve Perl kullanıcılarının yabancı olmayacağı benzerliktedir. İlk olarak 1994′de Rasmus Lerdorf tarafından başlatılmış bir Open Source çalışmadır. Daha sonrasından bu çalışmaya yetenekli insanların katkıları olmuş ve şuan günümüzde birçok kişinin vazgeçilmezi olmuştur. Gün geçtikçe de yeni özellikleriyle büyümeye devam etmektedir (Kesici, 2012).

2007 verilerine göre yaklaşık 21 milyon domain PHP kullanmış olduğunu söylersek bu oranın günümüzde daha fazla olduğunu söyleyebiliriz. PHP kısaltması Personel Home Page olmasına karşın GNU ile birlikte yeniden adlandırılarak şimdilerde Hypertext Preprocessor olarakta bilinmektedir. PHP daha çok Zend alt yapısı altında yazılmaktadır (Kesici, 2012).



Şekil 4.2. PHP-sunucu ilişkisi

4.7.1. PHP avantajları

PHP'nin rakiplerinden üstün kılan bir çok avatanjı olmasından dolayı ilgi görmektedir (Şekil 4.3.) (Kesici, 2012). Bunlardan bazıları ise;

Perfonmans: PHP hızlıdır, Zend firması Benchmark'ları sitesinden sürekli yayınlamaktadır.

Database Entegrasyonu: PHP; MySQL, Oracle, IBM DB2, PostgreSQL, Informix, Sybase ve bir çok veri tabanıyla uyumludur. ODBC (Open Database Connectivity Standart) kullanılarak herhangi bir database ile bağlantı kullanılabilinir.

Ücretsiz: PHP ücretsiz bir üründür. Kendi sitesinden indirilerek kullanıma hemen başlayabilirsiniz.

Öğrenme: Birçok dilde taban alan bir yapı olduğundan programlamayla uğraşan biri için öğrenilmesi çok kolaydır.

Nesneye Yönelik: PHP 5′den itibaren nesneye yöneliğe tamamen geçilmiştir. Böylece nesneye yönelik programlama modelinin getirdiği birçok avantajı da sağlamaktadır.

Taşınabilirlik: Farklı işletim sistemlerine destek sağlamaktadır.

Kaynak Kod: PHP'nin kodlarına erişebilinir. Böylece PHP'ye eklentide yapabilirsiniz.

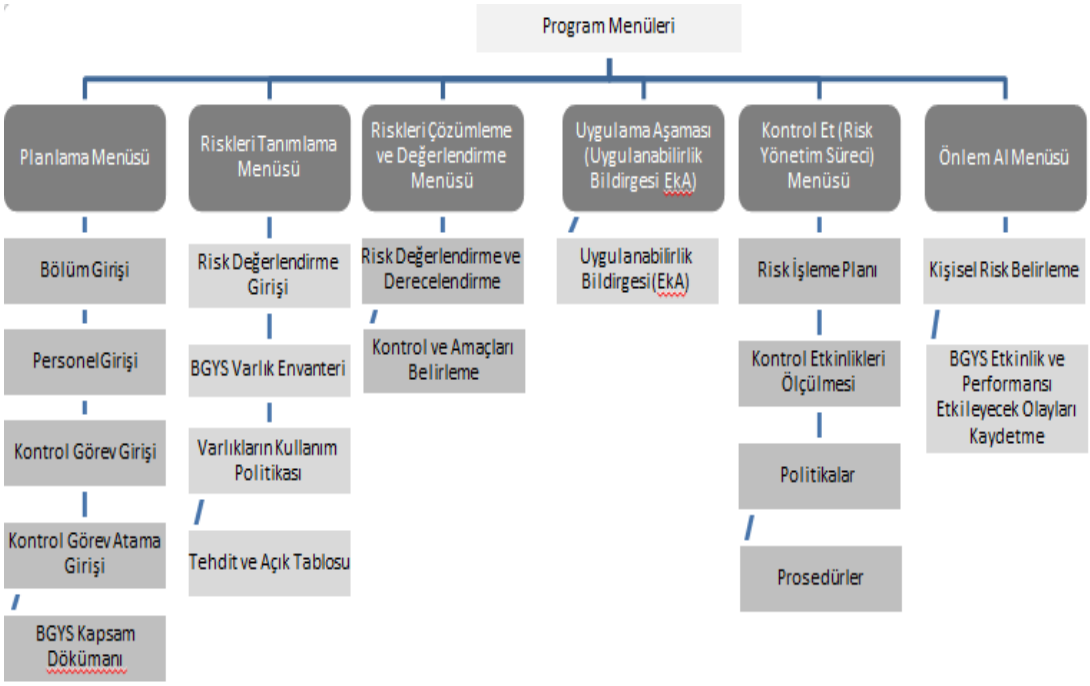
Döküman: PHP öğrenmek için internet üzerinde birçok kaynak bulabilir ve destek alabiliriz.

Şekil 4.3. PHP ve java script karşılaştırılması

MySQL İlişkisel Veri tabanı Sistemleri (RDBMS)'nin web platformlarında en çok tercih edilme sebeplerinden adının PHP duyurulmuş olmasıdır. MySQL, 1979′lardan oluşan bir fikir olsa da 1996′da oluşmuş bir veri tabanıdır. PHP gibi MySQL'de OpenSource'dur. Ücretsiz olarak GPL lisansına sahip uygulamalarda kullanabilirken GPL lisansına sahip olmayan bir uygulama geliştirmek istenildiğinde lisans satın almak gerekmektedir.

4.8. Veri Tabanı Yazılım Geliştirme

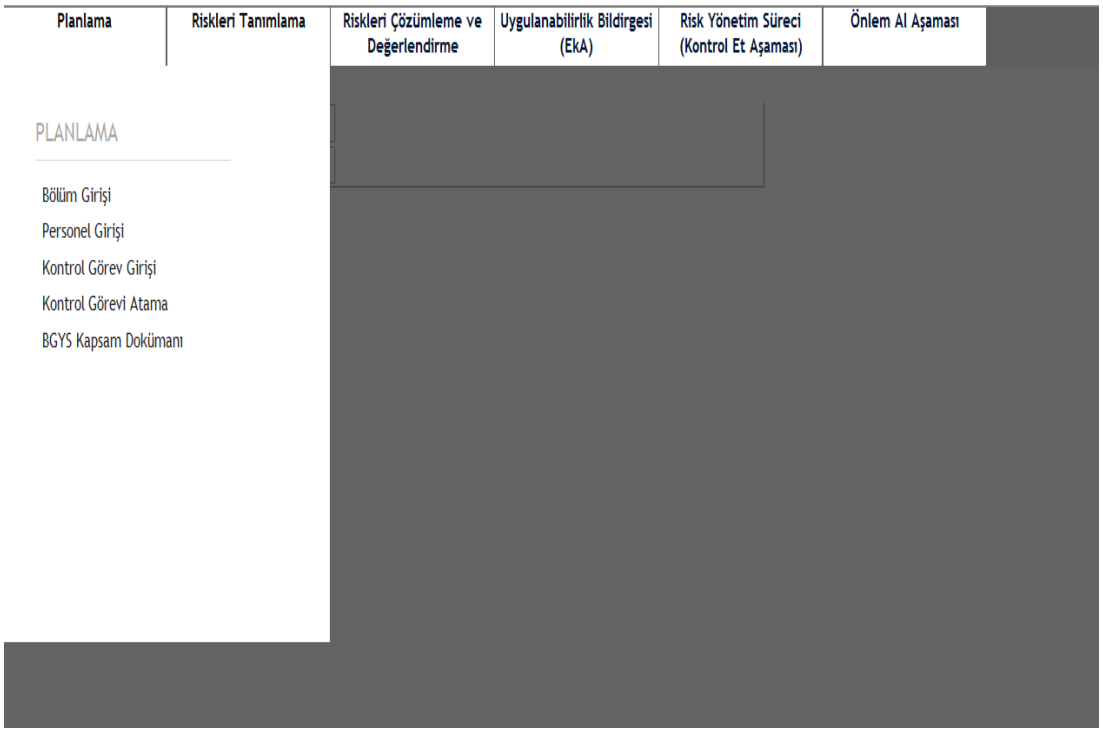
Bu bölümde programımız hakkında bilgiler verilecektir. Şekil 4.4.'de programımızın menüleri gösterilmiştir.



Şekil 4.4 Program menülerinin gösterimi

Programımız altı menüden meydana gelecektir. Bunlar;

1- Planlama Menüsü
2- Riskleri Tanımlama Menüsü
3- Riskleri Çözümleme ve Değerlendirme Menüsü
4- Uygulama Menüsü
5- Risk Yönetim Süreci (Kontrol Et) Menüsü
6- Önlem Al Menüsü



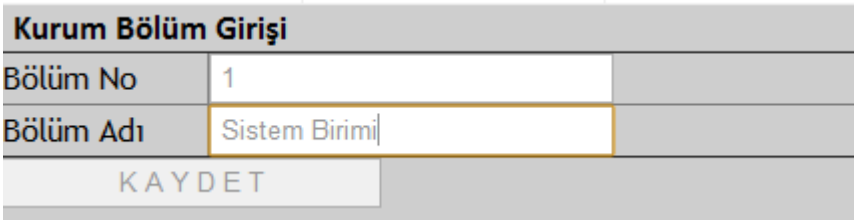
Şekil 4.5. Programın genel görüntüsü

Ayrıca, programlamada kullanılan tablolar NetBeans IDE programında çizilmiştir.

Programımızda bulunan bölümler aşağıda anlatılmıştır:

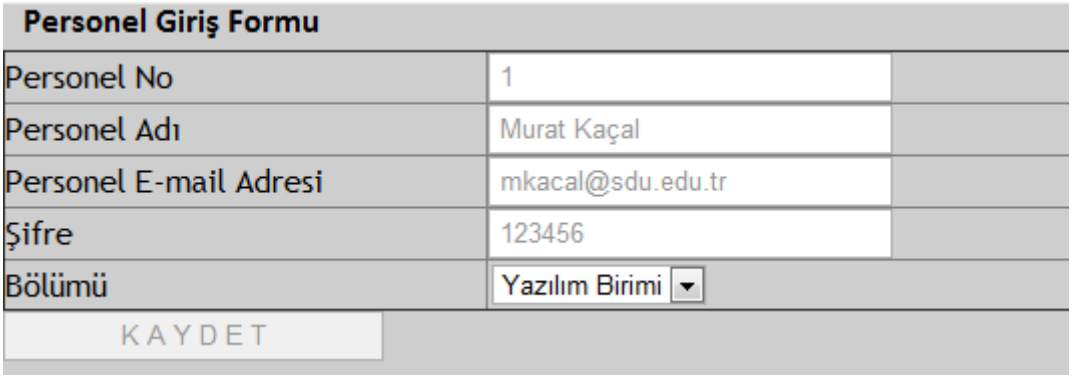
4.8.1. Planlama aşaması

Bölüm Girişi: Bu bölümde, BGYS uygulanacak kurumlarda bulunan tüm bölümlerin kayıt girişi yapılmaktadır. Bölüm Numararası ve Bölüm Adı kayıt altında tutulacaktır (Şekil 4.6.).



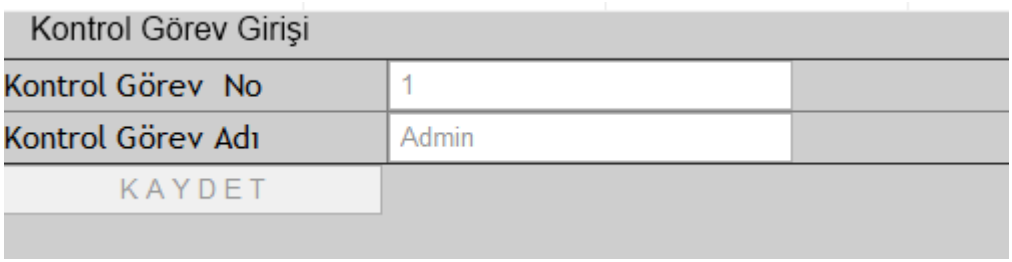
Şekil 4.6. Bölüm girişi formu

Personel Girişi: Bu bölümde, BGYS uygulanacak kurumlarda bulunan tüm bölümlerde çalışan personelin kayıt girişi yapılmaktadır. Personel Numarası, Personel Adı, Personel E-mail Adresi, Şifre ve Bölümü kayıt altında tutulacaktır (Şekil 4.7.).



Şekil 4.7. Personel girişi formu

Kontrol Görev Girişi: Bu bölümde, BGYS uygulanacak kurumlarda bulunan tüm personelin hangi görevde çalışacağının belirlenebilmesi için kayıt girişi yapılmaktadır. Kontrol Görev Numarası ve Kontrol Görev Adı kayıt altında tutulacaktır (Şekil 4.8.).



Şekil 4.8. Kontrol görev girişi formu

Kontrol Görevi Atama: Bu bölümde, BGYS uygulanacak kurumlarda bulunan personel için görev ataması yapılmaktadır. Personel Adı, Kontrol Görev Adı, Kontrol Süresi kayıt altında tutulacaktır (Şekil 4.9.).

Şekil 4.9. Kontrol görevi atama formu

BGYS Kapsam Dokümanı: Proje ekibinin oluşturulmasından sonra ekibin yapacağı çalışmaların sınırları çizilmelidir. Burada kapsamın oluşturulması işlemi, proje ekibi tavsiyesine göre yönetim kurulu kararları çerçevesinde gerçekleştirilecektir. Kapsam her an değişikliğe uğrayabilecek bir olgu olmamasına rağmen genellikle yapılacak ilk çalışmaların neticesinde sınırlarının genişleyebildiği ya da azaltılabildiği görülmektedir (Parendi, 2008).

Yapılacak ilk iş olarak amaç ve kapsam net bir şekilde belirlenmekte ve kapsam dokümanının ilk maddesi olarak yazılmaktadır. Daha sonra organizasyonun yapısı görsel şekilde oluşturulan çizimler üzerinden anlatılmaktadır. Burada merkez, şube ve depoların açık adresleri ile birlikte belirtilmesi daha uygun olacaktır (Mete,2010) (Şekil 4.10.).

BGYS Kapsam Dökümanı Formu	
Kuruluş Yılı	2000
Kurum Adı	S.D.Ü. Bilgi İşlem Daire Başkanlı
Amaç	2000 yılında Isparta'da Süleyman Demirel Üniversitesi İdari Birimi olarak kurulan Bilgi İşlem Daire Başkanlığı kendi personeli, diğer birimlerde bulunan personelin kullandığı bilgi varlıklarının risk yönetimi ve değerlendirilmesi çerçevesinde korunması amacıyla ISO/IEC 27001 BGYS'nin kurulmasına karar vermiştir.
Kapsam	Uygulanacak sistem Bilgi İşlem Daire Başkanlığı'nın tüm bölümlerini kapsayacaktır.
Organizasyon (Kurum Bölümleri)	Bilgi İşlem Daire Başkanlığı BGYS Kapsamına; Sistem & Bilişim Güvenliği Birimi, Teknik Servis Birimi, Yazılım Birimi, Network Birimi, Diğer Kurum ve Kuruluşlar, Bilgi Paylaşımı Güvenlik Yönetimi girmektedir (Perendi 2008:8).
Yerleşke	Süleyman Demirel Üniversitesi, Bilgi İşlem Daire Başkanlığı, Çünür-Isparta.
Varlıklar ve Teknoloji	Personel Kişisel Bilgileri, Tüm BT Sistemleri, Tüm Dokümantasyon Bilgileri.
Hazırlayan	Nilay Temelli
Kontrol Eden	Güncel Sarıman
Onaylayan	Yrd. Doç.Dr. Ecir Uğur Küçüksille

Şekil 4.10. BGYS kapsam dokümanı formu

4.8.2. Riskleri tanımlama aşaması

Riskleri Değerlendirme Yönetim Dokümanı: BGYS standardının gerekliliklerinden biri olan Risk Değerlendirme Yaklaşımı'nın tanımı ile kurum/kuruluşlar, tanımlanmış bilgi güvenliğine uygun bir risk değerlendirme metodolojisi oluşturmalıdırlar. Tanımlanacak yöntemde riskleri kabul etmek için hangi kriterlerin aranacağı ve kabul edilebilir risk seviyeleri belirtilmelidir (ATSEC,2007) (Şekil 4.11.).

