T.C.
SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ OTOMASYONU

YÜKSEK LİSANS TEZİ

Ufuk BİNGÖL

Enstitü Anabilim Dalı: Çalışma Ekonomisi ve Endüstri İlişkileri
Enstitü Bilim Dalı: İnsan Kaynakları Yönetimi ve Endüstriyel İlişkiler

Tez Danışmanı: Prof. Dr. Yılmaz ÖZKAN

HAZİRAN 2010

T.C
SAKARYA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

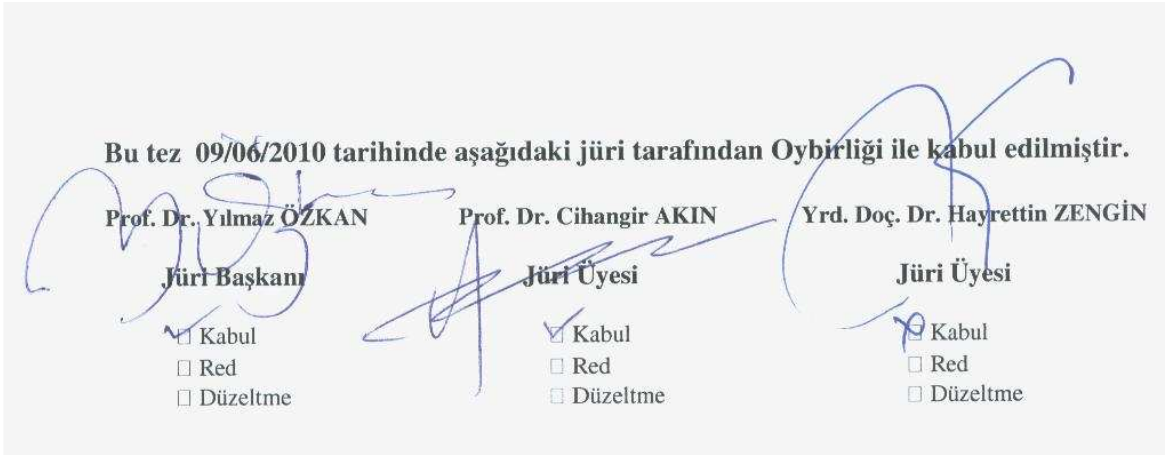
ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ OTOMASYONU

YÜKSEK LİSANS TEZİ

Ufuk BİNGÖL

Enstitü Anabilim Dalı: Çalışma Ekonomisi Ve Endüstri İlişkileri
Enstitü Bilim Dalı: İnsan Kaynakları Yönetimi Ve Endüstriyel İlişkiler

Bu tez 09/06/2010 tarihinde aşağıdaki jüri tarafından oybirliği ile kabul edilmiştir.



BEYAN

Bu tezin yazılmasında bilimsel ahlak kurallarına uyulduğunu, başkalarının eserlerinden yararlanılması durumunda bilimsel normlara uygun olarak atıfta bulunulduğunu, kullanılan verilerde herhangi bir tahrifat yapılmadığını, tezin herhangi bir kısmının bu üniversite veya başka bir üniversitedeki başka bir tez çalışması olarak sunulmadığını beyan ederim.

Ufuk BİNGÖL
09/06/2010

ÖNSÖZ

“ISO 27001 Bilgi Güvenliği Yönetim Sistemi Otomasyonu” konusu, günümüz işletmelerinin rekabet üstünlüğü sağlamada en önemli üretim faktörlerinden biri olan bilgi faktörünün korunmasında kullanılacak sistemlerin özellikle küçük işletmeler tarafından ücretsiz Açık Kaynak Kodlu yazılımlar tarafından otomatikleştirme imkânı konusu üzerinde durmuştur. Bu çalışmanın hazırlanmasında yardımlarını esirgemeyen danışman hocam Prof.Dr. Yılmaz ÖZKAN’a teşekkürlerimi sunmayı bir borç bilirim. Ayrıca bugünlere ulaşmamda haklarını ve emeklerini hiçbir zaman ödeyemeyeceğim aileme ve çalışmalarım sırasında bana her zaman anlayış gösteren sevgili eşime şükranlarımı sunarım. Yetişmemde katkıları olan tüm hocalarıma saygılarımı arz ederim.

Ufuk BİNGÖL
09/06/2010

İÇİNDEKİLER

KISALTMALAR

AKK : Açık Kaynak Kod

ASP : Active Server Pages (Aktif Sunucu Sayfaları)

BGYS : Bilgi Güvenliği Yönetim Sistemi

BSI : British Standards Institution (İngiliz Standartları Enstitüsü)

GNU : Gnu's Not Unix (GNU Unix Değildir)

GPL : General Public Licence (Genel Kamu Lisansı)

IP : Internet Protokolü

IPSEC : Internet Protocol Security (İnternet Protokolü Güvenliği)

ISO : International Organization for Standardization

JSP : Java Server Pages (Java Sunucu Sayfaları)

OECD : Organisation for Economic Co-operation and Development (İktisadi İşbirliği ve Gelişme Teşkilatı)

PHP : Personel Home Pages (Kişisel Ana Sayfalar)

PUKÖ : Planla – Uygula – Kontrol Et – Önlem Al

RYS : Risk Yönetim Sistemi

SSL : Secure Socket Layer (Soket Katmanı Güvenliği)

TÜBİTAK : Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

TABLO LİSTESİ

ŞEKİL LİSTESİ

SAÜ, Sosyal Bilimler Enstitüsü **Yüksek Lisans Tez Özeti**

Tezin Başlığı: ISO 27001 Bilgi Güvenliği Yönetim Sistemi Otomasyonu	
Tezin Yazarı: Ufuk BİNGÖL	**Danışman:** Prof. Dr. Yılmaz ÖZKAN
Kabul Tarihi: 09.06.2010	**Sayfa Sayısı:** viii (ön kısım) + 86 (tez)
Anabilimdalı:Çalışma Ekonomisi ve Endüstriyel İlişkiler	**Bilimdalı:** İnsan Kaynakları Yönetimi ve Endüstriyel İlişkiler

Bilgi Güvenliği özellikle hızla gelişen teknoloji ile birlikte son yıllarda kurumların en büyük sorunlarından biri olmuştur. İşletmelerin günümüzdeki en belirgin rekabet dayanağı icra ettikleri üretim faaliyetlerindeki sahip oldukları bilgi varlıkları ve tecrübeleridir. Kurumlar rekabet üstünlüğü sağlamak maksadıyla kurumsal verilerinin güvenliğini sağlamak zorundadır. Bilgi Güvenliği ile ilgili ülkemizde ve uluslarası platformda hukuki bazı düzenlemeler mevcuttur. Bu düzenlemelere ek olarak işletmelerin kendi bilgi güvenliği faaliyetlerini yönetmesi maksadıyla uluslararası geçerliliği olan ISO 27001 Bilgi Güvenliği Yönetim Sistemi Kalite standardı bulunmaktadır. İşletmeler süreç yaklaşımı kapsamında Bilgi Güvenliği yönetim faaliyetlerini bu standardla gerçekleştirebilirler. İşletmeler BGYS faaliyetlerini dış kaynak tedariki ile danışmanlık alarak veya hazır paket programlar vasıtasıyla yürütebilirler.

Bu çalışmanın araştırma problemi, Sözkonusu BGYS faaliyetini tamamen Açık Kaynak Kodlu yazılımları tekrar BGYS kapsamında düzenleyerek BGYS sürecinin yönetimini çok düşük maliyetle sağlanabileceğini belirtmek olarak ifade edilebilir. BGYS kurmak ve yönetmek isteyen bir işletmenin sürecin yönetimi esnasında ne tür bir sisteme ihtiyaç duyulduğu dikkate alınmalıdır. Bu bağlamda bu çalışmanın amaçlarını şu şekilde ifade etmek mümkündür:

a) İşletmelerin BGYS sürecinin yönetiminde ISO 27001 standardı kapsamında bir süreç takvimi oluşturan, bu kapsamda belirlenen görevlere sorumlulukları atama işleminin gerçekleştirildiği ve aynı görev için görev ilerleme kayıtlarının alınabildiği, sürecin tamamen belgelendirildiği, BGYS süreci ekibinin birbirleri ile bilgi alışverişinde bulunabildiği, BGYS süreç yönetimi faaliyetinin de "Bilmesi gereken" prensibi kapsamında yetkilendirme yoluyla erişilebilen bir süreç yönetimini oluşturmak,

b) ISO 27001 standardının en önemli unsuru olan risk yönetim sistemi sürecinin gerçekleştirildiği birçok düşük maliyetli bir risk yönetim süreci oluşturmaktır.

Bu ihtiyaçlara cevap ararken literatür taramasına ek olarak konu ile ilgili ticari yazılımların deneme sürümleri incelenmiştir. Veri edinmede ticari yazılım incelemesinin tercih edilmesinin temel gerekçesi örnek ticari yazılımlara karşılık hazır A.K.K. yazılımların olup olmadığının araştırılmasıdır. Yapılan araştırmalar neticesinde sadece ISO 27001 süreçleri ile ilgili A.K.K. bir yazılım bulunamamıştır. Fakat bazı açık kaynak kodlu yazılımları ve programlama dillerini kullanarak orta-yüksek derecede bilgisayar bilgisi vasıtasıyla bir süreç yönetim ve risk yönetim otomasyonu meydana getirilebileceği görülmüştür. Ve konu ile ilgili çalışmalara başlanmıştır.

Bu çerçevede yapılan çalışma sonucunda meydana getirilen otomasyon ile birlikte yukarıdaki ihtiyaçlara cevap veren bir süreç yönetim sistemi ve risk yönetim sistemi oluşturulmuştur. İşletmelerin bu tip A.K.K. yazılımları küçük düzenlemelerle yeniden derleyerek kendi sistemlerinde kullanmaları mümkündür. Bu sayede yalnızca maliyetlerin düşürülmesi değil aynı zamanda dışa bağımlılık problemlerinin çözüme ulaşacağı söylenebilir.

Anahtar kelimeler: ISO 27001, Bilgi Güvenliği Süreç Yönetim Sistemi, Bilgi Güvenliği Risk Yönetim Sistemi

Sakarya University Insitute of Social Sciences **Abstract of Master's Thesis**

Title of the Thesis: ISO 27001 Information Security Management System Automation	
Author: Ufuk BİNGÖL	**Supervisor:** Prof. Dr. Yılmaz ÖZKAN
Date: 09.06.2010	**Nu. of pages:** vii (pre text) + 86 (main body)
Department: Labour Economics and Industrial Relations	**Subfield:** Human Resource Management and Industrial Relations

With rapidly evolving technologies, especially information security in recent years has been one of the biggest problem of the organizations. The most significant competition for business today in support of production activities as they pursue their knowledge and experiences are assets. Organizations to provide competitive advantage in order to ensure the security of corporate assets are secure and difficult. There are some regulations about Information security in our country and international legal platform. In addition to these regulations, organizations are able to manage their information security activities with the purpose of internationally recognized quality standard ISO 27001 Information Security Management System if they want. Information Security in the context of business process management approach to these standards can perform their activities. ISMS activities of enterprises can be achieved with foreign sources of supply advisory or to buy counseling through the commercial softwares.

This study's research problem, the question of ISMS activities entirely Open Source software to re-organize under the ISMS process management can be achieved by specifying a very low cost can be expressed as. ISMS who want to build and manage a business process management are needed to exactly what such a system should be taken into consideration.In this context, the objectives of this study can be expressed as follows:

a) Business of the ISMS process management ISO 27001 standard as part of a process schedule by, in this context defined roles responsibilities, appointment procedures carried out the same task for the task progress records are able to process fully documented, built, ISMS process, the ISMS team with each other to exchange information can be found, ISMS process management activities also "Know needed "basis under the management of authorization to create a process that can be accessed through,

b) ISO 27001 standard as the most important element of the risk management system, many low-cost process was carried out to establish a risk management process.

When searching for the answer to this need, in addition to the literature about the subject some of the trial (Demo) versions of commercial software are examined. Obtain review of the data in the commercial software to commercial software are preferred examples of the basic reasons for the stock of Open Source Software to evaluate whether or not. Findings of these studies are only concern with the process of ISO 27001 There are no Open Source software. But with some open source software, knowledge of using programming language and medium-high degree of computer, process and risk management can be carried out through this automation has been seen. And set to work-related issues.

In this context, the studies resulted in the return to the automated reply with the above requirements and risk management system, a process management system has been established. Open Source Software of this type of organizations recompiled with minor editing software as it is possible to use their own systems. In this way, not only lowering costs but also to reach out to say outsource problems.

Keywords: ISO 27001, Information Security Process management System automation, Information Security Risk Management System

GİRİŞ

İçerisinde bulunduğumuz çağa ismini veren bilgi kavramı yüzyıllar önce insanlığın tarım toplumundan başlayıp sanayii toplumuyla günümüze kadar sürekli gelişen, teknolojik gelişmelerle beraber bilgi toplumuna dönüştüğü süreçte üretime etki eden en önemli unsurlardan biri olmuştur. İşletmelerde bireylerin becerileri yerine bilgi seviyelerinin ve analitik düşünce yeteneklerinin aranması da bunun en önemli örneklerinden biridir. Bilginin üretimde en önemli kaynak olması ve işletmelere rekabet üstünlüğü sağlaması sebebiyle işletmelerin bilgi varlıklarını amacına uygun olarak kullanıp bu varlıklarını koruması hiç süphesiz zorunluk arz etmektedir. Özellikle 90'lı yıllardan itibaren internet sayesinde organizasyonların bazı hizmetlerini sözkonusu büyük küresel ağ üzerinden sağlamaları ile birlikte kurumların bilgi varlıklarını koruma ihtiyacı artmıştır.

İnternet üzerinden hizmet veren sosyal paylaşım siteleri, görüntülü ve sesli haberleşme olanakları gibi hizmetler sayesinde bugün toplumun bilgiye ulaşması çok kolaylaşmıştır. Bunun yanında insanların bilerek veya bilmeden şahsına, ailesine veya çalıştığı kuruma ait hassas bilgilerini internet ve diğer bilgi iletişim platformlarına sızdırması ihtimali artmıştır. Kurumlar faaliyetleri ile ilgili her türlü veriyi koruyup, veri sızmalarını engellemelidir. Kişiler de bu kapsamda şahsi bilgilerinin üçüncü kişiler tarafından izinsiz olarak kullanılmasını engellemek zorundadır. İşletmeler, gelişen teknolojiler ile paralel olarak bilgi varlıklarının güvenliğini sağlamak ve geliştirmek zorundadır.

İşletmelerin, toplumun ve devletlerin bilgi varlıklarının korunması ile ilgili yani bilgi güvenliği ile ilgili uluslararası ve ulusal düzeyde hukuki düzenlemeler bulunmaktadır. Kurumların hukuki çerçeveye bağlı kalmak koşuluyla kendi bilgi güvenliği sistemlerini oluşturmak ve yönetmek maksadıyla uygulayacağı ISO 27001 Bilgi Güvenliği Yönetim Sistemi Standardı ve bu kapsamda kullanmaya hak kazandığı belgeler, kurumların rekabet üstünlüklerini pekiştirmelerini sağlayacaktır. İşletmeler ISO 27001 standardını uygulama esnasında, söz konusu sürecin yönetiminin sağlanacağı, konu ile ilgili detaylı proje ve faaliyet takvimlerinin çıkarılacağı, süreç ile ilgili çalışanların iletişim ve koordinesini sağlayacağı ve en önemlisi sürecin belgelendireceği bir süreç yönetim faaliyeti icra etmeleri gerekmektedir. İşletmeler adım adım ISO 27001 süreçlerinin

incelendiği, görev ve sorumlulukların açık olarak tanımlandığı sürecin gerekliliklerini yerine getiren çalışma gruplarının birbirleri ile bilgi alışverişini sağlayan bir ISO 27001 süreç yönetimine ihtiyaç duymaktadırlar. Bu sebepten bir süreç yönetimi otomasyonuna sahip olmak işletmeler için zorunlu olmasa da gereklidir. ISO 27001 Sürecinin içerisindeki en önemli unsur olarak göze çarpan husus risk yönetimidir. BGYS'de doğru ve etkin olarak icra edilen Risk Yönetim Faaliyetinde kurumların hiç bir zaman yüzde yüz bilgi güvenliği sağlaması mümkün olmasa da yüzde yüze yakın bir güvenlik sağlamaları mümkündür. İşletmeler açık ve gerçek olarak belirlediği zaafiyetleri ve tehditleri karşısında meydana çıkan risklere karşı standartta belirtilmiş veya standardın haricinde ihtiyaca yönetlik gerekli kontrolleri uygulaması sonucunda mevcut açık ve tehditleri de ortadan kaldırmış olur.

Çalışmanın Amacı ve Önemi

Bu çalışmanın amacı, BGYS sürecinin icrasında kullanılacak açık kaynak kodlu yazılımlardan oluşan bir süreç yönetim sistemi ve alt yönetim faaliyeti olan risk yönetimi sistemini oluşturmaktır. Sözkonusu yazılımların kurumlara sağlayacağı kazanç çok yüksektir. Bu süreç kapsamında bütün koordinasyonun sağlandığı bu sistem sayesinde kurumlar ISO 27001 sürecini kolaylıkla yönetebileceklerdir. Artan teknolojik imkanlar ve danışmanlıklar ile sözkonusu işlemleri gerçekleştirmek mümkündür. Fakat özellikle yeni büyüyen firmalarda ve KOBİ'lerde maliyet sıkıntıları nedeniyle bu tip danışmanlıkların veya ticari otomasyonların hizmet olarak alınması mümkün olamamaktadır. Dolayısıyla bu çalışmanın hedefi, internet üzerinde yapılan araştırmalar ile birlikte orta derecede bir bilgisayar bilgisi vasıtasıyla açık kaynak yazılımlar kullanılarak bir ISO 27001 BGYS otomasyonu sistemi oluşturmaktır.

Çalışmanın Önemi

Açık kaynak kodlu yazılımların desteği ve açık kaynak kodlu programlama dilleri ile birlikte maliyet sorununu tamamen olmasa da yüksek bir oranda ortadan kaldırarak kurumları amaç bölümünde bahsedilen sorunlardan kurtaran etkileşimli bir süreç yönetim sistemi ve risk yönetim sistemi oluşturmak mümkündür. Bu sayede ise işletmelerin danışmanlık ve otomasyon çözümlerini içeren, ticari maliyetlerden tasarruf ve aynı zamanda işletmenin tamamen kendisine özgü bir ISO 27001 otomasyonuna sahip olabilecekleri unutulmamalıdır. Bütün bu maliyetlerden işletmeler kısmen

korunmuş olacak, aynı zamanda kendi BGYS süreçlerini PUKÖ döngüsüne göre tamamen Açık Kaynak Kodlu yazılımlar kullanarak sürekli iyileştireceklerdir.

Çalışmanın Yapısı

Bu çalışma dört bölümden oluşmaktadır. Bu kapsamda BGYS sürecinin önemini kavrayabilmek için çalışmanın birinci bölümünde öncelikle bilginin ve güvenliğinin önemi belirtilerek bilgi ve bilgi güvenliği kavramları incelenmiştir. Bilgi kavramının gelişimi ve işletmelerdeki önemi arz edilmiş, bilgi güvenliği ile ilgili ülkemizdeki ve dünyadaki hukuki uygulamalar özetlenmiştir. İkinci bölümde bilgi güvenliği standartları ailesi olan ISO 27000 stardardı ailesinin tanıtımı yapılmış, ISO 27001 Bilgi Güvenliği Yönetim Sistemi içeriği incelenmiş ve kurumlarda Bilgi Güvenliği Yönetim Sistemi kurma ve işletme süreçleri anlatılmıştır. Tez kapsamında üçüncü bölümde tez konusu olan Açık Kaynak Kodlu Bilgi Güvenliği Yönetim Sistemi sürecinin otomasyonunda kullanılan alt yazılımlar, programlama dilleri tanıtılmış, otomasyon kapsamında düzenlenen Süreç Yönetim sistemi ve Risk Yönetim Sistemi yazılımlarının sunumu yapılmıştır. Dördüncü bölümde tamamen bu tez kapsamında oluşturulan gerçek olmayan hayali bir bilişim teknolojileri üretim şirketinde üçüncü bölümde anlatılmış olan yazılımların desteği ile BGYS süreç yönetim sistemi örneği kurulmuş ve işletilmeye başlanmıştır. Örnek sürecin uygulanması sonuçların çeşitli örneklerle açıklanmasını müteakiben Sonuç bölümünde, Bilgi Güvenliği Yönetim Sistemini detaylı olarak işleyen süreç yönetim sistemi ve risk yönetim sistemi otomasyonu ile uygulayan kurumların elde edeceği olumlu sonuçların ve kazançların incelenmesi ve ilave geliştirme önerileri ile tez çalışması tamamlanmıştır.

Çalışmanın Yöntemi ve Sınırlılıkları

Çalışmada çoğunlukla kitap, dergi, bu tip sistemleri oluşturan kurumların kısıtlı ölçüde hazırladıkları dökümanlar ve özellikle internet üzerinden elde edilen ikincil veriler kullanılmıştır. Kuramsal ve kavramsal çerçevede daha çok makale ve konu ile ilgili kitaplardan faydalanılmıştır. Bu anlamda konu ile ilgili tez sahibinin halihazırdaki mesleki ilgileri dolayısıyla konular pekiştirilmiştir. Tez kapsamında belirtilen şekiller ve tabloların çoğunluğu oluşturulan system üzerinden alınan görüntülerdir.

Çalışmanın en önemli kısıtlılığı, bilgi güvenliğinin kurumlardaki hassasiyeti nedeniyle BGYS'ni uygulayan kurumlardan konu ile ilgili yeterince veri alınamamasıdır. Yapılan tüm araştırmaların neticesinde örnek uygulamalardan sonuca ulaşılmaya çalışılmış ve oluşturulmaya çalışılan otomasyon sistemi bu örneklerin üzerinde inşa edilmiştir.

BÖLÜM 1: BİLGİ VE BİLGİ GÜVENLİĞİ NEDİR ?

1.1. Bilgi Kavramı

İnsanı diğer canlılardan ayıran en önemli özelliği, düşünebilme ve bu düşüncelerini yorumlayabilme yeteneğidir. Düşünebilen bir varlık olan insan, duyuları ile elde ettiği gözlem, yönelme ve ilgileriyle birlikte bunların sonuçlarını anlamlandırarak idrak etme özelliğine sahiptir. Bununla birlikte insanoğlu, idrak etmiş olduğu gözlem ve ilgilerinin sonucu olarak üzerinde hayatını idame ettirdiği dünyadaki diğer unsurlara karşı algısını değiştiren bir varlıktır. İşte genel anlamıyla ifade edecek olursak, bir gözlem, algılama, işlem sonucunda zihin tarafından değerlendirilerek, muhakeme edilerek oluşturulan bir anlam parçası veya kümesine bilgi denir. Sözlük anlamı açısından baktığımızda bilgi, duyu organları aracılığıyla nesneler hakkında verdiğimiz veya oluşturduğumuz yargılardır. Bilgi nesneden başlar. Duyu organları aracılığıyla algılanır. Algılardan kavramlara ulaşılır ve kavramlar arasında bağlantılar kurularak yargılar verilir. Böylece elde edilen ürüne bilgi denir. Bu anlayışa göre bilgi özne ile nesne arasındaki ilişkiden kaynaklanmaktadır. Burada bilgiyi alan özne, hakkında bilgi alınan ise nesnedir. Sonuç olarak bilgi insanoğlunun kendisinin ve bunun paralelinde toplumun gelişmesinde en önemli unsurdur. Bilginin ekonomik anlamdaki önemine değinmek gerekirse, bilgi hali hazırdaki üç üretim faktörüne (Emek, Sermaye, Müteşebbis) etki etmekte, hatta yeni bir üretim faktörü olarak karşımıza çıkmaktadır. Günümüz ekonomisinde rekabet avantajı sağlanmasında en önemli faktör belki de bilgi faktörüdür. Drucker'a göre "Bilgi kavramının anlamı son 250 yılda değişmeye başlamış, bu durum toplumu ve ekonomiyi değiştirmiştir. Günümüzde ise, anlamlı tek kaynak olarak görünmektedir."(Drucker, 1994). Drucker, aynı eserinde, dünyanın 1980 yılından sonra aldığı durumu ve bilginin ekonomideki üstünlüğünü "enformasyon kapitalizmi" olarak ifade etmektedir. Firmalar, bilginin ekonomideki sözkonusu üstünlüğünü kavrayıp bunu kendi lehlerinde kullanmaları için etkin bir bilgi yönetim sistemini oluşturmaları gerekir. Günümüz teknolojik imkanları bu konuda firmalara çok büyük imkanlar sunmaktadır. Artık Teknoloji sayesinde herhangi bir zamanda, bir yerde ve durumda bilgiye erişim çok kolay olmaktadır. Bu sayede günümüzde bilgi yönetim sistemini halihazırdaki üretim prosedürünün içerisine dahil eden firmalar rakiplerinden bir adım öteye geçmektedir. Fakat bilgiye erişimin bu kadar kolaylaşması, beraberinde bazı sorunları da ortaya

çıkarmıştır. Bu bağlamda bilginin “Bilmesi gereken” prensibine gore erişim sağlanması, yani bilginin yetkisiz erişimlerden korunması gereklidir. Bu husus, ancak etkin bir bilgi güvenliği sistemi ile sağlanabilir.

1.2. Bilgi Güvenliği Kavramı

Bilgi güvenliği kavramını açıklamadan önce güvenlik kavramının evrimi incelenmelidir. Güvenlik kavramı 80’ler hatta 90’ların ortalarına kadar, şahsımızın, ailemizin yaşadığı, çalıştığı alanlardaki fiziki emniyet tedbirleri olarak, yani sahip olunan fiziksel nesnelerin veya alanların emniyeti olarak karşımıza çıkarken, teknolojik sistemlerin gelişmesi ve bunun yanında evrensel bilgi ağı olan internetin ortaya çıkması ile birlikte haberleşme, bilgi teknolojilerinin güvenliği ihtiyacı eklenerek değişime uğramıştır. Giderek artan bir hızla internetin kullanımı, bu evrensel ağda insanların, kurumların bazı kişisel veya kurumsal bilgilerinin paylaşılması zorunluluğunu getirmiştir. İnternet üzerinden yapılan alışverişler, firmaların tedarikçilerinden elde edeceği hammaddelerini internet üzerinden sipariş etmesi, internet bankacılığı, elektronik kütüphaneler, uzaktan eğitim vb. bahsettiğimiz bilgi paylaşımlarının oluşmasına sebep olmaktadır. İnternet günümüzde insanoğluna veya kurumlara sunmuş olduğu bu imkanların kolaylığı yanında bu bilgilerin paylaşılması sebebi ile bir o kadar tehlikeli bir ortam sunar. Çünkü bilgi, yeterince önlem alınamazsa yetkisiz kişilerin erişimine açılabilir. Ve sözkonusu bilgi, kullanım maksadından saptırılarak farklı maksatlarla kullanılabilir. Örneğin bir müşterinin kredi kartı bilgileri internet üzerinden alışveriş imkanı sunan bir firma tarafından tamamen güvenli olmayan bir mekanizma üzerinden temin edilebilir ve üçüncü kişilerin bu bilgileri çalması sözkonusu olursa, bu hem firma tarafından, hem de müşteri tarafından belkide geri dönülemeyecek zararlara sebep olabilir. Bunun yanında güvenliği yeterince sağlanmamış elektronik devlet (E-devlet) uygulamaları ile devlet kurumlarının hem dünya sathında, hem de vatandaşlarının gözünde kaybedeceği itibarı ve devletin güvenilirliğinin de çok ciddi bir şekilde kaybedileceğini de unutmamak gerekir.

İnternetin yanında kurumlar bilgi alışverişi maksadıyla teknolojinin diğer imkanlarından da yoğunlukla faydalanmaktadırlar. Uydu haberleşmesi, Sesli ve görüntülü telefon ve televizyon haberleşmesi bunlardan bazılarıdır. Kurumlar bilgi alışverişinde bu

sistemlerden faydalanırken bilerek veya bilmeyerek olası bazı tehditlerinde etkisindedir. Dinleme tehditleri bu konudaki belki de en önemli örnektir.

Bu tanımlardan yola çıktığımızda bilgi güvenliğinin amacı; Bilginin sadece erişim yetkisi verilmiş kişilerce erişebilir olmasını (Gizlilik), söz konusu bilginin işleme yöntemlerinin bütünlük ve doğruluğunu ve yetkili kullanıcılar için bilginin ve ilişkili kaynaklarının gerekli olduğu anda erişilebilmesini ve kullanılabilmesini (kullanılabilirlik) sağlamaktır. Bunların yanında kimlik kanıtlama (Authentication) ve inkâr edememe (Non-Repudiation) bilgi güvenliğinin en temel unsurlarındandır. Ayrıca Söz konusu beş unsuru sorumluluk (accountability), erişim denetimi (access control), güvenilirlik (reliability) ve emniyet (safety) desteklemektedir.