Amaç	Risklerin hangi kriterlere göre kontrol uygulanıp uygulanmayacağı, Risk Yönetim Süreci'nde risklerin ne şekilde değerlendirileceği, hangi kritere göre artık risk olarak kabullenileceğini belirleyen Risk Değerlendirme Yöntemi'nin belirlenmesi ve ne şekilde çalışacağının düzenlenmesi.
Kapsam	Tüm BGYS süreçlerini kapsar.
Tarih	10/07/2012
Düzenleyen (Personel Adı)	Murat Kaçal
Olasılık Değeri	2
Etki Değeri	2
Toplam Risk Skoru	2*2=4
Değerlendirme	"Orta" risk seviyesi bulunmaktadı
Hazırlayan	Tuna Göksu
Kontrol Eden	Murat Kaçal
Onaylayan	Yrd. Doç.Dr. Ecir Uğur Küçüksille

Olasılık Değeri		Etki Değeri	
	Düşük	1	Düşük
	Orta	2	Orta
	Yüksek	3	Yüksek

Risk Derecelendirme Matrisi (Risk Skoru Hesaplama)

	OLASILIK		
ETKİ	1 (Düşük)	2(Orta)	3(Yüksek)
1 (Düşük)	1	2	3
2(Orta)	2	4	6
3(Yüksek)	3	6	9

Şekil 4.11. Risk değerlendirme formu

BGYS Varlık Envanteri: Kapsam belirleme işleminin tamamlanmasından sonra üzerinde risk değerlendirmesinin yapılacağı bilgi varlıklarının belirlenmesi işlemi gerçekleştirilecektir. Varlık, kuruluş için değeri olan her şeydir (TSE ISO/IEC 27001, 2006).

Kuruluş için değer taşıyan her olgunun güvenliğinin sağlanması gerekliliği yapılacak çalışmanın amacını oluşturmakta ve tüm varlıkların koruma altına alınması hedeflenmektedir. Bunun için öncelikle varlıkları envanter dahilinde açıklayıcı bir şekilde sıralamak ve sınıflandırmak gerekmektedir (Mete,2010) (Şekil 4.12.).

BGYS Varlık Envanteri Formu

Amaç	Kurumda risk yönetim sürecinin uygulanacağı mevcut tüm bilgi varlıklarının listesini çıkarmaktır.
Kapsam	Yazılım, donanım, fiziksel güvenlik dahil tüm bilgi varlıklarını kapsamaktadır.
Varlık No	5
Varlık Adı	Veritabanları
Varlık Grubu (Bölümü)	Sistem Birimi
Sahibi (Personel Adı)	Tuna Göksu
Varlığın Bulunduğu Yer	Veritabanı Sunucusu
Gizlilik Değeri	2
Bütünlük Değeri	2
Erişebilirlik Değeri	3
Toplam Değer	2*2*3=12
Varlığın Eklenme Tarihi	12/07/2012
Açıklama	Personel Sunucusunda tutulan personel veritabanı, tüm personelin bilgilerinin tutulduğu bilgi varlığıdır
Hazırlayan	Buket Çapalı
Kontrol Eden	Veli Çapalı
Onaylayan	Yrd. Doç.Dr. Ecir Uğur Küçüksille

KAYDET

Gizlilik Değeri		Bütünlük Değeri		Erişebilirlik Değeri	
1	Düşük	1	Düşük	1	Düşük
2	Orta	2	Orta	2	Orta
3	Yüksek	3	Yüksek	3	Yüksek

Şekil 4.12. BGYS varlık envanteri formu

Varlık: Kuruluş için değeri olan ve korunması gereken her şeydir. En somut varlık donanımdan en soyut varlık bilgiye kadar tüm unsurlar belirtilmelidir.

Varlık Grubu: Varlık envanterinin kolayca tasnif edilebilmesi, listede aranan varlığa kolay erişim sağlanabilmesi, düzenli yapının oluşturulması gibi amaçlarla varlıkların gruplandırılması işlemine gidilmektedir. Burada aynı süreç için kullanılan varlıklar gruplandırılabileceği gibi (yedekleme, sistem yönetimi, insan kaynakları) varlığın kendi yapısına göre de gruplandırma (donanım, yazılım, doküman) yapılabilir.

Varlık Sahibi: Varlığın sahibi, onu kullanan ve aynı zamanda bilgi güvenliğini sağlamakla sorumlu olan kişi ve kişilerdir. Burada sorumluluk anlamında kullanılan varlık sahibi örnek vermek gerekirse insan Kaynakları Yönetimi Departmanı ile ilgili bilgilerin sahibi İKY Departman Müdürü'dür. Varlık değerlerinin belirlenmesi ve risk tanımlamalarında BGYS ekibine yardımcı olmak ya da çalışmalarda bizzat görev almak sorumluluğundadır.

Bulunduğu Yer: Hem envanteri yeni okuyan bir yönetici için varlıkların yerlerinin öğrenilmesi, hem de felaket durumlarında ve sonralarında hareket tarzlarının varlıklarının yerlerine göre oluşturulduğu göz önüne alındığında envanterde fiziksel mevkilerin belirtilmesi uygun olacaktır.

Gizlilik Değeri: Varlığın erişimine izin verilmeyen kişiler tarafından erişilip, açığa çıkması ve kötü niyetle kullanılması sonucunda doğacak zararın değerini belirtir. Açığa çıkacak bilginin kurum açısından kritikliğine, kurumun bu bilginin öğrenilmesiyle göreceği etki derecesine göre Düşük, Orta ya da Yüksek olarak sınıflandırılabilmektedir (Mete, 2010).

Bütünlük Değeri: Varlığın bütünlüğünün silinerek ya da değiştirilerek bozulması sonucu doğacak zararın değerini belirtir. Kontrol dışı değişen bilginin değişmesi ya da silinmesi durumunda kurumun göreceği etki derecesine göre Düşük, Orta ya da Yüksek olarak sınıflandırılabilmektedir.

Erişilebilirlik Değeri: Varlığın istenilen anda ve durumda erişilebilirliğinin sekteye uğraması durumunda doğacak zararın değerini belirtir. Varlığa zarar gelmesi durumunda bilginin erişilebilirliği ve bu erişememe durumunda kurumun göreceği etki derecesine göre Düşük, Orta ve Yüksek olarak sınıflandırılabilmektedir.

Toplam Değer: Gizlilik, bütünlük ve erişilebilirlik değerleri kullanılarak bunların matematiksel değerlerinin toplanması ya da çarpılması ile belirlenebilecek bir değerdir.

Varlığın Eklenme Tarihi: Varlığın daha sonraki tarihsel gelişiminin takip edilmesi ya da risk değerlendirilmesinin yapılıp yapılmadığını kontrol edilebilmesi için envantere eklendiği tarihin belirtilmesi uygun olacaktır.

Açıklama: BGYS ekibine varlık hakkında kısaca bilgiler verecek, varlığın kısa tanımı ve ilgili açıklamalar eklenmelidir (Mete, 2010).

Varlıkların Kullanım Politikası: BGYS ekibi tarafından varlıkların ve güvenlik derecelendirmelerinin yapılmasından sonra bu belirlemelere uygun olarak hangi varlığın ne şekilde kullanılması gerektiği, hangi bilginin ne şekilde depolanıp, işlenebileceği ve ne şekilde kurum dışına çıkarılabileceği gibi konularda personeline bilgilendirme konusunda gerekli prosedür ve talimatları oluşturmalıdır. Örnek olarak dizüstü bilgisayar sahibi olan tüm personele dizüstü bilgisayar kullanım prosedürü hazırlanarak bilgisayarın ne şekilde kullanılacağı ve bilgilerin nerelerde depolanacağını bildirmelidir (Mete,2010) (Şekil 4.13.).

Varlıkların Kullanım Politikası

Varlık Adı	Masaüstü Bilgisayarlar
Amaç	Kurum içerisindeki masaüstü bilgisayarların kullanım şartlarını belirlemek.
Kapsam	Kurum içerisinde kullanılan tüm masaüstü bilgisayarları kapsar.
Uygulama(Kullanım Şekli)	Dizüstü bilgisayar kullanıcıları ha
Personel Adı	Mustafa Kestellioğlu
Hazırlayan	Nilay Temelli
Kontrol Eden	Mustafa Kestellioğlu
Onaylayan	Yrd. Doç.Dr. Ecir Uğur Küçüksille

KAYDET

Şekil 4.13. Varlıkların kullanım politikası formu

Tehdit ve Açık Tablosu: Tehdit, herhangi bir bilgi varlığının bilerek ya da kazayla zarar görmesine neden olabilecek olay ya da durumlardır. Tehditlere örnek olarak deprem, sel gibi doğal tehditler, elektrik kesintisi gibi çevresel tehditler, ağ saldırısı, yetkisiz erişim gibi insan kaynaklı tehditler sayılabilir. Burada önemli olan her bir varlık üzerinde oluşabilecek tüm tehditlerin detaylı bir şekilde incelenerek göz ardı edilmemesidir. Bununla ilgili olarak daha önce yaşanmış tecrübeler, bilgi teknolojilerinin ve güvenlik konularının yakından takibi, mevcut tehdit tabloları kaynak olarak kullanılmalıdır (Şekil 4.14.).

Açık ise, bilgi güvenliğini zedeleyebilecek zayıflık, hata ve kusurlardır. Bir tehdidin var olduğu durumlarda tehlike arz etmektedir. Örnek olarak web sunucunun yazılım

port açığı, bu açığı kullanarak kötü niyetli bir kişinin sisteme sızmaya çalışması ile tehlike arz edecektir (Mete,2010).

Tehdit ve Açık Formu	
Sıra No	1
Olayın Cinsi (Tehdit/Açık)	Açık
Tehdit yada Açığın Açıklaması	Donanım ve yazılımların yanlış kullanılması.
Kaynağı	İnsan kaynaklı personel hataları
Hazırlayan	Mustafa Kestellioğlu
Kontrol Eden	Mustafa Kestellioğlu
Onaylayan	Yrd. Doç.Dr. Ecir Uğur Küçüksille
KAYDET	

Şekil 4.14. Tehdit ve açık tablosu formu

4.8.3. Riskleri çözümleme ve değerlendirme aşaması

Risk çözümleme; kuruluş varlık envanterine göre gerçekleştirilen tehdit ve açık belirleme işlemlerinden sonra, varlık, tehdit ve açıkların BGYS ekibi tarafından topluca göz önünde bulundurularak potansiyel risklerin üzerinde detaylı bir şekilde çalışılmasıdır.

Risk derecelendirme, risk çözümleme işleminde BGYS ekibi tarafından kuruluş bilgi varlıkları üzerindeki risklerin nicel ya da nitel olarak ifade edilmesidir. Buradan çıkacak sonuca göre risklere müdahale, önceliklendirilecektir. Tehdit ve açıkların meydana gelme olasılıkları ve etkilerinin çarpımı olarak ifade edilir.

Olasılık değerlendirmede ilk yapılacak işlem BGYS ekibi tarafından kaç kademeli bir değerlendirme yapılacağı ve bu değerlendirmelerin ne şekilde standartlaştırılacağının belirlenmesidir. Burada düşük, orta, yüksek gibi niteleyici ifadeler kullanılabileceği gibi bu ifadelerin rakamsal olarak karşılıkları da kullanılabilmektedir. Etki analizi ise mevcut açıkların meydana gelmesi durumunda

kurumun yaşayacağı etkinin nicel ya da nitel ifadesidir (Eskiyörük, 2007:13) (Şekil 4.15.).

Risk Değerlendirme ve Derecelendirme Formu

Amaç	Uygulanan tüm risk derecelendirme işlemlerinin dokümante edilerek kayıt altına alınmasıdır.
Kapsam	Kurum bilgi varlıkları çerçevesinde mevcut ve potansiyel tüm riskleri kapsamaktadır.
Varlık Adı	Masaüstü Bilgisayarlar
Toplam Değer (Varlık Değeri)	12
Tehdit/Açığın Ne Olduğu	Ağa bağlı masaüstü bilgisayarın içerisindeki önemli bilginin kötü niyetli kişiler tarafından ele geçirilmesi
Olasılık Değeri	3
Etki Değeri	3
Risk Değeri (Olasılık*Etki)	3*3=9
Açıklama	Kurum, Bilgi İşlem Daire Başkanlığı'nın belirleyeceği Risk İşleme Planı'na göre risk işlenecek
Hazırlayan	Nilay Temelli
Kontrol Eden	Güncel Sarıman
Onaylayan	Yrd. Doç.Dr. Ecir Uğur Küçüksille

KAYDET

Olasılık seviyeleri ve Açıklamaları

Olasılık Seviyesi	Açıklama
Düşük (1)	Tehdit kaynağının açıklığı öğrenip, kullanma olanağı düşük ve açıklığın gerçekleşmesini önleyecek kontroller mevcut
Orta (2)	Tehdit kaynağının açıklığı öğrenip, kullanma olanağı yüksek fakat açıklığın gerçekleşmesini önleyecek kontroller mevcut
Yüksek (3)	Tehdit kaynağının açıklığı öğrenip, kullanma olanağı yüksek ve alınan önlemler bulunmamakta ya da etkisiz kalmaktadır.

Etki Analizi Dereceleri ve Açıklamaları

Etki Derecesi	Açıklama
Düşük (1)	Açığın gerçekleşmesi durumunda kurumun kritik bilgileri az etkilenir, kurumun misyonu ve prestiji etkilenmez.
Orta (2)	Açığın gerçekleşmesi durumunda kurumun hassas bilgileri etkilenir, kurum zarara uğrayabilir, misyon ve prestij etkilenebilir.
Yüksek (3)	Açığın gerçekleşmesi durumunda kurumun en hassas bilgileri etkilenir ya da kaybedilir, maddi zarar büyük olur. İnsan hayat kaybı ya da yaralanmalar yaşanabilir, misyon ve kurum çıkarları büyük zarar görebilir.

Risk Dereceleri ve Açıklamaları

Risk Derecesi	Açıklama
Düşük (0-3)	Riske karşı önlem alınıp alınmayacağı sorumlusu tarafından karar verilebilir ve önlem alınmayacaksa risk kabul edilebilir.
Orta (4-6)	Riske karşı önlem alınması gerekmektedir. Alınacak önlemler uygun bir sürede planlanmalı ve uygulanmalıdır.
Yüksek (9)	Riske karşı en yakın zamanda önlem almak gerekmektedir. Sistemin güvenli bir şekilde

Şekil 4.15. Risk değerlendirme ve derecelendirme formu

Kontrol ve Amaçlarını Belirleme: Bu formda belirtilen tehditlere göre risk değeri belirlenecek ve belirlenen risk değerine göre uygun kontroller belirlenecektir.

Varlık: Varlık envanterinden, üzerinde tehdit ve açık olduğu tahmin edilen ve ona göre risk değerlendirmesi yapılan varlığın kendisi.

Tehdit/Açık: Risk değerlendirmesinin yapıldığı ve varlığın güvenlik kriterlerine göre zarar vermesi muhtemel olay.

Risk Değeri: Olasılık ve etki analizi sonuçlarının çarpıldığı değer ya da bu değere karşılık gelen risk önemidir. ("6" ya da "Orta" gibi) Bu değer kontrollerin uygulanmasındaki önceliklerin belirlenmesinde önemli bir kriterdir.