Buraya kadar geldiğimizde; yapılan tanımlardan belki de daha önemli olan unsur ise insan kaynağının güvenliğidir. Unutulmamalıdır ki, Bilgi güvenliğindeki en zayıf halka hiç kuşkusuz insandır. Kurumumuzda çalışan bir personelin müşteri kimlik numarasını yanlış girdiğini, çok önemli bir dosyayı yanlışlıkla sildiğini veya yanlış bir kablonun bilinçsizce yerinden çıkarıldığını düşünelim. Bunun yanında işe alımlarda yapılan yanlış tercihleri unutmayalım. Ayrıca günümüzde ortaya çıkmış olan sosyal mühendislik kavramı kapsamında bir çağrı merkezi personelinin bir takım kurumsal veya müşteriye ait olan bir bilgiyi paylaştığını düşünelim. İşte biraz önceki ve daha birçok güvenlik zafiyetini insan kaynağı unsuru meydana getirmektedir. Bu kapsamda insan kaynağının önemi büyüktür. Uluslararası denetim ve danışmanlık firması Ernst & Young, Türkiye'nin de içinde bulunduğu 61 ülke ve çeşitli sektörlerden 1865 kuruluşun katılımıyla gerçekleştirdiği "2009 Küresel Bilgi Güvenliği Anketi" adlı bir çalışmada 2009 yılında bilgi güvenliğini sağlamanın önündeki en önemli engel olarak yeterli sayıda nitelikli insan kaynağının bulunamaması olarak belirlenmiş ayrıca ankete katılan kurumlarının dörtte üçlük bir kısmının ise işten çıkardıkları personelin kurumlarına zarar vermesinden endişe ettiği vurgulanmıştır. Bu araştırmadan ve daha önce edinilen tecrübelerden çıkan sonuçlara göre Bilgi Güvenliğindeki en önemli ve en zayıf unsur insan kaynağıdır.

Ülkemizde ve dünyada bilgi güvenliğinin sağlanmasına yönelik yasal mevzuatlar ve kalite standartları mevcuttur. Bu kapsamda bazı kanun tasarılarıda sözkonusudur. (Bkz.Ulusal Bilgi Güvenliği Teşkilatı Ve Görevleri Hakkında Kanun Tasarısı).

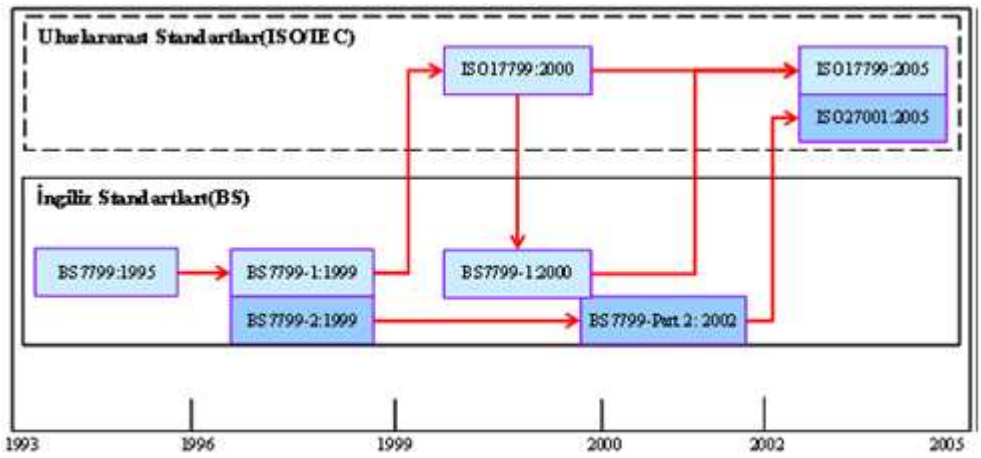
Ülkemizde, sanal ortamda işlenen suçlar ile ilgili olarak 5237 sayılı Türk Ceza Kanunu'nun "Bilişim Alanındaki Suçlar" başlıklı onuncu bölümünde yaptırımlar yer almaktadır. Ayrıca 5070 sayılı elektronik imza kanunu ile birlikte güvenli elektronik imza, elle atılan ıslak imzaya eşdeğer kabul edilmiş ve aynı hukuki sonuçları doğuracağı belirtilmiştir. Yine Aynı şekilde 5809 sayılı elektronik haberleşme kanununun dört numaralı maddesinde elektronik haberleşme hizmeti sağlayan mercilerin bu hizmetlerinde "Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi" ilkesinin kesinlikle göz önüne alınması gerektiğinden açıkça bahsedilmiştir. Yine aynı şekilde T.C. Başbakanlık Personel ve Prensipler Genel Müdürlüğü tarafından hazırlanan ve 17 Şubat 2003 tarihinde imzalanan "Bilgi Sistem ve Ağları için Güvenlik Kültürü" konulu Başbakanlık Genelgesi, OECD Bilgi Güvenliği ve Kişisel Mahremiyet Çalışma Grubu tarafından hazırlanmış olan rehberin Türkçe çevirisidir (Karabacak,2009). Bütün bu çalışmaların yanında organizasyonların bilgi güvenliği uygulamalarını verimli bir şekilde yürütmeleri maksadıyla uluslararası kalite standartları da mevcuttur. Bu kapsamda, ISO 27000 ailesi Bilgi Güvenliği Yönetiminde en etkili rehber ve kalite sistemidir.

BÖLÜM 2: ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN TANITIMI

2.1. ISO 27000 AİLESİ VE TARİHÇESİ

Kurumların Bilgi Güvenliği konusunda karşı karşıya kaldıkları tehditler sebebiyle bilgi güvenliği sürecinin yönetilebilmesi maksadıyla yapılan çalışmalar neticesinde İngiliz Standartları Enstitüsü(British Standards Institutition-BSI) tarafından 1995 yılında BS-7799 standardının ilk bölümü olan BS7799-1, devamında ise 1999 yılında aynı standardın ikinci bölümü olarak tanımlanan BS7799-2, İngiliz Standardı olarak yayımlanmıştır. 2000 yılında küçük belli başlı düzenlemelerden ve uyumlulaştırma çalışmalarından sonra ise ISO tarafından ISO/IEC–17799 adıyla kabul edilerek uluslararası bir standart haline gelmiştir. Bu arada 2002 yılında BSI'ın yapmış olduğu çalışma sonunda BS7799-2 yeniden düzenlenerek İngiliz Standardı olarak birkez daha yayımlanmıştır. 2005 Yılında ISO tarafından ISO/IEC–17799 kabul edilen standart üzerinde değişiklikler yapılarak ISO/IEC–17799:2005 olarak yeniden yayımlanmıştır. Son olarak yine 2005 Yılının sonunda yapılan bir çalışma neticesinde BSI tarafından yeniden hazırlanan BS7799-2 incelenip üzerine eklentiler yapılıp düzenlendikten sonra ISO/IEC:27001 adıyla uluslar arası standart olarak yayımlanmıştır. Bu Kapsamda Bilgi Güvenliği Yönetim Sistemlerinin esasını oluşturan standartların tarihsel gelişimi Şekil-1'de gösterilmiştir.

Şekil 1. ISO/IEC:27001 Tarihçesi



BS-7799 standardı bilgi varlıklarının güvenliğinin sağlanması için oluşturulmuş ilk standarttır. İki bölümden oluşan bu standardın ilk bölümünde bilişim güvenliği ile ilgili çalışma kuralları (Information Technology – Code of Practice for Information Security Management) anlatılmış olup toplam 10 alt bölümde konu ile ilgili 36 kontrol ve 127 alt kontrol maddesi bulunmaktadır. Standardın ikinci bölümünde (Information Technology–Code of Practice for Information Security Management) ise bilgi güvenliği yönetimi sistemini planlamak, kurmak ve devam ettirmek için gerekli olan süreçlerden bahsedilmektedir. Konu ile ilgili belgelendirme ve sertifikasyon bu bölümde yapılmaktadır. BS-7799 yalnızca kurumun kendi prosedürlerinin oluşmasını değil, aynı zamanda üçüncü kişi iş ortaklarınında sözkonusu sürece dahil olması imkanını sağlamaktadır. Bu Kapsamda BS-7799'un oluşumu endüstri, devlet ve diğer ticari kuruluşlardan gelen talepler doğrultusunda BSI kuruluşu ve BOC, BT, Marks&Spencer, Midland Bank, Nationwide Building Society, Shell, Unilever ve diğer bazı şirketlerin katılımıyla oluşturulmuş bir standarttır.

Uluslararası Elektroteknik Komisyonu (The International Electrotechnical Organization-IEC) ve Uluslararası Standartlar Organizasyonu (International Organization for Standardization-ISO) teknik çalışma grupları oluşturarak BS-7799 standardına uluslararası bir boyut kazandıramak için nihai olarak ISO/IEC:27001:2005 standardını yayımlamıştır. ISO ve IEC sözkonusu çalışmalarını birlikte oluşturmuş oldukları teknik çalışma grupları (Joint Technical Committee-JTC) bünyesinde sürdürmektedir. Bununla birlikte Bilgi Güvenliği standartları ile ilgili çalışmalar JTC-1 Bilişim Teknolojileri Komitesine bağlı 41 ülkenin katılımıyla oluşturulmuş SC27: Bilişim Teknolojileri Güvenlik Teknikleri Alt Komisyonunda ele alınmaktadır. Bu Komisyonun sorumluluklarından bazıları aşağıda belirtilmiştir. Buna Göre;

a) Bilgi teknolojileri sistemleri güvenlik hizmetlerinin ve ihtiyaçların tanımlanması

b) Güvenlik Teknikleri ve mekanizmalarının geliştirilmesi

c) Güvenlik kılavuzlarının oluşturulması

d) Yönetim destek dökümanlarının ve standartların geliştirilmesidir.

Bu Kapsamda SC27 alt komisyonu bu görevleri yerine getirirken komisyon içerisinde bulunan 5 ayrı çalışma grubu ile sağlamaktadır. Bu çalışma gruplarından Çalışma Grubu–1 (JTC 1/SC 27/WG 1): Bilgi güvenliği yönetim sistemleri standartları ile ilgili çalışmaları yürütmektedir. ISO, 2005 yılında yaptığı bir düzenleme ile yukarıda bahsedilen ISO/IEC 17779 standardının yerine 27000 serisini bilgi güvenliği ile ilgili standartlara ayırmıştır. Tablo-1'de ISO 27000 serisinin hazırlanan standartları arz edilmiştir. [1]

Tablo 1. Yayımlanan ISO 27000 Ailesi Standartları

Standart Adı	Açıklaması
ISO/IEC 27000–27059	Bilgi Güvenliği ile ilgili standartlar için ayrılmış aralık
ISO/IEC 27000	BGYS standartları için genel bir sözlük (Yayımlanma Tarihi: 2009)
ISO/IEC 27001	BGYS için kurulum, uygulama, kontrol ve geliştirme ile ilgili standart (İlk Yayımlanma Tarihi: 2005)
ISO/IEC 27002	BGYS Uygulama ilkeleri ve tavsiyeleri (Yayımlanma Tarihi: 2007)
ISO/IEC 27003	BGYS Uygulama Rehberi (Yayımlanma Tarihi: 2010)
ISO/IEC 27004	BGYS Ölçüm ve Metrikleri (Yayımlanma Tarihi: 2009)
ISO/IEC 27005	BGYS Risk Yönetim Sistemi (Yayımlanma Tarihi: 2008)
ISO/IEC 27006	BGYS Belge kaydı ve belgelendirme süreçleri kılavuzu (Yayımlanma Tarihi: 2007)
ISO/IEC 27011	Telekomünikasyon endüstrisi için BGYS rehberi

1 Yılmaz VURAL, Şeref SAĞIROĞLU Kurumsal Bilgi Güvenliği: Güncel Gelişmeler,Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı, Ankara ,2007. Ayrıca bkz. http://en.wikipedia.org/wiki/ISO/IEC_27000-series

Yayımlanan standartlar haricinde yayımlanması planlanmış ve üzerinde çalışma gruplarının halen çalışmakta olduğu standartlar ise Tablo-2'de belirtilmiştir.

Tablo 2. Planlanan ISO 27000 Ailesi Standartları

Standart Adı	**Açıklaması**
ISO/IEC 27007-27008	BGYS izleme rehberi (Yönetim sistemi ve güvenlik kontrolleri odaklı)
ISO/IEC 27000	BGYS standartları için genel bir sözlük (Yayımlanma Tarihi : 2009)
ISO/IEC 27013	ISO/IEC 20000-1 and ISO/IEC 27000 standartlarının birleşik olarak uygulama rehberi
ISO/IEC 27014	Bilgi Güvenliği Yönetişimi Çerçevesi
ISO/IEC 27015	Finans ve Sigorta Sektörlerinde BGYS Uygulama rehberi
ISO/IEC 27031	BGYS İş Sürekliliği standart rehberi
ISO/IEC 27032	İnternet için sibergüvenlik rehberi
ISO/IEC 27033	ISO/IEC 18028:2006 temel alınarak Bilişim Sistemleri Ağ güvenliği Rehberi
ISO/IEC 27034	Uygulama Güvenliği rehberi

Uluslararası çalışmaların paralelinde Türkiye'de Bilgi güvenliği ile ilgili çalışmalar ve belgelendirmeler Türk Standartları Enstitüsü tarafından yapılmaktadır. Bu Kapsamda ISO/IEC 17799:2000 standardını tercüme ederek 2002 yılında alınan karar ile TS ISO/IEC 17799 Bilgi Teknolojisi-Bilgi GüvenliğiYönetimi için Uygulama Prensipleri Türk standardı olarak kabul edilmiştir. Bunun yanında BS-7799-2'nin tercümesi yapılarak "Bilgi güvenliği yönetim sistemleri–Özellikler ve kullanım kılavuzu" ismiyle

TS 17799–2 standardı olarak 2005'de yürürlüğe girmiştir. Fakat 2006 yılında TS ISO/IEC 27001:2006 "Bilgi teknolojisi–Güvenlik teknikleri-Bilgi güvenliği yönetim sistemleri ve Gereksinimler" standardının yürürlüğe girmesi ile birlikte iptal edilmiştir. Sözkonusu standart hali hazırda ISO/IEC 27001:2005 standardının tercümesi şeklindedir. Dünyada ve Türkiye'de Bilgi Güvenliği Yönetim Sistemleri Standartlarının tarihçesinden bahsettikten sonra Sözkonusu standardın içeriği hakkında detaylı bilgiler bir sonraki bölümde anlatılacaktır.

2.2. ISO 27001 BGYS İçeriği

2.2.1.BGYS kavramı

Bilgi Güvenliği Yönetim Sistemi, kurumlarda bilgi güvenliği yapısını kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve geliştirmek için, iş riski yaklaşımına dayalı tüm yönetim sisteminin bir parçasıdır. BGYS'nin kurulmasıyla; olası risk ve tehditlerin tespit edilmesi, güvenlik politikalarının oluşturulması, denetimlerin ve uygulamaların kontrolü, uygun yöntemlerin geliştirilmesi, örgütsel yapılar kurulması ve yazılım/donanım fonksiyonlarının sağlanması gibi bir dizi denetimin birbirini tamamlayacak şekilde gerçekleştirilmesi anlamına gelmektedir.

BGYS için gereklilikleri belirten standart olan ISO/IEC 27001'in temelindeki düşünce, kurumun hassas bilgilerinin yönetilmesini sağlamak ve etkili bir bilgi güvenliği elde etmek için yönetim sistem süreçlerinin oluşturulması, gerçekleştirilmesi ve sürdürülmesidir. Ayrıca çeşitli büyüklüklerdeki kurumlara uygulanabilecek şekilde planlanmıştır. Söz konusu standart, kurumun sahip olduğu teknolojik imkanlar ve bunların güvenliğiyle ilgilenmez. Bu yönüyle de ISO/IEC 27001 teknik ve teknoloji bağımlı bir standart değil, asıl olarak bilginin güvenliği ile ilgili bir standarttır.

2.2.2.Süreç Yaklaşımı

BGYS sürekli devam etmek zorunda olan bir süreçtir. Ayrıca diğer Kalite Yönetim sistemleri standartlarıyla (ISO 9001, ISO 14001) uyumlu olarak geliştirilmesi sebebiyle ISO/IEC 27001 standardı planla-uygula-kontrol et-önlem al (PUKÖ) döngüsünü benimsemiştir. Bu standart ile birlikte yapılacak olan bütün faaliyetler bir süreç olarak değerlendirilmektedir. Bu süreçlere yapılan girdilerle elde edilen veriler ile süreç sonucunda çıktılar üretilmektedir. Ayrıca bir sürecin çıktısı diğer sürecin girdisi

olmaktadır. Bir kuruluş içerisinde, tanımları ve bunların etkileşimi ve yönetimleriyle birlikte süreçlerin oluşturduğu bir sistem uygulaması "süreç yaklaşımı" olarak tanımlanabilir. Bilgi Güvenliği Yönetimi Süreç Yaklaşımı, kullanıcılarına aşağıdaki konuların önemini vurgular:

a) İş bilgi güvenliği gereksinimlerini ve bilgi güvenliği için politika ve amaçların belirlenmesi ihtiyacını anlamak,

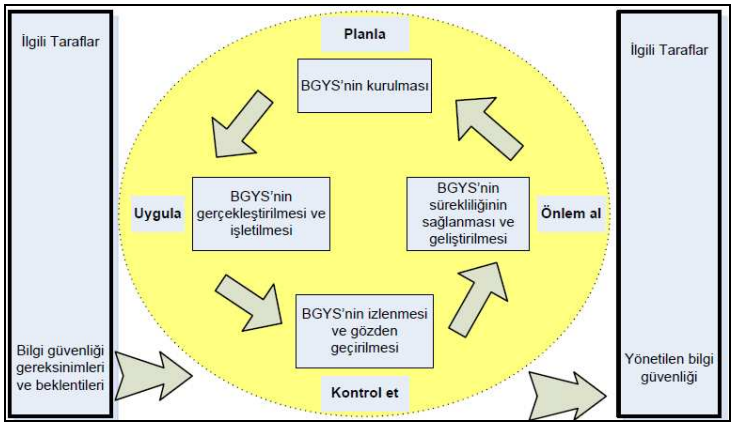
b) Kuruluşun tüm iş risklerini yönetmek bağlamında kuruluşun bilgi güvenliği risklerini yönetmek için kontrolleri gerçekleştirmek ve işletmek,

c) BGYS'nin performansı ve etkinliğini izlemek ve gözden geçirmek,

d) Nesnel ölçmeye dayalı olarak sürekli iyileştirmek(Doğantimur,2008).

BGYS'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl alındığını, gerekli eylemler ve süreçler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak bilgi güvenliği sonuçlarını üretilme biçimi Şekil-2'de gösterilmiştir.

Şekil 2. ISO/IEC 27001 PUKÖ Döngüsü



Kaynak:Önel ve Dinçkan (2007:8)

ISO/IEC 27001 standardında belirlenmiş olan BGYS süreçlerine ilişkin uygulanan PUKÖ döngüsünün hedefleri;

Planlama Safhası(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, süreçler ve prosedürlerin gerçekleştirilip işletilmesi,

Kontrol Et (BGYS'nin sürekli izlenmesi ve Gözden geçirilmesi)

BGYS politikası, amaçlar ve kullanım deneyimlerine göre süreç performansının değerlendirilmesi ve uygulanabilen yerlerde ölçülmesi ve sonuçların gözden geçirilmek üzere yönetime rapor edilmesi,

Önlem Al (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi)

BGYS'in sürekli gelişiminin sağlanması için içsel BGYS denetim ve sonuçlarına, yönetimin gözden geçirmesine ve konuyla ilgili diğer bilgilere göre düzeltici ve koruyucu önlemlerin alınmasıdır.

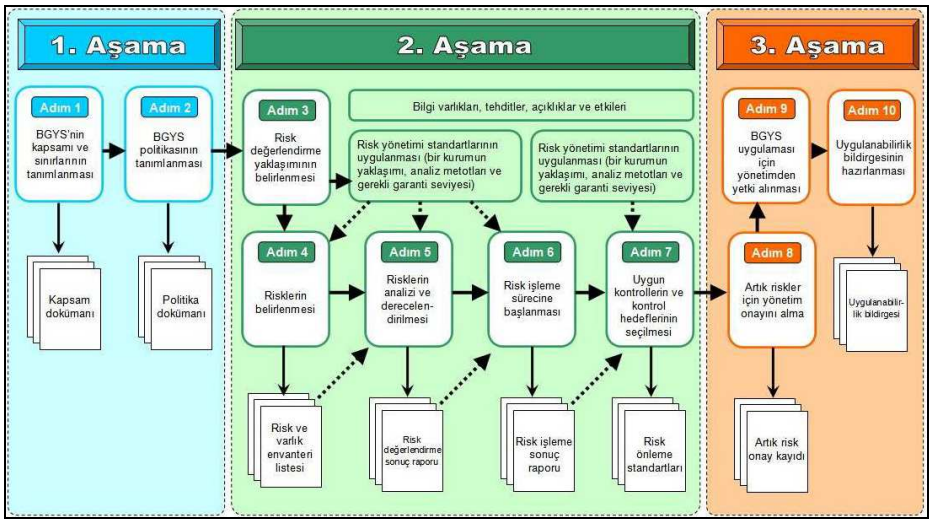
Hiç Şüphesiz BGYS sürecinin en önemli adımı planlama safhasıdır. Etkin olarak tasarlanmış, kurumun amaç ve hedeflerine ulaşmada aktif bir rol oynayacak bir BGYS'nin kurulumu bir sonraki adım olan uygulama safhasında kurumun maksimum verim almasını sağlayacaktır. Nitekim BGYS; Uygulanacağı kurum için iş devamlılığı, beklenmedik felaket durumlarında kaybın en aza indirilmesi, firmaların yapı taşları sayılan kaynakların her koşulda gizliliğinin, ulaşılabilirliğinin ve bütünlüğünün korunması amaçlarını taşır. Bununla beraber ISO/IEC 27001 standardına göre oluşturulmuş olan bir BGYS'ye sahip olmak kuruma hiçbir zaman yüzde yüz bir güvenlik seviyesi sağlamayacaktır. Fakat kurumun çıkarlarını en yüksek düzeyde tutmayı ve bilgi güvenliği ile ilgili açıklarını ve risklerini en düşük düzeye indirmeyi hedefleyecek ve sağlayacaktır.

2.3. Bilgi Güvenliği Yönetim Sisteminin Kurulması ve Yönetilmesi

Bir kurumda bilgi sadece bilgisayarlarda, sunucularda yani teknolojik donanımlarda değil, her yerde ve durumda bulunabilir. Örnek olarak kâğıt üzerindeki bilgi, kurumda

herhangi bir görevi icra eden personelin görev ile ilgili teknik bilgisi vb. birçok bilgi, kurumun bilgi envanterinde bulunabilir. Bundan dolayıdır ki; ISO/IEC 27001 standardı yalnızca bilgisayar veya bilişim güvenliği ile ilgilenmez. Sözkonusu bilgisayar ve bilişim güvenliği yanında kurumun bilgi ile ilgili süreçlerinin de güvenliğini sağlamayı hedefleyen bir standartdır. Bu standart, bir Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) kurmak, gerçekleştirmek, işletmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için bir model sağlamak üzere hazırlanmıştır. BGYS, bilgi varlıklarını koruyan ve ilgili bütün taraflara güven veren tatmin edici ve kapsamı ile orantılı güvenlik kontrollerini sağlamak için tasarlanmıştır. ISO/IEC 27001 standardına göre bir kurumda BGYS kurulumunu gerçekleştirmek üzere tüm dünyada ve ülkemizde çeşitli çalışmalar yapılmıştır ve halen yapılmaktadır. Bu çalışmaların ülkemizde belki de en kapsamlı ve diğer kurum ve kuruluşlara katkı sağlayacak şekilde uygulanışı TÜBİTAK/UEKAE tarafından yapılan çalışmadır. Sözkonusu çalışma ile birlikte uygulamadan, toplumun bu çalışma hakkında bilgilendirilmesi kapsamına kadar yapılan çalışmalar www.bilgiguvenligi.gov.tr sitesinde yayımlanarak konu hakkında çalışma yapan ve yapacak olan kurumların hizmetine sunulmuştur. Bu kapsamda BGYS'nin kurulma aşamasının TÜBİTAK/UEKAE modeli Şekil-3'de gösterilmiştir.

Şekil 3. ISO/IEC 27001 TÜBİTAK/UEKAE Modeli



Kaynak: Önel ve Dinçkan (2007:14)

ISO/IEC 27001 standardına bağlı kalarak ve TÜBİTAK/UAKAE Modeli ışığında Bilgi Güvenliği Yönetim Sistemi'ni kurmak ve devamında uygulamak isteyen bir kurumda yapılması gereken adımlar aşağıda maddeler halinde belirtilmiştir.

2.3.1.Bilgi Güvenliği Organizasyonunun (Komisyonunun) oluşturulması

Her çalışmanın en başında olduğu gibi BGYS kurulumu çalışmalarında da bu çalışmaları düzenleyecek, uygulayacak ve bu sistemi yönetebilecek bir ekibin oluşturulması çok önemlidir. Standart, bilgi güvenliği organizasyonlarını iki bölüm halinde ele almaktadır. Bu anlamda iç organizasyon ve dış taraflar kavramı ortaya çıkmaktadır. İç Organizasyon, kuruluş içerisinde bilgi güvenliği faaliyetini yöneten organizasyon, dış taraflar ise iç organizasyon haricinde kuruluşun ürettiği bilgiye erişen ve bu sözkonusu bilgileri işleyen gruptur. İç Organizasyonun temel sorumlulukları ;

a) Kurumun ihtiyacına istinaden Bilgi güvenliği hedeflerini tanımlamak, bu hedeflere ulaşırken ihtiyaç duyulan yeterli kaynak kullanımını sağlamak ve kurumun süreçlerine BGYS'nin doğru entegre edilmesini sağlamak,

b) BGYS Politikasının belirlenmesini ve uygulanmasını, BGYS Kapsamının oluşturulmasını, BGYS hedef ve planlarının belirlenmesini ve BGYS politikasına bağlı kalarak kurum içerisindek bilgi güvenliği ile ilgili rollerin ve sorumlulukların belirlenmesini sağlamak,

c) BGYS'nin kurulumu, uygulanması, işletilmesi ve sürekli güncel tutulması için yeterli kaynak tahsisi sağlamak,

d) Bilgi güvenliği ihtiyaçları ile kurum amaçlarını uyumlaştırarak BGYS ile maksimum verim almaya çalışmaktır (Calder ve Watkins,2008).

Kurum içerisinde bu çalışmayı sürdürecek BGYS organizasyonu bilgi güvenliği yönetimi konusunda mutlaka eğitim almış olmaları gerekir. Ayrıca dış tarafların da mutlaka bilgi güvenliği konusunda bilgilendirilmesi gerekmektedir. Ayrıca Risk yönetimi, politika oluşturma, güvenlik prosedürlerinin hazırlanması ve uygun kontrollerin seçilerek uygulanması aşamalarında uzman desteği ve daha önce bu süreçleri uygulamış olan kurumlardan danışmanlık almaları faydalı olacaktır. Böylece BGYS'yi en iyi nasıl uygulayacağı konusunda bağımsız danışmanlardan görüş ve tavsiye alabilir.

2.3.2.Kapsamın Belirlenmesi

Kurumda BGYS kapsamında olacak tüm alt organizasyonların, bölgelerin ve aktivitelerin açıkça belirlenmesi gerekir. Kapsam dışında bırakılan bütün diğer öğelerin kapsam dışı tutulma gerekçeleri açıklanmalıdır. Gelişmeler ve değişen ihtiyaçlarla birlikte kapsamın içeriği değiştirilebilir. Fakat kapsamın yönetilebilir boyutta tutulması önemlidir. Bu yüzden organizasyonun fiziksel yapısı ve süreçleri göz önüne alınmalıdır. Bunun yanında büyük kurumlar için iki BGYS uygulanması da sözkonusu olabilir (Perendi). Organizasyon, konu ile ilgili kapsama dahil olan bütün öğeleri içeren , hedeflerin açıkça belirtilmiş olduğu, kurumun bilgi işleme vasıtalarının açıklandığı, konusu ile ilgili yasal zorunlulukların bulunduğu organizasyonların bu zorunluluklarını belirttiği, kapsam dışı tutulan öğeler ile bunların kapsam dışı tutulma gerekçelerinin belirlendiği ayrıntılı fakat anlaşılabilir bir kapsam dökümanı hazırlaması gerekmektedir.

2.3.3.Bilgi Güvenliği Politikasının Oluşturulması

BGYS kurulumunda, organizasyonun oluşturulmasından sonra ilk atılması gereken adım bilgi güvenliği politikasının oluşturulmasıdır. Bilgi güvenliği politikaları, kurumun bilgilerinin yönetimini ve güvenliğini düzenleyen kurallar ve uygulamalar bütünüdür. İyi hazırlanmış bir bilgi güvenliği politikasının özellikleri kısa ve anlaşılabilir olması, uygulanabilir olması, değişebilen durumlara ve iş stratejilerine karşı esnekliğidir. Bunun yanında çok az kısaltma ve teknik ifadeler kullanılmalıdır. Politika dökümanının kurumun her kademesindeki çalışanları tarafından net bir biçimde anlaşılır olması gerekir. ISO/IEC 27002 BGYS uygulama ilkeleri ve tavsiyeleri standardına bağlı kalarak bir bilgi güvenliği politikasının işlemesi gereken maddeler;

- **a)** BGYS Kapsamı ve bilgi güvenliğinin kurum için ihtiyacı ve önemi,
- **b)** Bilgi güvenliği Hedefleri,
- **c)** Yönetimin Bilgi Güvenliğini Sağlama Sözü ve Politika Dokümanının Onayı,
- **d)** Bilgi güvenliği için belirlenmiş sorumlulukları,
- **e)** Kurumun Risk Yönetim çerçevesinin tanıtımı,
- **f)** Bilgi güvenliği ilkeleri ve bilgi güvenliği ile ilgili genel kurallar ve ihlallerindeki yaptırımlar,
- **g)** Standartlar ve Yasal mevzuatlar ile uyum ve koordine,

h) Gelişen ve değişen durumlar ve stratejiler, aynı zamanda rutin yapılacak olan gözden geçirme faaliyetleri ve dökümanı hazırlayanlar ile gözden geçirme tarihleri belirtilmelidir.

2.3.4. Risk Yönetimi Süreci

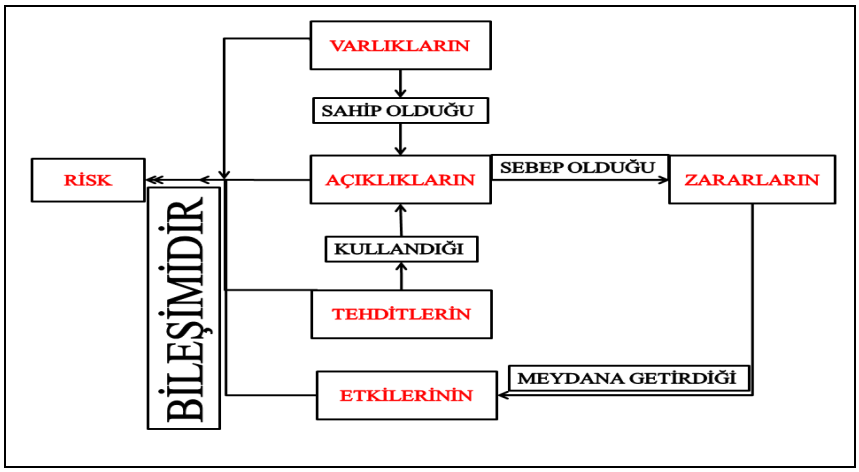
"TS ISO/IEC 27001:2005 Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardına göre risk yönetimi, bir kuruluşu risk ile ilgili olarak kontrol etmek ve yönlendirmek amacıyla kullanılan koordineli faaliyetler olarak tanımlanmıştır. Risk Sözlük anlamı ile zarar ve kayıp durumuna sebebiyet verecek beklenen veya beklenmeyen olayların ortaya çıkma olasılığıdır. Bu anlamda Riskin iki temel bileşeni bulunmaktadır. Bunlar ;

a) Belirli bir sonuca ulaşamama olasılığı ve istenmeyen bir olayın oluşma olasılığı

b) Sonuca ulaşamama veya riskin gerçekleşmesi durumunda meydana gelen olay (Etki)

Bu temel bileşenler ışığında risk bir olasılık ile olayın sonucunda meydana gelen etkinin fonksiyonu şeklinde ifade edilebilir (Fıkırkoca,2003). Yani matematiksel risk fonksiyonu Risk = f (olasılık, etki) şeklindedir. Şekil-4'te bir başka anlatımla risk kavramının tarifi yapılmıştır.

Şekil 4. Risk Tanımı Şeması



Kaynak: Vacca (2009:104)

Risk Yönetimi sürecinde risk kavramının tanımı yapıldıktan sonra Risk analizi kavramını incelemekte yarar vardır. Risk değerlendirme sürecinin alt süreci olan risk

analizi sürecinde kurumun risk tahminleri yapılır ve riskler tanımlanır. Sözkonusu riskler, risk değerlendirme aşamasına veri olur. Risk analizi temel olarak iki yöntem vasıtasıyla yapılabilir. Bunlardan risk analizinin girdilerinin sayısal değerlere aktarılarak matematiksel hesaplamalarla yapılan analize Nicel Risk Analizi, girdilerin sayısal değerler yerine "yüksek","düşük" gibi tanımlayıcı değerlere aktarılarak yapılan analize ise Nitel Risk Analizi denir. Bütün kurumlar iş süreçleri veya çeşitli konularla ilgili hergün veya herhangi bir zamanda çeşitli risklerle karşılaşabilirler. Kurumun bilgi güvenliği ile ilgili riskleri kontrol altında tutma ve yönlendirmek maksadıyla risk yönetim sürecini oluşturulması gerekmektedir. Çünkü Risk analizi ve yönetiminin amacı, kurum içinde meydana gelecek tehlikelere uygun yanıt verebilecek, bilinçli veya bilinçsiz tehditlerin etkisini ve olma ihtimalini azaltacak hazırlıkları prosedürleri ve kontrolleri teşhis ve tespit etmektir (Durmuş,2002). Genel olarak risk yönetim planlarının dört temel hedefi bulunmaktadır. Bunlar;

a) Konu ile ilgili Riskleri ortadan kaldırmak,

b) Riskleri yaratan sebepleri ortadan kaldırmak,

c) Oluşturulacak olan kontroller ve önlemlerle birlikte sözkonusu riskler ile yaşamak,

d) Bu riskleri diğer kurumlara (Örneğin sigorta kuruluşları) sevketmektir (Calder ve Watkins).

Kurumlar risk analizinde öncelikle kapsamlarını belirlemelidir. Bu aşamada Risk yönetimi ve analizi kapsamında olacak bütün bilgi teknolojileri sistemlerinin sınırları oluşturulur, tanımlanır. Bilişim teknolojileri sistemleri için riskleri tanımlamada bir sonraki adım varlıkların belirlenmesi aşamasıdır. Bu manada varlık, kurumun bilgi süreçleri ile ilgili kurum için değeri olan bütün öğelerdir. Ayrıca varlık kavramını sadece yazılım ve donanım varlıkları olarak düşünmemek gerekir. Bunların yanında dosyalarda tutulan satış bilgileri, faturalar, toplantı tutanakları, üretim süreçleri, üretilen hizmet veya mallar, mali değeri olan öğeler, personel ve kurumun imajı kurumun varlıkları arasında yer almaktadır. Kurum varlıklarını belirlemede çeşitli yöntemler kullanabilir. Kurum içerisinde bir anket ile bilgi sistemlerini kullanan ve yöneten çalışan ve yöneticilere ulaşarak varlıklarını belirleyebilir. Ayrıca yine bilgi sistemleri kullanıcıları ve yöneticileri ile yapılacak birebir görüşmelerde varlıklar belirlenebilir. Tüm bunlara destek olarak teknolojik ve organizasyonel imkanlar doğrultusunda varlık belirleme ekipleri oluşturulabilir veya çeşitli tarama metodları ile varlık envanteri

oluşturulabilir. Kurumun bilgi güvenliği ile alakalı varlıkları belirlenmesine müteakip sözkonusu varlıkların bazı kriterlere göre sınıflandırılması risk analiz için temel adımdır. Sınıflandırma bazı varlıkların maddi değerlerine bağlı olarak yapılabileceği gibi bazı varlıklarında niteliksel özelliklerine göre düşük, yüksek, ortak vb. de yapılabilir. Veya eşleştirme yapılarak tek bir derecelendirme usulü belirlenebilir. Örneğin kurumun maddi değeri 1000 TL'den olan varlıklarının derecelendirilmesi "düşük" olarak kararlaştırılabilir. Sözkonusu sınıflandırma işlemi için büyük kurumlarda 5-6, küçük kurumlarda ise 3-4 adet derecelendirme seviyesinin belirlenmesi TÜBİTAK/UEKAE tarafından tavsiye edilmektedir. Bilgi güvenliği açısından varlıkların korunmasında gözetilecek bir diğer husus ise varlıkların gizlilik, bütünlük ve erişebilirlik açısından derecelendirilmesidir. Örneğin bazı verilerin gizliliği, erişebilirlik niteliğinden daha büyük öneme sahip olabilir. Bu sebepten verilerin bu derecelendirilmesi bu üç nitelik bakımından yapılmalıdır. Kurumun bilgi güvenliği kapsamındaki varlıklarının bu anlamda derecelendirilip sınıflandırılması aşamasından sonra bu varlıklara yönelik tehditler belirlenmelidir. Tehdit kavramını bilgi güvenliği açısından inceleyecek olursak, tehdit herhangi bilgi varlığının yada kaynağının bir zayıf noktasının yani açıklığının kasıtlı olarak veya kazayla sözkonusu varlık veya kaynaklara zarar verme potansiyeli olarak tanımlayabiliriz. Tehdit kaynağı ise bu açıklıkları kullanarak varlıklara zarar verme olasılığı olan durum ve olaylardır. Bir diğer ifade ile tehditlerin değerlendirilerek kategorize edilmeleridir. Tehdit kaynakları ise en bilinen sınıflandırma ile ;

a) Deprem, sel, yıldırım gibi oluşmasına engel olunamayan **doğal tehditler,**

b) Elektrik Kesintileri , Çeşitli sızıntılar ve hava kirliliği gibi **çevresel tehditler,**

c) Korsan yazılım yükleme, ağa sızma, yanlış veri girişi gibi bilfiil insan tarafından sebep olunan kasıtlı veya kasıtsız **insan kaynaklı tehditler**dir**.**

Kurumun bilgi varlıklarına yönelik tehditlerin yanında bu varlıklarında çeşitli sebeplerden dolayı bilgi güvenliği ihlallerine neden olabilecek bazı hatalar, zayıflıklar veya uygulamadan kaynaklanan kusurlar bulunabilir. İşte bu zayıflıkları bilgi güvenliği kapsamında kurumun bilgi varlıklarının açıklarıdır. Ve BGYS'nin risk yönetimi unsuru tarafından çok büyük önemle tahlil edilmesi gerekmektedir. Bu manada açıklar tek

başlarına bir tehlike oluşturmazlar. Fakat konu ile alakalı bir tehdit durumunun ortaya çıkmasıyla kurum açısından tehlikeli olabilirler. Kurumun BGYS komisyonu kapsamında oluşturmuş olduğu alt risk yönetim grubu sözkonusu açıkları belirlenmesinde çeşitli metodlar izleyebilir. Bu metodlardan biri gelişen teknolojinin imkanları ile çeşitli taramalar ve testler yaparak mevcut açıkları tesbit etmek olabilir. Ayrıca kurum içerisinde bir anket veya birebir görüşmelerle hemen hemen tüm personele ulaşarak açıklar konusunda onlardan bir geri besleme sağlayabilirler. Bunun yanında internette güncel olarak yayımlanan çeşitli açık listelerinden de faydalanılabilir. Tehditler ve açıkların belirlenmesinden sonra oluşan tehditlerin sonucunda gerçekleşecek olan açıkların gerçekleşme olasılıklarının teşhis ve tesbiti gereklidir. Olasılıkları derecelendirirken tehdit kaynağının özellikleri ve açıkların etkinlikleri dikkatli bir şekilde analiz edilmeli bunun yanında kurumun bu açıklar ve tehditler karşısında uyguladığı kontrollerin gözönünde bulundurulması gerekir. Tehditler, açıklar ve uygulanan kontrollere göre Tablo-3'te belirtilen şekilde düşük, orta ve yüksek gibi üç kademeli bir olasılık cetveli çıkarılabilir.

Tablo 3. Olasılık Değerlendirmesi Cetveli

Olasılık Derecesi	Olasılık Tanımı
Yüksek	Tehdit ve kaynağı etkili, açıkların gerçekleşmesini engelleyecek kontroller yok veya yetersiz
Orta	Tehdit ve kaynağı etkili, açıkların gerçekleşmesini engelleyecek kontroller mevcut
Düşük	Tehdit ve kaynağı az etkili, açıkların gerçekleşmesini engelleyecek ve zorlaştıracak kontroller mevcut

Kaynak: Eskiyörük (2007:13)

Olasılıkların değerlendirilmesine müteakip sözkonusu açıkların neticesinde gerçekleşen tehditlerin olumsuz etkileri analiz edilmelidir. Etki analizi aşamasında, gerçekleşen tehditlerin bilgi varlıklarının temel özellikleri olan gizlilik, bütünlük ve erişilebilirliklerini ne kadar etkilediği ile oluşması muhtemel mali kayıplar incelenir. Ve olasılık değerlendirmesi işleminde anlatıldığı gibi varlıklara olan etkisi ve mali kayıplar göz önüne alındığında yine düşük, orta ve yüksek gibi etki seviyeleri belirlenebilir.

Risk Yönetimi sürecinde olasılık seviyelerimiz ve etki analizi seviyeleri belirlendikten sonra kurumun bu süreçleri sonucunda etkileneceği risk faktörleri belirlenir. Ve bu faktörler derecelendirilir. Bu işlem maksadıyla Kurum için bir risk değerlendirme

matrisi oluşturulması gerekir. Örnek olabilecek bir risk değerlendirme matrisi Tablo-4'te sunulmuştur.

Tablo 4. Risk Değerlendirme Matrisi

		ETKİ		
OLASILIK	YÜKSEK	YÜKSEK	ORTA	DÜŞÜK
		YÜKSEK	YÜKSEK	ORTA
	ORTA	YÜKSEK	ORTAK	DÜŞÜK
	DÜŞÜK	ORTA	DÜŞÜK	DÜŞÜK

Kaynak: Eskiyörük (2007:15)

YÜKSEK →Düzeltici önlemler mutlaka uygulanmalı

ORTA →Düzeltici önlemler uygulanmalı

DÜŞÜK →Herhangi bir önleme gerek yok

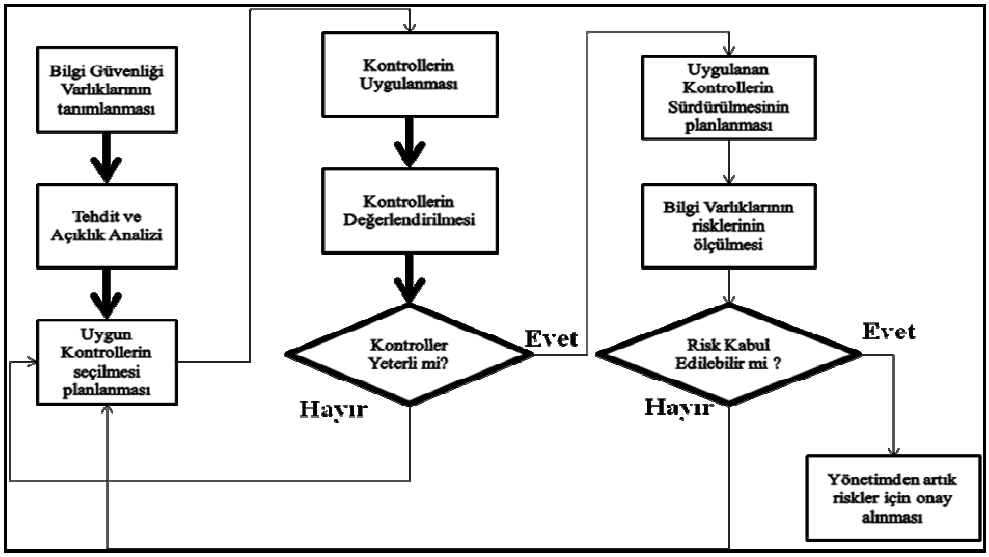
Kurum, Tablo-4'te belirtilen bir matris ile birlikte tehditlerin meydana gelme olasılıklarını ve bu ihtimaller ile birlikte varlıkların gizliliğinin, bütünlüğünün ve kullanışlılığının zarar görmesinin sonuçlarını ve varlıklara olacak olan olumsuz etkilerini derecelendirebilir. Çünkü risk derecelendirmesi tehdit ve açıklıkların olma olasılığı ile bunların etkilerinin çarpımından oluşur. Risk değerlendirme matrisi bu konuda kuruma yardımcı olabilir. Bu matriste belirlenen risk dereceleri bir açığın veya tehditin gerçekleşmesi halinde meydana gelen riski belirlemektedir. İşte bu aşamada kurum, kabul edebileceği risk seviyesini belirlemelidir. Kurumun risklerinin belirlenmesinden sonra kurum sözkonusu riskleri azaltmak ve ortadan kaldırmak için maksadıyla çeşitli önlemler ve iyileştirmeler yapmalıdır. Bu aşama karşımıza risk işleme adımı olarak çıkmaktadır. Risklerin işlenmesi aşamasında kurumun belirlenen risklere karşı uygulayacağı kontroller belirlenir. Bu kontoller ISO/IEC 27001 standardının EK-A dökümanında belirlenmiş olan kontroller olabileceği gibi yasal uygulamalara ve prosedürlere bağlı kalmak koşuluyla teknik, yönetimsel veya fiziksel başka kontroller de uygulanabilir. Uygun kontrollerin seçiminde maliyet, emniyet, kurumun prestij ve itibarı, yasal zorunluluklar, kurum kültürü ve politikaları gibi

faktörler de gözönünde bulundurulmalıdır. ISO/IEC 27001 standardı kurumlara önleyici, destekleyici, düzeltici, düzenleyici teknik, yönetimsel ve operasyonel kontroller sağlamaktadır. Bu sebeple BGYS'de risk yönetimi aşamasının en önemli öğelerinden biri olan uygun kontrollerin belirlenmesi aşamasında BGYS komisyonunun ve yönetimin ISO/IEC 27001 standardına son derece hakim olması gerekmektedir. Uygun kontrollerin belirlenmesi esnasında risk seviyelerinin değerlendirilmesi gerekir. Ayrıca fizibilite çalışmaları ve Fayda-Maliyet analizleri yapılmalıdır. Fayda-Maliyet Analizi kapsamında kontroller için yeni donanım ve yazılım ihtiyaçlarının, yeni çalışanlar ve onların eğitim ihtiyaçlarının göz önünde bulundurulması önemlidir. BGYS komisyonu ve yönetim tarafından belirlenen kontrollerin uygulanması maksadıyla bir uygulama planının oluşturulması gerekir. Bu planın içeriğinde;

a) Belirlenen Riskleri ve risk seviyeleri
b) Risklerin analizi sonucunda belirlenen kontrol önerilerini
c) Risklerin önceliklendirilmesini
d) Öneriler sonucu seçilen kontrolleri ve kontroller için kaynakları
e) Kontrollerin uygulanmasından ve tetkikinden sorumlu personeli
f) Ve kontrollerin başlayış/bitiş tarihleri bulunması gerekir (Eskiyörük,2007).

Seçilen kontrollerin uygulanmasını müteakiben ayrı ayrı veya bir bütün olarak kontrol sonuçlarının raporlaması işleminin yapılması gerekir. Risk yönetimi bir döngü şeklinde sürekli devam etmesi gereken bir süreçtir. Bu sebepten gelişen ve değişen olaylara karşı belirlenecek veya yürürlükten kaldırılacak kontrollerin sürekli tetkik edilmesi gerekir. Şekil-5'te Risk Yönetimi döngüsü ve risk yönetimi hakkında genel çerçeve oluşturulmaktadır.

Şekil 5. Risk Yönetim Döngüsü



Şekil-5'teki risk yönetim döngüsüne göre sonuç olarak bir kurum bilgi güvenliği risk yönetimi sistemini oluşturacak olursak, öncelikle bilgi varlıklarımızı tesbit etmeli daha sonra açıkları ve Şekil-4'te belirtildiği şekliyle bu açıklıkları kullanan tehditleri belirleyip ISO/IEC 27001 standardına göre uygun kontrolleri seçerek ve bu kontrolleri uygulayarak bu sistemin geri beslemelerini analiz ederek sürekli ilave önlem veya yaptırımlarda bulunulması gerekmektedir. Kurumların iş stratejilerini etkileyen ve gelişen durumlarla ilgili ilave kontrolleri zamanında uygulaması için sözkonusu döngünün uygulanması kaçınılmazdır. Sonuç olarak bilgi güvenliği yönetimindeki en önemli aşama varlıkların, açıkların, tehditlerin doğru tanımlanıp bunlar karşısında maliyet etkin kontrollerin belirlendiği ve geliştirildiği risk yönetimi aşamasıdır. Bu sürecin tamamlanmasından sonra Risk yönetimi çalışma grubu ve BGYS komisyonu BGYS'yi gerçekleştirmek ve işletmek maksadıyla yönetimden yetkilendirilmesini talep etmelidir. Yetki devrinden sonra ISO/IEC 27001 standardının kurumda uygulanabilmesi maksadıyla uygulanabilirlik bildirgesinin oluşturulması gerektir. Söz konusu bildirgede risk yönetimi sonucunda uygulanmasına karar verilen kontrollerin amaçları ve seçilme nedenleri, ISO/IEC 27001 standardının öngördüğü kontrollerden seçilmeyen kontrollerin seçilmeme gerekçeleri belirten, risk işleme sürecini ilgilendiren kararların özetini sunan bilgileri içermelidir. Bu aşamadan itibaren BGYS gerçekleştirilmektedir.

2.3.5. BGYS'nin Gerçekleştirilmesi Ve İşletilmesi

Etkin bir risk yönetimini müteakip kurumun risklerinin risk yönetiminin çıktıları ile belirlenen kontrollerle giderilmesini sağlamak maksadıyla uygulandığı aşamada BGYS'nin gerçekleştirilmesi sağlanmış olmaktadır. Bu aşamada BGYS komisyonunun Risk yönetimi çalışma grubu komisyona bir risk işleme planı sunmalıdır. Bu plan içeriğinde tanımlanmış risklere karşı yönetimin yapması gereken eylemleri, bu eylemlerin öncelik sırasını, sınırlayıcı etkenleri ve bu eylemler için gerekli kaynakları barındırmalıdır. Risk işleme planının oluşturulması işleminden sonra tanımlanan riskleri ortadan kaldırmak veya azaltmak maksadıyla seçilen kontrollerin gerçekleştirilmesi ve kontrollerin etkinliğinin ölçülmesi işlemi gerçekleştirilmelidir. Sonuç olarak kontrollerin etkinliğinin ölçülmesi yöneticiler ve personele kontrollerin planlanan kontrol amaçlarının ne düzeyde uygulanıp başarıldığına dair karar verme imkanı sağlar. [2] Seçilen kontrollerin uygulanmasındaki en önemli hedef, tanımlanmış riskleri en aza indirecek veya ortadan kaldıracak, aynı zamanda kurum için en düşük maliyeti getiren kontrolün uygulanmasını sağlamaktır. Kontrollerin uygulama süreçleri zaman olarak mutlaka belirtilmelidir. Uzun zaman alacak kontrol uygulama süreçleri için BGYS komisyonu çeşitli aralıklarla bu kontrollerle alakalı değerlendirme toplantıları yapmalıdır. Kontrollerin uygulanması sonucunda uygulanan kontrollerin etkinliğinin ölçülmesi önemlidir. Bu kapsamda ISO/IEC 27004 BGYS ölçüm ve metrikleri standardı başvurulacak en önemli kaynaklardan birisidir. Kontrol etkinliğinin belirlenmesinde kullanılan ölçütler, karşılaştırılabilir ve yeniden elde edilebilir sonuçlar vermelidir. Yani ölçüm sonuçları kontrollerin uygulanmasından önceki durumu mutlaka yansıtmalıdır.

Kontrollerin uygulanması aşaması ve tüm BGYS süreçleri paralelinde yürütülmesi gereken en önemli işlem maddelerinden birisi farkındalık sağlama ve eğitim sürecidir. Bilgi güvenliği yalnızca teknik bir konu değildir. Bilgi güvenliğinin en önemli halkası daha önceki bölümlerde bahsedildiği gibi insan kaynağıdır. Aynı zamanda unutulmamalıdır ki; bilgi güvenliği sadece kurumun bilgi sistemleri personeli ile alakalı değil, tüm çalışanların ortak sorumluluğundadır. Çalışanların bilgi güvenliği kapsamında rollerini gerçekleştirmeleri için BGYS komisyonunun, tüm çalışanlara bilgi güvenliğinin önemi hakkında farkındalık sağlaması gerekir. Kişi herhangi bir konu

2 TS ISO/IEC 27001:2006 BİLGİ TEKNOLOJİSİ-GÜVENLİK TEKNİKLERİ-BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMLERİ STANDARDI,2006.

hakkında üzerine düşen sorumluluğu yerine getirmesi için öncelikle konunun farkına varması gerekir. Farkındalık ise eğitimle sağlanır. Bu kapsamda bilgi güvenliği ile ilgili çeşitli zaman aralıklarında kurum içerisinden veya kurum dışından bilgi güvenliği konusundan uzmanlaşmış kişiler vasıtasıyla eğitimler düzenlenmelidir. Bu eğitimlerin yanında kurumun bilgi güvenliği personelinin de eğitimi unutulmamalıdır. Gelişen ve değişen teknoloji ile birlikte uygun kontrollerin uygulanmasına yönelik eğitimlerin kurumun bilgi güvenliği personeli tarafından alınması gerekir. Söz konusu eğitimlerin etkinliği mutlaka değerlendirilmeli ve eğitimler sonucunda elde edilen beceriler ve nitelikler eğitim yönetim dökümanlarına eklenmelidir. Eğitim süreci tüm BGYS süreçlerinde sürekli gelişim felsefesine göre uygulanmalıdır. Çalışanlar ancak bilgi güvenliği konusunda sürekli geliştirildiği sürece BGYS'ye katkıda bulunacaklardır.

BGYS'nin kurumlarda uygulanmasının temel amacı belirlenen risklere karşı kurumun bilgi ve bilgi varlıklarının gizlilik, kullanılabilirlik ve bütünlüğün kabul edilebilir seviyelerde korunmasını sağlamaktır (Arnason ve Willet,2008). Bu sebeple kurum BGYS'yi belirlenen kontrolleri uygulayarak, oluşturulan politikalar ve prosedürlere uygun olarak süreç yaklaşımında üçüncü aşama olan "Kontrol Et" aşaması için gerekli bilgiyi sağlamak hedefi ile işletilmelidir. İşletim esnasında dokümanların ve kayıtların yönetimi önemlidir. Söz konusu doküman ve kayıtlar bir sonraki aşamanın girdisi olacaktır. Bu bağlamda yönetimin bir diğer görevi ise BGYS süreç yaklaşımının her aşamasında gerekli kaynakları sağlamaktır. BGYS işletimindeki diğer önemli husus bilgi güvenliği olaylarının yönetimidir. Bu maksatla kurum, bilgi güvenliği ihlal olaylarında süratle yanıt verebilme özelliğine sahip bir mimari oluşturmalıdır. BGYS bilgi güvenliği olaylarını tanımlayabilmeli ve bunları rapor edebilmeli, bunların yanında ihlal olaylarında meydana gelecek zararları azaltacak şekilde işletilebilmelidir. Ancak bu şekilde işletilen bir BGYS sonucunda süreç yaklaşımının "Kontrol et" aşamasında BGYS'nin etkinliği izlenebilir ve geliştirilebilir.

2.3.6. BGYS'nin İzlenmesi ve Gözden Geçirilmesi

Süreç yaklaşımının "Kontrol Et" aşaması olan bu aşamada BGYS'nin işletiminde ortaya çıkan eksik hususlar tespit edilmeli, uygulanan kontrollerinin etkinliği ölçülmeli başarısız ve başarılı olan güvenlik kontrolleri tanımlanmalı, bilgi güvenliği olayları ortaya koyulmalı, alınan önlemlerin güvenlik açıklıklarını giderip gidermediği ya da işe

yarayıp yaramadığı tespit edilmelidir. Kurumda düzenli aralıklarla BGYS kapsamındaki politikalar, prosedürler ve kontrollerin etkinliklerinin ölçülerek gözden geçirilmesi gerekmektedir. Bu kapsamda daha önce belirtildiği gibi ISO/IEC 27004 BGYS ölçüm ve metrikleri standardı kurumlara kılavuz olacaktır. Gözden geçirme aşamasında iş ortamı kapsamının, iş hedeflerinin değişimi veya yeni ortaya çıkan yasal zorunluluklar gibi kurumun gelişen ve değişen olaylara neticesinde ortaya çıkması muhtemel olan risklere karşı uygulanacak yeni kontrollerin belirlenmesi de çok önemlidir. Kurumlar, kontrol hedeflerinin, kontrollerin, prosedürlerin ve proseslerin tanımlanan güvenlik gereksinimlerini karşılayıp karşılamadığını ve yürürlükteki yasal mevzuatla uyumlu olup olmadığını tespit etmek için düzenli aralıklarla BGYS'nin iç denetimlerini gerçekleştirmelidir. Bu şekilde BGYS'nin ISO/IEC 27001 standardına uygunluğu ile birlikte kurumun süreçlerine uygunluğu da denetlenir. Bu sayede sürekli etkin ve güncel bir BGYS işletilmesi sağlanır. Aynı zamanda PUKÖ yaklaşımının "Önlem al" aşaması olarak tanımlanan BGYS iyileştirme çalışmalarına girdi oluşturulur.

2.3.7. BGYS'nin Sürekliliğinin Sağlanması Ve İyileştirilmesi

BGYS'nin izlenmesi ve gözden geçirmesi safhasında yani "Kontrol" bölümünde uygulanan BGYS'nin etkinliği ve kullanılabilirliği gözden geçirilir. Bu bölümden alınan veriler ise iyileştirme safhası yani "Önlem al" aşaması için bazı ilerleme ve geliştirme tavsiyeleri girdisi olarak sunulur. İç ve dış tetkikler neticesinde halihazırda uygulanan BGYS'nin geliştirilmesi gereken tarafları tesbit edilerek iyileştirme safhasında bu hususların gereği yapılır. Bu anlamda yapılacak iyileştirmelerin ulaşılmak istenen hedeflere uygunluğu mutlaka analiz edilmelidir.

2.3.8. ISO 27001 BGYS Dokümantasyon Sistemi

Kurum, BGYS'nin süreçleri ile paralel olarak BGYS işletirken aynı zamanda ISO/IEC 27001'in ilgili maddesinde belirtilen dökümantasyon gereksinimlerini de yerine getirmek mecburiyetindedir. Bu Kapsamda ;

a) BGYS politikası ve kontrol amaçları dökümanı

b) BGYS kapsam dökümanı

c) BGYS'yi destekleyici prosedürler ve kontrol dökümanları

d) Risk değerlendirme metodolojisi

e) Risk değerlendirme raporu

f) Risk işleme planı

g) Kuruluş tarafından, bilgi güvenliği proseslerinin etkin planlanlanmasını, işletilmesini ve kontrolünü sağlamak için ihtiyaç duyulan dokümante edilmiş prosedürler ve kontrollerin etkinliğinin ölçüm dökümanı

h) Bu standart tarafından gerek duyulan kayıtlar

i) Uygulanabilirlik Bildirgesi.