Uygulanacak Kontrol: Risklerin giderilmesi ya da makul bir seviyeye çekilmesinde kullanılacak kontrolün açıklandığı bölümdür. BGYS'nin pratiği olarak görülen kontrollerin uygulanması bu bölümler kullanılarak yapılacağından açıklamaların eksiksiz ve istenilen durumu tam yansıtır şekilde olması kritik öneme sahiptir.

Sorumlular: Kontrolleri uygulayacak kişilerin listelendiği bu bölümde ilgili kontrollerin hangi departmanda ve kimler aracılığıyla uygulanacağı belirtilecektir. Sorumlular belirtilirken yardım alacağı kişilerin de belirtilmesi ile açıklık kazanmış olacaktır. Örneğin Personel Şube ile ilgili bir kontrol gerçekleştirilecekse bu şube personelinin de sorumlu bölümünde belirtilmesi uygun olacaktır.

Atıfta Bulunulan Doküman: Eğer uygulanacak kontrol, oluşturulan/oluşturulacak politika ya da prosedürler ile desteklenecekse burada dokümanın adı ve numarası belirlenecektir. Bu durumda kontrol üzerinde kısa açıklama yapılarak dokümanın okunmasına işaret edilecektir (Şekil 4.15.).

Kontrol ve Amaçlarını Belirleme Formu	
Amaç	Bütün bilgi varlıkları çerçevesince kurumca bulura risklerin işlenmesi için yapılacak kontrollerin belirlenmesidir.
Kapsam	Mevcut ve potansiyel tüm riskleri ve tüm bilgi varlıklarını kapsamaktadır.
Varlık Adı	Masaüstü Bilgisayarlar
Tehdit/Açığın Ne Olduğu	Ağa bağlı masaüstü bilgisayarın kurum dışında kullanımında çalınması
Risk Değeri (Olasılık*Etki)	9
Uygulanacak Kontrol	Öncelikle dizüstü bilgisayarlara Bios özelleriklerinden giriş şifresi tanımlanacaktır. Daha sonra bir klasör oluşturulacak, dizüstü bilgisayar kullanıcıları tarafından işlenen önemli bilgi ve belgeler bu klasöre taşınacak ve klasöre şifre verilerek güvenlik arttırılacaktır. klasöre şifre verilerek güvenlik arttırılacaktır.
Sorumlu (Personel Adı)	Mustafa Kestellioğlu
Atıfta Bulunan Dökümanlar	Bilgi Güvenlik Politikası Dokümanı
Hazırlayan	Nilay Temelli
KAYDET	

Şekil 4.16. Kontrol ve amaçlarını belirleme formu

4.8.4. Uygulanabilirlik bildirgesi (EkA) uygulama aşaması

Birçok proje ve uygulamada kullanılan Uygulanabilirlik Bildirgesi (Statement of Applicability SoA) oluşturulacak ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nde tüm resmin göz önüne getirilmesi ile tanımlanabilir. Standartta geçen tüm maddeler için daha önce nelerin yapıldığı, oluşturulan risk yönetim sürecine göre neler yapılacağı ve atıfta bulunulan dokümanlar belirtilerek sistemi uygulamaya geçirmeden önce tüm işlemlerin eylem planı seklinde sistematik olarak görülmesini sağlar (www.praxiom.com).

Madde: ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi içeriğine göre uygulanması gereken maddeler.

Madde Numarası: İlgili madde numarası (ISO/IEC 27001 ya da kurumun belirleyeceği başka bir numaralandırma).

Kontrol: ISO/IEC 27001 EK-A'sında, ISO/IEC 27002 standardında ve oluşturulan Risk Yönetim Süreci'nde belirtilen gerekliliklerin kurumun Bilgi Güvenliği Yönetim Sistemi'ne uyumun sağlanacağı adımlar olan kontroller.

Mevcut Kontrol: İlgili maddeye göre şu ana kadar yapılan kontrol ve işlemlerdir. Bu maddeye daha önce kaynak alınan bir doküman varsa eklenebilir. İlk defa uygulanacak BGYS'de idari birçok maddenin olmadığı görülmektedir. Fakat teknik olarak birçok konu zaten güvenlik yapısı tarafından oluşturulmuş olacağından teknik konularda yapılanların varsa prosedür/talimatlarıyla birlikte bu bölümde dokümante edilmesi karşılaştırma yapılabilmesi açısından önemlidir.

Artık Risk Açıklaması: Risk Yönetim Süreci'ne göre ilgili madde/kontrol artık risk olarak belirlenmişse bunun nedeninin açıklandığı bölüm.

Kontrolün Seçilme Kaynağı: Burada uygulanacak kontrolün hangi kaynaktan seçildiği belirtilir. Kaynaklara örnek olarak Kanuni Zorunluluklar, Sözleşme Zorunlulukları, İşletmenin Kendi Zorunlulukları, Karşılaşılan ya da Örnek Alınan Olaylar, Risk Yönetim Sonuçları verilebilir. Bu kaynaklar Kurumun yapılarına göre düzenlenecektir (Şekil 4.17.).

Açıklama: İşlem görmesi için onay alınan kontrolün açıklanması. İlgili kontrol kısaca ve açıkça burada belirtilmelidir (Mete,2010).

Uygulanabilirlik Politikası (EkA)	
Madde Numarası	A.5
Kontrol Maddesi	A.5 Güvenlik Politikası
Amaç	Çalışanları kurum bünyesinde kur
Kapsam	Tüm çalışanları kapsamaktadır
Mevcut Kontrol	Bilgi Güvenliği Politikası; Kurumu
Artık Risk Açıklaması	Artık Risk olarak belirlenmemiştir
Kontrolün Seçilme Kaynağı	Karşılaşılan ve Örnek Alınan Olaylar (O)
Açıklama (Bundan Sonra Yapılacak çalışmalar)	Doküman, tüm kurumumuzca üz
Personel Adı	Veli Çapalı
Tarih	12/07/2012
Hazırlayan	Buket Çapalı
Kontrol Eden	Tuna Göksu
Onaylayan	Yrd. Doç.Dr. Ecir Uğur Küçüksille

KAYDET

Kontrolün Seçilme Kaynağı	
IZ	İşletmenin Kendi Zorlukları
O	Karşılaşılan ve Örnek Alınan Olaylar
RY	Risk Yönetim Süreçleri

Şekil 4.17. Uygulanabilirlik bildirgesi (EkA) formu

4.8.5. Risk yönetim süreci (kontrol et aşaması)

Risk İşleme Planı: Risk yönetim sürecinde esas amaç olan risklerin yönetilmesiyle ilgili olarak planlama işlemi yapılıp, bu planların yönetim kurulu tarafından onaylanmasından sonra risk işleme planı hazırlanarak eylem aşamasına geçilecektir. Bu aşamada daha önce seçenekleri belirtilen risk işleme yöntemleri kuruluşun mevcut tüm riskleri üzerine uygulanarak o riske yönelik en uygun yöntemin seçilmesi ve dokümante edilmesi işlemi gerçekleştirilecektir (Brenner, 2007).

Amaç: Risklerin giderme yöntemlerinin, önceliklerinin, planlanan tarihlerin ve sorumluların belirlenmesi.

Kapsam: Mevcut ve potansiyel tüm riskleri kapsamaktadır.

Risk: Bu bölümde üzerinde işlem yapılacak riskler sıralanacaktır.

Risk İşleme Yöntemi: Risk işleme yöntemlerinden hangisinin kullanılacağı açıklanacaktır. Bunlar riski gidermek veya azaltmak için kontrol uygulanması, riskin tamamının veya bir kısmının sigorta ya da başka kurumlara aktarılması ve riskin önemsizliği ya da teknolojik imkanların el vermemesi gibi nedenlerle kabul edilmesidir.

Risk İşleme Yönteminin Açıklanması: Burada seçilen risk isleme yönteminin neye göre ve nasıl seçildiğinden kısaca bahsedilecek ve referans dokümana atıfta bulunulacaktır.

Öncelik: Burada Risk Yönetim Süreci'nde belirlenen risk değerine göre öncelikler belirtilecek ve bunlara göre müdahale yapılacağı beyan edilecektir.

Zaman: Riske uygulanacak kontrolün planlanan başlangıç ve bitiş tarihleri belirtilerek bu tarihler arasında yapılması amaçlanacaktır (Şekil 4.18.).

Sorumlu: Riskin işlenmesi ve sonuçlarının dokümante edilmesi ile ilgili kimlerin görev aldığı burada belirtilecektir (Mete, 2010).

Risk Yönetim Süreci Formu

Amaç	Riskleri çözme yöntemlerinin, ayarlanan tarihlerin, ilk önce yapılacakların, risk işleme sorumlularının belirlenmesi
Kapsam	Kurumda bulunan ve yeni oluşabilen tüm riskleri kapsamaktadır.
Risk	Elektronik Posta Sunucusuna aynı anda birden fazla istek yapılmasıyla hizmetin cevap vereemeyerek durdurulması
Uygun Kontrol Maddesi	A.10.8 Bilgi değişimi
Risk İşleme Yöntemi	Kontrollerin Uygulanarak Riski Azaltma/Giderme
Açıklama(Kontrol)	Bilgi İşlem Daire Başkanlığı tarafından personel bu konu ile ilgili bilgi verilecek ve gelen elektronik postalar incelenerek
Öncelik Sırası	Yüksek
Başlangıç Tarihi	15/07/2012
Bitiş Tarihi	12 Ağustos 2012
Sorumlular(Personel)	Tuna Göksu
Hazırlayan	Buket Çapalı
Kontrol Eden	Veli Çapalı
Onaylayan	Tuna Göksu

KAYDET

NOT:Risk İşleme Yöntemi: Kontrollerin uygulanarak riski azaltma giderme
Öncelik Sırası: Düşük,Orta,Yüksek

Şekil 4.18. Risk yönetim süreci formu

Kontrol Etkinlikleri Ölçülmesi Dokümanı: Bir doküman hazırlanarak tüm kontrollerin etkinliğinin ne şekilde ölçüleceğini belirtmek en doğru yaklaşım olacaktır. Kamu kurumları tarafından yapılacak kontrol etkinliği ölçümü oluşturulacak kontrollerde yapılacak bir hata ya da eksiklikten dolayı oluşacak güvenlik zafiyetlerinin önüne geçecek ve büyük sıkıntılar yaşanmadan önlem alınmasını kolaylaştıracaktır. Uygulanacak kontrol etkinliğini ölçme yöntemleri bir tabloda toplanacak ve tüm kontrollere ayrı ayrı belirtilecektir (Şekil 4.19.).

Kontrol Etkinlikleri Ölçülmesi Dokümanı

Amaç	Riskleri ortadan kaldırmak ya da işlemek için uygulanan kontrollerin etkinliğinin nasıl ölçüleceğini belirlemek.
Kapsam	Uygulanacak tüm yöntem içeren kontrolleri kapsamaktadır.
Risk	Elektronik Posta Sunucusuna aynı anda birden fazla istek yapılmasıyla hizmetin cevap veremeyerek durdurulması.
Açıklama(Kontrol)	Gelen elektronik postaların kontrol edilmesi
Etkinlik Yöntemi (Ayrıca yapılan etkinlikler)	Elektronik postaların kontrol edilerek gereksiz elektronik postaların kullanıcıya gönderilmeden önce silinmesi
Açıklama ve Atıfta Bulunulan Dokuman	Elektronik Posta Kullanımı Dokümanı
Sorumlular(Personel)	Tuna Göksu
Hazırlayan	Veli Çapalı
Kontrol Eden	Buket Çapalı
Onaylayan	Yrd. Doç.Dr. Ecir Uğur Küçüksille

KAYDET

Şekil 4.19. Kontrol etkinlikleri ölçülmesi formu

Politikalar: Kontrol et aşaması ile planlanan ve uygulanan tüm kontrol ve işlemlerin daha önceden kararlaştırılan politika ve talimatlara göre kontrol edilmesi işlemleri gerçekleştirilecektir (Şekil 4.20.).

Politika Formu

Politika No	2
Politika Adı	Elektronik Posta Alt politikası
Amaç	E- posta kullanımını anlatma
Kapsam	Tüm birimleri kapsar
Uygulama	Toplantı ile birimler bilgilendirili
Hazırlayan	Buket Çapalı
Kontrol Eden	Veli Çapalı
Onaylayan	Tuna Göksu

KAYDET

Şekil 4.20. Politika formu

Prosedürler: Kontrol et aşaması ile planlanan ve uygulanan tüm kontrol ve işlemlerin daha önceden kararlaştırılan prosedür ve talimatlara göre kontrol edilmesi işlemleri gerçekleştirilecektir (Mete, 2010) (Şekil 4.21.).

Prosedür Formu

Prosedür No	1
Prosedür Adı	Eğitim ve farkındalık prosedürü
Amaç	Personeli BGYS için bilinçlendir
Kapsam	Tüm birimleri kapsar
Uygulama	Toplantı ile birimler bilgilendirili
Hazırlayan	Nilay Temelli
Kontrol Eden	Murat Kaçal
Onaylayan	Yrd. Doç.Dr. Ecir Uğur Küçüksille

KAYDET

Şekil 4.21. Prosedür formu

4.8.6. Önlem al aşaması

Kişisel Risk Belirleme: Bu bölümde internet üzerinden sorunla karşılaşan personel, sorununu bu ekran üzerinden ilgili kişilere iletebilir (Şekil 4.22.).

Kişisel Risk Belirleme Formu

Problem(Risk)(Olay)	Elektronik posta açılmıyor
Problemle İlgilenecek Olan Bölüm	Sistem Birimi
Problemin Hangi Bölümde Olduğu	Teknik Servis Birimi
Tarih	14/07/2012
Problemi Yazan Kişi (Personel)	Nilay Temelli

KAYDET

Şekil 4.22. Kişisel risk belirleme formu

BGYS Etkinlik Ve Performansını Etkileyecek Olayları Kaydetme: Bilgi Güvenliği Yönetim Sistemi'nin kurulup işletilmesinde ideal yaklaşım meydana gelen tüm bilgi işlem faaliyet ve olaylarının kaydedilmesidir. Bu bilgilerin yazılım üzerinden ya da

kağıt ortamında tutulması, sistemin isleyişinin gözler önüne serilmesi, nereden nereye gelindiğinin bir göstergesi olması gibi yönetimsel nedenlerinin yanında, daha önceki olaylara karsı müdahale yöntemleri, bir daha oluşmaması için alınması gereken önlemler gibi teknik nedenlerden dolayı kritik öneme sahiptir (Şekil 4.23.).

BGYS Etkinlik ve Performansı Etkileyecek Olayları Kaydetme Formu

Sıra No	1
Varlık Adı	Elektronik Posta
Olay(Problem-Risk)	Elektronik Posta Sunucusuna aynı anda birden fazla istek yapılmasıyla hizmetin cevap veremeyerek durdurulması.
Tarih	16/07/2012
Yapılan İşlem (Kontrol)	Sistemde oluşturulacak bir filtreleme sunucusu ile istenmeyen e-postaların alınmamasının sağlanması.
Açıklama	Toplantı sonucu öneriler doğrultusunda Elektronik Posta Sunucu önüne bir adet filtreleme sunucusu kurulacak
Problemi Çözen Kişi (Personel)	Tuna Göksu

KAYDET

Şekil 4.23. BGYS etkinlik ve performansı etkileyecek olayları kaydetme formu

5. TARTIŞMA VE SONUÇ

Günümüzde kamu kurumları içerisinde bilgi güvenliğini uygulamak isteyen yöneticiler için tüm dünyada kabul görmüş en önemli kaynak, ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'dir. Ayrıca kamu kurumlarının ve şirketlerin birçok konuda faaliyet gösterebilmeleri için kurulup, belgelendirilmiş olmaları istenen standart, yine Bilgi Güvenliği Yönetim Sistemi'dir.