Yukarıda oluşturulacak dökümantasyona ilave olarak kurum BGYS'nin doğru, düzgün ve etkin bir biçimde işlediğini kanıtlamak için yönetim kurulu toplantıları ve kararlarının kayıtlarını da içeren kuruluşun BGYS ile ilgili aldığı kararları ve/veya politikaları ve standardları uyguladığını belirten ek dökümanları da sözkonusu kütüphaneye eklemelidir. Bunun yanında tutulan kayıtların tekrar elde edilebilir olması da sağlanmalıdır. BGYS'yi işletmek ve BGYS'nin doğru, düzgün ve etkin bir biçimde çalıştığını göstermek için gerekli olan tüm dokümanlar ve kayıtlar sürekli olarak elde bulundurulmalı, kullanılabilir, güncel ve ilişkili olmalıdır. Bu sebepten Dökümantasyon kontrolü çok önemlidir. Düzenli aralıklarla dökümantasyonun gözden geçirilip güncelliğini yitiren dökümanların yenilenmesi çalışmaları yapılmalıdır.Bu kapsamda halihazırda ISO 9001 kalite yönetim sistemlerini benimsemiş olan kurumlarda, ISO/IEC 27001'deki dokümantasyon ve kayıtlar için kontrol gereksinimleri sözkonusu standarda uygun şekilde tasarlandığı için kuruma dokümantasyon, kayıtların yönetimi ve muhafazası maksadıyla gerekli olan kaynaklarda tasarruf edilmesi gibi bir çok yararlar sağlar.

2.3.9. Yönetimin Sorumluluğu

PUKÖ döngüsü, süreç yaklaşımına ve ISO/IEC 27001 Standardına göre yönetimin BGYS için bazı sorumlulukları bulunmaktadır. BGYS'nin kurulması, gerçekleştirilmesi, işletilmesi, izlenmesi ve gözden geçirilmesi süreçlerinde ISO/IEC 27001 Standardının beşinci maddesindeki özellikleri taşımalıdır. Bu kapsamda BGYS politikalarının belirlenmesinde, kabul edilecek risk seviyelerinin belirlenmesinde,

BGYS’nin uygulanması esnasında yeterli kaynak sağlanmasında, ilgili standart ile birlikte diğer yasal sorumluluklara uyum sürecinde ve iyileştirmelere olan gereksinimleri belirlemede en önemli sorumluluğu yönetim bağlılığını göstererek taşımalıdır.Bunların yanında BGYS süreçleri için gerekli kaynakların ve eğitim ihtiyaçlarının tedarik edilmesini sağlamalıdır.Ayrıca yönetim iç denetimin gerçekleştirilmesinden ve denetimlerin neticesinde gerekli olan iyileştirmelerin uygulanmasından sorumludur.

BÖLÜM 3: ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ OTOMASYONU

3.1.BGYS Yönetim Otomasyonu Uygulamasında Kullanılan Alt Yazılımların Ve Araçların Tanıtımı

3.1.1. Açık Kaynak Kodlu (AKK) Yazılım Kavramı

Açık kaynak Kodlu yazılım (Open-Source Software) üretilen üretilen yazılımın üretim süreçlerinin ve kodlarının tüm dünyada herkese açık olarak sunulduğu ve ilgilileri tarafından üzerinde isteğe bağlı tüm değişikliklerin yapılabildiği yazılım türüdür. Hızla gelişen teknoloji sayesinde artık dijital teknolojiler üzerindeki bir bilgi, basılı yayımlar üzerindeki bir bilgiye göre çok büyük bir hızla paylaşılabilmektedir. Bilgi teknolojilerinde üretilen veya geliştirilen bir yazılım ticari bir amaçla üretilip pazarlanabilir. Fakat sözkonusu pazarlama stratejisi kamuoyunu söz konusu üretilen yazılım ile elde edeceği faydalardan mahrum bırakmaktadır. Bir başka açıdan bakacak olursak, sözkonusu üreticilerin de bu üretimleri sonucunda elde ettikleri telif hakları bulunmaktadır. Bu sebepten bilgi teknolojilerindeki telif hakları kavramı açık kaynak kodlu yazılımlar ile yeni bir boyut kazanmıştır. AKK'nun duayeni olarak tanımlayabileceğimiz Richard M. Stallman, 1970'li yıllarda MIT (Massachusetts Institute of Technology)'nin Yapay Zekâ laboratuvarlarında ticari kaygı yerine kamu yararını düşünen serbest yazılımı fikrini benimseyen bir grup araştırmacı ile birlikte 1980'li yıllara kadar yazılım üretme çalışmalarında bulunmuştur. 1984 yılında tamamen bu ekibin ürettiği açık kaynak kodlu yazılımların meydana getirdiği bir işletim sistemi ve işletim sisteminin araçlarının geliştirilmesi çalışması böylece başlamış ve çalışmanın adına 'GNU, Unix değildir' anlamına gelen özyinelemeli (rekürsif) bir kelime olan GNU verilmiştir. GNU projesi kapsamında GPL (Genaral Public Licence) kavramı ortaya çıkmıştır. Bu lisans açık kaynak kodlu yazılım sürecinin belkemiğini oluşturur. Sözkonusu yazılımın üçüncü sürümünün Türkçe sürümü yayımlanmıştır. Buna göre genel olarak GPL altında üretilen yazılımın kaynak kodları herkese açık olmalıdır. Ve yazılım ile ilgilenen diğer geliştiriciler sözkonusu açık kaynak kodlu yazılımı kendilerine uyarlayabilmektedir. AKK yazılımın avantajlarından bir diğeri üretici firmaya veya kişiye bağlı kalmadan AKK yazılımı kullanan bir kurumun tamamen kendi ihtiyaçları doğrultusunda değiştirebilmesidir. Ayrıca popüler olarak kullanılan

AKK yazılımlar tüm dünyada sözkonusu yazılım ile ilgilenen tüm geliştiriciler tarafından dikkatle incelenerek yazılımda olabilecek muhtemel hata ve eksiklikleri ortaya çıkarılacağı için AKK yazılım kullanan kurumlar için bir avantaj sağlayacaktır. Güvenlik hususunda ise kapalı kapılar ardında geliştirilmiş olan bir yazılımın kurumsal bilgi teknolojilerimiz üzerinde ne yaptığını bilememiz, bilgi güvenliği açısından da bir takım zafiyetler sunmaktadır. Bir diğer husus ise maliyettir. İthal edilmiş hazır pahalı yazılımlar yerine yerel olarak üretilmiş yazılımların kullanım maliyeti düşüktür. Ayrıca teknoloji donanımı üreten birçok firmanın da AKK yazılım üretimine verdiği destek önemlidir. Öte yandan Almanya, İspanya, Meksika, Brezilya, Çin, Kore, Hindistan, İran (bkz. Building a National Operating System: Iran's Experience in GNU/Linux) gibi birçok ülkenin, kamu kurumlarında AKK yazılımlarını kullanması söz konusu ülkelerin bilgi teknolojilerinin güvenliği ve maliyetleri konusunda göstermiş olduğu hassasiyeti de vurgulamaktadır. Ülkemizde de özellikle devlet kurumlarının ve üniversitelerimizin çalışmaları sayesinde AKK yazılımlarının kullanımı ve geliştirilmesi teşvik edilmektedir. Sonuç olarak içinde bulunduğumuz bilgi çağında, bilgi teknolojisi üretimi için hazır çözüm ithal etmek yerine bu teknolojiyi üretebilecek iş gücünü yetiştirerek ülkemizin ihtiyaçlarına güvenli, sağlam ve uygun maliyetli yazılımların üretilmesi ülkemizin bilgi toplumu stratejisine en önemli katkıyı sağlayacaktır.

3.1.2. BGYS Yönetim Otomasyonunda kullanılan yazılımlar

3.1.2.1. PHP Web Programlama Dili

İnternetin tüm dünyada yaygınlaşması ile birlikte web siteleri üzerinden bilgi paylaşımı imkânı artmış, bununla birlikte bilgiye erişim kolaylaşmıştır. Özellikle internet ağı üzerinden çalışan “www” hizmeti sayesinde bilgi yönetimi ve transferi sağlanmaya ve paralelinde gün geçtikçe tüm dünya kişisel veya kurumsal web siteleri oluşturmaya ve kullanmaya başlamıştır. İlk internet siteleri HTML (**H**yper **T**ext **M**arkup **L**anguage) tabanında çalışan tek taraflı, web sitesinden kullanıcıya bilgi aktarımı yapan statik bir mantık üzerine çalışmaktaydı. Fakat internet teknolojilerinin gelişmesi ile birlikte kullanıcının da web sitesi vasıtasıyla bilgi transferi yapması ihtiyacı ortaya çıkmıştır. Bu kapsamda internet siteleri üzerinden kullanıcılara bilgi transferi sağlama imkanı sunan dinamik web siteleri oluşturulmaya başlanmıştır. Sözkonusu dinamik web siteleri yalnızca HTML web programlama dili değil bunun yanında PHP, ASP, JSP gibi

dinamik web programlama dilleri kullanılarak oluşturulmaktadır. PHP ilk olarak '**P**ersonal **H**ome **P**ages' adıyla 1990'lı yılların ortalarında Rasmus Lerdorf tarafından geliştirilmeye başlanmıştır. Geliştiricinin bu programlama dilini geliştirmekteki amacı, başlangıçta kişisel bilgilerini internet üzerinde yayımlamak ve internet sitesini ziyaret edenleri izlemek olsa da daha sonradan tüm dünyadaki internet sitesi programcılarının ilgisini çekmesi neticesinde büyük bilgi teknolojileri firmalarının da desteği ile birlikte öncelikle kurumsal fakat aynı zamanda kişisel olabilecek internet programcılığı yazılım geliştirme platformuna dönüşmüştür. PHP resmi internet sitesi www.php.net tarafından yapılan araştırma sonucunda tüm dünyada PHP dilinin kullanımı Nisan 2007 itibariyle yaklaşık yirmi milyon internet sitesi civarındadır. Günümüzde bu rakam tahmini olarak Otuz milyonu aşmıştır. PHP dili aynı zamanda açık kaynak kodlu yazılım mimarisi kapsamında GPL lisansı altında dağıtılmaktadır. Böylece GPL şartlarına uygun olarak "**P**HP: **H**ypertext **P**reprocessor" anlamına gelen özyinelemeli bir tanım ile yeniden adlandırılmıştır. PHP programlama dilinin temelinde "C" programlama dili vardır. PHP dosyaları mantık olarak, hizmet veren bir web sunucusu üzerinde bulunan metin dosyalarıdır. En büyük özelliği olan HTML ile bütünleşik çalışabilmesi özelliği ile birlikte internet siteleri vasıtasıyla PHP dili ile gelen komutlar sunucu tarafından yorumlanarak kullanıcıya tekrar bilgi olarak iletilmektedir. Bu şekilde iki yönlü veri transferi imkânı mümkündür. Aynı zamanda geliştiriciler PHP programlama dili ile kullanıma ve ihtiyaca göre değiştirilmeye hazır internet programları da üretmektedir. Açık Kaynak kodlu yazılımlar adı altında internet ortamında diğer kullanıcı ve geliştiricilerin bilgilerine sunulmaktadır. Günümüzde PHP programlama dili kişisel günlük (blog)sayfalarından, alışveriş siteleri ve kurumsal portallara kadar yaygın olarak kullanılmaktadır.

3.1.2.2. Apache Yazılımı

Apache Yazılımı, PHP başta olmak üzere birçok web programlama dilini destekleyen açık kaynak kodlu bir internet web sunucusudur. Unix, GNU, FreeBSD, Linux, Solaris, Novell NetWare, Mac OS X, Microsoft Windows, OS/2, TPF, ve eComStation gibi hemen hemen bütün işletim sistemleri üzerinde çalışabilen ve "Dünya Yaygın Ağı" yani WWW'nin yaygınlaşmasında en etkin rolü oynayan web sunucusudur. Yapılan araştırmalarda hali hazırda dünya genelinde en çok kullanılan web sunucusu yazılımıdır.

Açık kaynaklı bir yazılım olarak ücretsiz olarak dağıtılması ve yeniden düzenlenebilmesi esnekliğinden dolayı halen popülerliği artmaktadır.

3.1.2.3. MYSQL Yazılımı

Mysql yazılımı çok hızlı ve sağlam bir ilişkisel veritabanı yönetim sistemidir. Adından da anlaşılağı üzere bir veritabanı her türlü veriyi depolamamıza, depoladığımız verilerden arama yapmamıza ve aramalarımız sonucunda istediğimiz veriyi almamıza yarayan sistemdir. Mysql veritabanı yazılımı web sunucularında kullanılan en popüler veritabanı uygulamasıdır. Geliştiricilerin elde ettiği deneyimler neticesinde PHP web programlama dili ile birlikte kullanılan en önemli veritabanıdır. Mysql yazılımı, PHP veya diğer web programlama dili ile tasarlanmış web sitelerinde kullanıcıdan alınacak verilerin depolanmasında veya kullanıcıya sunulacak verilerin derlenmesinde performansı en yüksek veritabanıdır. Ayrıca veri tutarlılığı açısından en güvenilir veri tabanıdır. Mysql yazılımı açık kaynak kodlu bir yazılım olmasının yanında aynı zamanda ticari lisansı da mevcuttur.

3.1.2.4. XAMPP Yazılımı

Xampp yazılımı da daha önceki bölümlerde anlatılan diğer yazılımlarımız gibi AKK bir yazılımdır. Xampp bir web sunucusu oluşturmak ve geliştirmek için gerekli olan bütün AKK yazılımları bir paket altında toplayan, çeşitli işletim sistemleri üzerinde çalışabilen ve bütünleşik olarak web sistemimizi oluşturmamızı sağlayan bir yazılımdır. Xampp üzerinde web sunucusu olarak Apache'yi, Veritabanı uygulaması olarak Mysql'i ve programlama dili kapsamında PHP temel olmakla birlikte tüm web programlama dilleri desteğini barındıran AKK bir yazılım paketidir. www.apachefriends.org sitesinden bu paketi indirip, aynı sitedeki kurulum talimatlarını takip ederek bütünleşik ve php destekli bir web sunucusu oluşturulabilmektedir.

3.1.2.5. Java Programlama Dili

Java programlama dili ve teknolojisi, 1995 yılında nesneye dayalı programlama dillerine alternatif ve açık kaynaklı olarak SUN Microsystems tarafından piyasaya sürülen ve gün geçtikçe tüm bilişim alanlarında kullanılmaya başlanan bir bilişim uygulama platformudur. Java platformu, mobil iletişim araçlarından büyük bilişim projelerine kadar hemen hemen tüm bilgi işlem vasıtalarında etkin olarak kullanılan ve

geliştirilen bir programlama teknolojisidir. Özellikle AKK yazılım olması ve işletim sistemi bağımsız olarak çalışıp geliştirilebilmesi özellikleri sebebiyle tüm yazılım geliştiricileri tarafından benimsenmiştir. Günümüzde cep telefonları yazılımları ve internet teknolojileri üzerinde geliştirilen uygulamalar kullanıcıya en yakın java teknolojileri ürünlerindendir.

3.1.3. BGYS Otomasyonunda Kullanılan Yazılımların Tanıtılması

BGYS'nin Otomasyon işlemi Yönetim, BGYS komisyonu üyeleri ve BGYS'nin ihtiyaç duyduğu tüm çalışanların internet veya kurumun dahili bilgisayar ağı üzerinden erişebileceği web tarayıcıları (İnternet Explorer, Mozilla Firefox, Opera, Netscape Communicator, Safari) vasıtasıyla kullanılacak web tabanlı süreç yönetim uygulaması aşaması ve yalnızca BGYS'nin risk analizi ve yönetimini sağlayacak risk yönetimi komisyonunun erişebileceği java tabanlı bu yüksek lisans tezi kapsamında Türkçeleştirilen AKK risk yönetimi uygulaması aşamasından oluşmaktadır.

3.1.3.1. BGYS Süreç Yönetimi Maksatlı Web Uygulamasının Tanıtımı

3.1.3.1.1. Sistemin Kurulum Aşaması

BGYS sürecinin yönetiminde kurum içi koordinasyon en önemli hususlardan biridir. BGYS komisyonunun ve diğer bütün ilgililerin BGYS hakkında bilgi alışverişini ve BGYS sürecinin yönetimini güvenilir ve kolay erişilebilir bir sistem vasıtasıyla sağlamak amacıyla günümüz web teknolojilerinden ve AKK yazılımlardan faydalanarak BGYS süreç yönetim sistemi oluşturulmalıdır. AKK olan bir süreç yönetim yazılımın benimsenmesi kurumun ihtiyaçları doğrultusunda yeniden düzenlenerek kullanıma sokulabilmesi ve düşük maliyetli olması özellikleri nedeniyle kuruma fayda sağlayacaktır. Bu kapsamda AKK proje ve süreç yönetim yazılımı olan DOTPROJECT yazılımı benimsenmiştir. Web tabanlı olarak PHP web programlama dili ile geliştirilen ve Mysql veritabanı yazılımını kullanan yazılım yüksek lisans tezi kapsamında BGYS Süreç Yönetim Sistemi adı altında Türkçeleştirilip bazı özellikleri değiştirilerek yeniden BGYS süreç yönetim sistemi yazılımı olarak kullanıma sunulmuştur. Yazılım tamamen web tabanlı olarak kullanılmaktadır. BGYS süreç yönetim sisteminin kurulumuna ait işlem maddeleri aşağıda belirtilmiştir.

a) Yazılımın çalışması için gerek duyduğu PHP, Veritabanı ve Web Sunucu hizmetinin sağlanacağı XAMPP yazılımının kurulumu, ve güvenliğinin sağlanması,

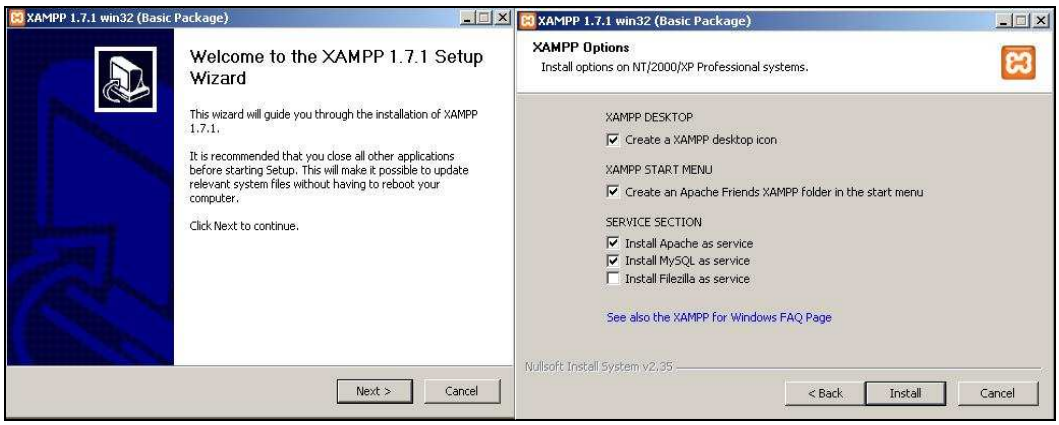
b) İnternetten indirilmiş olan DOTPROJECT Yazılımının kurulumu,

c) Yazılımın Türkçeleştirilerek kullanıma hazır hale getirilmesi,

d) Gereksiz eklentilerin devreden çıkarılarak yazılımın yeni bir proje oluşturmak için hazır hale getirilmesi.

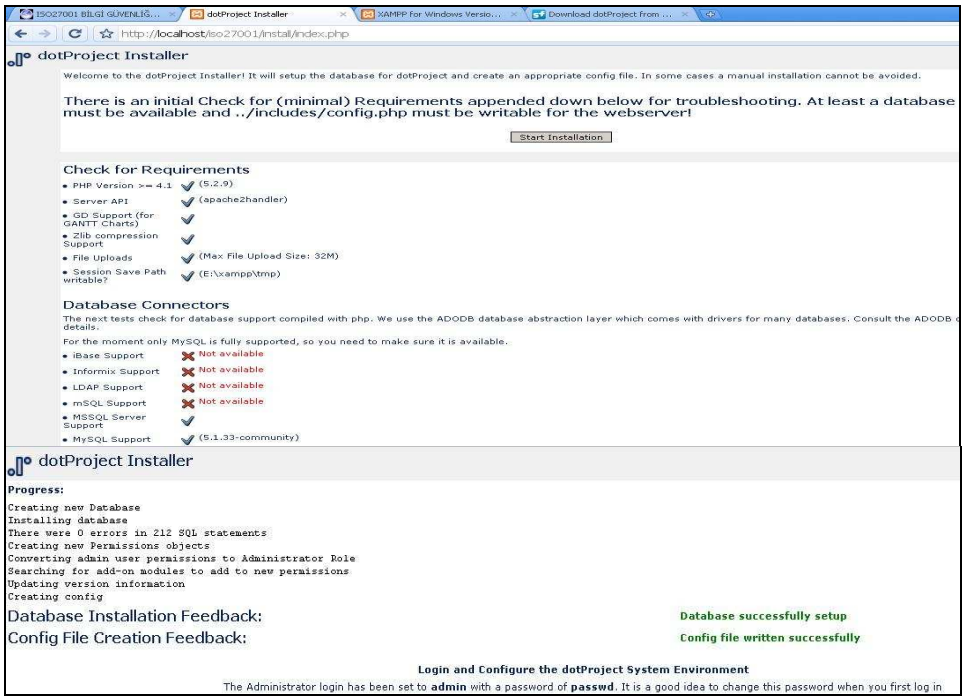
BGYS süreç yönetimi yazılımı faal hale gelmesi için PHP destekli, Mysql veritabanını kullanan bir web sunucusuna ihtiyaç duymaktadır. Bu maksatla bahse konu ihtiyaçları tek bir pakette ihtiva eden, Windows işletim sistemi üzerinde çalışabilen AKK XAMPP yazılımı kullanılmaktadır. XAMPP yazılımının kurulum aşamasından bazı bölümler Şekil-6'da gösterilmiştir. Ayrıca kurulum maksadıyla detaylı bilgiler internet üzerindeki çeşitli forumlardan veya XAMPP resmi internet sitesi olan http://www.apachefriends.org adresinden elde edilebilir.

Şekil 6. XAMPP Kurulum Örneği



İhtiyacımız olan veritabanı ve web sunucusu yazılımının kurulumundan sonra BGYS süreç yönetim sisteminin en önemli unsuru olan DOTPROJECT yazılımının kurulumu yapılmalıdır. Bu maksatla www.dotproject.net internet sitesinden indirilecek yazılım yine aynı web sitesindeki kurulum adımlarına uygun olarak kurulması gerekmektedir. Dotproject yazılımının kurulum aşamasından bazı bölümler Şekil-7'de gösterilmiştir.

Şekil 7 Proje Yönetim Yazılımının Kurulumu

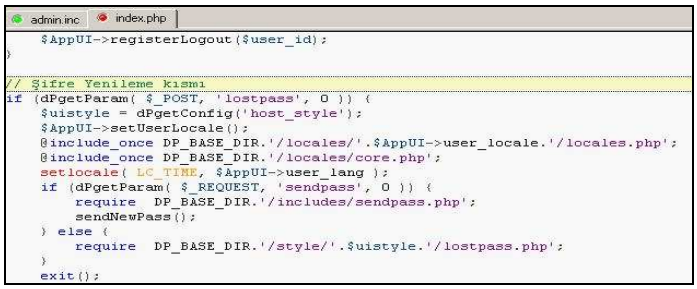


Yazılımın kurulumunun tamamlanmasından sonra internet tarayıcı herhangi bir yazılım vasıtasıyla DOTPROJECT yazılımına erişilebilir. Yazılımın Giriş ekranı Şekil-8'de gösterilmiştir.

Şekil 8. Proje Yönetim Sistemi Varsayılan Erişim Kontrol Sayfası

Yazılımın kurulumundan sonra Türkçeleştirme ve gereksiz eklentilerin devreden çıkarılması işlemleri yapılmalıdır. Sözkonusu değişikliklerin yapılması esnasında PHP dosyalarının değiştirilmesi ve bazı diğer değişiklikleri yine AKK bir düzenleyici yazılım (Code Editor) kullanılmaktadır. Ticari bir düzenleyici yazılım kullanmak isteyen veya hali hazırda bir düzenleyici ticari lisansı bulunan kurumlar bu ürünlerini de kullanabilirler. Yapılan işlemler esnasındaki değişikliklere ilişkin bir düzenleme süreci Şekil-9'de gösterilmiştir.

Şekil 9. PHP Kodu Düzeltme Örneği



BGYS Süreç Yönetim sisteminin temel olarak yukarıda bahsedilen adımlar vasıtasıyla kurulumu tamamlanacaktır. Buraya kadar uygulanan işlem adımlarıyla birlikte başlangıçtan yani sıfırdan hazırlanarak kurumun kendi ihtiyacı neticesinde kurulum yapılabilmektedir. Fakat bu yüksek lisans tezi kapsamında Türkçeleştirilip kullanıma hazır hale getirilmiş olan BGYS süreç Yönetim Sisteminin kurulumu daha da kolaylaştırılmıştır. BGYS Süreç Yönetim Sisteminin kurulumunu yapmak için Yüksek Lisans Tezi kapsamında CD Ortamında hazırlanan yazılım kolaylıkla kurulabilmektedir. Aynı CD'nin içeriğinde Resimli Görsel bir kurulum dökümanı eklenmiştir.

3.1.3.1.2. Sistemin İşletim Aşaması

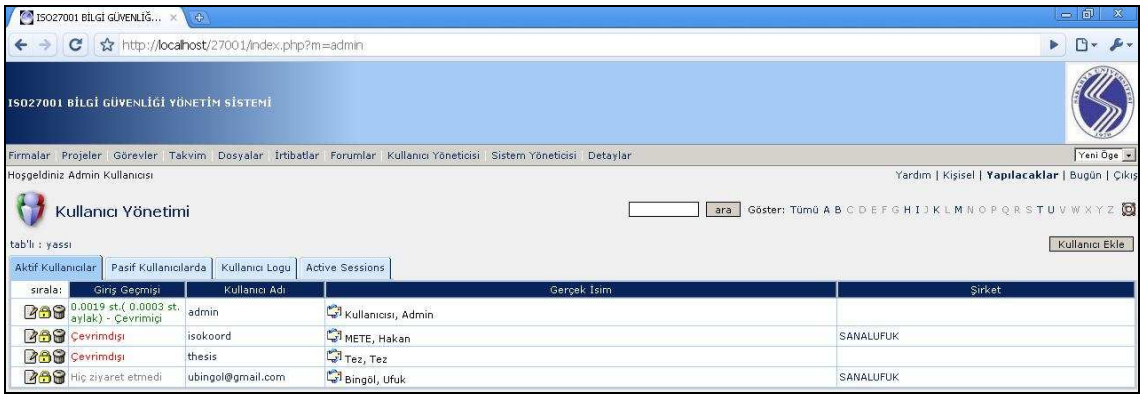
BGYS Süreç Yönetimi Sistemi daha önce bahsedildiği gibi bir Web tarayıcı yazılım vasıtasıyla kullanılabilmektedir. Web sunucusu üzerine kurulumu tamamlanmış yazılıma erişim kimlik doğrulama (User Authentication) vasıtasıyla yapılmaktadır. Bu maksatla yazılıma erişim sağlanmak istediğinde kullanıcının karşısına ilk olarak kimlik kontrolü sayfası çıkacaktır. Şekil-10'da kullanıcı kimlik kontrolü sayfası gösterilmiştir.

Şekil 10. ISO/IEC 27001 Süreç Yönetim Sistemi Erişim Kontrol Ekranı

Sistemin varsayılan olarak bir yönetici hesabı bulunmaktadır. Bu Kapsamda BGYS süreç yönetim sisteminin yöneticisi BGYS Komisyonunda bulunan tüm personele,

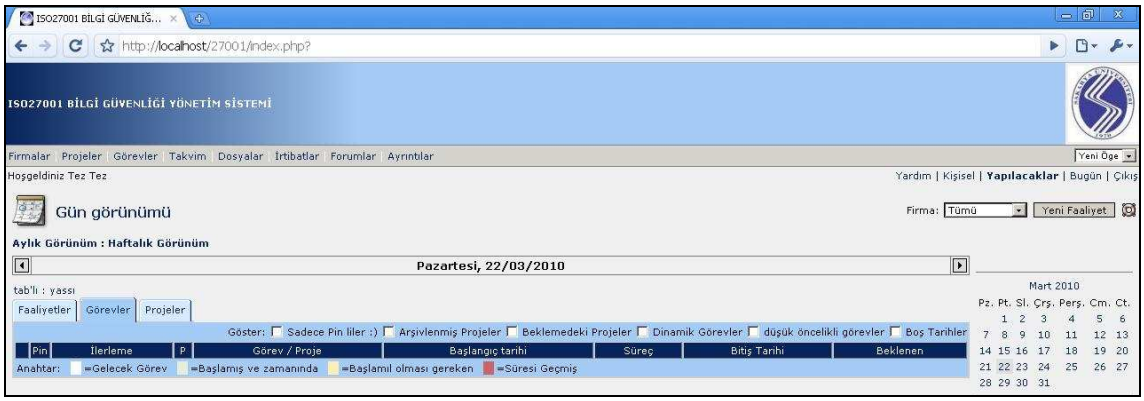
sistemin kullanıcı yöneticisi bölümünden birer kullanıcı hesabı açması suretiyle sisteme erişimlerini sağlamalıdır. Kullanıcılara hesap açma işlemlerine ait örnekler Şekil-11'de gösterilmiştir.

Şekil 11. ISO/IEC 27001 Süreç Yönetim Sistemi Kullanıcı Hesap Yönetimi



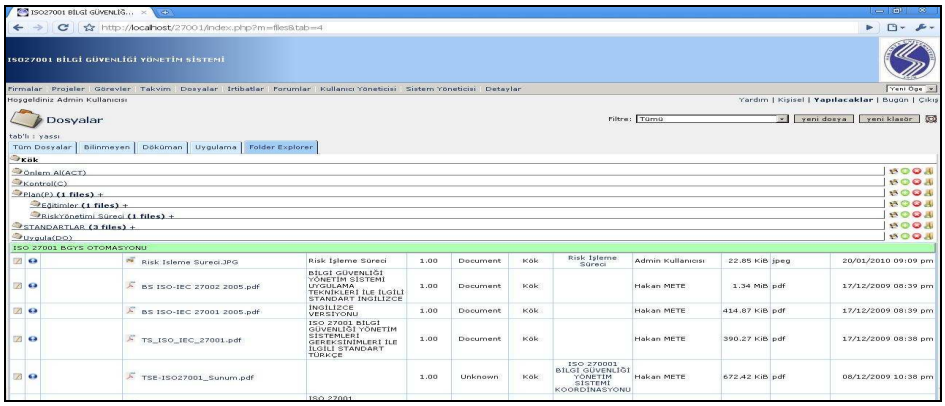
Sistem Yöneticisinin komisyon üyelerine açmış oldukları kullanıcı hesapları vasıtasıyla kullanıcılar sisteme giriş yapabileceklerdir. BGYS süreç yönetim sisteminin hedefi BGYS kurulum işletim ve idamesini sağlayan bir proje yönetimini sağlamaktır. Bu sebeplerden dolayı sistem tamamen proje odaklı bir mantıkla çalışmaktadır. BGYS'yi uygulayacak olan kurumların sürecin yöneticisi yani BGYS Komisyonu Başkanı ve ekibi tarafından oluşturulmuş olan bir proje yönetim takviminin bulunması gerekmektedir. Proje takviminin oluşturulmasından sonra Komisyon üyelerinin görevleri belirlenmelidir. BGYS süreç yönetim sisteminin proje ve görev odaklı çalışmasının mantığı, BGYS komisyonu tarafından komisyon üyelerine tanımlanmış sorumlulukların proje takvimine bağlı olarak ilerleme raporlarının süreç yöneticisine ve diğer komisyon üyelerine "Bilmesi gereken" prensibine göre sunulması imkânına dayanmaktadır. Yani BGYS Süreci yöneticisi görev atadığı kullanıcının görevini yalnızca bizzat kendisi veya kontrol görevi tanımladığı bir başka alt yöneticiye takip ettirebilecektir. Bu Kapsamda Sistem yöneticisinin tanımladığı kullanıcı vasıtasıyla sisteme giriş yapan kullanıcıların açılış sayfasında en başta atanan görevler ve tarihleri belirtilecektir. Örnek Kullanıcının sisteme giriş yapmasını müteakiben çıkacak olan açılış sayfası Şekil-12'de gösterilmiştir.

Şekil 12.ISO/IEC 27001 Süreç Yönetim Sistemi Varsayılan Kullanıcı Sayfası



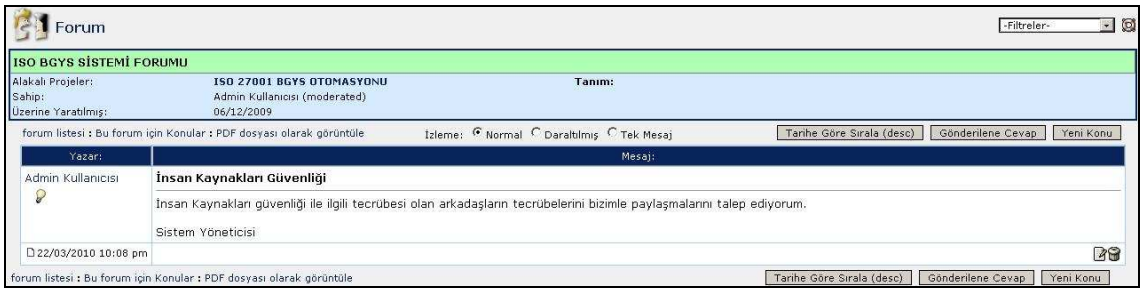
Kullanıcılara atanan görevler aynı zamanda kurumun varsa E-Posta sunucusu ile uyumlu çalışarak, atanan görevler ve yapılan geri beslemeler E-Posta vasıtasıyla gönderilebilmektedir. Kullanıcıya atanacak görevlerin nitelikleri, bağımlılıkları ve miadları da BGYS süreç yönetim sistemi üzerinden sağlanabilmektedir. BGYS Süreç Yönetimi sistemi kapsamında kurumun BGYS faaliyetlerinin yürütülmesi esnasında ihtiyaç duyulacak veya kurumun Belgelendirme sürecinde ihtiyacı olacak olan dosyaların yönetilmesi maksadıyla Dosya depolama bölümü bulunmaktadır. Bu bölümde Kullanıcılara kotalar verilmek suretiyle dosya transferi yapma imkânları sağlanmaktadır. Dosya depolama bölümüne ait örnek Şekil-13'de gösterilmiştir. Hazırlanmış olan dökümanların yeni sürümlerinin de sisteme yüklenebilme özelliği sayesinde belgeler üzerinde gözden geçirme ve karşılaştırma olanakları artırılmıştır. Dosyalama özelliği sayesinde BGYS faaliyetleri kapsamında oluşturulacak tüm dökümanların merkezi olarak tek bir noktadan yönetilmesi, bu sayede veri kaybı yaşanmaması ve konunun hassasiyeti sebebiyle güvenliği sağlanmış olacaktır.

Şekil 13. ISO/IEC 27001 Süreç Yönetim Sistemi Dökümantasyon Sistemi



BGYS süreç yönetim sisteminin bir diğer özelliği forum özelliğini de bünyesinde barındırmasıdır. BGYS sürecinde, herhangi bir bölümünde güncel veya eksik bilgilerin paylaşılması ve BGYS komisyonu içersinde eğitimi ve gelişmeyi tetikleyecek, bunun yanında BGYS süreçleri içerisinde bir konu hakkında eksik bilgisi olan bir komisyon üyesinin bilgilendirilmesinde tecrübelerini paylaşacak kullanıcılara hazırlanacak bir ortam meydana getirilmiş olacaktır. Oluşturulan bu forum veya alt forumlar sayesinde kullanıcılar daha önceki forum tartışmalarında yaptıkları aramalar sonucunda ihtiyaç duydukları herhangi bir konu hakkında bilgiye daha kısa süre içerisinde ulaşacaklardır. Forum sistemine ait örnek resim Şekil-14'de gösterilmiştir.

Şekil 14. ISO/IEC 27001 Süreç Yönetim Sistemi Forumu



Yazılımın çok kısıtlı olan bir risk yönetim eklentisi de bulunmaktadır. Fakat BGYS'nin risk yönetimi sürecinde kullanmak için oldukça yetersiz kalmaktadır. Fakat daha ufak çaplı proje yönetim faaliyetlerinde projelere dönük riskler kapsamında kullanılabilir.

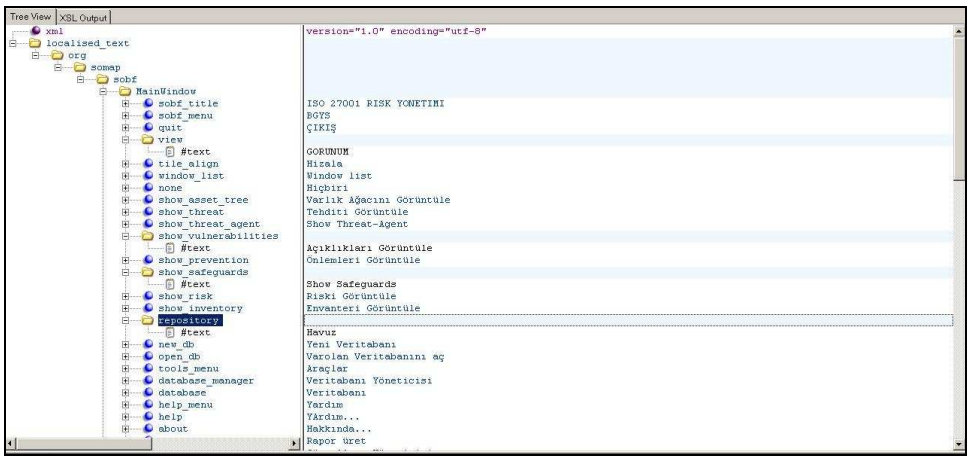
BGYS süreç yönetim sisteminin etkin kullanılabilmesi için öncelikle kullanıcıların konu hakkında detaylı olarak bilgilendirilmesi gerekmektedir. Sistemin verimli çalışması maksadıyla ISO/IEC 27001 Standardına göre BGYS'nin uygulanması sürecinde görev ve sorumlulukların net olarak belirlenmesi gerekmektedir. Bu Maksatla BGYS kurulumumun ilk maddesi olan BGYS komisyonunun oluşturulması gerekmektedir. Söz konusu Komisyonun belirlenmesi işleminden sonra BGYS sürecinin yöneticisi tarafından bir proje takvimi çıkarılmalıdır. Aynı zamanda Komisyon içerisindeki rollerin belirlenmesi gerekir. Daha sonra görev paylaşımının süreç liderinin nezaretinde yapılması gerekir. ISO/IEC 27001 Standardına göre belirlenen görevler, BGYS süreç yönetim sistemi vasıtasıyla Süreç lideri tarafından komisyon üyelerine atanmalıdır. Görevler sonucu yapılan geri beslemeler ve dosyalar ile en son aşamada belgelendirme faaliyeti ile sonuçlandırılır. BGYS süreç yönetim sisteminin sürekli işler vaziyette bulunması maksadıyla Komisyon üyelerinin değişimleri esnasında gizlilik kurallarına

uygun olarak ayrılan üyelerinin sistem üzerinde kullanıcı hesaplarını kapatılması gerekir. Bir diğer önemli husus ise yönetimin BGYS Süreç yönetim sisteminin izlemesi maksadıyla yönetim kademesine inceleme ve denetleme yetkisinin tanımlanmasıdır. Sonuç olarak Yönetim desteği ile birlikte BGYS süreci tamamlanacaktır. Bu maksatla Yönetimin girdilerini ve ve yorumlarını alabilmek için yöneticilere sisteme erişim yetkisi tanımlanmalıdır. Atanan sorumluluklar ve görevler bu sayede yönetim kademesi tarafından da takip edilebilecektir. Gerektiğinde yönetimin de değişme ve düzeltmeler yapma imkânı sağlanacaktır.

3.1.3.2. BGYS Risk Yönetimi Maksatlı Yazılımın Tanıtımı

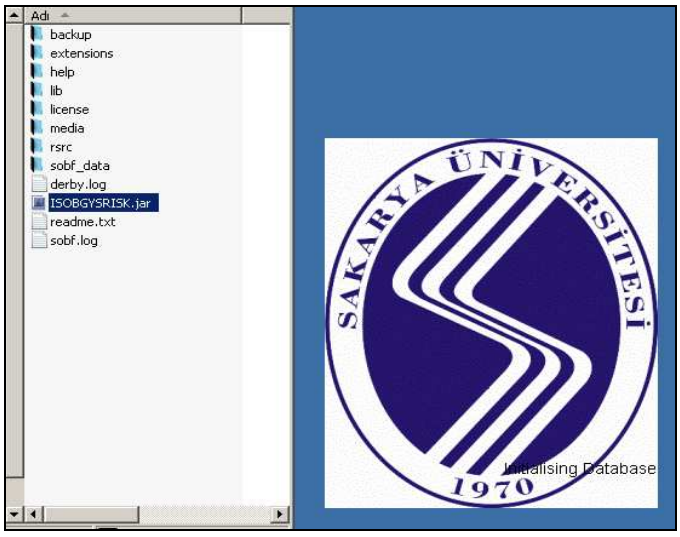
Kurumlar, BGYS sürecinin en önemli bölümlerinden biri olan risk yönetim sürecini birinci bölümde bahsedildiği üzere detaylı ve dikkatli bir şekilde sürdürmelidirler. Bu maksatla BGYS komisyonunun alt grubu olan risk yönetim çalışma grubu risk yönetimi sürecinde kesin ve detaylı bilgi sunarak bu sürece katkıda bulunabilecek sayısal yöntem ve hesaplamalara ihtiyaç duyabilirler. İşte risk yönetim çalışma grubunun risk yönetim sürecinde ihtiyaç duyduğu verileri tek bir kaynak vasıtasıyla elde edebileceği, yeni veri girişi yapabileceği ve bu verilere sonuç olarak değerlendirme raporları alabileceği bir yazılımın katkısı risk yönetim sürecinde çok faydalı olacaktır. Bu kapsamda yapılan araştırmalar neticesinde güvenlik ve merkezi olarak herhangi bir noktadan değil tek bir noktadan veri girişinin yapılabildiği ve risk yönetim süreci esnasında gerekli raporların alınabildiği bir yazılım gizlilik açısından da daha faydalı olacağı düşünülmektedir. Kurumun ihtiyaçlarına göre yeniden düzenlenmiş bir AKK risk yönetim yazılımın maliyet açısından da kuruma sağlayacağı katkı göz önünde bulundurulmalıdır. Bu sebeplerden JAVA tabanlı AKK bir risk yönetim yazılımı olan “Security Officer’s Best Friend” yazılımı temel olarak kullanılmıştır. Yazılım bu yüksek lisans tezi kapsamında Türkçeleştirilerek kullanıma hazır hale getirilmiştir. Bu işlem sırasında yapılan çalışmalara ait örnek resim Şekil-15‘de gösterilmiştir.

Şekil 15. Risk Yönetim Sistemi XML Kodu Düzenleme Örneği



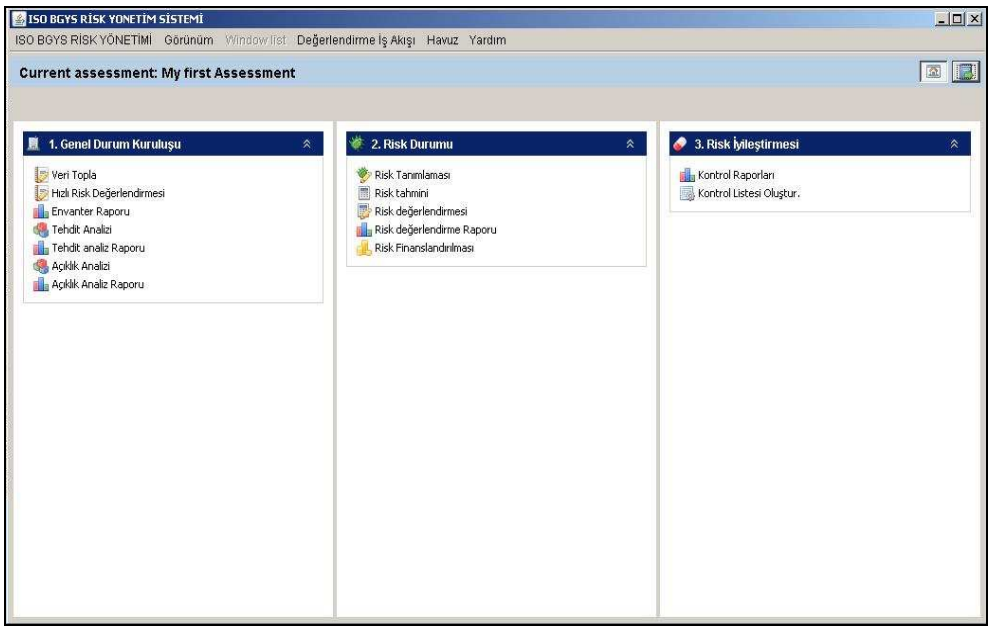
Yazılımın paket halinde indirme işlemi www.somap.org internet web sitesi üzerinden yapıldıktan sonra java uygulamasının platform bağımsız olmasından dolayı hemen hemen bütün işletim sistemleri üzerinde çalışabilmektedir. Yazılımın kullanımına başlamadan önce Risk Yönetim Yazılımının kullanılacağı bilgisayar üzerinde mutlaka http://java.com/tr/download/index.jsp internet adresinden indirilebilen java yazılımının kurulu olması gerekir. Verilen örneklerde sistem Windows XP Home Edition işletim sistemi üzerinde çalıştırılmıştır. Java yazılımının sisteme kurulu olduğu tesbit edildikten sonra BGYS Yazılımının kopyalandığı klasör içerisindeki ISOBGYSRISK.jar isimli dosyayı çift tıklamak yoluyla yazılım çalıştırılabilmektedir. Çalıştırılması ile ilgili örnek Şekil-16'de gösterilmiştir.

Şekil 16. Risk Yönetim Sisteminin Çalıştırılması



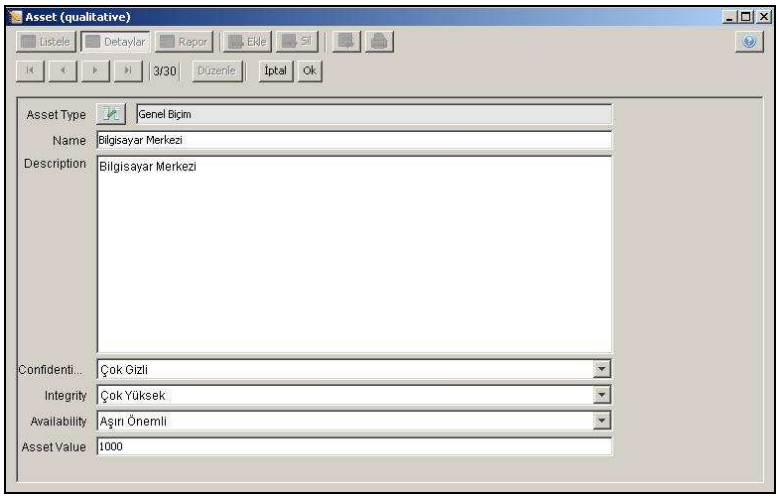
Yazılımın çalıştırılması işleminden sonra ise ekrana risk yönetim sistemi penceresi ve isteğe bağlı olarak yardım penceresi açılacaktır. Açılan pencere vasıtasıyla Risk yönetimi kapsamında kurumun uygulaması gereken adımlar sırasıyla kullanıcıya sunulmaktadır. Örnek Açılış penceresi Şekil-17'de gösterilmiştir.

Şekil 17. Risk Yönetim Sistemi Ana Penceresi



Risk Yönetim Sistemi kapsamında ilk adım olan BGYS kapsamındaki varlıkların belirlenmesi işlemi için "Veri topla" seçeneği vasıtasıyla BGYS varlık envanteri oluşturulacaktır. Varlıkların veritabanına kaydedilirken Gizlilik, Bütünlük ve Kullanılabilirlik niteliklerinin belirlenmesi önemlidir. Ayrıca BGYS komisyonunun ve Risk Yönetim Grubunun, yönetimin desteği ile belirleyeceği varlık değerlerinin de sisteme girişi sağlanmalıdır. Buna göre varlıkları tanımlarken gizlilik, bütünlük ve kullanılabilirlik standartlarının belirlenmiş olması gerekmektedir. Hâlihazırda yazılımda Niteliksel metod kapsamında Tasnif Dışı, Hizmete Özel, Gizli, Çok Gizli, Kozmik Gizli gizlilik dereceleri, Çok Yüksek, Yüksek, Orta, Düşük, Çok Düşük bütünlük dereceleri ve Aşırı Önemli, Çok Önemli, Önemli, Önemli Değil, Hiç Önemli Değil kalıplarında kullanılabilirlik dereceleri belirlenmiştir. Kurumun standartlaştırma düzenlemesine göre değiştirilme imkânı bulunmaktadır. Varlık envanteri girişi yapılırken bu değerlerin belirlenmesi aşamasına ait örnek Şekil-18'de gösterilmiştir.

Şekil 18. Risk Yönetim Sistemi Varlık Envanteri Veri Girişi

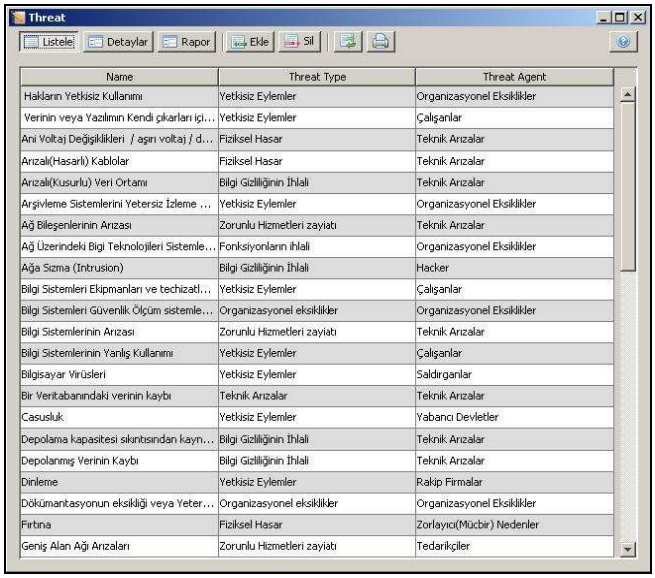


Varlık envanterinin, veritabanına girilmesinden hemen sonrasında envanter raporunun oluşturulması gerekir. Raporun Çeşitli formatlarda çıktı alınabilecek şekilde olması ise daha sonradan düzenleme açısından Risk Yönetim Grubuna kolaylık sağlayacaktır. Alınan Envanter Raporu BGYS Süreç Yönetiminde Belgelendirme alt süreci kapsamında ilgili Dosya Veritabanına kopyalanmalıdır. Örnek olarak Alınan bir raporun görünüşü Şekil-19'da sunulmuştur.

Şekil 19. RYS Varlık Envanter Raporu

Kurum varlık envanterinin oluşturulmasından sonra sözkonusu varlıklar için olası tehditlerin seçilerek sisteme girilmesi gerekmektedir. BGYS varlıklarının maruz kaldığı tehditler değişen ve gelişen durumlara göre yeniden gözden geçirilmelidir. Bu kapsamda örnek Tehdit verileri Şekil-20'de gösterilmiştir.

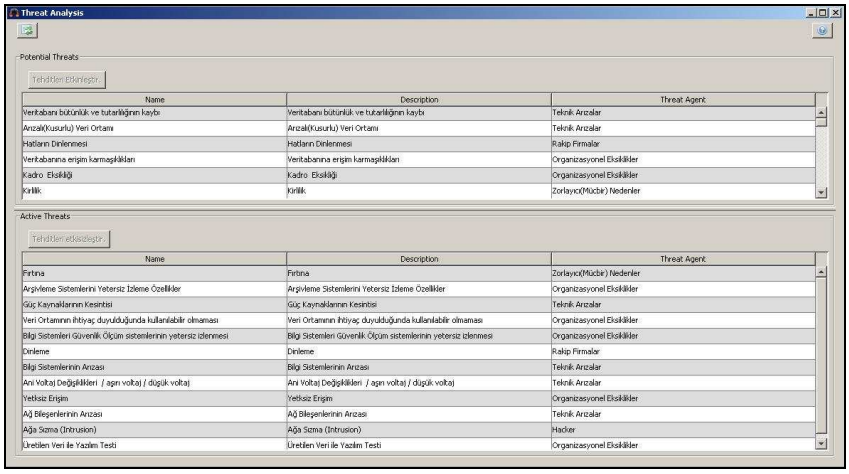
Şekil 20. Örnek Tehdit verileri



Name	Threat Type	Threat Agent
Hakların Yetkisiz Kullanımı	Yetkisiz Eylemler	Organizasyonel Eksiklikler
Verinin veya Yazılımın Kendi çıkarları içi...	Yetkisiz Eylemler	Çalışanlar
Ani Voltaj Değişiklikleri / aşırı voltaj / d...	Fiziksel Hasar	Teknik Arızalar
Arızalı(Hasarlı) Kablolar	Fiziksel Hasar	Teknik Arızalar
Arızalı(Kusurlu) Veri Ortamı	Bilgi Gizliliğinin İhlali	Teknik Arızalar
Arşivleme Sistemlerini Yetersiz İzleme ...	Yetkisiz Eylemler	Organizasyonel Eksiklikler
Ağ Bileşenlerinin Arızası	Zorunlu Hizmetleri zayiatı	Teknik Arızalar
Ağ Üzerindeki Bigi Teknolojileri Sistemle...	Fonksiyonların ihlali	Organizasyonel Eksiklikler
Ağa Sızma (Intrusion)	Bilgi Gizliliğinin İhlali	Hacker
Bilgi Sistemleri Ekipmanları ve techizatl...	Yetkisiz Eylemler	Çalışanlar
Bilgi Sistemleri Güvenlik Ölçüm sistemle...	Organizasyonel eksiklikler	Organizasyonel Eksiklikler
Bilgi Sistemlerinin Arızası	Zorunlu Hizmetleri zayiatı	Teknik Arızalar
Bilgi Sistemlerinin Yanlış Kullanımı	Yetkisiz Eylemler	Çalışanlar
Bilgisayar Virüsleri	Yetkisiz Eylemler	Saldırganlar
Bir Veritabanındaki verinin kaybı	Teknik Arızalar	Teknik Arızalar
Casusluk	Yetkisiz Eylemler	Yabancı Devletler
Depolama kapasitesi sınırlısından kayn...	Bilgi Gizliliğinin İhlali	Teknik Arızalar
Depolanmış Verinin Kaybı	Bilgi Gizliliğinin İhlali	Teknik Arızalar
Dinleme	Yetkisiz Eylemler	Rakip Firmalar
Dökümantasyonun eksikliği veya Yeter...	Organizasyonel eksiklikler	Organizasyonel Eksiklikler
Fırtına	Fiziksel Hasar	Zorlayıcı(Mücbir) Nedenler
Geniş Alan Ağı Arızaları	Zorunlu Hizmetleri zayiatı	Tedarikçiler

Kurum için tehditlerin belirlenmesi aşamasından sonra Ana pencerede bulunan "Tehdit Analizi" bölümünde olası tehditlerin etkinleştirilmesi ve detaylı raporlandırılması işlemi bulunmaktadır. Kurum tehdit havuzundan kendi varlık envanterine etki edebilecek tehditleri belirlemelidir. Bu kapsamda örnek tehdit seçimi Şekil-21'de gösterilmiştir.

Şekil 21. Uygun Tehditlerin Seçimi



Name	Description	Threat Agent
Veritabanı bütünlük ve tutarlığının kaybı	Veritabanı bütünlük ve tutarlığının kaybı	Teknik Arızalar
Arızalı(Kusurlu) Veri Ortamı	Arızalı(Kusurlu) Veri Ortamı	Teknik Arızalar
Hatların Dinlenmesi	Hatların Dinlenmesi	Rakip Firmalar
Veritabanına erişim karmaşıklıkları	Veritabanına erişim karmaşıklıkları	Organizasyonel Eksiklikler
Kadro Eksikliği	Kadro Eksikliği	Organizasyonel Eksiklikler
Kirlilik	Kirlilik	Zorlayıcı(Mücbir) Nedenler

Name	Description	Threat Agent
Fırtına	Fırtına	Zorlayıcı(Mücbir) Nedenler
Arşivleme Sistemlerini Yetersiz İzleme Özellikler	Arşivleme Sistemlerini Yetersiz İzleme Özellikler	Organizasyonel Eksiklikler
Güç Kaynaklarının Kesintisi	Güç Kaynaklarının Kesintisi	Teknik Arızalar
Veri Ortamının ihtiyaç duyulduğunda kullanılabilir olmaması	Veri Ortamının ihtiyaç duyulduğunda kullanılabilir olmaması	Organizasyonel Eksiklikler
Bilgi Sistemleri Güvenlik Ölçüm sistemlerinin yetersiz izlenmesi	Bilgi Sistemleri Güvenlik Ölçüm sistemlerinin yetersiz izlenmesi	Organizasyonel Eksiklikler
Dinleme	Dinleme	Rakip Firmalar
Bilgi Sistemlerinin Arızası	Bilgi Sistemlerinin Arızası	Teknik Arızalar
Ani Voltaj Değişiklikleri / aşırı voltaj / düşük voltaj	Ani Voltaj Değişiklikleri / aşırı voltaj / düşük voltaj	Teknik Arızalar
Yetkisiz Erişim	Yetkisiz Erişim	Organizasyonel Eksiklikler
Ağ Bileşenlerinin Arızası	Ağ Bileşenlerinin Arızası	Teknik Arızalar
Ağa Sızma (Intrusion)	Ağa Sızma (Intrusion)	Hacker
Üretilen Veri ile Yazılım Testi	Üretilen Veri ile Yazılım Testi	Organizasyonel Eksiklikler

Kurumun BGYS varlıklarının tehditleri için belirlenen tehdit analiz raporu ana penceredeki "Tehdit Analiz Raporu" başlığından istenilen formatta alınabilmektedir. Örnek rapor Şekil-22'de gösterilmiştir.