Tüm BGYS çalışmaları bilgi varlıklarına yönelik olduğundan, sistemin kurulup işletilmesi aşamalarının ilk muhatabı bilgilerin işlendiği, depolandığı ve saklandığı ortamları yöneten Bilgi İşlem Merkezleri'dir. Standardın pratiğini oluşturan yönetimsel ve teknik uygulamaların büyük bir çoğunluğu bu departman/kuruluşlarda gerçekleştirilmektedir. Bu yüzden tez çalışmasında, Bilgi İşlem Merkezleri'nde ISO/IEC 27001 BGYS Standardının ne şekilde kurulacağı ve hangi adımlar uygulanacağı sorusunun cevabı aranarak gerekli yazılım oluşturulmuştur. Tüm süreçler örnekler verilerek detaylandırılmış, çalışma Bilgi İşlem Merkezi bölümlerine uygulanmış ve örnek dokümanlar oluşturulmuş gerekli raporlar alınmıştır..

Bu uygulama sayesinde kamu kurumları çalışanları bilgi güvenliği konusunda daha bilinçli ve eğitimli olacaktır.

Bu eğitim ve uygulama zor durumlarında dahi bilgi varlıkları kapsamında kurumu en az zararla kurtarma becerisi kazandıracaktır. Bunlardan hareketle Bilişim Teknolojileri piyasasında faaliyet gösteren ya da bünyesinde bu hizmetleri kullanan kurum ve kuruluşlar, kendileri için büyük önem arz eden bilginin ve dolayısıyla süreçlerinin güvenliğini sağlamak amacıyla konuya profesyonel bir bakış açısı getiren Bilgi Güvenliği Yönetim Sistemi'ni benimsemeli ve tüm personeline bilgi güvenliği farkındalığını oluşturmalıdır. Bu kurumlarda, Bilgi Güvenliği Yönetim Sistemi'nin sonsuz PUKÖ döngüsü içerisinde sürekli yaşayacak yapıda kurulup, sistematik bir şekilde yönetilmesinden sonra faaliyet konularındaki tüm işlemlerinin hissedilebilir derecede daha güvenli olduğu ve daha sağlam temeller üzerine oturduğu görülecektir.

Yapılan çalışmaların tüm aşama ve bölümlerini gösteren Türkçe kaynağın çok az olması ve uygulamaların ve bilgilerin sadece danışmanlık şirketleri tarafından ücretler karşılığı verildiği günümüzde, yapılan bu program sayesinde kamu kurum ve şirketlerin Bilgi Güvenliği Yönetim Sistemini kurarken ve bu sitemi geliştirirken zaman ve kaynak ihtiyaçlarını düşüreceği görülmektedir. Bu tez çalışmasında Bilgi Güvenliği Yönetim Sistemini kurup, yönetirken yapılması gereken tüm adımlar sırasıyla programda belirtilmiş ve örneklerle anlatılmıştır. Diğer yapılan çalışmalardan farklı olarak bu tez çalışması ile ilk defa, yapılan program sayesinde, çalışmaların bilgisayar ortamında kayıt altına alınması imkânı yaratılmıştır. İstenildiği zaman bilgisayar ortamında bu bilgilere ulaşılıp, gerektiğinde raporlar alınabilecektir.

"Bilgi Güvenliği Standartları ve Kamu Kurumları İçin Bir Model Önerisi" adındaki bu çalışmada; kamu kurum ve kuruluşlarında kullanılacak yeni Bilgi Güvenliği Modeli önerilmiştir. Kamu kuruluşunda bu modelin nasıl uygulanacağı açıklanmıştır. Kamu kuruluşları bünyesinde bilgi güvenliği kültürünü oluşturacak ISO/IEC 27001 BGYS (Bilgi Güvenliği Yönetim Sistemi) Standardını kurmak ve yönetmek isteyen Kamu Kurum yöneticilerine, yapılan yazılım sayesinde yol gösterici olunmaya çalışılmıştır.

6. KAYNAKLAR

Ayan, Z., 2010. PHP ve MySQL'in Tarihçesi ve Güçlü Yanları, http://www.yazilimprojesi.com, Erişim Tarihi: 02 Nisan 2012.

Bahtiyar, Ş., 2011. Core-crust Modeling Approach For Formal Representation Of Trust In Relation to Computer Security, Boğaziçi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Anabilim Dalı, Doktora Tezi, 229s, İstanbul.

Bilgi Site, 2009. Veri Tabanı Nedir? Veri Tabanı Yönetim Sistemleri. İnternet Sitesi. http://www.bilgisite.com/oracle/vty_07.html. Erişim Tarihi:26.03.2012.

Bingöl, U., 2010. ISO 27001 Bilgi Güvenliği Yönetim Sistemi Otomasyonu, Sakarya Üniversitesi, Sosyal Bilimler Enstitüsü, Çalışma Ekonomisi ve Endüstri İlişkileri Anabilim Dalı, Yüksek Lisans Tezi, 98s, Sakarya.

Boehmer, W., 2010. Toward a target function of an Information SecurityManagement System, Toward a target function of an Information Security Management System, Technische Universität Darmstadt, Germany.

Brenner J., Risk Management, ABD, 2007 http://www.allbusiness.com/ finance/business-insurance-risk- management/ 4060499-1.html. Erişim Tarihi: 02.05.2012.

BSI, 2012. İnternet Sitesi. http://www.bsi-turkey.com/. Erişim Tarihi: 02.05.2011.

Carlson, T., Information Security Management: Understanding ISO 17799. Lucent Technologies, September 2001.

Çetinkaya, M., 2008. Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi İçin Bir Test Aracı Geliştirilmesi, İstanbul Kültür Üniversitesi, Bilgisayar Mühendisliği Bölümü, Yüksek Lisans Tezi, 71s, İstanbul.

Cobit, İnternet Sitesi. http://www.cobit.org. Erişim Tarihi: 02.05.2011.

DoD 5000.2-R, 2006. Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated.

Information Systems (MAIS) Acquisition Programs,1996. Authorized byDoD 5000.1, Defense Acquisition.

DoD 5200.1-I, 1995. DoD Index of Security Classification Guides, authorized by DoD Directive 5200.1.

Doğantimur, F., 2009. ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği, Mesleki Yeterlik Tezi, T.C. Maliye Bakanlığı Strateji Geliştirme Daire Başkanlığı.

Emiral, F., Bilgi Güvenliği Bilincinin Genele Yayılması, http://www.deloitte.com/dtt/article/0,1002,sid%253D8497%2526cid%253D53205,00.html, Erişim Tarihi: 02 Mayıs 2006.

Erkan, A., 2006. An Automated Tool For Information Security Management System, The Middle East Technical University, Master, 96s, Ankara.

Eskiyörük, D., 2007. TÜBİTAK-UEKAE BGYS Risk Yönetim Süreci Kılavuzu.

Gökalp, Z., 2003. İnternet ve Güvenlik. www.bilgiyonetimi.org. Erişim Tarihi: 30.11.2011.

International Standard ISO/IEC 27001, Information technology – Security techniques – Information security management systems – Requirements. İnternet Sitesi. www.iso.org. Erişim Tarihi: 30.12.2011.

ISO 27001 and ISO 27002 are Information Security Standards. İnternet Sitesi. http://www.praxiom.com/iso-27001-definitions.htm. Erişim Tarihi: 28.12.2011.

ISO/IEC 13335-1 :2004, Information technology – Security techniques – Management of information and communications technology security – Part 1: Concepts and models for information and communications technology security management explains the concepts and models for information and communications technology security management. İnternet Sitesi:www.iso.org. Erişim tarihi: 03.01.2012.

ISO 27000 Bilgi Güvenliği Yönetim Sistemi Standartları Nelerdir?. İnternet Sitesi. http://www.isokalitebelgesi.com/iso_belgeleri_egitim_danismanlik/TS_ISO_IEC_27000_27001_27002_27003_27004_27005_22096/Bilgi_g%C3%BCvenligi_yonetim_sistemi_standart_standardi_standartlari_1.php. Erişim tarihi: 03.01.2008.

ISO 27001 Security, 2011. İnternet Sitesi. http://www.iso27001security.com/html/others.html, Erişim Tarihi: 03.01.2012.

ISO 27001 Security, 2011, İnternet Sitesi. http://www.iso27001security.com/html/27002.html, Erişim Tarihi: 03.01.2012.

ISO/IEC 27002:2005 Information technology —— Code of practice for information security management. İnternet Sitesi: www.iso.org. Erişim tarihi: 30.12.2011.

ISO/IEC TR 18044:2004, Information Tecnology- Security techniques -Information security incident management. İnternet Sitesi. www.iso.org. Erişim tarihi: 30.12.2011.

Karabacak, B., 2003. Bilgi Güvenliği Risk Analizi Yöntemi, Gebze Yüksek Teknolojisi Enstitüsü, Bilgisayar Mühendisliği Bölümü, Yüksek Lisans Tezi, 180s, Gebze.

Karabacak, B., 2009. Bilgi Güvenliğinde Risk'in Beş Hali-Kargaşayı Önleme Çabası. http://www.bilgiguvenligi.gov.tr/risk-analizi/bilgi-guvenliginde-risk-in-bes-hali-kargasayi-onleme-cabasi-3.html. Erişim tarihi: 30.05.2012

Kandemirli, B.,M., 2011. Bilgi Teknolojileri Güvenliği ve Sigorta Şirketinde ISO/IEC 27001 Standartları Çerçevesinde Bilgi Güvenlik Yönetim Sistemi Uygulaması, Yıldız Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Endüstri Mühendisliği Anabilim Dalı, Yüksek Lisans Tezi, 301s, İstanbul.

Kesici, 2012. PHP ve MySQL Nedir?. http://blog.gokhankesici.com/php-ve-mysql-nedir/, Erişim Tarihi: 12.03.2012.

Mete, H., 2010. ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi'nin Bilgi İşlem Merkezlerinde Uygulanması. Sakarya Üniversitesi Sosyal Bilimler Enstitüsü, Çalışma Ekonomisi ve Endüstri İlişkileri Anabilim Dalı, Yüksek Lisans Tezi, s.142, Sakarya.

Mysql Komutları Listesi, İnternet Sitesi. http://www.phpkodlari.com/mysql-dersleri/mysql-komutlari-listesi/, Erişim Tarihi:26.05.2012.

OECD, July 2002, Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security, Paris:OECD. İnternet Sitesi. http://www.oecd.org. Erişim Tarihi: 14.05.2011.

OECD, Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security, Paris:OECD, July 2002. İnternet Sitesi. http://www.oecd.org/dataoecd/42/59/32493366.PDF. Erişim Tarihi: 14.05.2011

Ottekin F., 17.10.2008, Bilgi Güvenliğinde ISO 27000 Standartlarının Yeri ve Öncelikli ISO 27002 Kontrolleri. http://www.bilgiguvenligi.gov.tr/teknik-yazilar-kategorisi/bilgi-guvenliginde-iso-27000-standartlarinin-yeri-ve-oncelikli-iso-27002-kontrolleri.html. Erişim Tarihi:20.06.2011.

Önel D., Dinçkan A., 28.08.2007, Bilgi Güvenliği Yönetim Sistemi Kurulumu. www.bilgiguvenligi.gov.tr, Erişim Tarihi: 14.05.2011.

Özkan, Ö., 2004. Veri güvenliğinde saldırı ve savunma yöntemleri, Süleyman Demirel Üniversitesi, Elektronik Haberleşme Mühendisliği, Yüksek Lisans Tezi, Isparta.

Perendi, Ü., 2008. BGYS Kapsamı Belirleme Klavuzu, http://www.bilgiguvenligi.gov.tr/ dokuman - yukle/bgys/uekae - bgys0002 - byskapsami - belirleme-kilavuzu/download.html, Erişim Tarihi:26.03.2011.

Schlienger, T., Teufel, S., 2001. Analyzing Information Security Culture: Increased Trust by an Appropriate Information Security Culture, University of Fribourg, Fribourg.

Sevgi, M., 2008. Bilgi Güvenliği. http://blog.milliyet.com.tr/bilgi-guvenligi-/Blog/?BlogNo=120971, Erişim Tarihi:26.03.2012.

Şahinaslan, E., Kandemir, R., Kantürk A., 2011. Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme, Trakya Üniversitesi, Bilgisayar Mühendisliği Bölümü, Bank Asya, İstanbul.

Tan, H., 2011. IS (Information System) Security Of An Organization And An Application, Başkent Üniversitesi, Fen Bilimleri Enstitüsü, Bilgisayar Mühendisliği Bölümü, Yüksek Lisans Tezi, 113s, Ankara.

Torun, C., 2011. Çizgi-TAGEM e-Kampüs Eğitim Seti PHP & MySQL Eğitimi, http://www.youtube.com/watch?v=1L_Cug3kzv4, Erişim Tarihi: 12.04.2012.

TS ISO/IEC 27001, Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi güvenliği Yönetim Sistemleri, Gereksinimler, Ankara:TSE, Mart 2006, s.1.

TS ISO/IEC 27001,Bilgi Teknolojisi,Güvenlik Teknikleri, Bilgi güvenliği Yönetim Sistemleri, Gereksinimler, Ankara:TSE, Mart 2006, s.2-13.

Tok, H., 2010. Kamu Kurumları İçin Bilgi Güvenliği Yönetişim Modeli, Gebze Yüksek Teknoloji Enstitüsü, Mühendislik ve Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi, 69s, Gebze.

Vikipedi, 2012. İnternet Sitesi. http://tr.wikipedia.org/wiki/ Bilgisayar_güvenliği, Erişim Tarihi: 18 Haziran 2012.

Vural, Y., 2007. Kurumsal Bilgi Güvenliği ve Sızma (Penetrasyon) Testleri, Gazi Üniversitesi, Bilgisayar Mühendisliği Bölümü, Yüksek Lisans, 297s, Ankara.

EKLER

EK-1

ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi Temel ve İç Tetkik Eğitimi Sertifikası

KAS CERT INTERNATIONAL

TRAINING

Sertifika

Sayın, Tuğba HAKLI

20-21-22 Mayıs 2011 tarihlerinde

ISO 27001:2005 Bilgi Güvenliği Yönetim Sistemi

Temel ve İç Tetkik Eğitimi

programını BAŞARI ile tamamlamış ve bu sertifikayı almaya hak kazanmıştır.

Eğitimi Veren
Uğur EKİCİ
IRCA Onaylı Baş Eğitici

Onay
Yusuf ARPACIOĞLU
Genel Müdür

Sertifika No: KAS-27001/TE-İT/35-11-01-01

Standartların her 5 yılda bir gün güncellenmesi sebebi ile ve katılımcının bilgi ve deneyiminin sürdürdüğünden emin olunması amacı ile bu sertifika 5 yılda bir güncelleme eğitimi/değerlendirmesi sonucu yenilenir. Güncelleme tarihi: 06/2016

info@kascert.com www.kascert.com

EK-2

Ek A: Kontrol amaçları ve kontroller

		UYGULANABİLİRLİK BİLDİRGESİ (EK A)
No	Adı	Kontrol
A.5	Güvenlik Politikası	
A.5.1	Bilgi güvenliği politika dökümanı	Amaç:Bilgi güvenliği için, iş gereksininmleri ve ilgili yasa ve düzenlemelere göre yönetim yönlendirmesi ve desteği sağlamak
A.5.1.1	Bilgi güvenliği politika dökümanı	Bilgi güvenliği politika dökümanı, yönetim tarafından onaylanmalı, yayınlanmalı ve tüm çalışanlar ve ilgili dış taraflara bildirilmelidir.
A.5.1.2	Bilgi güvenliği politikasını gözden geçirme	Bilgi güvenliği politikası, belirli aralıklarda veya önemli değişklikler ortaya çıktığında sürekli uygunluğunu, doğruluğunu ve etkinliğini sağlamak için gözden geçirilmelidir.
A.6	Bilgi Güvenliği organizasyonu	
A.6.1	İç Organizasyon	Amaç:Kuruluş içindeki bilgi güvenliğini yönetmek.
A.6.1.1	Yönetimin bilgi güvenliğine bağlılığı	Yönetim kuruluş içinde güvenliği, açık yönlendirme, gösterilen bağlılık, açık atama ve bilgi güvenliği sorumluluklarının kabulu ile etkin bir şekilde desteklemelidir.
A.6.1.2	Bilgi güvenliği koordinasyonu	Bilgi güvenliği faaliyetleri, kuruluşun farklı bölümlerinden uygun rolleri ve iş fonksiyonları olan temsilciler tarafından koordine edilmelidir.
A.6.1.3	Bilgi güvenliği sorumluluklarının tahsisi	Tüm bilgi güvenliği sorumlulukları açıkça tanınmalıdır.
A.6.1.4	Bilgi işleme tesisleri için yetki prosesi	Yeni bilgi işleme tesisleri için, bir yönetim yetki prosesi tanınmalı ve gerçekleştirilmelidir.
A.6.1.5	Gizlilik anlaşmaları	Bilginin korunması için kuruluşun ihtiyaçlarını yansıtan gizlilik ya da açıklamama anlaşmalarının gereksinimleri tanımlanmalı ve düzenli olarak gözden geçirilmelidir.
A.6.1.6	Otoritelerle iletişim	İlgili otoritelerle uygun iletişim kurulmalıdır.
A.6.1.7	Özel ilgi grupları ile iletişim	Özel ilgi grupları veya diğer uzman güvenlik forumları ve profesyonel dernekler ile uygun iletişim kurulmalıdır.
A.6.1.8	Bilgi güvenliği	Kuruluşun bilgi güvenliği yönetimi yaklaşımı ve gerçekleştirilmesi belli aralıklarda veya güvenlik gerçekleştirmesinde önemli değişiklikler olduğunda bağımsız şekilde gözden geçirilmelidir.
A.6.2	Dış Taraflar	Amaç:Kuruluşun dış taraflarca erişilen, işlenen, iletişim kurulan veya yönetilen bilgi ve bilgi işleme olanaklarının güvenliğini sağlamak.
A.6.2.1	Dış taraflarla ilgili riskleri tanmlama	Dış tarafları içeren iş proseslerinden kuruluşun bilgi ve bilgi işleme olanaklarına olan riskler tanımlanmalıve erişim verilmeden önce uygun kontroller yapılmalı.
A.6.2.2	Müşterilerle ilgilenirken güvenliği ifade etme.	Tanımlanmış tüm güvenlik gereksinimleri, müşterilere kuruluşunbilgi ve varlıklarına erişim vermeden önce ifade edilmelidir.
A.6.2.3	Üçüncü taraf antlaşmalarında güvenliği ifade etme.	Üçüncü tarafların, kuruluşun bilgi veya bilgi işleme olanaklarına erişimini, bunlar işlemelerini, bunlarla iletişimni veya bunları yönetmelerini içeren ya da bilgi işleme olanaklarına ürün veya hizmetler ekleyen anlaşmalar
A.7	Varlık Yönetimi	
A.7.1	Varlıkların sorumluluğu	Amaç: Kurumsal varlıkların uygun korumasını sağlamak ve sürdürmek.
A.7.1.1	Varlıkların envanteri	Tüm varlıklar açıkça tanımlanmalı ve önemli varlıkların bir envanteri hazırlanmalı ve tutulmalıdır.
A.7.1.2	Varlıkların sahipliği	Bilgi işleme olanakları ile ilişkili tüm bilgi ve varlıklar kuruluşun belirlenmiş bir bölümü tarafından sahiplenilmelidir.
A.7.1.3	Varlıkların kabul edilebilir kullanımı	Bilgi işleme olanakları ile ilişkili tüm bilgi ve varlıkların kabul edilebilir kullanım kuralları tanımlanmalı, dökümante edilmeli ve gerçekleştirilmelidir.
A.7.2	Bilgi Sınıflandırılması	Amaç:Bilgi varlıklarının uygun seviyede koruma almalrını sağlamak.
A.7.2.1	Sınıflandırma kılavuzu	Bilgi, değeri, yasal gereksinimleri, hassaslığı ve kuruluş için kritikliğine göre sınıflandırılmalıdır.
A.7.2.2	Bilgi etiketleme ve işleme	Bilgi etiketleme ve işleme için kuruluş tarafından benimsenen sınıflandırma düzenine uygun olarak bir dizi uygun prosedür geliştirilmeli ve gerçekleştirilmelidir.

A.8	İnsan Kaynakları Güvenliği	
A.8.1	İstihdam öncesi	Amaç:Çalışanlar, yükleniciler ve üçüncü taraf kullanıcılarınkendi sorumluluklarını anlamalarını ve düşündükleri roller için uygun olmalarını sağlamak ve hırsızlık, sahtecilik ya da olanakların yanlış kullanımı risklerini azatmak.
A.8.1.1	Roller ve sorumluluklar	Çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların güvenlik rolleri ve sorumlulukları kuruluşun bilgi güvenliği politikasına uygun olarak tanımlanmalı ve dökümante edilmelidir.
A.8.1.2	Tarama	Tüm işe alım adayları, yükleniciler ve üçüncü taraf kullanıcılar için ilgili yasa, düzenleme ve etiğe göre ve iş gereksinimleri, erişilecek bilginin sınıflandırması ve alınan risklerle orantılı olarak geçmiş doğrulama kontrolleri gerçekleştirilmelidir.
A.8.1.3	İstihdam Koşulları	Sözleşme yükümlülüklerinin parçası olarak , çalışanlar, yükleniciler ve üçüncü taraf kullanıcılar, kendilerinin ve kuruluşun bilgi güvenliği sorumluluklarını belirten kendi işe alım sözleşmelerinin koşullarına katılmalı ve bunu imzalamalıdırlar.
A.8.2	Çalışma esnasında	Amaç:Tüm çalışanlar , yükleniciler ve üçüncü taraf kullanıcılarının bilgi güvenliğine ilişkin tehditler ve kaygıların ve kendi sorumluluklarının farkında olmalarını ve normal çalışmaları sırasında kurumsal güvenlik politikasını desteklemek ve insan hatası riskini azaltmak üzere donatıl
A.8.2.1	Yönetim sorumlulukları	Yönetim, çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların, kuruluşun yerleşik politika ve prosedürlerine göre güvenliği uygulamalarını istemelidir.
A.8.2.2	Bilgi güvenliği farkındalığı, eğitim ve öğretimi	kuruluştaki tüm çalışanlar ve ilgili olan yerlerde yükleniciler ve üçüncü taraf kullanıcılar, kendi iş fonksiyonları ile ilgili olduğunda, kurumsal politikalar ve prosedürlerle ilgili uygun farkında olma eğitimi ve düzenli güncelleme almalıdırlar.
A.8.2.3	Disiplin prosesi	Bir güvenlik kırılmasına yol açan çalışanlar için resmi bir disiplin prsesi olmalıdır.
A.8.3	İstihdamın sonlandırılması veya değiştirilmesi	Amaç:Çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların düzenli bir şekilde kuruluştan ayrılmalarını veya istihdamın değiştirilmesini sağlamak.
A.8.3.1	Sonlandırma sorumlulukları	İstihdamın sonlandırılmasını veya değiştirilmesini gerçekleştirme sorumlulukları açıkça tanımlanmalı ve atanmalıdır.
A.8.3.2	Varlıkların iadesi	Tüm çalışanlar, yükleniciler ve üçüncü taraf kullanıcılar, çalışmaları, sözleşmeleri veya anlaşmalarının sonlandırılmasıyla birlikte kendilerinde bulunan kuruluşun tüm varlıklarını iade etmelidirler.
A.8.3.3	Erişim haklarının kaldırılması	Tüm çalışanlar, yükleniciler ve üçüncü taraf kullanıcıların bilgi ve bilgi işleme olanaklarına olan erişim hakları, istihdam, sözleşme veya anlaşmalarının sonlandırılmasıyla birlikte kaldırılmalı ya da değiştirilmesiyle birlikte ayarlanmalıdır.
A.9	Fiziksel Çevre ve Güvenlik	
A.9.1	Güvenli Alanlar	Amaç: Kuruluş binalarına, ünitelerine ve bilgilerine yetki dışı fiziksel erşimi, hasarı ve müdahaleyi engellemek.
A.9.1.1	Fiziksel Güvenlik çevresi	Bilgi ve bilgi işleme olanaklarını içeren alanları korumak için güvenlik çevreleri (duvarlar gibi engeller, kart kontrollü giriş kapıları, güvenli bulunan resepsiyon masaları) kullanılmalıdır.
A.9.1.2	Fiziksel giriş kontrolleri	Güvenli alanlar, yalnız yetkili personelin erişime izin verilmesini sağlamak için uygun giriş kontrolleriyle korunmalıdır.
A.9.1.3	Ofisler, odalar ve olanakları korumaya alma	Ofisler, odalar ve olanaklar için fiziksel güvenlik tasarlanmalı ve uygulanmalıdır.
A.9.1.4	Dış ve çevresel tehditlere karşı koruma	Yangın, sel, deprem, patlama, yağma ve diğer doğal ya da insan kaynaklı felaketlerden kaynaklanan hasara karşı fiziksel koruma tasarlanmalı ve uygulanmalıdır.
A.9.1.5	Güvenli alanlarda çalışma	Güvenli alanlarda çalışma için fiziksel koruma tasarlanmalı ve uygulanmalıdır.
A.9.1.6	Açık erişim, dağıtım ve yükleme alanları	Dağıtım ve yükleme alanları gibi erişim noktaları ve yetkisiz kişilerin içeri girebileceği diğer noktalar kontrol edilmeli ve mümkünse yetkisiz erişimden kaçınmak için bilgi işleme olanaklarından yalıtılmalıdır.
A.9.2	Teçhizat Güvenliği	Amaç: Varlıkların kaybını, hasarını, çalınmasını ya da tehlikeye girmesini ve kuruluşun faaliyetlerinin kesintiye uğramasını engellemek.
A.9.2.1	Teçhizat yerleştirme ve koruma	Teçhizat, çevresel tehditlerden ve tehlikelerden kaynaklanan riskleri ve yetkisiz erişim fırsatlarını azaltmak için yerleştirilmeli ve korunmalıdır.
A.9.2.2	Destek hizmetleri	Teçhizat, elektrik kesintileri ve destek hizmetlerindeki arızalardan kaynaklanan diğer bozulmalara karşı korunmalıdır.
A.9.2.3	Kablolama güvenliği	Veri taşıyan ya da bilgi hizmetlerini destekleyen elektrik ve haberleşme kabloları, kesilme ya da hasarlardan korunmalıdır.
A.9.2.4	Teçhizat bakımı	Teçhizatın sürekli kullanabilirliğini ve bütünlüğünü sağlamak için doğru şekilde bakımı yapılmalıdır.
A.9.2.5	Kuruluş dışındaki teçhizatın güvenliği	Kuruluş çevresi dışında çalışmanın farklı risklerini hesaba katarak kuruluş dışındaki teçhizata güvenlik uygulanmalıdır.

A.9.2.6	Teçhizatın güvenli olarak elden çıkarılması ya da tekrar kullanımı	Teçhizatın depolama ortamı içeren tüm parçaları elden çıkarılmadan önce, herhangi bir hassas veri ve lisanslı yazılım varsa kaldırılmasını veya güvenli bir şekilde üzerine yazılmasını sağlamak için kontrol edilmelidir.
A.9.2.7	Mülkiyet çıkarımı	Ön yetkilendirme olmaksızın teçhizat, bilgi veya yazılım bulunduğu yerden çıkarılmamalıdır.
A.10	Haberleşme ve İşletim Yönetimi	
A.10.1	Operasyonel prosedürler ve sorumluluklar	Amaç: Bilgi işleme olanaklarının doğru ve güvenli işletimini sağlamak.
A.10.1.1	Dökümante edilmiş işletim prosedürleri	İşletim prosedürleri dökümante edilmeli, sürdürülmeli ve ihtiyacı olan tüm kullanıcılara kullanılabilir yapılmalıdır.
A.10.1.2	Değişim Yönetimi	Bilgi işleme olanakları ve sistemlerinde olan değişiklikler kontrol edilmelidir.
A.10.1.3	Görev Ayrımları	Kuruluşun varlıklarının yetkisiz veya farkında olmadan değiştirilme ya da kötüye kullanılma fırsatlarını azaltmak için, görevler ve sorumluluk alanları ayrılmalıdır.
A.10.1.4	Geliştirme, test ve işletim olanaklarının ayrımı	Geliştirme, test ve işletim olanakları, işletilen sisteme yetkisiz erişim veya değişiklik risklerini azaltmak için ayrılmalıdır.
A.10.2	Üçüncü taraf hizmet sağlama yönetimi	Amaç:Üçüncü taraf hizmet sağlama anlaşmalarıyla uyumlu olarak uygun bilgi güvenliği ve hizmet dağıtımı seviyesi gerçekleştirmek ve sürdürmek.
A.10.2.1	Hizmet sağlama	Güvenlik kontrolleri, hizmet tanımları ve sağlama seviyelerinin üçüncü taraf hizmet sağlama anlaşmasında bulunması ve üçüncü tarafça gerçekleşirilmesi, işletilmesi ve sürdürülmesi sağlanmalıdır.
A.10.2.2	Üçüncü taraf hizmetleri izleme ve gözden geçirme	Üçüncü tarafa sağlanan hizmetler, raporlar ve kayıtlardüzenli olarak izlenmeli, gözden geçirilmeli ve düzenli olarak denetimler gerçekleştirilmelidir.
A.10.2.3	Üçüncü taraf hizmetlerdeki değişiklikleri yönetme	Mevcut bilgi güvenliği politikaları, prosedürleri ve kontrollerini sürdürme ve iyileştirmeyi içeren hizmet tedariği değişiklikleri, ilgili iş sistemleri ve proseslerinin kritikliğini ve risklerin yeniden değerlendirmesini hesaba katark yönetilmelidir.
A.10.3	Sistem planlama ve kabul	Amaç: Sistem başarısızlıkları riskini en aza indirmek
A.10.3.1	Kapasite planlama	Gerekli sistem performansını sağlamak için kaynakların kullanımı izlenmeli, ayarlanmalı ve gelecekteki kapasite gereksinimleri için projeksiyonlar yapılmalıdır.
A.10.3.2	Sistem kabulu	Yeni bilgi sistemleri sistem yükseltmleri ve yeni sürümler için kabul kriterleri kurulmalı ve geliştirme esnasında ve kabul öncesinde sistem(ler)e ilişkin uygun testler gerçekleştirilmelidir.
A.10.4	Kötü niyetli ve mobil koda karşı koruma	Amaç:Yazılım ve bilginin bütünlüğünü korumak
A.10.4.1	Kötü niyetli koda karşı kontroller	Kötü niyetli koda karşı korunmak için saptanan önleme ve kurtarma kontrolleri ve uygun kullanıcı farkındalığı prosedürleri gerçekleştirilmelidir.
A.10.4.2	Mobil koda karşı kontroller	Mobil kod kullanımı yetkilendirildiğinde,konfigürasyon yetkilendirilmiş mobil kodun açıkça tanımlanmış bir güvenlik politikasına göre işletilmesini sağlamalı ve yetkilendirilmemiş mobil kodun yürütülmesi önlenmelidir.
A.10.5	Yedekleme	Amaç: Bilgi ve bilgi işleme olanaklarının bütünlüğünü ve kullanabilirliğini sağlamak.
A.10.5.1	Bilgi yedekleme	Bilgi ve yazılımlara ait yedekleme kopyalarının alınmalı ve anlaşılan yedekleme politikasına uygun şekilde düzenli olarak test edilmelidir.
A.10.6	Ağ güvenliği yönetimi	Amaç: Ağdaki bilginin ve destekleyici alt yapının korunmasını sağlamak
A.10.6.1	Ağ kontrolleri	Tehditlerden korunmak için ve iletilmekte olan bilgi dahil ağı kullanan sistemler ve uygulamalar için güvenliği sağlamak için ağlar uygun şekilde yönetilmeli ve kontrol edilmelidir.
A.10.6.2	Ağ hizmetleri güvenliği	Tüm ağ hizmetlerinin güvenlik özellikleri hizmet seviyeleri ve yönetim gereksinimleri tanımlanmalı ve hizmetler kuruluşu içinden ya da dışından sağlanmış olsun her ağ hizmetleri anlaşmasında bulunmalıdır.
A.10.7	Ortam işleme	Amaç:Varlıkların yetkisiz ifşa edilmesi, değiştirilmesi, kaldırılması veya yok edilmesini ve iş faaliyetlerinin kesintiye uğramasını önlemek.
A.10.7.1	Taşınabilir ortam yönetimi	Taşınabilir ortam yönetimi için mevcut prosedürler olmalıdır.
A.10.7.2	Ortamın yok edilmesi	Ortam gereksinimi ortadan kalktığında resmi prosedürler kullanılarak güvenli ve emniyetli biçimde yok edilmelidir.
A.10.7.3	Bilgi işleme prosedürleri	Bilgi işleme ve depolama prosedürleri bu bilgileri yetkisiz ifşa edilmeye ya da kötüye kullanılmaya karşı korumak için kurulmalıdır.
A.10.7.4	Sistem dökümantasyonu güvenliği	Sistem dökümantasyonu yetkisiz erişime karşı korunmalıdır.