Şekil 22. Tehdit Analiz Raporu Örneği

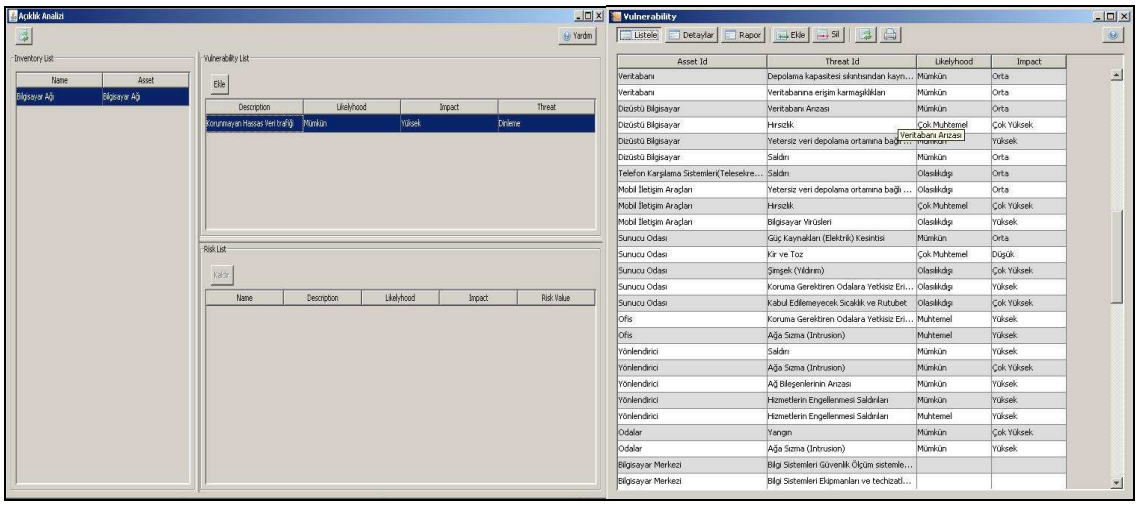
Tehdit Analiz Raporu

Tehdit Adı	Tehdit Biçimi	Tehdit Kaynağı
Fırtına	Fiziksel Hasar	Zorlayıcı(Mücbir) Nedenler
Arşivleme Sistemlerini Yetersiz İzleme Özellikler	Yetkisiz Eylemler	Organizasyonel Eksiklikler
Güç Kaynaklarının Kesintisi	Zorunlu Hizmetleri zayiatı	Teknik Arızalar
Veri Ortamının ihtiyaç duyulduğunda kullanılabilir olmaması	Fonksiyonların İhlali	Organizasyonel Eksiklikler
Bilgi Sistemleri Güvenlik Ölçüm sistemlerinin yetersiz izlenmesi	Organizasyonel eksiklikler	Organizasyonel Eksiklikler
Dinleme	Yetkisiz Eylemler	Rakip Firmalar
Bilgi Sistemlerinin Arızası	Zorunlu Hizmetleri zayiatı	Teknik Arızalar
Ani Voltaj Değişiklikleri / aşırı voltaj / düşük voltaj	Fiziksel Hasar	Teknik Arızalar
Yetkisiz Erişim	Bilgi Gizliliğinin İhlali	Organizasyonel Eksiklikler
Ağ Bileşenlerinin Arızası	Zorunlu Hizmetleri zayiatı	Teknik Arızalar
Ağa Sızma (Intrusion)	Bilgi Gizliliğinin İhlali	Hacker
Üretilen Veri ile Yazılım Testi	Organizasyonel eksiklikler	Organizasyonel Eksiklikler

1 / # BGYS RISK YS 26.03.2010 20: ISO BGYS RISK YONETIM SISTEMI DOKUMAN NO: ###

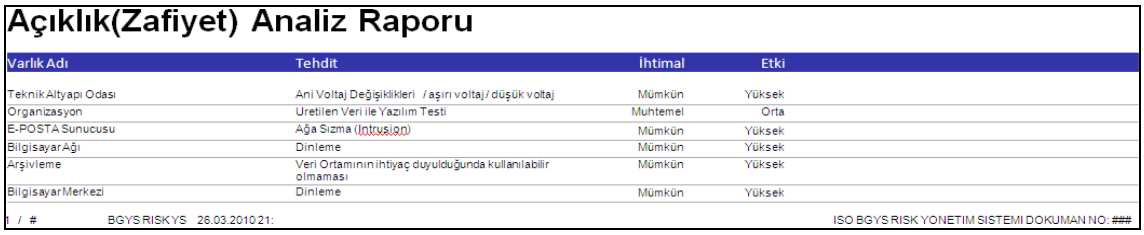
Varlıklara etki edebilecek tehditlerin belirlenmesi aşamasından sonra Varlıkların sözkonusu tehditlerin kullanabileceği açıklarının tespit edilmesi işlemi yapılmalıdır. Bu aşamada BGYS Risk Yönetim sistemi havuzuna kurumun varlık envanterine etki edebilecek tehditlerin kullanacağı varlık açıklarının girişi yapılmalıdır. Tehditlerin belirlenen açıkları kullanıp tehditlerin gerçekleşme ihtimalleri ve gerçekleşme sonucunda meydana gelecek etkisi de sistemde belirtilmelidir. Risk Yönetimi Veritabanına girişi yapılan, kurumların varlıklarının tehditler karşısında olası açıkları örnekleri Şekil-15'de gösterilmiştir.

Şekil 23. Açık Analizi Örneği



Açıkların tesbit edilmesi işleminden sonra Ana pencerede bulunan "Açık Analizi Raporu" başlığından istenilen ve düzeltilebilen biçimde açık analiz raporu alınabilmektedir. Örnek rapor Şekil-24'de gösterilmiştir. Belirtilen raporda Tehdit sahibi olan varlık, tehdit açıklaması, açık sonucu tehditin meydana gelme ihtimali ve bu riskin olası etkileri sunulmaktadır.

Şekil 24. Açık Analizi Raporu Örneği



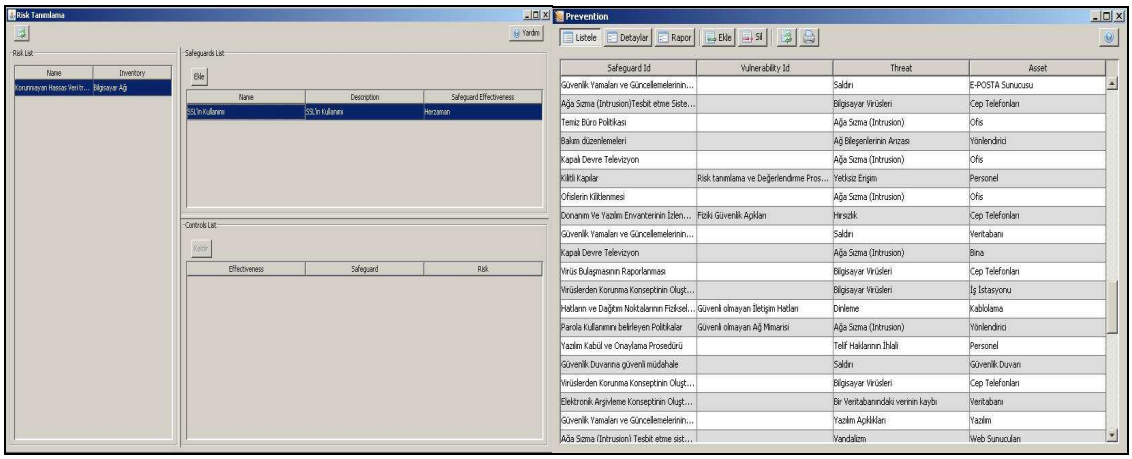
Açıklık(Zafiyet) Analiz Raporu

Varlık Adı	Tehdit	İhtimal	Etki
Teknik Altyapı Odası	Ani Voltaj Değişiklikleri / aşırı voltaj / düşük voltaj	Mümkün	Yüksek
Organizasyon	Üretilen Veri ile Yazılım Testi	Muhtemel	Orta
E-POSTA Sunucusu	Ağa Sızma (Intrusion)	Mümkün	Yüksek
Bilgisayar Ağı	Dinleme	Mümkün	Yüksek
Arşivleme	Veri Ortamının ihtiyaç duyulduğunda kullanılabilir olmaması	Mümkün	Yüksek
Bilgisayar Merkezi	Dinleme	Mümkün	Yüksek

1 / # BGYS RISK YS 26.03.2010 21: ISO BGYS RISK YONETIM SISTEMI DOKUMAN NO: ###

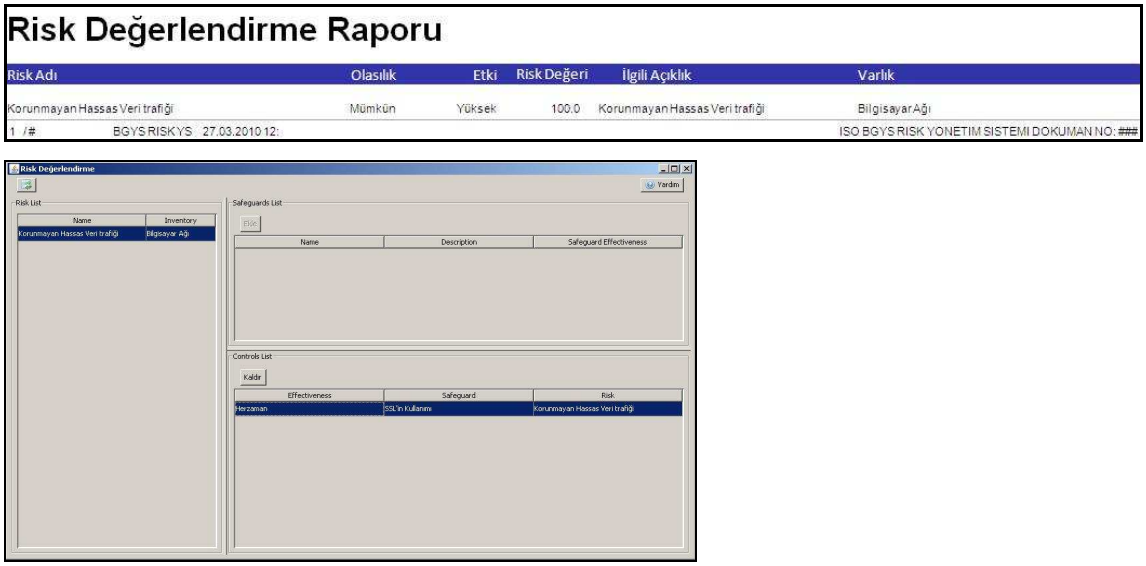
Açık analizi sonucu elde edilen veriler risk tanımlanması ve gerekli kontrollerin uygulanması aşamalarına girdi olacaktır. Bu maksatla açıklıklar sonucu Şekil-25'de örnek olarak risk listesine eklene risklerin tanımlanması işlemi gerçekleştirilecektir. Ana Pencerede "Risk Tanımlaması" seçeneği vasıtasıyla tanımlanan risklere karşı yazılımın havuzunda bulunan veya eklenecek önleme ve kontroller seçilecektir. Örnek çalışma Şekil-25'de gösterilmiştir.

Şekil 25. Risk Tanımlaması ve Uygun Kontrollerin Seçimi Aşaması



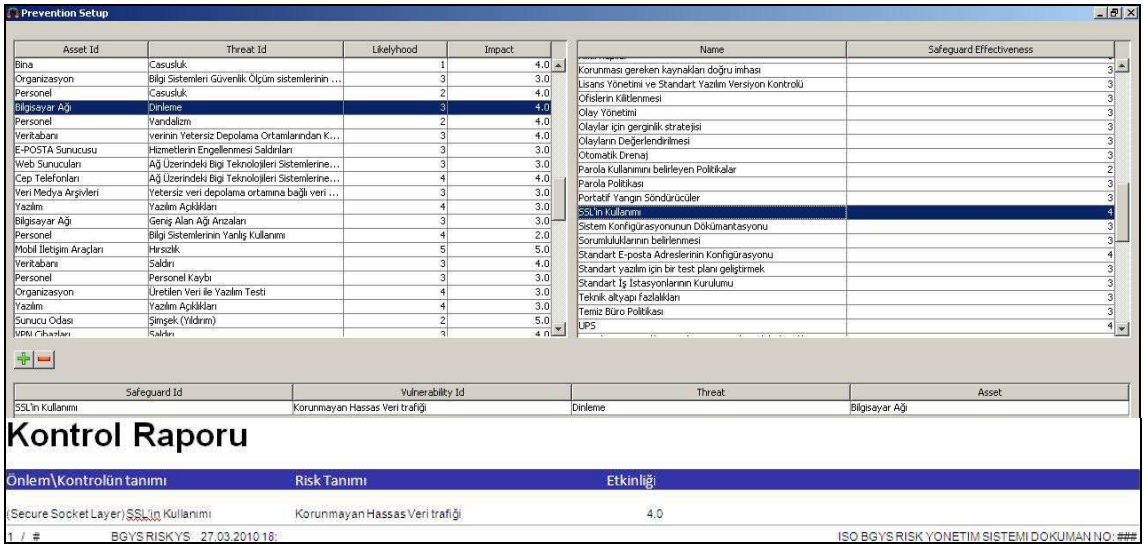
Risklerin belirlenmesi işleminin devamında tanımlanan risklerin derecelendirilmesi işlemi yazılım tarafından otomatik olarak yapılmaktadır. Bu kapsamda riskler, risk değeri yüksek olandan düşük olana kadar sıralandırılarak tehdidin kullandığı açıklık ve riskin meydana gelme ihtimali ve olası etkileri belirlenmektedir. BGYS Risk Yönetim sisteminin ana penceresinde bulunan "Risk Değerlendirme" ve "Risk Değerlendirme Raporu" seçeneklerinden bu verilere erişilebilmektedir. Örnek veriler Şekil-26'da gösterilmiştir.

Şekil 26. Risk Değerlendirme Raporu Örneği



Risk değerlendirme işleminin tamamlanmasından sonra uygun kontrollerin seçilerek uygulanması işlemi gerçekleştirilmelidir. BGYS Risk Yönetim Sistemi yazılımında belirlenmiş olan risklere karşı alınacak önlemler için uygulanacak kontrollerin belirlenmesi ve bu kontrollerin etkinlikleri belirlenmelidir. Veritabanına alınmış olan varlıklara yönelik tehditlere karşı kullanılacak kontrollerin seçimi "Engelleme Ayarları" bölümünden yapılmaktadır. Sözkonusu örnek Şekil-27'de gösterilmiştir. Ayrıca Yazılımın ana penceresindeki "Kontrol Raporları" bölümü seçilerek alınabilmektedir. Kontrol raporları içeriğinde meydana gelen riskin tanımı, uygun önlem veya kontrolün tanımı ve kontrolün etkinliği bulunmaktadır.

Şekil 27. Engelleme Ayarları ve Kontrol Raporu Örneği



BGYS Komisyonu; varlıkları tehdit eden riskleri önceliklendirerek uygun kontrolleri ve kontrollerin etkinlikleri sonucunda geriye kalacak olan artık riskler için yönetimin onayını almak durumundadır. Bu sebepten dolayı BGYS Risk yönetimi sistemi kapsamında yazılımdan alınan veriler BGYS süreç yönetim sisteminde Risk yönetimi başlığı altında mutlaka sunulmalıdır. Aynı verilerin çıktısı olan raporlar BGYS süreç yönetim sisteminde "Dökümanlar" başlığı altında mutlaka tüm BGYS komisyonu ve Yönetim ile paylaşılmalıdır. Bu nedenle elde edilen verilerin raporlanması işlemi önemlidir. Risk Yönetim sisteminin girdileri ile birlikte seçilen kontroller neticesinde kurumlar kendi uygulanabilirlik bildirgesini hazırlamaktadırlar. BGYS varlıklarına yönelik olan muhtemel risklerin yönetiminde ve kurumlara karar aşamasında yardımcı olacak olan bu yazılım veritabanının, sürekli değişen ve gelişen bilgi teknolojileri kapsamında kuruma dâhil edilecek yeni varlıklarının da risk yönetim sürecine dâhil edilmesi ile birlikte güncellenmesi gerekmektedir. Bunun yanında kurumun iş hedefleri, iş gerçekleştirme yöntemleri veya BGYS kapsamında önem verilen konular değişebilir. Bu değişiklikler nedeniyle varlık değerleri, tehditleri ve açıklıkları da değişime uğrayabilir. Bu sebepten ötürü bir döngü sistemi olan Risk yönetim sistemi sürecinde kullanılacak olan BGYS Risk yönetim sistemi yazılımının verilerinin de güncel tutulması önemlidir. Ayrıca Bilgi Güvenliği kapsamında yazılımın ve veri tabanının düzenli aralıklarla yedeklenmesi tavsiye edilmektedir. Yazılım hali hazırda tamamen geliştirilmeye açık bir yazılım olması sebebiyle uluslararası platformda çeşitli düzenlemeler ve güncellemeler yapılmaktadır. Yazılımın aynı zamanda web tabanlı olarak kullanılması çalışmaları devam etmektedir.

BÖLÜM 4: ÖRNEK UYGULAMA SÜRECİNİN TANITIMI

4.1. Giriş ve Açıklama

Üçüncü bölümde anlatılan BGYS otomasyon süreci kapsamında uygulanacak yöntemler örnek aşamaları ile birlikte bu bölümde anlatılacaktır. Bu kapsamda bir bilişim teknolojileri firmasında uygulanacak BGYS süreci işlenecektir. Örnek uygulama içerisinde işlenen tüm veriler tez kapsamında Yoğun Disk (CD) içerisinde toplanmıştır. Ayrıca Sistemin kurulum ve örnek dosyaları da söz konusu yoğun disk ortamında bulunacaktır. Örnek uygulama süreci içerisinde kullanılan verilerin tamamı hayal ürünüdür. BGYS'nin uygulanacağı Sanalufuk Bilişim Teknolojileri A.Ş. tamamen sanal ve bu yüksek lisans tezi kapsamında senaryo gereği örnek olarak oluşturulmuş gerçek olmayan bir firmadır. Firmanın faaliyet alanı temel olarak internet teknolojileri geliştirme, yapay zekâ tasarımı, karar destek yazılımları geliştirme ve bilgi sistemleri geliştirme sahalarıdır. Aynı zamanda kurum servis sağlayıcı hizmetleri de sunmaktadır. Kurumun personel sayısı genel olarak Teknik personel olmakla birlikte yaklaşık 200 kişidir. Senaryoya göre kurumun kadro yapısı en başta temel faaliyet alanı olan Bilgi Teknolojilerinden sorumlu Yazılım Geliştirme ve Veritabanı Yönetim Birimi, Bilgisayar Olaylarına müdahale birimi, Sistem Yönetim Birimi, Ağ Yönetim birimi, Bilgi sistemleri Bakım ve Onarım Birimi olmak üzere beş alt birimden oluşan Bilgi İşlem Şube Müdürlüğü olmak üzere Satış ve Pazarlama Müdürlüğü, İnsan Kaynakları Yönetimi Müdürlüğü, Muhasebe ve Finans Müdürlüklerinden teşkil edilmiştir. Sanalufuk Bilişim Teknolojileri A.Ş. için bu kapsamda hazırlanan örnek uygulama ile ilgili tüm verilerin kullanım sorumluluğu bu verileri kullanacak üçüncü kişilerin sorumluluğundadır. Firmaya ISO/IEC 27001 kapsamında uygulanan süreçler, prosedürler ve politikalar tamamen sanaldır. Oluşturulan bütün veriler örnek senaryo gereği üretilmiştir. Bu senaryo haricinde uygulanmamıştır. Sanalufuk Bilişim Teknolojileri A.Ş. senaryo kapsamında BGYS süreçlerinin tamamını Otomasyon kapsamında Süreç yönetim sistemi ve Risk Yönetim sistemi vasıtasıyla yönetmektedir. Ayrıca kurum içerisindeki cep telefonu, telefon, E-Posta gibi haberleşme sistemleri de yardımcı vasıtalar olarak kullanılmaktadır. Kurum BGYS kapsamında aynı zamanda rutin toplantılarını icra etmektedir. BGYS süreci tamamen bu sistem üzerinden çalışmaktadır.

4.2. BGYS Kurulum ve Gerçekleştirme Sürecinin Tanıtımı

4.2.1. Firma Tarafından BGYS Oluşturulmasına Karar Verilmesi Aşaması

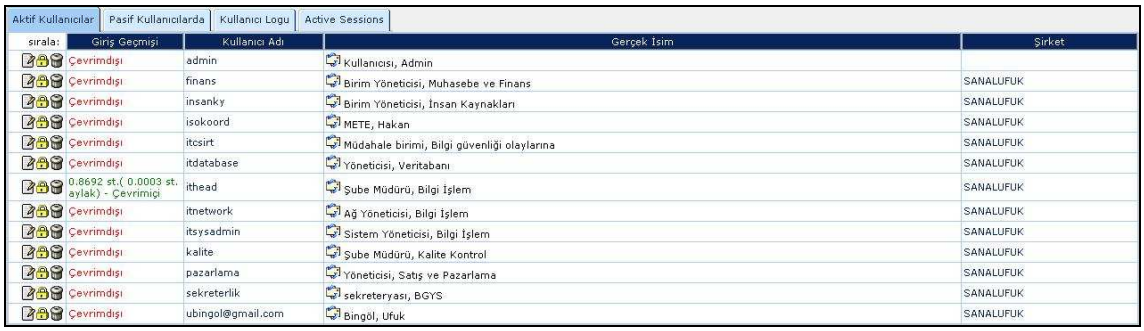
BGYS süreci 3 Eylül 2009 tarihinde yapılan Sanalufuk Bilişim Teknolojileri A.ş. yönetim kurulu toplantısında alınan karar neticesinde kurum olarak ISO/IEC 27001 standardının gerekliliklerini yerine getirerek kurum için Bilgi Güvenliği Yönetim Sistemi oluşturulmasına karar verilmesi ile başlatılmıştır. Bu kapsamda Yönetim Kurulu üyelerinden seçilen bir üye ISO/IEC 27001 BGYS süreci faaliyetlerinden sorumlu yönetim kurulu üyesi olarak seçilmiştir. Söz konusu üye kurumun BGYS koordinatörü olmuştur. Bu kapsamda BGYS koordinatöründen konu ile ilgili detaylı bir çalışma hazırlanıp yönetim kuruluna sunulması istenmiştir. Aynı toplantıya kurumun Bilgi İşlem Şube Müdürü de danışman olarak iştirak etmiş ve çalışmaların fiili olarak 7 Eylül 2009 tarihinde başlatılmasına karar verilmiştir.

4.2.2. BGYS Sürecinin Kurulması Aşaması

4.2.2.1. BGYS Süreç Takviminin, Görev Ve Sorumluluklarının Oluşturulması

BGYS koordinatörü ve Bilgi İşlem Şube Müdürünün beraber yürüteceği faaliyet kapsamında Bilgi İşlem Şube Müdürü BGYS süreci için ilgili standartlara ve konu ile ilgili teamüllere uygun bir faaliyet takvimi çıkarmıştır. Bu faaliyet takvimine göre BGYS sürecinin yönetilmesine karar verilmiştir. BGYS koordinasyon ekibi için tüm müdürlüklerden bir komisyon üyesi talep edilmiştir. Bilgi İşlem Müdürlüğünün alt birimlerinden birer personelin katılımıyla BGYS koordinasyon ekibi oluşturulmuştur. Bilgi İşlem Müdürü sekreteri, BGYS komisyonu sekreteryası görevini icra edecektir. Süreç Yönetim sisteminde görev ve sorumlulukların tanımlanması maksadıyla Sistem yöneticisine komisyon üyeleri için Şekil-28'de belirtilen şekilde kullanıcı hesaplarının açılması talep edilmiştir. Açılan Kullanıcı hesapları katılımı sağlayan ilgili müdürlüklerin kullanıcı hesabı şeklinde açılmıştır.

Şekil 28. Kullanıcı Hesaplarının Oluşturulması

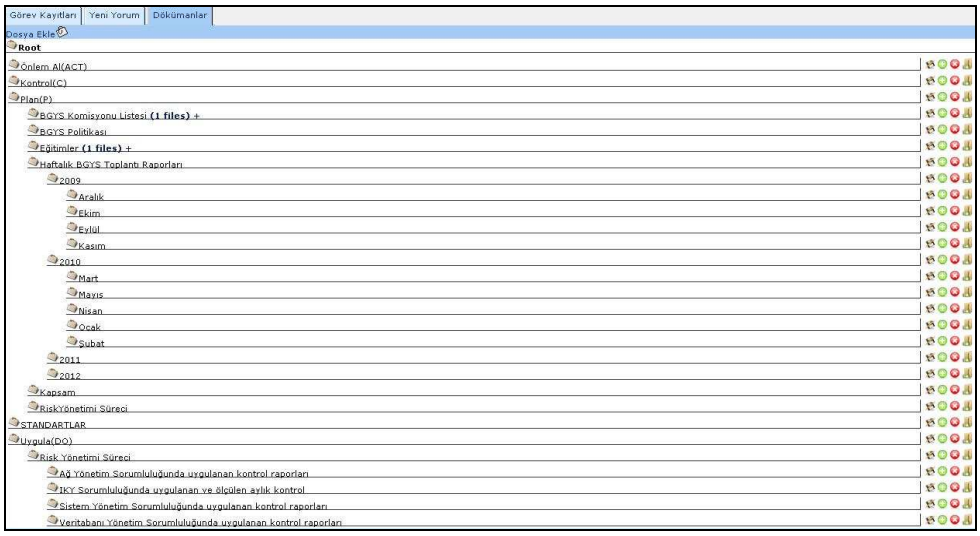


Belirlenen süreç takvimi ve ilgili görevler BGYS süreç Yönetim sistemine aktarılmıştır. Ayrıca Görevlerin sorumlulukları başlangıç ve bitiş tarihleri ile görev tanımları sistemde detaylı olarak belirtilmiştir. Süreç yönetimi sisteminde BGYS koordinatörü yönetim kurulu üyesi asli görevleri uhdesinde kalmak üzere operatif yöneticilik yetkilerini Bilgi İşlem Şube Müdürüne devretmiştir. Senaryoya göre kararlaştırılmış haftalık BGYS ilerleme toplantılarında koordinatör yönetim kurulu üyesine sunum yapılacaktır. Ayrıca kendisine açılan “isokoord” kullanıcı hesabı ile dilediği zamanlarda sisteme giriş yaparak süreci denetleyecek, yorumlarını ve direktiflerini belirtebilecektir. Belirlenen ve sorumlulukları atanan görevlerin sorumluları süreç yönetim sistemine giriş yaptıklarında kendilerine atanan görevleri takip edebilecektir. Tüm görevleri ve bunların alt görevlerin izleme ve yönetim yetkisi sadece sekreteryada, Bilgi İşlem Müdüründe ve ISOKOORD kullanıcısında bulunmaktadır. Atanan Görev ve sorumluluklar BGYS komisyonu üyelerine E-POSTA olarak kendilerine tebliğ edilmektedir. Belirlenmiş BGYS kurulum ve gerçekleştirme aşamaları görevle vesorumlukları Şekil-29’da gösterilmiştir. Aynı ekrandan detaylı gantt grafiğini de temin etmek mümkündür.

Şekil 29. Görev ve Sorumluluklar Ekranı

BGYS komisyonu, BGYS sürecinin en başından itibaren BGYS kapsamında oluşturulacak zorunlu ve isteğe bağlı dökümanları sürüm şeklinde düzenleyecek dökümantasyon sistemini benimsemiştir. Bu maksatla süreç yönetim sisteminin dökümantasyon kısmının kullanılması kararlaştırılmıştır. Dökümantasyon kısmında PUKÖ modeline uygun olarak dosya ve klasör hiyerarşisi oluşturulmuştur. BGYS süreci boyunca hazırlanan veya yeniden gözden geçirilip düzeltilen tüm dökümanlar dökümantasyon kısmında depolanmaktadır. Oluşturulan dökümanlar yönetim kurulu adına BGYS koordinatörü tarafından incelenip onaylandıktan sonra sekreterya tarafından ilgili göreve atıfta bulunmak suretiyle Dökümantasyon bölümünde yayımlanmaktadır. Dökümantasyona ilişkin örnek Şekil-30'da gösterilmiştir.

Şekil 30. Dökümantasyon Sistemi



4.2.2.2. BGYS Kapsamında İcra Edilecek Faaliyetlerin Uygulanması

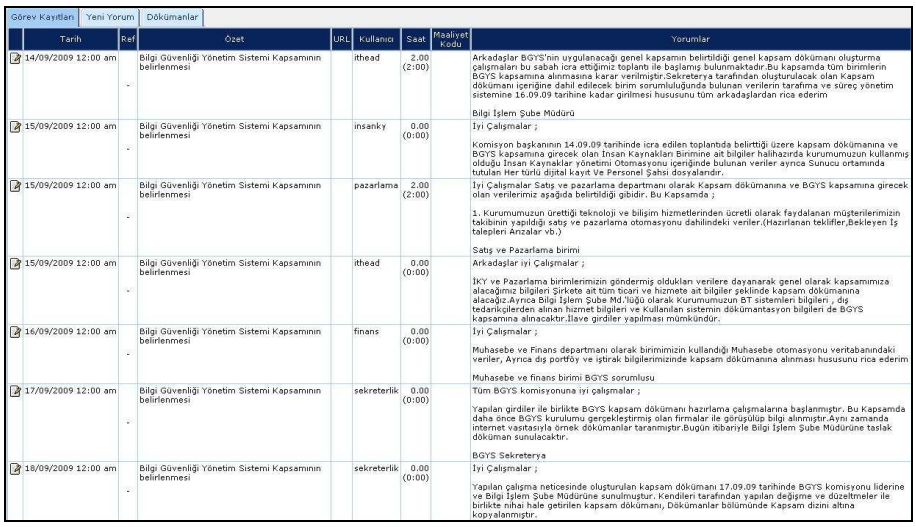
4.2.2.2.1. BGYS Kapsamının Ve Politikalarının Belirlenmesi

BGYS Süreç yönetim sisteminde görevler kapsamında BGYS komisyonunun oluşturulması işleminden sonraki adım, BGYS kapsamının belirlenmesi görevidir. Söz konusu görevin icrasına yönelik faaliyetlerde komisyonun tamamı görev alacaktır. BGYS kapsam dökümanı hazırlama çalışmaları kapsamında kurumun tamamının tüm alt organizasyonlarla birlikte BGYS kapsamına alınmasına 14.09.09 tarihinde icra edilen toplantı sonucunda karar verilmiştir. Bu kapsamda BGYS koordinatörü tarafından diğer birim üyelerinden kendi birimlerine yönelik kapsam dökümanına alınacak materyallerin süreç yönetim vasıtasıyla sekreteryaya gönderilmesini talep etmiştir. Diğer Birimlerden gelen girdiler sonucu TÜBİTAK-UEKAE Eğitim dökümanları örnek alınarak BGYS kapsam dökümanı hazırlanarak 17.09.09 tarihinde hazırlanarak yönetime sunulduktan sonra sistemde yayınlanmıştır. Süreç faaliyet kayıtları ve doküman yayını Şekil-31 ve Şekil-32'te gösterilmiştir. Kapsam dökümanı yayınlandıktan sonra tüm personele E-Posta ile bildirilmiştir.