A.10.8	Bilgi Değişimi	Amaç:Bir kuruluş içindeki ve herhangi bir dış varlık ile değiştirilen bilgi ve yazılımın güvenliğini sağlamak.
A.10.8.1	Bilgi değişim politikaları ve prosedürleri	Tüm iletişim olanağı türlerinin kullanımıyla bilgi değişimini korumak için resmi değişim politikaları, prosedürleri ve kontrolleri mevcut olmalıdır.
A.10.8.2	Değişim anlaşmaları	Kuruluş ve dış taraflar arasında bilgi ve yazılımın değişimi için anlaşmalar yapılmalıdır.
A.10.8.3	Aktarılan fiziksel ortam	Bilgi içeren ortam kuruluşun fiziksel sınırları ötesinde taşıma esnasında yetkisiz erişime, kötüye kullanıma ya da bozulmalara karşı korunmalıdır.
A.10.8.4	Elektronik mesajlaşma	Elektronik mesajlaşmadaki bilgi uygun şekilde korunmalıdır.
A.10.8.5	iş bilgi sistemleri	iş bilgi sistemlerinin birbirine bağlantısı ile ilişkili bilgiyi korumak için politikalar ve prosedürler geliştirilmeli ve gerçekleştirilmelidir.
A.10.9	Elektronik ticaret hizmetleri	Amaç: Elektronik ticaret hizmetlerinin güvenliğini ve bunların güvenli kullanımını sağlamak.
A.10.9.1	Elektronik ticaret	Açık ağlardan geçen elektronik ticaretteki bilgi, hileli faaliyet, anlaşma uyuşmazlığı ve yetkisiz ifşa ve değiştirmeden korunmalıdır.
A.10.9.2	Çevrimiçi işlemler	Çevrimiçi işlemlerdeki bilgi, eksik iletimi, yanlış yönlendirmeyi, yetkisiz mesaj değiştirmeyi, yetkisiz ifşayı, yetkisiz mesaj çoğaltmayı ya da yeniden yürütmeyi önlemek için korunmalıdır.
A.10.9.3	Herkese açık bilgi	Herkese açık bir sistemde kullanılabilir yapılmış bilginin bütünlüğü yetkisiz değiştirmeyiönlemek için korunmalıdır.
A.10.10	İzleme	Amaç:Yetkisiz bilgi işleme faaliyetlerini algılamak.
A.10.10.	Denetim kaydetme	Kullanıcı faaliyetleri, ayrıcalıkları ve bilgi güvenliği olaylarını kaydeden denetim kayıtları üretilmeli ve ileride yapılabilecek soruşturmalar ve erişim kontrolü izlemeye yardımcı olmak için anlaşılmış bir süre tutulmalıdır.
A.10.10.	Sistem kullanımını izleme	Bilgi işleme olanaklarının kullanımını izlemek için prosedürler oluşturulmalıve izleme faaliyetlerinin sonuçları düzenli şekilde gözden geçirilmelidir.
A.10.10.	Kayıt bilgisinin korunması	Kayıt olanakları ve kayıt bilgisi kurcalanma ve yetkisiz erişime karşı korunmalıdır.
A.10.10.	Yönetici ve operatör kayıtları	Sistem yöneticisi ve operatör faaliyetleri kaydedilmelidir.
A.10.10.	Hata kaydı	Hatalar kaydedilmeli, çözümlenmeli ve uygun önlemler alınmalıdır.
A.10.10.	Saat senkronizasyonu	Bir kuruluş ya da güvenlik etki alanındakitüm ilgili bilgi işleme sistemlerinin saatleri, üzerinde uzlaşıya varılmış doğru bir zaman kaynağı ile senkronize edilmelidir.
A.11	Erişim Kontrolü	
A.11.1	Erişim kontrolü için iş gereksinimi	Amaç:Bilgiye erşimi kontrol etmek.
A.11.1.1	Erişim kontrolü politikası	Erişim için iş ve güvenlik gereksinimlerini temel alan bir erişim kontrol politikası kurulmalı, dökümante edilmeli ve gözden geçirilmelidir.
A.11.2	Kullanıcı erişim yönetimi	Amaç:Bilgi sistemlerine yetkili kullanıcı erişimi sağlamak ve yetkisiz erişimi önlemek.
A.11.2.1	Kullanıcı Kaydı	Tüm bilgi sistemlerine ve hizmetlerine erişim izni vermek ve bunu kaldırmak için resmi bir kullanıcı kaydetme ve kayıttan çıkarma prosedürü olmalıdır.
A.11.2.2	Ayrıcalık yönetimi	Ayrıcalıkların tahsisi ve kullanımı sınırlandırılmalı ve kontrol edilmelidir.
A.11.2.3	Kullanıcı parola yönetimi	Parolaların tahsisi, resmi bir yönetim prosesi aracılığıyla kontrol edilmelidir.
A.11.2.4	Kullanıcı erişim haklarının gözden gerçirilmesi	Yönetim, kullanıcıların erişim haklarını resmi bir proses kullanarak düzenli aralıklarda gözden geçirmelidir.
A.11.3	Kullanıcı sorumlulukları	Amaç:Yetkisiz kullanıcı erişimini ve bilgi ve bilgi işleme olanaklarının tehlikeye atılmasını ya da çalınmasını önlemek.
A.11.3.1	Parola Kullanımı	Kullanıcılardan, parolaların seçiminde ve kullanımında iyi güvenlik uygulamalarını izlemeleri istenmelidir.
A.11.3.2	Gözetimsiz kullanıcı teçhizatı	Kullanıcılar, gözetimsiz teçhizatın uygun bir korumaya sahip olmasını sağlamalıdır.
A.11.3.3	Temiz masa ve temiz ekran politikası	Kağıtlar ve taşınabilir depolama ortamları için bir temiz masa politikası ve bilgi işleme olanakları için bir temiz ekran politikası benimsenmelidir.

A.11.3.3	Temiz masa ve temiz ekran politikası	Kağıtlar ve taşınabilir depolama ortamları için bir temiz masa politikası ve bilgi işleme olanakları için bir temiz ekran politikası benimsenmelidir.
A.11.4	Ağ Erişim Kontrolü	Amaç: Ağ bağlantılı hizmetlere yetkisiz erişimi önlemek.
A.11.4.1	Ağ hizmetlerinin kullanımına ilişkin politika	Kullanıcıların sadece, özellikle kullanımlarına yetki verilen hizmetlereerişime sahip olmaları sağlanmalıdır.
A.11.4.2	Dış bağlantılar için kullanıcı kimlik doğrulama	Uzaktan kullanıcıların erişimini kontrol etmek için uygun kimlik doğrulama metodları kullanılmalıdır.
A.11.4.3	Ağlarda teçhizat tanımlama	Otomatik teçhizat tanımlama, belirli yerler ve teçhizattan bağlantıların kimliğini doğrulamak için bir yöntem olarak düşünülmelidir.
A.11.4.4	Uzak tanı ve yapılandırma portu koruma	Tanı ve yapılandırma portlarına fiziksel ve mantıksal erişim kontrol edilmelidir.
A.11.4.5	Ağlarda ayrım	Ağlarda, bilgi hizmetleri, kullanıcıları ve bilgi sistemleri grupları ayrılmalıdır.
A.11.4.6	Ağ bağlantı kontrolü	Özellikle kuruluşun sınırlarını aşan paylaşılan ağlar için, kullanıcıların ağa bağlanabilme yetenekleri erişim kontrol politikası ve iş uygulamalrının gereksinimlerine uygun olarak sınırlanmalıdır.
A.11.4.7	Ağ yönlendirme kontrolü	Ağlar için, bilgisayar bağlantılarının ve bilgi akışlarının iş uygulamalarının erişim kontrol politikasını ihlal etmemesini sağlamak için yönlendirme kontrolleri gerçekleştirilmelidir.
A.11.5	İşletim sistemi erişim kontrolü	Amaç: İşletim sistemine yetkisiz erişimi önlemek.
A.11.5.1	Güvenli oturum açma prosedürleri	İşletim sistemelerine erişim güvenli bir oturum açma prosedürü ile kontrol edilmelidir.
A.11.5.2	Kullanıcı kimlik tanımlama ve doğrulama	Tüm kullanıcılar, kendi kişisel kullanımları için, benzersiz bir kimliğe (kullanıcı kimliği) sahip olmalıdırlar ve bir kullanıcının öne sürdüğü kimliğini ispatlamak için uygun bir kimlik doğrulama tekniği seçilmelidir.
A.11.5.3	Parola yönetim sistemi	Parola yönetim sistemleri etkileşimli olmalı ve nitelikli parolalar sağlamalıdır.
A.11.5.4	Yardımcı sistem programlarının kullanımı	Sistemin üzerine yazabilme yeteneği olabilecek yardımcı sistem programlarının kullanımı kısıtlanmalı ve sıkıca kontrol edilmelidir.
A.11.5.5	Oturum zaman aşımı	Etkin olmayan oturumlar tanımlanmış belirli bir hareketsizlik süresinden sonra kapatılmalıdır.
A.11.5.6	Bağlantı süresinin sınırlandırılması	Bağlantı sürelerinde sınırlandırılmalar, yüksek riskli uygulamalara ek güvenlik sağlamak için kullanılmalıdır.
A.11.6	Uygulama ve bilgi erişim kontrolü	Amaç: Uygulama sistemlerinde tutulan bilgilere yetkisiz erişimi önlemek.
A.11.6.1	Bilgi erişim kısıtlaması	Kullanıcılar ve destek personeli tarafından bilgi ve uygulama sistem işlevlerine erişim, tanımlanmış erişim kontrol politikasına uygun olarak kısıtlanmalıdır.
A.11.6.2	Hassas sistem yalıtımı	Hassas sistemler adanmış (yalıtılmış) bir bilgi işlem ortamına sahip olmalıdır.
A.11.7	Mobil bilgi işleme ve uzaktan çalışma	Amaç: Mobil bilgi işleme ve uzaktan çalışma hizmetlerini kullanırken bilgi güvenliğini sağlamak.
A.11.7.1	Mobil bilgi işleme ve iletişim	Resmi bir politika bulunmalı ve mobil bilgi işleme ve iletişim olanaklarının kullanılma risklerine karşı korunmak için uygun güvenlik önlemleri benimsenmelidir.
A.11.7.2	Uzaktan çalışma	Uzaktan çalışma faaliyetleri için bir politika, operasyonel planlar ve prosedürler geliştirilmeli ve gerçekleştirilmelidir.
A.12	Bilgi sistemleri edinim, geliştirme ve bakımı	
A.12.1	Bilgi sistemlerinin güvenlik gereksinimleri	Amaç:Güvenliğin bilgi sistemlerinin dahili bir parçası olmasını sağlamak.
A.12.1.1	Güvenlik gereksinimleri analizi ve belirtimi	Yeni bilgi sistemleri için iş gereksinimleri bildirgeleri ya da mevcut bilgi sistemlerine yapılan iyileştirmeler güvenlik kontrolleri için gereksinimleri belirlemelidir.
A.12.2	Uygulamalarda doğru işleme	Amaç:Uygulamalardaki bilginin hatalarını, kaybını, yetkisiz değiştirilmesini ve kötüye kullanımını önlemek.
A.12.2.1	Giriş verisi geçerleme	Uygulamalara veri girişi, bu verinin doğruluğunun ve uygunluğunun sağlanması için geçerlenmelidir.
A.12.2.2	İç işleme kontrolü	İşleme hataları veya kasıtlı eylemler nedeniyle herhangi bir bilgi bozulmasını saptamak için geçerleme kontrolleri uygulamalar içine dahil edilmelidir.
A.12.2.3	Mesaj bütünlüğü	Uygulamalarda verinin kimliğinin doğruluğunu sağlama ve mesaj bütünlüğünü koruma gereksinimleri tanımlanmalı ve uygun kontroller tanımlanıp gerçekleştirilmelidir.