Şekil 31. Dökümantasyon Yayını

Döküman Adı	Tanım	Sürümler	Category	Görev Adı	Sahip	Boyut	Tip
Kapsam Dokümanı.pdf		1.00	Unknown	Bilgi Güvenliği Yönetim Sistemi Kapsamının belirlenmesi	BGYS sekreteryası	229.53 KiB	application/pdf

Şekil 32. Kapsam Dökümanı Hazırlık Çalışmaları Görev Kayıtları



Görev Kayıtları | Yeni Yorum | Dökümanlar

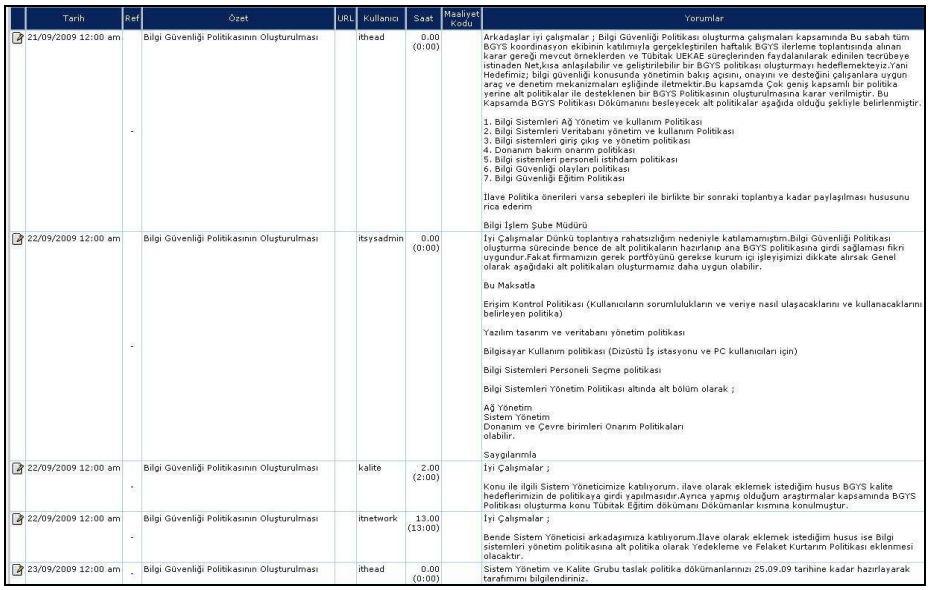
	Tarih	Ref	Özet	URL	Kullanıcı	Saat	Maaliyet Kodu	Yorumlar
	14/09/2009 12:00 am	-	Bilgi Güvenliği Yönetim Sistemi Kapsamının belirlenmesi		ithead	2.00 (2:00)		Arkadaşlar BGYS'nin uygulanacağı genel kapsamın belirtildiği genel kapsam dökümanı oluşturma çalışmaları bu sabah icra ettiğimiz toplantı ile başlamış bulunmaktadır.Bu kapsamda tüm birimlerin BGYS kapsamına alınmasına karar verilmiştir.Sekreterya tarafından oluşturulacak olan Kapsam dökümanı içeriğine dahil edilecek birim sorumluluğunda bulunan verilerin tarafıma ve süreç yönetim sistemine 16.09.09 tarihine kadar girilmesi hususunu tüm arkadaşlardan rica ederim Bilgi İşlem Şube Müdürü
	15/09/2009 12:00 am	-	Bilgi Güvenliği Yönetim Sistemi Kapsamının belirlenmesi		insanky	0.00 (0:00)		İyi Çalışmalar ; Komisyon başkanının 14.09.09 tarihinde icra edilen toplantıda belirttiği üzere kapsam dökümanına ve BGYS kapsamına girecek olan İnsan Kaynakları Birimine ait bilgiler halihazırda kurumumuzun kullanmış olduğu İnsan Kaynaklar yönetimi Otomasyonu içeriğinde bulunan veriler ayrıca Sunucu ortamında tutulan Her türlü dijital kayıt Ve Personel Şahsi dosyalarıdır.
	15/09/2009 12:00 am	-	Bilgi Güvenliği Yönetim Sistemi Kapsamının belirlenmesi		pazarlama	2.00 (2:00)		İyi Çalışmalar Satış ve pazarlama departmanı olarak Kapsam dökümanına ve BGYS kapsamına girecek olan verilerimiz aşağıda belirtildiği gibidir. Bu Kapsamda ; 1. Kurumumuzun ürettiği teknoloji ve bilişim hizmetlerinden ücretli olarak faydalanan müşterilerimizin takibinin yapıldığı satış ve pazarlama otomasyonu dahilindeki veriler.(Hazırlanan teklifler,Bekleyen İş talepleri Arızalar vb.) Satış ve Pazarlama birimi
	15/09/2009 12:00 am	-	Bilgi Güvenliği Yönetim Sistemi Kapsamının belirlenmesi		ithead	0.00 (0:00)		Arkadaşlar iyi Çalışmalar ; İKY ve Pazarlama birimlerimizin göndermiş olduklan verilere dayanarak genel olarak kapsamımıza alacağımız bilgileri Şirkete ait tüm ticari ve hizmete ait bilgiler çeklinde kapsam dökümanına alacağız.Ayrıca Bilgi İşlem Şube Md.'lüğü olarak Kurumumuzun BT sistemleri bilgileri , dış tedarikçilerden alınan hizmet bilgileri ve Kullanılan sistemin dökümantasyon bilgileri de BGYS kapsamına alınacaktır.İlave girdiler yapılması mümkündür.
	16/09/2009 12:00 am	-	Bilgi Güvenliği Yönetim Sistemi Kapsamının belirlenmesi		finans	0.00 (0:00)		İyi Çalışmalar ; Muhasebe ve Finans departmanı olarak birimimizin kullandığı Muhasebe otomasyonu veritabanındaki veriler, Ayrıca dış portföy ve iştirak bilgilerimizinde kapsam dökümanına alınması hususunu rica ederim Muhasebe ve finans birimi BGYS sorumlusu
	17/09/2009 12:00 am	-	Bilgi Güvenliği Yönetim Sistemi Kapsamının belirlenmesi		sekreterlik	0.00 (0:00)		Tüm BGYS komisyonuna iyi çalışmalar ; Yapılan girdiler ile birlikte BGYS kapsam dökümanı hazırlama çalışmalarına başlanmıştır. Bu Kapsamda daha önce BGYS kurulumu gerçekleştirmiş olan firmalar ile görüşülüp bilgi alınmıştır.Aynı zamanda internet vasıtasıyla örnek dökümanlar taranmıştır.Bugün itibariyle Bilgi İşlem Şube Müdürüne taslak döküman sunulacaktır. BGYS Sekreterya
	18/09/2009 12:00 am	-	Bilgi Güvenliği Yönetim Sistemi Kapsamının belirlenmesi		sekreterlik	0.00 (0:00)		İyi Çalışmalar ; Yapılan çalışma neticesinde oluşturulan kapsam dökümanı 17.09.09 tarihinde BGYS komisyonu liderine ve Bilgi İşlem Şube Müdürüne sunulmuştur. Kendileri tarafından yapılan değişme ve düzeltmeler ile birlikte nihai hale getirilen kapsam dökümanı, Dökümanlar bölümünde Kapsam dizini altına kopyalanmıştır.

BGYS koordinatörü tarafından hazırlanan görevlerin tamamlanmasını müteakiben görevin koordinatörü personel tarafından faaliyetine son verilir. Bu işlemden sonra diğer kullanıcıların ekranlarında tamamlanmış görevler görüntülenmez.

ISO/IEC 27001 standardı kapsamında ikinci adımda kurum, bilgi güvenliği politikası oluşturma çalışmalarını başlatmıştır. Bu çalışmanın kapsamı haftalık icra edilen BGYS ilerleme toplantılarında belirlenen başlıklar altında oluşturulan genel bilgi güvenliği politikasını destekleyen alt bilgi güvenliği politikaları ve bu politikalara bağlı prosedürler şeklinde düzenlenmiştir. Oluşturulan bilgi güvenliği politikası çalışmasında belirlenen alt politikalara ve alt politikalara bağlı prosedürlerin hazırlanması çalışmalarına ait görevlendirme “Bilgi Güvenliği Politikası Hazırlama Çalışmaları” görevi altında açılan alt görevler şeklinde belirtilmiştir. Bu süreçte SANALUFUK firması beş adet alt politika ve bu politikalara bağlı alt prosedür ve politikalarla Bilgi güvenliği politikası oluşturulmuştur. Görevlere atanan alt çalışma grupları ile sürdürülen bu çalışmalar neticesinde çalışma grupları kendilerine atan görevler neticesinde süreç yönetimi vasıtasıyla yapılan girdileri de göz önünde bulundurarak politika dökümanlarının oluşturulması işlemini gerçekleştirmişlerdir. Ayrıca Politika dökümanlarının tüm kullanıcılara tebliğ edilmesini müteakip “Dökümanlar” kısmında şablon tebellüğ dosyası vasıtasıyla bütün çalışanlara tebellüğ edilmesi gerektiği belirtilmiştir. Hazırlanan tebellüğ formlarından iki adet imzalatılması ve birinin şahsi dosyada diğerinin ise BGYS klasöründe muhafaza edilmesi gerektiği de sistem

kayıtlarına BGYS koordinatörü tarafından girilmiştir. Görev Kayıtları sistemde ilgili görev altında yeralmaktadır. Örnek görev kayıtları Şekil-33'de gösterilmiştir

Şekil 33. Politika Hazırlamaları Çalışmaları



	Tarih	Ref	Özet	URL	Kullanıcı	Saat	Maaliyet Kodu	Yorumlar
	21/09/2009 12:00 am	-	Bilgi Güvenliği Politikasının Oluşturulması		ithead	0.00 (0:00)		Arkadaşlar iyi çalışmalar ; Bilgi Güvenliği Politikası oluşturma çalışmaları kapsamında Bu sabah tüm BGYS koordinasyon ekibinin katılımıyla gerçekleştirilen haftalık BGYS ilerleme toplantısında alınan karar gereği mevcut örneklerden ve Tübitak UEKAE süreçlerinden faydalanılarak edinilen tecrübeye istinaden Net,kısa anlaşılabilir ve geliştirilebilir bir BGYS politikası oluşturmayı hedeflemekteyiz.Yani Hedefimiz; bilgi güvenliği konusunda yönetimin bakış açısını, onayını ve desteğini çalışanlara uygun araç ve denetim mekanizmaları eşliğinde iletmektir.Bu kapsamda Çok geniş kapsamlı bir politika yerine alt politikalar ile desteklenen bir BGYS Politikasının oluşturulmasına karar verilmiştir. Bu Kapsamda BGYS Politikası Dökümanını besleyecek alt politikalar aşağıda olduğu şekliyle belirlenmiştir. 1. Bilgi Sistemleri Ağ Yönetim ve kullanım Politikası 2. Bilgi Sistemleri Veritabanı yönetim ve kullanım Politikası 3. Bilgi sistemleri giriş çıkış ve yönetim politikası 4. Donanım bakım onarım politikası 5. Bilgi sistemleri personeli istihdam politikası 6. Bilgi Güvenliği olayları politikası 7. Bilgi Güvenliği Eğitim Politikası İlave Politika önerileri varsa sebepleri ile birlikte bir sonraki toplantıya kadar paylaşılması hususunu rica ederim Bilgi İşlem Şube Müdürü
	22/09/2009 12:00 am	-	Bilgi Güvenliği Politikasının Oluşturulması		itsysadmin	0.00 (0:00)		İyi Çalışmalar Dünkü toplantıya rahatsızlığım nedeniyle katılamamıştım.Bilgi Güvenliği Politikası oluşturma sürecinde bence de alt politikaların hazırlanıp ana BGYS politikasına girdi sağlaması fikri uygundur.Fakat firmamızın gerek portföyünü gerekse kurum içi işleyişimizi dikkate alırsak Genel olarak aşağıdaki alt politikaları oluşturmamız daha uygun olabilir. Bu Maksatla Erişim Kontrol Politikası (Kullanıcıların sorumlulukların ve veriye nasıl ulaşacaklarını ve kullanacaklarını belirleyen politika) Yazılım tasarım ve veritabanı yönetim politikası Bilgisayar Kullanım politikası (Dizüstü İş istasyonu ve PC kullanıcıları için) Bilgi Sistemleri Personeli Seçme politikası Bilgi Sistemleri Yönetim Politikası altında alt bölüm olarak ; Ağ Yönetim Sistem Yönetim Donanım ve Çevre birimleri Onarım Politikaları olabilir. Saygılarımla
	22/09/2009 12:00 am	-	Bilgi Güvenliği Politikasının Oluşturulması		kalite	2.00 (2:00)		İyi Çalışmalar ; Konu ile ilgili Sistem Yöneticimize katılıyorum. ilave olarak eklemek istediğim husus BGYS kalite hedeflerimizin de politikaya girdi yapılmasıdır.Ayrıca yapmış olduğum araştırmalar kapsamında BGYS Politikası oluşturma konu Tübitak Eğitim dökümanı Dökümanlar kısmına konulmuştur.
	22/09/2009 12:00 am	-	Bilgi Güvenliği Politikasının Oluşturulması		itnetwork	13.00 (13:00)		İyi Çalışmalar ; Bende Sistem Yöneticisi arkadaşımıza katılıyorum.İlave olarak eklemek istediğim husus ise Bilgi sistemleri yönetim politikasına alt politika olarak Yedekleme ve Felaket Kurtarım Politikası eklenmesi olacaktır.
	23/09/2009 12:00 am	-	Bilgi Güvenliği Politikasının Oluşturulması		ithead	0.00 (0:00)		Sistem Yönetim ve Kalite Grubu taslak politika dökümanlarınızı 25.09.09 tarihine kadar hazırlayarak tarafımıma bilgilendiriniz.

BGYS komisyonu tarafından politika belirleme sürecinde görüşülen ve karar verilen görev kayıtları, süreç yönetimi sisteminde "Görevler" Bölümünde "Bilgi Güvenliği Politikası oluşturma çalışmaları" görevinde ve bu göreve bağlı alt görev kayıtlarında bulunmaktadır. BGYS komisyonu tarafından yapılan araştırmalar ve görev yorumları yardımlarıyla oluşturulan bir şablon vasıtasıyla kurumun Bilgi Güvenliği Politikası oluşturulmuş, alt politika ve prosedürlerle birlikte yönetime sunulmuş, yönetimin onayını müteakiben sistemde yayınlanmıştır.

4.2.2.2.2. BGYS Risk Yönetimi Süreci

SANALUFUK Bilişim Teknolojileri A.Ş. kurumun BGYS kapsamı ve Bilgi Güvenliği politikalarının belirlenmesi işlemlerinden sonra risk yönetim süreci faaliyetine başlamıştır. Risk Yönetimi sürecini işletmek maksadıyla BGYS komisyonu içerisinde risk yönetim alt grubu oluşturulmuştur. Grup lideri olarak kurumun Bilgi İşlem Müdürlüğüne bağlı "Bilgisayar olaylarına müdahale" biriminde görevli bilgi güvenliği ve risk yönetim uzmanı atanmıştır. Sözkonusu uzman senaryoya göre bilgi güvenliği risk yönetimi konusunda yurtiçinde ve yurtdışında sertifikalı eğitimler almış durumdadır. Ayrıca Eğitim dökümanlarının paylaşımı dökümantasyon bölümünde yapılmaktadır. Risk yönetim grubunda BGYS komisyonu lideri, projeden sorumlu yönetim kurulu üyesi, Kalite Kontrol Müdürlüğü ve İnsan Kaynakları Müdürlüğü

üyeleri bulunmaktadır. Bu maksatla kurumu haftalık BGYS ilerleme toplantılarından sonra ve görev süresince hergün bir saat süreyle toplantı icra etmektedir. Kurum Risk yönetimi kapsamındaki görevlerini belirlemiş ve görev tanımlarını yapmıştır. Bu görevlere ait bilgiler Şekil-34'de sunulmuştur.

Şekil 34. Risk Yönetimi Görev Tanımları ve Sorumlulukları

Risk Yönetimi , Analizi ve Risk Analizi Sonucu uygulanacak Kontrolleri Belirleme	ithead	admin (100%) (+3)	11/10/2009 08:00 am	0 gün	23/10/2009 05:00 pm
Risk değerlendirme yaklaşımının belirlenmesi	ubingol@gmail.com	insanky (100%) (+4)	11/10/2009 08:00 am	0 gün	13/10/2009 05:00 pm
Risklerin Belirlenmesi	ubingol@gmail.com	insanky (100%) (+5)	13/10/2009 08:00 am	0 gün	16/10/2009 05:00 pm
Kurumun Bilgi Güvenliği Yönetim Sistemi Kapsamındaki Varlık Envanterinin Oluşturulması Ve Varlıkların sınıflandırılması(Gizlilik, bütünlük ve erisebilirlik kriterlerine göre varlıkların değerlendirilmesi)	ubingol@gmail.com	insanky (100%) (+5)	13/10/2009 08:00 am	0 gün	16/10/2009 05:00 pm
Açıklık Ve Tehditlerin Belirlenmesi	ubingol@gmail.com	admin (100%) (+5)	19/10/2009 08:00 am	0 gün	20/10/2009 05:00 pm
Risklerin Tanımlanması	ubingol@gmail.com	admin (100%) (+5)	19/10/2009 08:00 am	0 gün	20/10/2009 05:00 pm
Risk İşleme Süreci	ubingol@gmail.com	insanky (100%) (+5)	22/10/2009 08:00 am	0 gün	26/10/2009 05:00 pm
Risklerin Önceliklendirilerek Uygun Kontrollerin Uygulanması	ubingol@gmail.com	admin (100%) (+6)	22/10/2009 08:00 am	0 gün	26/10/2009 05:00 pm
Artık Risklerin Belirlenmesi ve Yönetimden Onay Alınması	ubingol@gmail.com	isokoord (100%) (+3)	27/10/2009 08:00 am	0 gün	30/10/2009 05:00 pm
Dokümantasyon	ithead	admin (100%) (+10)	18/10/2009 08:45 am	0 gün	22/01/2010 05:00 pm

Kurum, Risk Yönetimi sürecinde belirtilen görevleri icra ederken ISO 27001 BGYS Risk Yönetim sistemi yazılımını kullanacaktır. Sanalufuk firması risk yönetimi kapsamında ilk olarak Risk değerlendirme yaklaşımını benimseyecek ve uygulama dökümanı hazırlayacaktır. Senaryoya göre Risk yönetim koordinasyon toplantıları sonucunda kurum risk değerlendirme yaklaşımını belirlemiştir. Belirlenen yaklaşıma göre, kurum niteliksel risk yönetim metoduna karar vermiştir. Niteliksel Risk yönetim modeli kapsamında, risk yönetim liderinin belirlediği görevler icra edilecektir. İlk aşamada kurum bünyesinde bulunan bütün bilgi sistemleri içerisinde güvenlik kapsamında bulunan varlıklarının envanterini çıkaracaktır. Bu işlem kapsamında risk yönetim liderinin talimatıyla sekreterya, tüm birimlerin üyelerinden oluşan BGYS komisyonundaki tüm üyelere kendi birimleri dahilinde bilgi güvenliği varlıklarının envanterinin belirtilen özellikler ile düzenlenerek komisyona bildirilmesi konusunda miadlı bir E-Posta göndermiştir. Sözkonusu kayıtlar BGYS süreç yönetim sistemine girilmiştir. Tüm birimlerden alınan veriler ışığında toplam bilgi güvenliği envanteri oluşturulmaya başlanmıştır. Varlık envanteri oluşturulma aşamasında risk yönetim grubu varlıkların gizlilik, bütünlük ve kullanılabilirlik özelliklerine göre sıralandırılarak belirtilmesini istemiştir. Birimlerin belirlediği bu dereceler aynı zamanda birkez daha Risk yönetim grubu tarafından değerlendirilmektedir. Varlıkların bu niteliksel özellikleri alınırken aynı zamanda varlıkların bu değerlerinin matematiksel olarak belirlenip bilgi güvenliği varlığının değeri ortaya çıkarılmaktadır. Varlık Değeri, varlıkların Gizlilik, Bütünlük ve Kullanılabilirlik değerlerinin çarpımı şeklinde

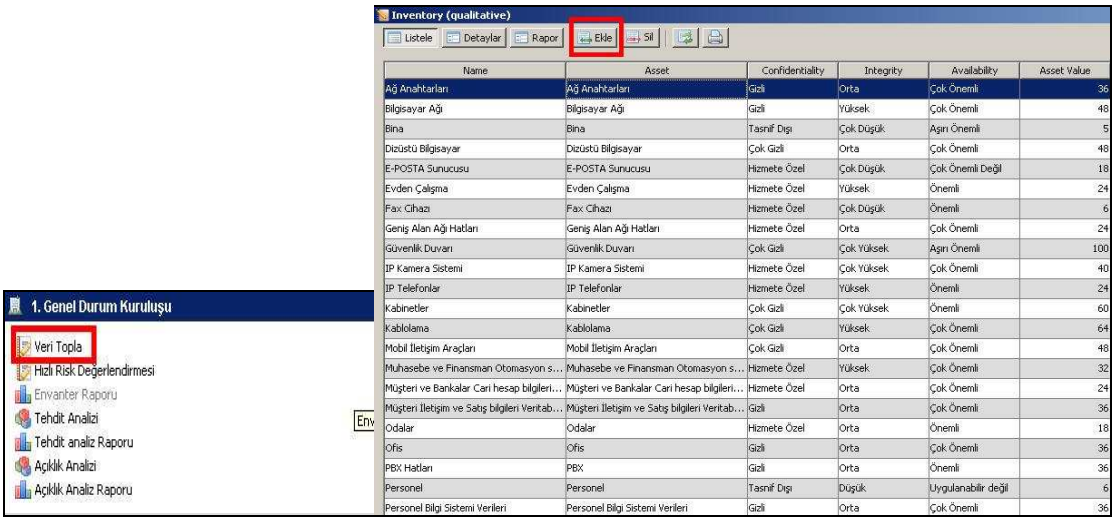
hesaplanmaktadır. Bu maksatla varlıkların özellikleri ve dereceleri Tablo-5'de belirtilmiştir.

Tablo 5. Varlıkların niteliksel özellikleri ve sayısal değerleri

Gizlilik Derecesi	Bütünlük Derecesi	Kullanılabilirlik Derecesi	Sayısal Değeri
Uygulanabilir Değil	Uygulanabilir Değil	Uygulanabilir Değil	0
Tasnif dışı	Çok Düşük	Çok Önemli Değil	1
Hizmete Özel	Düşük	Önemli Değil	2
Gizli	Orta	Önemli	3
Çok Gizli	Yüksek	Çok Önemli	4
Aşırı (Kozmik) Derecede Gizli	Çok Yüksek	Aşırı Önemli	5

Birimlerden toplanan verilerin tekrar risk yönetim grubu tarafından değerlendirilmesinden sonra özellikleri düzenlenen varlıklar BGYS Risk yönetim yazılımı veritabanına eklenme işlemine Şekil-35'te gösterildiği gibi başlanmış ve işlemin tamamlanmasından sonra varlık envanteri raporu alınmıştır.

Şekil 35. Varlık Envanteri Oluşturma Çalışmaları



Firma varlık envanteri çalışmalarının tamamlanması ile birlikte oluşturulan varlık envanterini süreç yönetim sisteminde dökümantasyon kısmında yönetimin onayının alınmasından sonra yayımlamıştır. Örnek raporun bir kısmı Şekil-36'da gösterilmiştir.

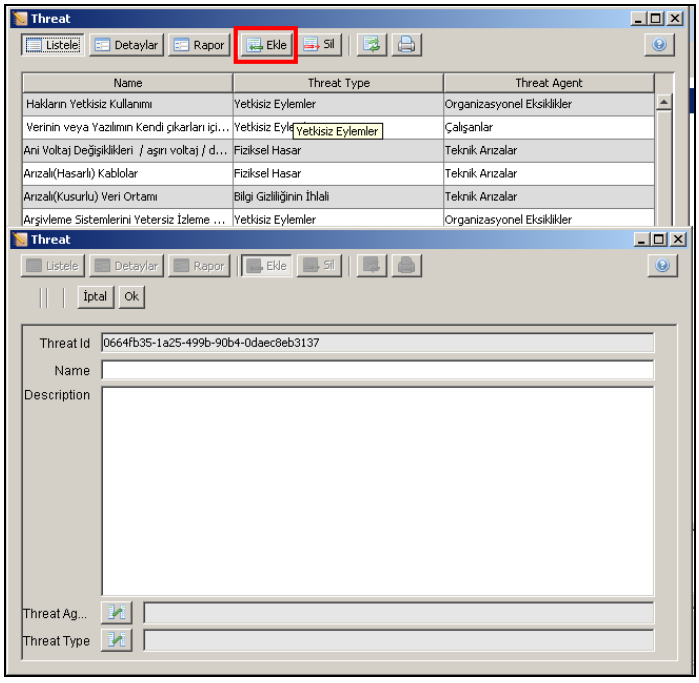
Şekil 36. Varlık Envanteri Rapor Örneği

Sanalufuk Bilişim Teknolojileri A.Ş. Varlık Envanteri

RYS ID	Varlık Adı	Gizlilik	Bütünlük	Kullanılabilirlik	Varlık Değeri
Teknik Altyapı Odası	Teknik Altyapı Odası	Uygulanabilir değil	Uygulanabilir değil	Önemli	0.0
Bina	Bina	Tasnif Dışı	Çok Düşük	Aşırı Önemli	5.0
Personel	Personel	Tasnif Dışı	Düşük	Uygulanabilir değil	6.0
Fax Cihazı	Fax Cihazı	Hizmete Özel	Çok Düşük	Önemli	6.0
İnce İstemciler	İnce İstemciler	Hizmete Özel	Düşük	Önemli	12.0
Yazılım	Yazılım	Hizmete Özel	Düşük	Çok Önemli	16.0
Odalar	Odalar	Hizmete Özel	Orta	Önemli	18.0
E-POSTA Sunucusu	E-POSTA Sunucusu	Hizmete Özel	Çok Düşük	Çok Önemli Değil	18.0

Süreç yönetimi sistemi tarafında risk yönetim grubuna varlık envanterinin oluşturulması aşamasından sonra belirlenen varlıkların muhtemel açıklarının belirlenmesi ve bu açıkları kullanarak risk meydana getiren olası tehditlerin tespit edilmesi görevi tanımlanmıştır. Risk Yönetim grubuna atanan bu görev sebebiyle senaryoya göre risk yönetim grubu bir toplantı icra etmiş ve icra edilen toplantıda kurumun Bilgi Güvenliği kapsamındaki varlıkların üzerinden tek tek gidilerek olası açıklıklarının ve bu açıklıkları kullanması sonucunda firmanın bilgi varlıklarına zarar verecek olan tehditlerin analizleri yapılmıştır. Belirlenen tehditler ve açıklıklar hazırlanarak BGYS Risk Yönetim sistemi veritabanına girilmiştir. Öncelikle tehdit havuzuna girilen verilere tehdit kaynağı ve tehdit nedeni bilgileri Şekil-37'de gösterildiği gibi eklenmiştir.

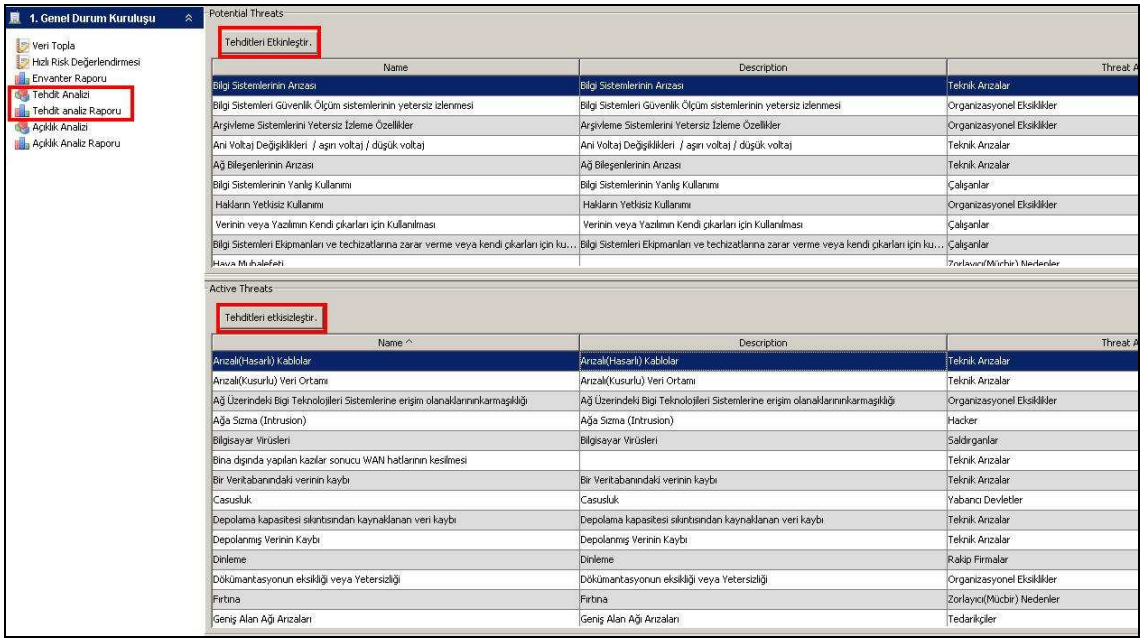
Şekil 37. Veritabanı Tehdit Ekleme Faaliyeti



Sistemin tehdit havuzunda bulunan tehditlerden kurum kendilerine uygun olan tehditleri etkinleştirmek kaydıyla belirlemiştir. Kurumun varlıklarına yönelik havuzda

bulunmayan tehditler Şekil-37'de bahsedildiği şekliyle Risk Yönetim sistemine eklenebilmektedir. Kurum kendilerine uygun tehditlerin seçimini ve analizini Şekil-38'de gösterildiği gibi yapmaktadır. Bu maksatla önce uygun tehditler etkinleştirilmekte daha sonra ise Şekil-39'de kısa özeti gösterilen detaylı tehdit analiz raporu alınabilmektedir.