A.12.2.4	Çıkış verisi geçerleme	Bir uygulamadan veri çıktısı, depolanan bilginin işlenmesinin koşullara göre doğrukuğunun ve uygunluğunun sağlanması için geçerlenmelidir.
A.12.3	Kriptografik kontroller	Amaç:Bilginin gizliliğini, aslına uygunluğunu ya da bütünlüğünü kriptografik yöntemlerle korumak.
A.12.3.1	Kriptografik kontrollerin kullanımına ilişkin politika	Bilginin korunması için kriptografik(şifreleme) kontrollerin kullanımına ilişkin bir politika geliştirilmeli ve gerçekleştirilmelidir.
A.12.3.2	Anahtar yönetimi	Kuruluşun kriptografik teknikleri kullanmasını desteklemek için anahtar yönetimi bulunmalıdır.
A.12.4	Sistem dosyalarının güvenliği	Amaç: Sistem dosyalarının güvenliğini sağlamak.
A.12.4.1	Operasyonel yazılımın kontrolü	Operasyonel sistemlerdeki yazılımların kurulmasını kontrol etmek için prosedürler bulunmalıdır.
A.12.4.2	Sistem test verisinin korunması	Test verisi dkkatlice seçilmeli, korunmalı ve kontrol edilmelidir.
A.12.4.3	Program kaynak koduna erişim kontrolü	Program kaynak koduna erişim kısıtlı olmalıdır.
A.12.5	Geliştirme ve destekleme proseslerinde güvenlik	Amaç:Uygulamam sistem yazılımı ve bilgisinin güvenliğini sağlamak
A.12.5.1	Değişim kontrol prosedürleri	Değişikliklerin gerçekleştirilmesi, resmi değişim kontrol prosedürlerinin kullanımı ile kontrol edilmelidir.
A.12.5.2	İşletim sistemindeki değişikliklerden sonra teknik gö	İşletim sistemindeki değişikliklerden sonra teknik gözden geçirme
A.12.5.3	Yazılım paketlerindeki değişikliklerdeki kısıtlamalar	Yazılım paketlerine yapılacak değişiklikler, gerek duyulanlar hariç önlenmeli ve tüm değişiklikler sıkı bir biçimde kontrol edilmelidir.
A.12.5.4	Bilgi sızması	Bilgi sızması fırsatları önlenmelidir.
A.12.5.5	Dışarıdan sağlanan yazılım geliştirme	Dışarıdan sağlanan yazılım geliştirme kuruluş tarafından denetlenmeli ve izlenmelidir.
A.12.6	Teknik açıklık yönetimi	Amaç:Yayınlanmış teknik açıklıkların istismarından kaynaklanan riskleri azaltmak.
A.12.6.1	Teknik açıklıkların kontrolü	Kullanılan bilgi sisteminin teknik açıklıkları hakkında zamanında bilgi elde edilmeli, kuruluşun bu tür açıklıklara maruz kalması değerlendirilmeli ve ilişkili riskleri hedef alan uygun önlemler alınmalıdır.
A.13	Bilgi güvenliği ihlal olayı yönetimi	
A.13.1	Bilgi güvenliği olayları ve zayıflıklarının rapor edilmeş	Amaç: Bilgi sistemleri ile ilişkili bilgi güvenliği olayları ve zayıflıklarının zamanında düzeltici önlemlerin alınabilmesine izin verecek şekilde bildirilmesini sağlamak.
A.13.1.1	Bilgi güvenliği olaylarının rapor edilmesi	Bilgi güvenliği olayları uygun yönetim kanalları aracılığıyla mümkün olduğu kadar hızlı biçimde rapor edilmelidir.
A.13.1.2	Güvenlik zayıflıklarının rapor edilmesi	Bilgi sistemleri ve hizmetlerinin tüm çalışanları, yüklenicileri ve üçüncü taraf kullanıcılarından, sistemler ve hizmetlerdeki gözlenen veya şüphelenilen herhangi bir güvenlik zayıflığını dikkat etmeleri ve rapor etmeleri istenmelidir.
A.13.2	Bilgi güvenliği ihlal olayları ve iyileştirmelerin yöneti	Amaç: Bilgi güvenliği ihlal olaylarının yönetimine tutarlı ve etkili bir yaklaşımın uygulanmasını sağlamak.
A.13.2.1	Sorumluluklar ve prosedürler	Bilgi güvenliği ihlal olaylarına hızlı, etkili ve düzenli bir yanıt verilmesini sağlamak için yönetim sorumlulukları ve prosedürleri oluşturulmalıdır.
A.13.2.2	Bilgi güvenliği ihlal olaylarından öğrenme	Bilgi güvenliği ihlal olaylarının türleri, miktarları ve maaliyetlerinin ölçülüp izlenebilmesini sağlayan mekanizmalar bulunmalıdır.
A.13.2.3	Kanıt toplama	Bir bilgi güvenliği ihlal olayından sonra bir kişi veya kuruluşa karşı alınan takip önlemi yasal eylem (ya sivil hukuk ya da ceza hukuku) içerdiğinde, ilgili yargılama kurallarında belirlenmiş olan kanıt kuralları ile uyumlu şekilde kanıt toplanmalı, tutulmalı ve sunu

A.14	İş sürekliliği yönetimi	
A.14.1	İş sürekliliği yönetiminin bilgi güvenliği hususları	Amaç: İş faaliyetlerindeki kesilmeleri önlemek ve önemli iş proseslerini büyük bilgi sistemleri başarısızlıklarından ya da felaketlerden korumak ve bunların zamanında devam etmesini sağlamak
A.14.1.1	Bilgi güvenliğini iş sürekliliği yönetim prosesine dahi	Kuruluş genelinde iş sürekliliği için, bu amaca ihtiyaç duyulan bilgi güvenliği gereksinimlerini ifade eden bir yönetilen proses geliştirilmeli ve sürdürülmelidir.
A.14.1.2	İş sürekliliği ve risk değerlendirme	İş proseslerinde kesintilere yol açan olaylar, bu tür kesintilerin olasılığı ve etkisi ve bunların bilgi güvenliği için sonuçları ile birlikte tanımlanmalıdır.
A.14.1.3	Bilgi güvenliğini içeren süreklilik planlarını geliştirme	Önemli iş proseslerinde yaşanan kesintileri ya da başarısızlıkları takiben iş oparasyonlarını sürdürmek ya da onarmak ve bilginin gerekli seviyede ve gerekli zaman ölçeklerinde kullanılabilirliğini sağlamak için planlar geliştirilmeli ve gerçekleştirilmelidir.
A.14.1.4	İş sürekliliği planlama çerçevesi	Tüm planların tutarlı olmasını sağlamak, tutarlı şekilde bilgi güvenliği gereksinimlerini ifade etmek ve test ve bakım önceliklerini tanımlamak için tek bir iş sürekliliği planları çerçevesi oluşturulmalıdır.
A.14.1.5	İş sürekliliği planlarını test etme, sürdürme ve yenide	İş sürekliliği planları, güncel ve etkili olmalarını sağlamak için, düzenli olarak test edilmeli ve güncelleştirilmelidir.
A.15	Uyum	
A.15.1	Yasal gereksinimlerle uyum	Amaç:Her türlü hukuka, yasal, düzenleyici ya da sözleşmeye tabi yükümlülüklere ve her türlü güvenlik gereksinimlerine ilişkin ihlalleri önlemek
A.15.1.1	Uygulanabilir yasaları tanımlama	İlgili tüm yasal, düzenleyici ve sözleşmeden doğan gereksinimleri ve kuruluşun bu gereksinimleri karşılama yaklaşımı her bilgi sistemi ve kuruluş için açıkça tanınlanmalı, dökümante edilmeli ve güncel tutulmalıdır.
A.15.1.2	Fikri mülkiyet hakları (IPR)	Fikri mülkiyet haklarına göre metaryallerin kullanmı ve patentli yazılım ürünlerinin kullanımı üzerindeki yasal, düzenleyici ve anlaşmalarla doğan gereksinimlere uyum sağlamak için uygun prosedürler gerçekleştirilmelidir.
A.15.1.3	Kurumsal kayıtların korunması	Önemli kayıtlar, kaybedilmeye, yok edilmeye ve sahteceiliğe karşı, yasal, düzenleyici, anlaşmalarla doğan gereksinimler ve iş gereksinimlerine uygun olarak korunmalıdır.
A.15.1.4	Veri koruma ve kişisel bilgilerin gizliliği	Uygun yasa, düzenlemeler ve varsa anlaşma maddelerinde belirtildiği gibi veri koruma ve gizlilik sağlanmalıdır.
A.15.1.5	Bilgi işleme olanaklarının kötüye kullanımını önleme	Kullanıcılar, yetki verilmemişamaçlarla bilgi işleme olanaklarını kullanmaktan caydırılmalıdır.
A.15.1.6	Kriptografik kontrolleri düzenleme	İlgili tüm sözleşmeler, yasalar ve düzenlemelerle uyum için krüptografik kontroller kullanılmalıdır.
A.15.2	Güvenlik politikaları ve standartlarla uyum ve teknik	Amaç:Sistemlerin kurumsal güvenlik politikaları ve standartlarıyla uyumunu sağlamak.
A.15.2.1	Güvenlik politikaları ve standartlarla uyum	Yöneticiler, güvenlik politikaları ve standartlarla uyumu başarmak için sorumluluk alanlarındaki tüm güvenlik prosedürlerinin doğru olarak gerçekleştirilmesini sağlamalıdır.
A.15.2.2	Teknik uyum ve kontrolü	Bilgi sistemleri, güvenlik gerçekleştirme standardlarıyla uyumlu olması için düzenli aralıklarla kontrol edilmelidir.
A.15.3	Bilgi sistemleri denetim hususları	Amaç:Bilgi sistemleri denetim prosesinin etkinliğini artırmak ve müdahaleleri azaltmak.
A.15.3.1	Bilgi sistemleri denetim kontrolleri	İş proseslerindeki bozulma risklerini en aza indirmek için, operasyonel sistemlerde kontrolleri içeren denetim gereksinimleri ve faaliyetleri dikkatlice planlamalı ve üzerinde anlaşmaya varılmalıdır.
A.15.3.2	Bilgi sistemleri denetim araçlarının korunması	Bilgi sistemleri denetim araçlarına erişim olası kötüye kullanımlara ya da uyuşmazlıklara karşı korunmalıdır.

EK-3

Yazılımdan Alınan Raporlar

Rapor Örnekleri

	SDÜ Bilgi İşlem Bölüm Giriş Formu	
Yayın No:27001-BGD01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Bölüm Giriş Formu

Bölüm No :1
Bölüm Adı :
Yazılım Birimi

	SDÜ Bilgi İşlem Personel Atama Dökümanı	
Yayın No:27001-AR01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Personel Atama Dökümanı

Personel No :1

Personel Adı : Murat Kaçal

Personel e-Posta : mkacal@sdu.edu.tr

Personel Şifre : 123456

Personel Bölümü : Yazılım Birimi

	SDÜ Bilgi İşlem Kontrol Görev Atama Dökümanı	
Yayın No:27001-AR01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Kontrol Görev Atama Dökümanı

Kontrol Görev No :1

Kontrol Görev Adı : Admin

	SDÜ Bilgi İşlem Kontrol Görev Atama Dökümanı	
Yayın No:27001-AR01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Kontrol Görev Atama Dökümanı

Kontrol Görev No :2

Kontrol Görev Adı : Yazılım Birimi Denetleyicisi

Kayıt Tamamlandı

	SDÜ Bilgi İşlem Kontrol Atama Formu	
Yayın No:27001-VD01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Kontrol Atama Formu

Personel Adı : Murat Kaçal
Kontrol Görev Adı : Yazılım Birimi Denetleyicisi
Kontrol Süresi : 30 gün

	SDÜ Bilgi İşlem Personel Atama Dökümanı	
Yayın No:27001-AR01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Personel Atama Dökümanı

Personel No :2

Personel Adı : Yrd. Doç.Dr. Ecir Uğur Küçüksille

Personel e-Posta : ecir@sdu.edu.tr

Personel Şifre : 567890

Personel Bölümü : Yönetim

	SDÜ Bilgi İşlem BGYS Kapsam Dökümanı	
Yayın No:27001-KD01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı BGYS Kapsam Dökümanı

Kuruluş Adı ve Kuruluş Yılı

S.D.Ü. Bilgi İşlem Daire Başkanlığı,2000

Amaç Ve Kapsam :

2000 yılında Isparta'da Süleyman Demirel Üniversitesi İdari Birimi olarak kurulan Bilgi İşlem Daire Başkanlığı kendi personeli, diğer birimlerde bulunan personelin kullandığı bilgi varlıklarının risk yönetimi ve değerlendirilmesi çerçevesinde korunması amacıyla ISO/IEC 27001 BGYS'nin kurulmasına karar vermiştir.
Uygulanacak sistem Bilgi İşlem Daire Başkanlığı'nın tüm bölümlerini kapsayacaktır.

Organizasyon

Bilgi İşlem Daire Başkanlığı BGYS Kapsamına; Sistem & Bilişim Güvenliği Birimi, Teknik Servis Birimi, Yazılım Birimi, Network Birimi, Diğer Kurum ve Kuruluşlar, Bilgi Paylaşımı Güvenlik Yönetimi girmektedir

Yerleşke

Süleyman Demirel Üniversitesi, Bilgi İşlem Daire Başkanlığı, Çünür-Isparta.

Varlıklar ve Teknoloji

BGYS aşağıda belirtilen tüm varlıkları kapsamaktadır. Bunlar; Personel Kişisel Bilgileri, Tüm BT Sistemleri, Tüm Dokümantasyon Bilgileri.

Hazırlayan	Kontrol Eden	Onaylayan
Murat Kaçal	Yrd. Doç.Dr. Ecir Uğur Küçüksille	Yrd. Doç.Dr. Ecir Uğur Küçüksille

	SDÜ Bilgi İşlem Riskleri Tanımlama Formu	
Yayın No:27001-VK01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Riskleri Tanımlama Formu

Amaç ve Kapsam :
Risklerin hangi kriterlere göre kontrol uygulanıp uygulanmayacağı, Risk Yönetim Süreci'nde risklerin ne şekilde değerlendirileceği, hangi kritere göre artık risk olarak kabullenileceğini belirleyen Risk Değerlendirme Yöntemi'nin belirlenmesi ve ne şekilde çalışacağının düzenlenmesi.

Tüm BGYS süreçlerini kapsar.
Tarih 10/07/2012
Düzenleyen (Personel Adı) : Murat Kaçal
Olasılık Değer :2
Etki Değeri :2
Toplam Risk Skoru :2*2=4
Değerlendirme : Kurumumuzun BGYS süreçlerinde, Risk Değerlendirme Yöntemi olarak, gerek sebep sonuç ilişkilerinin değerlendirilmesindeki genel kullanım alanı gerek öncelik belirlemesindeki hızlı cevap verme yeteneği nedeniyle "Risk Değerlendirme Karar Matrisi Yöntemi" kullanılacaktır. Öncelikle bilgi varlığının üzerinde mevcut ya da muhtemel riskin olasılık ve etki analiz değerleri çarpılarak toplam risk derecelendirme skoruna ulaşılacaktır. Olasılık ve etki analizinde 3 seviyeli derecelendirme kullanılacak ve toplam risk skoru 3 ve aşağısında olanların riski "Düşük", toplam risk skoru 4 ile 6 arasında olanların riski "Orta" ve son olarak 9 olanların riski "Yüksek" olarak nitelendirilecektir. Riskin toplam skorunun 1 olması, teknolojinin yüzde yüz güvenliğe imkan sağlayamadığı durumların var olması, verilen hizmetin kritiklik durumu ve yönetim kurulu kararı ile gerekçeleri belirtilen risklerin kabul edilmesi sağlanacaktır (Mete, 2010).

Hazırlayan	Kontrol Eden	Onaylayan
Tuna Göksu	Murat Kaçal	Yrd. Doç.Dr. Ecir Uğur Küçüksille

	SDÜ Bilgi İşlem BGYS Varlık Dökümanı	
Yayın No:27001-VD01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı BGYS Varlık Dökümanı

Amaç ve Kapsam

Kurumda risk yönetim sürecinin uygulanacağı mevcut tüm bilgi varlıklarının listesini çıkarmaktır.
Yazılım, donanım, fiziksel güvenlik dahil tüm bilgi varlıklarını kapsamaktadır.

Varlık No : 5
Varlık Adı : Veritabanları
Varlık Grubu : Sistem Birimi
Sahibi : Tuna Göksu
Bulunduğu Yer : Veri Tabanı Sunucusu
Gizlilik Değeri : 2
Bütünlük Değeri : 2
Erişebilirlik Değeri : 3
Toplam Değeri :Tuna Göksu
Eklenme Tarihi :
Açıklama :

Hazırlayan	Kontrol Eden	Onaylayan
Buket Çapalı	Tuna Göksu	Yrd. Doç.Dr. Ecir Uğur Küçüksille

	SDÜ Bilgi İşlem Varlıkların Kullanım Politikası	
Yayın No:27001-VK01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Varlıkların Kullanım Politikasıı

Varlık Adı : Masaüstü Bilgisayarlar
Amaç ve Kapsam :
Kurum içerisindeki masaüstü bilgisayarların kullanım şartlarını belirlemek

Kurum içerisinde kullanılan tüm masaüstü bilgisayarları kapsar.
Uygulama(Kullanım Şekli)
Dizüstü bilgisayar kullanıcıları hazırlanan dizüstü bilgisayar kullanım politikasını okuduğuna dair tebliğ formu imzalayacaklardır. Masaüstü bilgisayarların kullanımı konusunda Teknik Servis Birimi tarafından tüm personele kısa toplantı verilecek ve tarih, katılan kişi listeleri dokümana eklenecektir. Masaüstü bilgisayar kullanıcıları bilgisayarlarını Teknik Servis Birimin'den zimmet belgesi imzalayarak alacaktır. Masaüstü Bilgisayar üzerlerine kurum numarası ve islenilen bilginin derecesini gösterir etiket basılacaktır. Ağa bağlı masaüstü bilgisayarlarda islenilen bilgi masaüstü bilgisayar hard disklerinde depolanmayacaktır. Üzerinde işlem yapılacak doküman merkezi dosya sunucusundan bilgisayar harddiskine alınarak düzenlemeler yapıldıktan sonra kopyalanacaktır. Kurum bilgi işlem ağına sadece izin verilmiş masaüstü bilgisayarlar bağlanacak, şahsi bilgisayarlar kesinlikle bağlanmayacaktır.
Personel Adı : Mustafa Kestellioğlu

Hazırlayan	Kontrol Eden	Onaylayan
Nilay Temelli	Mustafa Kestellioğlu	Yrd. Doç.Dr. Ecir Uğur Küçüksille

	SDÜ Bilgi İşlem Tehdit ve Açık FormuTehdit ve Açık Formu	
Yayın No:27001-TD01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Tehdit ve Açık Formu

Sıra No :1
Olayın Cinsi : Açık
Tehdit yada Açığın Açıklaması Donanım ve yazılımların yanlış kullanılması.
Kaynağı :İnsan kaynaklı personel hataları

Hazırlayan	Kontrol Eden	Onaylayan
Mustafa Kestellioğlu	Mustafa Kestellioğlu	Yrd. Doç.Dr. Ecir Uğur Küçüksille

	SDÜ Bilgi İşlem Risk Değerlendirme ve Derecelendirme Formu	
Yayın No:27001-RD01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Risk Değerlendirme ve Derecelendirme Formu

Amaç ve Kapsam
Uygulanan tüm risk derecelendirme işlemlerinin dokümante edilerek kayıt altına alınmasıdır

Kurum bilgi varlıkları çerçevesinde mevcut ve potansiyel tüm riskleri kapsamaktadır.
Varlık Adı: Masaüstü Bilgisayarlar
Toplam Değer (Varlık Değeri) : 12
Tehdit/Açığın Ne OlduğuAğa bağlı masaüstü bilgisayarın içerisindeki önemli bilginin kötü niyetli kişiler tarafından ele geçirilmesi
Olasılık Değeri :3
Etki Değeri :3
Risk Değeri (Olasılık*Etki) :3*3=9
Açıklama
3 x 3 = 9 olarak belirlenerek dokümante edilecektir. Kurum, Bilgi İşlem Daire Başkanlığı'nın belirleyeceği Risk İşleme Planı'na göre risk işlenecek ve buna göre uygulama yapılacaktır. Risk derecelendirmesi de bu işleme göre yapılacaktır. Kurumun ortaya koyduğu kriterlere göre 9 değeri hangi bölümde incelenecek ise (Düşük-Orta- Yüksek) buna göre işlem yapılacaktır. Risk değeri 9 olan bir tehdit eğer kurumun göze alamayacağı değerde ise karşı kontroller oluşturulacak, eğer bu kontrollerin maliyeti fazla ve karar o yönde alınacaksa aktarılacak, ya da 9 değeri göze alınabilirse artık risk olarak yönetim onayı istenecektir. 9 değeri yüksek değer olduğu için önem arz eder ve karşı kontroller oluşturulmalıdır.

Hazırlayan	Kontrol Eden	Onaylayan
Nilay Temelli	Güncel Sarıman	Yrd. Doç.Dr. Ecir Uğur Küçüksille

	SDÜ Bilgi İşlem **Kontrol ve Amaçlarını Belirleme Formu**	
Yayın No:27001-VD01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı **Kontrol ve Amaçlarını Belirleme Formu**

Amaç ve Kapsam

Bütün bilgi varlıkları çerçevesinde kurumda buluna risklerin işlenmesi için yapılacak kontrollerin belirlenmesidir. Mevcut ve potansiyel tüm riskleri ve tüm bilgi varlıklarını kapsamaktadır.

Varlık Adı : Masaüstü Bilgisayarlar
Tehdit/Açığın Ne Olduğu : Ağa bağlı masaüstü bilgisayarın kurum dışında kullanımında çalınması ve içerisindeki önemli bilginin yanlış ellere geçirilmesi.
Risk Değeri (Olasılık*Etki) : 9
Uygulanacak Kontrol : Öncelikle dizüstü bilgisayarlara Bios özelleriklerinden giriş şifresi tanımlanacaktır. Daha sonra bir klasör oluşturulacak, dizüstü bilgisayar kullanıcıları tarafından işlenen önemli bilgi ve belgeler bu klasöre taşınacak ve klasöre şifre verilerek güvenlik arttırılacaktır.
Sorumlu (Personel Adı) : Mustafa Kestellioğlu
Atıfta Bulunan Dökümanlar : Bilgi Güvenlik Politikası Dokümanı , Dizüstü Bilgisayarı Kullanım Politikası , Bilgisayarla Uygulanacak Güvenlik İşlemleri Süreci

Hazırlayan	Kontrol Eden	Onaylayan
Nilay Temelli	Murat Kaçal	Yrd. Doç.Dr. Ecir Uğur Küçüksille

	SDÜ Bilgi İşlem Uygulanabilirlik Politikası (EkA)	
Yayın No:27001-UP01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Uygulanabilirlik Politikası (EkA)

Madde Numarası :
Kontrol Maddesi A.5 Güvenlik Politikası
Amaç ve Kapsam :
Çalışanları kurum bünyesinde kurulan ISO/IEC 27001 BGYS Standardı hakkında bilgilendirmek ve bilgi güvenliği gerekliliklerini belirlemek.
Tüm çalışanları kapsamaktadır
Mevcut Kontrol : Bilgi Güvenliği Politikası; Kurumumuzca kullanılan tüm bilişim hizmetleri ve teknolojileri her geçen gün gelişmekte ve yenilenmektedir. Bunun bir sonucu olarak birçok ağ yapıları, sistem işletimi ve fazla sayıda iş uygulamaları ortaya çıkmaktadır. Bu çeşitlilik içerisinde kurumumuz, sistemlerini organize ederken, bilginin gizliliği, bütünlüğü ve erişebilirliği konularında hassasiyet ile durmaktadır. Verinin ve dolayısıyla bilginin elektronik ortamda saklanması, işlenmesi ve paylaşımı bu üç unsuru barındıran bilgi güvenliği açısından önem arz etmektedir.
Artık Risk Açıklaması : Artık Risk olarak belirlenmemiştir.
Kontrolün Seçilme Kaynağı :O
Açıklama (Bundan Sonra Yapılacak çalışmalar) : Doküman, tüm kurumumuzca üzerinde önemle durulan ve tüm birimlerce hassasiyet gösterilmesi beklenen bilgi sistemlerinin güvenliği konusunda uyulması gereken minimum standartları belirlemekte, tüm güvenlik sistemi için temel teşkil etmektedir. Kurumumuzun bilgi güvenliği kavramından anladığı ve tüm kullanıcı ve yöneticilerinden talep ettiği, bilgi varlıklarının şu üç temel ilkesinin sağlanmasıdır. Gizlilik: Bilginin sadece yetkili kişiler tarafından erişilebilir olması, Bütünlük: Bilginin bozulmadan korunması Kullanılabilirlik: Bilginin yetkili kullanıcılar tarafından gerek duyulduğu an ulaşılabilir olması. Bu politika, bilgi işlem altyapı, sistem ve programlarını kullanmakta olan tüm kurum çalışanlarını, diğer birimlerde bilgi sistemlerine erişen kullanıcıları ve bilgi sistemlerine teknik destek sağlamakta olan hizmet, yazılım veya donanım sağlayıcıları olarak sıralanan dış tarafları kapsamaktadır. Bu taraflar bilgi güvenliği çerçevesinde oluşturulan tüm politika, prosedür ve talimatlara uymakla sorumludurlar. Birimlerin bilgi güvenliği sorumlularından oluşan BGYS ekibi, BGYS altyapısını desteklemek ve devam ettirmekle sorumludur. Kurum yönetimi, kurumun güvenilirliğini ve imajını korumak, kurum bilişim hizmetlerinin gerçekleştirilmesinde kullanılan tüm fiziksel ve elektronik bilgi varlıklarının bilgi güvenliğini sağlamayı hedefler. Kurum bilgi işlem altyapısını, sistem ve uygulamalarını kullanan herkes; kişisel ve elektronik iletişimde ve üçüncü taraflarla yapılan bilgi alışverişlerinde kuruma ait bilginin gizliliğini sağlamalı, işlediği bilgiyi yedeklemeli, risk düzeylerine göre belirlenen güvenlik önlemlerini almalı, bilgi güvenliği ihlal olaylarını raporlamalı ve Bilgi Güvenliği Birimi'ne bildirmeli, bu ihlalleri engelleyecek önlemleri almalıdır. Bilgi güvenliği politika, prosedür ve talimatlarına uyulmaması halinde, kurum Personel Yönetmeliği gereğince aşağıdaki yaptırımlardan bir ya da birden fazla maddesini Uygulayabilir; Uyarma, Kınama, Para cezası (Mete, 2010). Kurum yönetimi olarak, "Kurum Bilgi Güvenliği Politikası"nın uygulanmasının ve devamlı kontrolünün sağlanmasının, güvenlik ihlallerinde de gerekli yaptırımın uygulanmasının yönetim tarafından desteklendiğini belirtirim. Personel Adı: Daire Başkanı Ecir Uğur KÜÇÜKSİLLE
Personel Adı : Veli Çapalı
Tarih :12/07/2012

Hazırlayan	Kontrol Eden	Onaylayan
Buket Çapalı	Tuna Göksu	Yrd. Doç.Dr. Ecir Uğur Küçüksille

	SDÜ Bilgi İşlem Artık Risk Dökümanı	
Yayın No:27001-AR01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Artık Risk Dökümanı

Artık Risk No :1

Varlık Adı : Masaüstü Bilgisayarlar

Artık Risk Adı : Masaüstü bilgisayarların kurum dışında kullanılması

Nedeni (Neden Artık Risk Olduğu) : Risk Değerinin Düşük değerli çıkması.

Yönetim Onayı : BGYS ekibi toplantı yaparak masaüstü bilgisayarların kurum dışında kullanılmasının güvenlik ihlali yapmayacağını karar vererek onaylar.

Hazırlayan	Kontrol Eden	Onaylayan
Mustafa Kestellioğlu	Murat Kaçal	Yrd. Doç.Dr. Ecir Uğur Küçüksille

	SDÜ Bilgi İşlem Risk Yönetim Süreci	
Yayın No:27001-RY01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Risk Yönetim Süreci

Amaç ve Kapsam
Riskleri çözme yöntemlerinin, ayarlanan tarihlerin, ilk önce yapılacakların, ve risk işleme sorumlularının belirlenmesi.

Kurumda bulunan ve yeni oluşabilen tüm riskleri kapsamaktadır.
Risk
Elektronik Posta Sunucusuna aynı anda birden fazla istek yapılmasıyla hizmetin cevap veremeyerek durdurulması.
Uygun Kontrol Maddesi
dddd
Risk İşleme Yöntemi
Kontrollerin Uygulanarak Riski Azaltma/Giderme
Açıklama (Kontrol)
Bilgi İşlem Daire Başkanlığı tarafından personel bu konu ile ilgili bilgi verilecek ve gelen elektronik postalar incelenerek gönderileni belli olmayan elektronik posta ve içeriklerindeki dosyalar açılmayacaktır.
Öncelik Sırası
Yüksek
Başlangıç Tarihi
15/07/2012
Bitiş Tarihi
12 Ağustos 2012
Sorumlular(Personel)
Tuna Göksu

Hazırlayan	Kontrol Eden	Onaylayan
Buket Çapalı	Veli Çapalı	Tuna Göksu

	SDÜ Bilgi İşlem Kontrol Etkinlikleri Ölçülmesi Dökümanı	
Yayın No:27001-VD01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı Kontrol Etkinlikleri Ölçülmesi

Amaç ve Kapsam

Riskleri ortadan kaldırmak ya da işlemek için uygulanan kontrollerin etkinliğinin nasıl ölçüleceğini belirlemek.
Uygulanacak tüm yöntem içeren kontrolleri kapsamaktadır.

Risk : Elektronik Posta Sunucusuna aynı anda birden fazla istek yapılmasıyla hizmetin cevap veremeyerek durdurulması.
Açıklama Kontrol : Gelen elektronik postaların kontrol edilmesi
Etkinlik Yöntemi (Ayrıca yapılan etkinlikler) : Elektronik postaların kontrol edilerek gereksiz elektronik postaların kullanıcıya gönderilmeden önce silinmesi
Açıklama ve Atıfta Bulunulan Dokumani : Elektronik Posta Kullanımı Dokümanı
Sorumlu : Tuna Göksu

Hazırlayan	Kontrol Eden	Onaylayan
Veli Çapalı	Buket Çapalı	Yrd. Doç.Dr. Ecir Uğur Küçüksille

	SDÜ Bilgi İşlem Politika Dökümanı	
Yayın No:27001-P01	Döküman Adı:DOK-KPS-V1	VER 0.1
SDÜ Bilgi İşlem Daire Başkanlığı Politika Dökümanı **Politika No : 2** **Politika Adı : Elektronik Posta Alt politikası** **Amaç ve Kapsam** **E- posta kullanımını anlatma** **Tüm birimleri kapsar** **Uygulama** **Toplantı ile birimler bilgilendirilir.**		
Hazırlayan	Kontrol Eden	Onaylayan
Tuna Göksu		

	SDÜ Bilgi İşlem Prosedür Formu	
Yayın No:27001-PF01	Döküman Adı:DOK-KPS-V1	VER 0.1
SDÜ Bilgi İşlem Daire Başkanlığı Prosedür Formu **Prosedür No : 1** **Prosedür Adı : Eğitim ve Farkındalık Prosedürü** **Amaç ve Kapsam** **Personele BGYS eğitimini vermek** **Tüm çalışanları kapsamaktadır** **Uygulama** **Toplantı ile birimler bilgilendirilir.**		
Hazırlayan	Kontrol Eden	Onaylayan
Nilay Temelli	Buket Çapalı	Yrd. Doç.Dr. Ecir Uğur Küçüksille

	SDÜ Bilgi İşlem Kişisel Risk Belirleme Formu	
Yayın No:27001-PF01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire BaşkanlığıKişisel Risk Belirleme Formu

Problem (Risk-Olay) : Elektronik posta açılmıyor
Problemle İlgilenecek Olan Bölüm : Sistem Birimi
Problemin Hangi Bölümde Olduğu
Teknik Servis Birimi
Tarih :
14/07/2012
Problemi Yazan Kişi (Personel)
Nilay Temelli

	SDÜ Bilgi İşlem BGYS Etkinlik ve Performansı Etkileyecek Olayları Kaydetme Formu	
Yayın No:27001-PEO01	Döküman Adı:DOK-KPS-V1	VER 0.1

SDÜ Bilgi İşlem Daire Başkanlığı BGYS Etkinlik ve Performansı Etkileyecek Olayları Kaydetme Formu

Sıra No :1

Varlık Adı : Elektronik Posta

Olay (Problem-Risk) : Elektronik Posta Sunucusuna aynı anda birden fazla istek yapılmasıyla hizmetin cevap veremeyerek durdurulması.

Tarih : 16/07/2012

Yapılan İşlem (Kontrol) : Tuna Göksu

Açıklama :

Çözen Kişi (Personel) :

ÖZGEÇMİŞ

Adı Soyadı : Tuğba HAKLI
Doğum Yeri ve Yılı : Isparta, 1981
Medeni Hali : Evli
Yabancı Dili : İngilizce

Eğitim Durumu (Kurum ve Yıl)

Lise :Isparta Şehit Ali İhsan Kalmaz Lisesi, 1995-1998
Lisans :Süleyman Demirel Üniversitesi Teknik Eğitim Fakültesi Bilgisayar Sistemleri Öğretmenliği, 1998-2002

Çalıştığı Kurum

Isparta Milli Eğitim Müdürlüğü, Halıkent İlköğretim Okulu, 2002-…