Şekil 38. Belirlenen tehditlerin Etkinleştirilmesi



Şekil 39. Tehdit Analizi Raporu Örneği

Sanalufuk Bilişim Teknolojileri A.Ş. Tehdit Analiz Raporu

Tehdiit Adı	Tehdit Nedeni	Tehdit Kaynağı
Hırsızlık	Kasıtlı Eylemler	Çalışanlar
Fırtına	Fiziksel Hasar	Zorlayıcı(Mücbir) Nedenler
Bir Veritabanındaki verinin kaybı	Teknik Arızalar	Teknik Arızalar
Telif Haklarının İhlali	Organizasyonel eksiklikler	Organizasyonel Eksiklikler
Arşivleme Sistemlerini Yetersiz İzleme Özellikler	Yetkisiz Eylemler	Organizasyonel Eksiklikler
Yazılım Açıklıkları	Yetkisiz Eylemler	Teknik Arızalar
Güç Kaynaklarının Kesintisi	Zorunlu Hizmetleri zayiatı	Teknik Arızalar
Kontrol sistemlerinin Arızaları	Arıza	Teknik Arızalar
Dökümantasyonun eksikliği veya Yetersizliği	Organizasyonel eksiklikler	Organizasyonel Eksiklikler
Kriptolama için Yetersiz Anahtar Yönetimi	Yetkisiz Eylemler	Organizasyonel Eksiklikler
Arızalı(Hasarlı) Kablolar	Fiziksel Hasar	Teknik Arızalar
Yangın	Fiziksel Hasar	Zorlayıcı(Mücbir) Nedenler
Kadro Eksikliği	Zorunlu Hizmetleri zayiatı	Organizasyonel Eksiklikler
Veritabanı bütünlük ve tutarlılığının kaybı	Bilgi Gizliliğinin İhlali	Teknik Arızalar

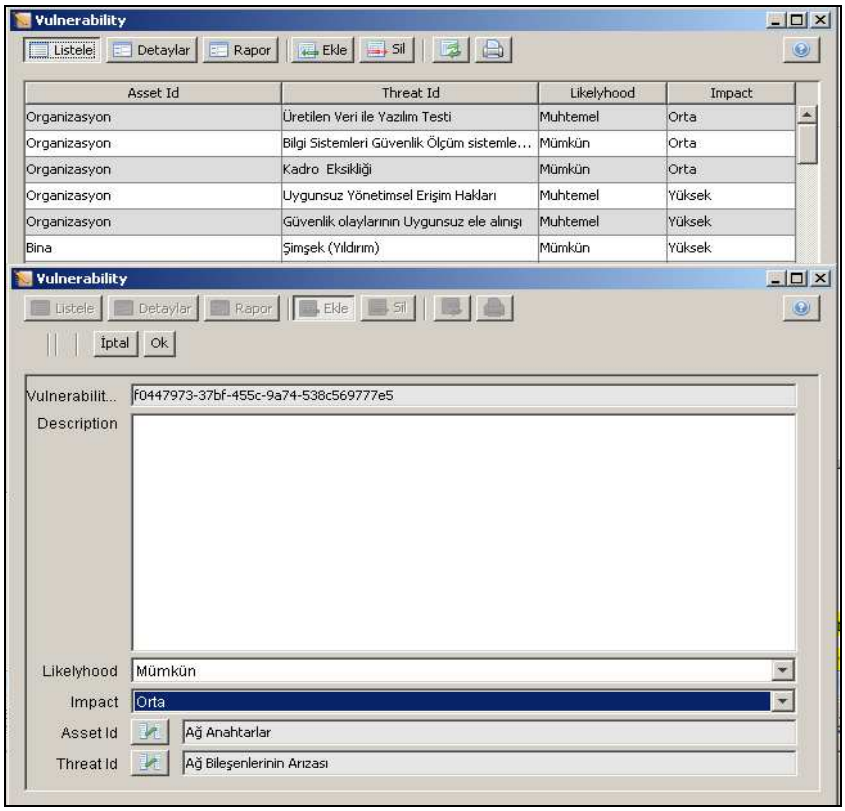
Firma tehditlerin kullanacağı açıkları öncelikle Risk Yönetim sistemi havuzuna girerek belirlemelidir. Bu kapsamda Risk Yönetim sistemine Açıklığın sahibi olan varlık bilgisi, açıklığı kullanan tehdit bilgisi, ilgili açık sonucu riskin meydana gelme olasılığı ve riskin kuruma olası etkisi Şekil-40'da belirtildiği şekliyle tanımlanmalıdır. Ayrıca bu aşamada ilgili riskin değeri oluşturulmaktadır. Bilgi varlıklarının açıklıklarının ilgili

tehditler sonucu ortaya çıkan risklerin değerinin ölçümü ise riskin olasılık değeri ile riskin kuruma olası etkisinin çarpımı ile elde edilmektedir. Risklerin meydana gelme olasılığı ve etki dereceleri Tablo-6'da belirtilmiştir.

Tablo 6. Risk Olasılık ve Etki Derecelendirmeleri

Olasılık Derecesi	Etki Derecesi	Sayısal Değeri
Uygulanabilir Değil	Uygulanabilir Değil	0
Olasılık dışı	Çok Düşük	1
Düşük İhtimal	Düşük	2
Mümkün	Orta	3
Muhtemel	Yüksek	4
Kesin	Çok Yüksek	5

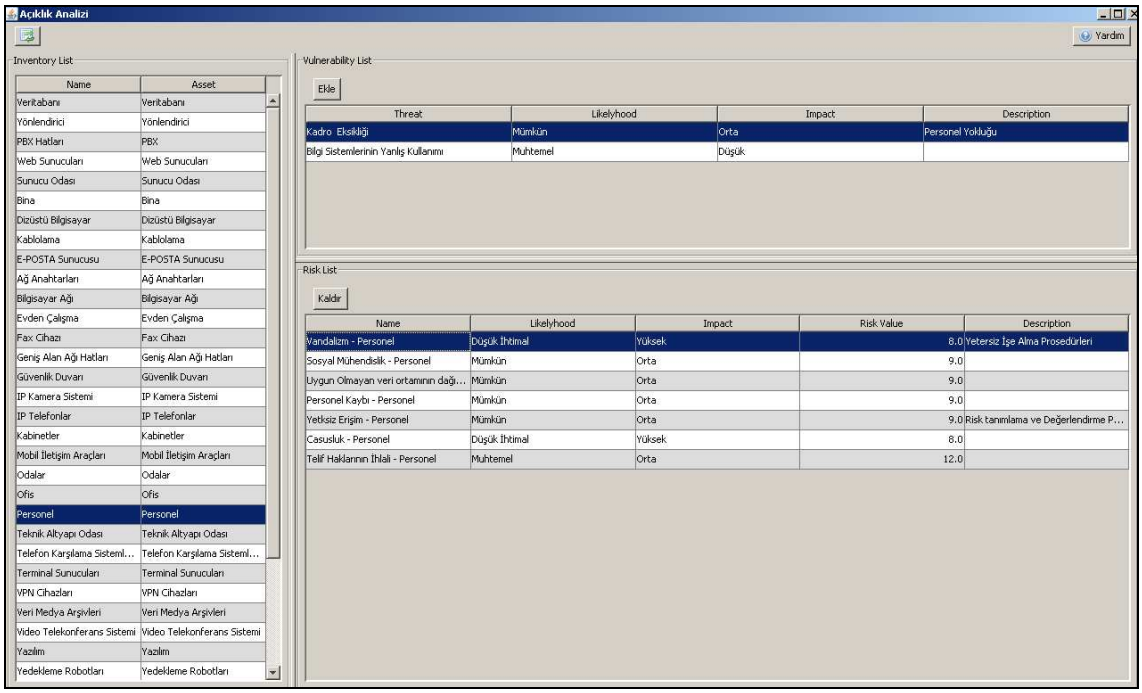
Şekil 40. Yeni Açık Ekleme İşlemi



Kurumun bilgi varlıklarının belirlenen açıkları yukarıda bahsedilen prosedüre uygun olarak veritabanına eklenmiştir. Ve ilgili açıkların varlıklara göre analizine başlanmıştır. Bu bölümde Açık Veritabanına eklenen açıklar, kurumun bilgi varlıklarına göre risk yönetim grubu tarafından seçilen tehditlerin kullandığı açıklar olarak açık analiz

raporunda yer alacaktır. Bu kapsamda yapılan çalışmaya ait örnek Şekil-41'de gösterilmiştir.

Şekil 41. Açık Analizi Süreci



Kurumun BGYS Komisyonu Risk Yönetim grubu tarafından yapılan tehdit ve açık analizleri sonuçları rapor halinde Risk Yönetim sistemi üzerinden alınarak BGYS komisyonuna sunulmuştur. BGYS komisyonu liderinin sözkonusu raporları yönetime sunması ve onayını almasını mütekiben BGYS Süreç yönetim sistemi Dökümantasyon kısmında yayımlamıştır. Oluşturulan tehdit ve açık analizi dökümanlarının örnek verileri Şekil-42'de gösterilmiştir.

Şekil 42. Tehdit ve Açık Analizi Raporları Örnekleri

Sanalufuk Bilişim Teknolojileri A.Ş. Açıklık Analiz Raporu

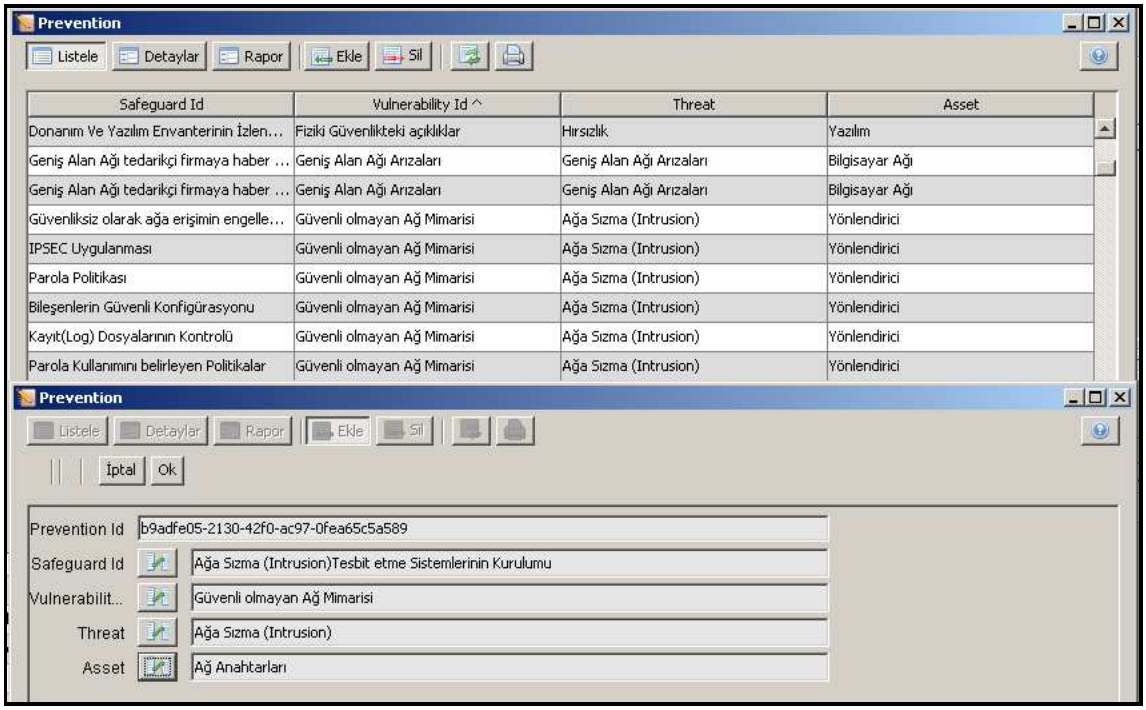
Varlık Adı	Tehdit Tanımı	Olasılık	Etki
Personel Şahsi Dosyaları	Saldırı	Düşük İhtimal	Yüksek
Teknik Altyapı Odası	Ani Voltaj Değişiklikleri / aşırı voltaj / düşük voltaj	Mümkün	Yüksek
IP Kamera Sistemi	Varsayılan Ağ Bileşenleri Şifreleri	Kesin	Yüksek
Veri Medya Arşivleri	Arızalı(Kusurlu) Veri Ortamı	Mümkün	Yüksek
Personel	Vandalizm	Düşük İhtimal	Yüksek
Personel	Kadro Eksikliği	Mümkün	Orta
Müşteri İletişim ve Satış bilgileri Veritabanı	Depolama kapasitesi sıkıntısından kaynaklanan veri kaybı	Düşük İhtimal	Orta
Sunucu Odası	Şimşek (Yıldırım)	Düşük İhtimal	Çok Yüksek
Kablolama	Saldırı	Mümkün	Orta
E-POSTA Sunucusu	Hizmetlerin Engellenmesi Saldırıları	Mümkün	Orta

Sanalufuk Bilişim Teknolojileri A.Ş. Tehdit Analiz Raporu

Tehdiit Adı	Tehdit Nedeni	Tehdit Kaynağı
Hırsızlık	Kasıtlı Eylemler	Çalışanlar
Fırtına	Fiziksel Hasar	Zorlayıcı(Mücbir) Nedenler
Bir Veritabanındaki verinin kaybı	Teknik Arızalar	Teknik Arızalar
Telif Haklarının İhlali	Organizasyonel eksiklikler	Organizasyonel Eksiklikler
Arşivleme Sistemlerini Yetersiz İzleme Özellikler	Yetkisiz Eylemler	Organizasyonel Eksiklikler
Yazılım Açıklıkları	Yetkisiz Eylemler	Teknik Arızalar
Güç Kaynaklarının Kesintisi	Zorunlu Hizmetleri zayiatı	Teknik Arızalar

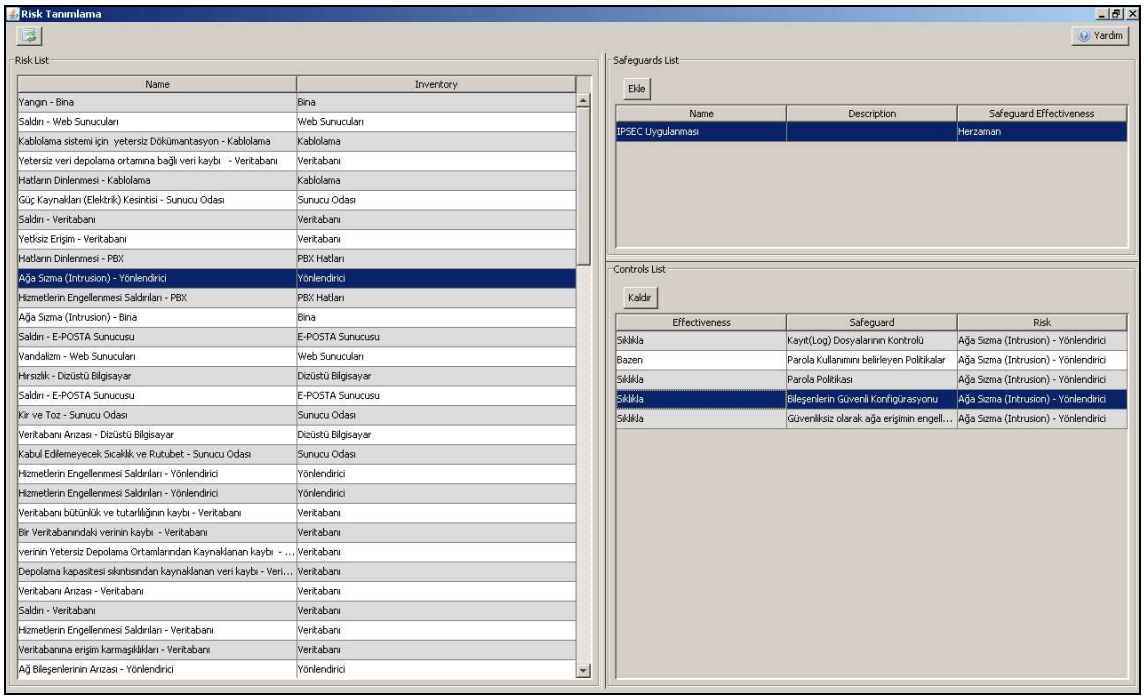
Sanalufuk Bilişim Teknolojileri A.Ş. BGYS komisyonu risk yönetim grubu icra ettiği tehdit ve açık analizi faaliyetinden sonra BGYS Süreç yönetiminde kendisine atanan görev kapsamında söz konusu analizlerin sonrasında ortaya çıkan riskleri tanımlama işlemine başlayacaktır. Bu maksatla BGYS Risk Yönetim sisteminin ana penceresinde bulunan risk durumu kısmında "Risk Tanımlaması" seçeneğini kullanacaktır. Risk tanımlaması işlemi aynı zamanda yazılımın, riskleri engellemek maksadıyla uygulanacak kontrollerin de seçildiği aşamadır. Şekil-43'de belirtildiği üzere Risk yönetim grubu tehdit ve açıklık analizleri sonucunda ortaya çıkan risklere karşı uygulanacak engellemeleri Risk Yönetim sistemi engelleme havuzuna uygun açık, tehdit ve riskin etkilediği varlıkları belirleyerek eklemiştir.

Şekil 43. Risk Engelleme Havuzuna Veri Girişi



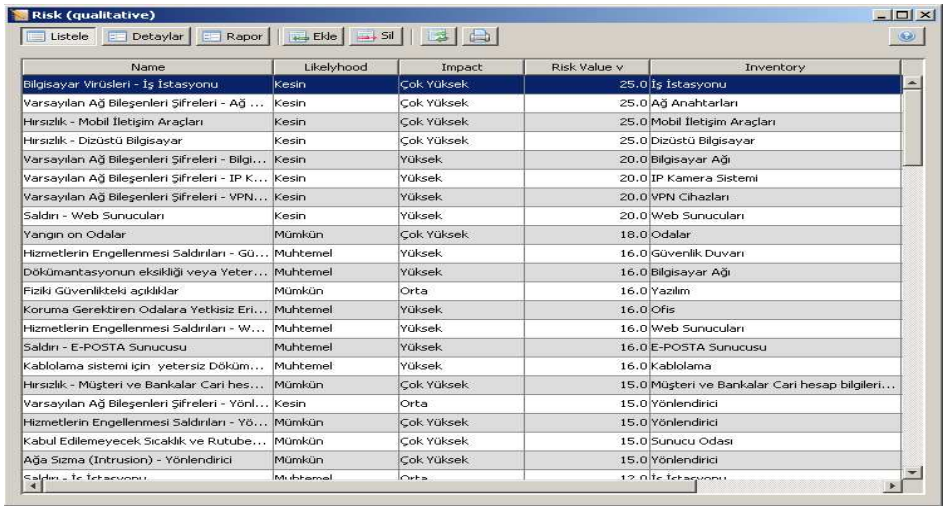
İlgili analizler sonucu ortaya çıkan risklerin engellenmesi için uygulanacak engelleme faaliyetlerinin neticesinde risklerin tanımlanması aşamasında ilgili engelleme faaliyetlerini seçerek kurumun tanımlanan riskleri için uygulanacak kontrollerini belirleme işlemi tamamlanmaktadır. Yani Risk tanımlanması aşamasında uygun kontrollerin belirlenmesi işlemi de yapılmaktadır. Kontrollerin önceliklendirilerek uygulanması kapsamında kontroller detaylı olarak incelenmektedir. Risk tanımlaması aşaması işlem örneği Şekil-44'de sunulmuştur.

Şekil 44. Risklerin ve Engellemelerin Tanımlanması



Risk yönetim grubu riskleri ve engellemeleri tanımladıktan sonra risk yönetim sisteminin hesapladığı risk değeri ile birlikte ilgilendirdiği varlıkları da belirleyen detaylı bir risk tahmin raporu hazırlayacaktır. Bu işlem için risk yönetim sisteminin ana penceresinde bulunan "Risk Tahmini" seçeneği kullanılacaktır. Risk tahmini bölümünde risk yönetim grubu kurumun bilgi varlıklarına yönelik riskleri, risk yönetim sistemi tarafından belirlenen risk değerine göre sıralayan detaylı bir risk tahmin raporu hazırlayacaktır. Risk yönetim grubunun yaptıkları toplantılar sonucu belirledikleri risklerin tahmini işlemi örneği Şekil-45'de gösterilmiştir.

Şekil 45. Kurumun Olasılıklı Risk Tahmini



Oluşturulan risk tahmini raporunun kısa başlangıç kısmı Şekil-46'da gösterilmiştir. Risk Yönetim grubu tarafından hazırlanan risk tahmin raporu BGYS komisyonuna sunulmasını müteakiben BGYS süreç yönetim sisteminden dökümantasyon kısmında yayımlanmıştır.

Şekil 46. Risk Tahmin Raporu Örneği

Sanalufuk Bilişim Teknolojileri A.Ş. Risk Tahmin Raporu v.2

Olası Riskin Tanımı	Olasılık	Etki	Risk Değeri	Açıklık (Zaafiyet) Açıklaması	Varlık
Bilgisayar Virüsleri - İş İstasyonu	Kesin	Çok Yüksek	25.0		İş İstasyonu
Varsayılan Ağ Bileşenleri Şifreleri - Ağ Anahtarları	Kesin	Çok Yüksek	25.0		Ağ Anahtarları
Hırsızlık - Mobil İletişim Araçları	Kesin	Çok Yüksek	25.0		Mobil İletişim Araçları
Hırsızlık - Dizüstü Bilgisayar	Kesin	Çok Yüksek	25.0	Fiziki Güvenlikteki açıklar	Dizüstü Bilgisayar
Varsayılan Ağ Bileşenleri Şifreleri - Bilgisayar Ağı	Kesin	Yüksek	20.0		Bilgisayar Ağı
Varsayılan Ağ Bileşenleri Şifreleri - IP Kamera Sistemi	Kesin	Yüksek	20.0		IP Kamera Sistemi
Varsayılan Ağ Bileşenleri Şifreleri - VPN Cihazları	Kesin	Yüksek	20.0		VPN Cihazları
Saldırı - Web Sunucuları	Kesin	Yüksek	20.0		Web Sunucuları
Yangın on Odalar	Mümkün	Çok Yüksek	18.0		Odalar

Risk yönetim grubunun kurumun risklerini ve risk değerlerini belirledikten sonraki görevi, söz konusu riskleri önceliklendirerek uygun kontrolleri uygulama ve uygulamalar sonucunda artık riskleri belirleyerek yönetimin onayını alma aşamasıdır. Bu aşama kurumun risklerini işleme aşamasıdır. BGYS süreç yönetim sisteminde risk yönetimi grubuna tanımlanan görev kapsamında BGYS komisyonuna sunduğu rapor doğrultusunda risklerin önceliklendirilmesi işlemi yapılacaktır. Bu aşamada risklerin önceliklendirilerek derecelendirilmesi işlemi maksadıyla icra edilecek toplantıya BGYS faaliyetlerinde sorumlu yönetim kurulu üyesinin de katılımı beklenmektedir. BGYS koordinatörü yönetim kurulu üyesinin katılımıyla gerçekleşen toplantı sonucunda senaryo gereği birinci öncelikli risk grubunun sayısal olarak risk değeri 6.0 üzerinde olan riskler ve niteliksel olarak ise bilgi sistemleri ağlarına yönelik riskler kabul edilmiştir. Ve uygun kontrollerin uygulanmasına karar verilmiştir. Konu ile ilgili karar kayıtları Şekil-47'de gösterilmiştir.

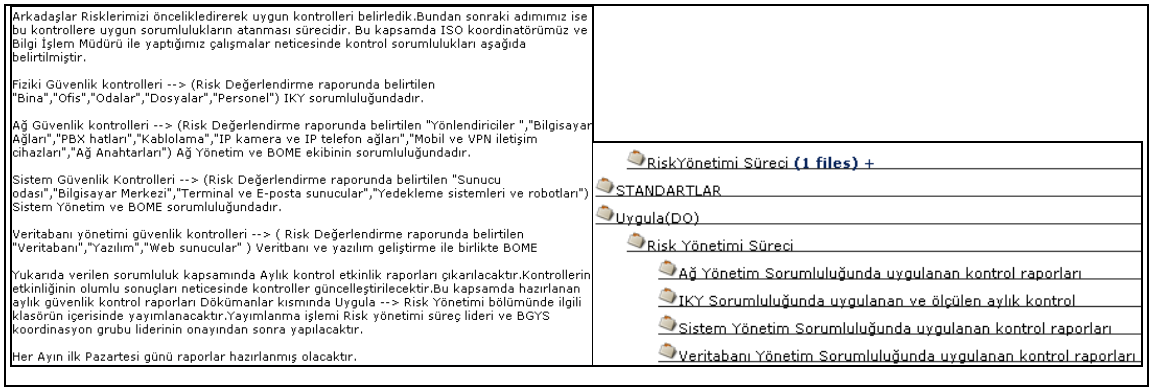
Şekil 47. Risklerin Önceliklendirilmesi Maksatlı Toplantı Kayıtları Örneği

29/10/2009 12:00 am	-	Artık Risklerin Belirlenmesi ve Yönetimden Onay Alınması		sekreterlik	0.00 (0:00)	İyi Çalışmalar ; Müdür bey uygunsa Risk Tahmin raporu üzerinde artık riskleri belirterek ikinci sürüm dökümanı oluşturabiliriz.
29/10/2009 12:00 am	-	Artık Risklerin Belirlenmesi ve Yönetimden Onay Alınması		ithead	0.00 (0:00)	Uygundur. Belirlenen risk seviyesi Risk yönetim grubu liderimizin belirttiği gibi zaten 6.0 seviyesine geliyor.Bu seviyenin altında olanları artık risk olarak sarı renkle işaretleyerek döküman sürüm 2 olarak yayınlayınız
30/10/2009 12:00 am	-	Artık Risklerin Belirlenmesi ve Yönetimden Onay Alınması		sekreterlik	0.00 (0:00)	İyi Çalışmalar Risk Tahmini raporu artık risklerin belirlenmesini müteakiben sürüm 2.0 olarak Risk Yönetimi süreci altında yayımlanmıştır.

Risk Yönetim grubu alınan bu karardan sonra riskleri alınan karara göre önceliklendirmiştir. Bu maksatla risk değeri 6.0'dan büyük olan risklere ve bilgi sistemleri ağlarına yönelik risklere öncelik verilmiş ve seçilen kontrollerin

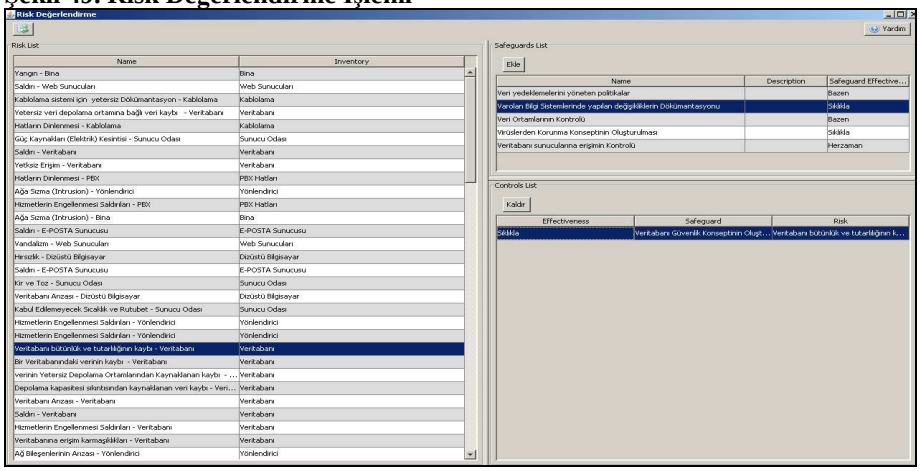
uygulanmasına karar verilmiştir. Bu maksatla yapılan değerlendirme sonucunda kontrol sorumlulukları belirlenmiştir. Belirlenen sorumlulukların aylık kontrol etkinlik raporları hazırlanması istenmiştir. Hazırlanan raporların ilgili sorumluluklara göre hazırlanmış olan bölümde yayınlanması direktifi verilmiştir. Uygulanan Kontrollerin Dökümantasyon örneği, görev ve sorumlulukların tahsisi Şekil-48'de gösterilmiştir.

Şekil 48. Kontrol Görev Ve Sorumluluklarının Tahsisi



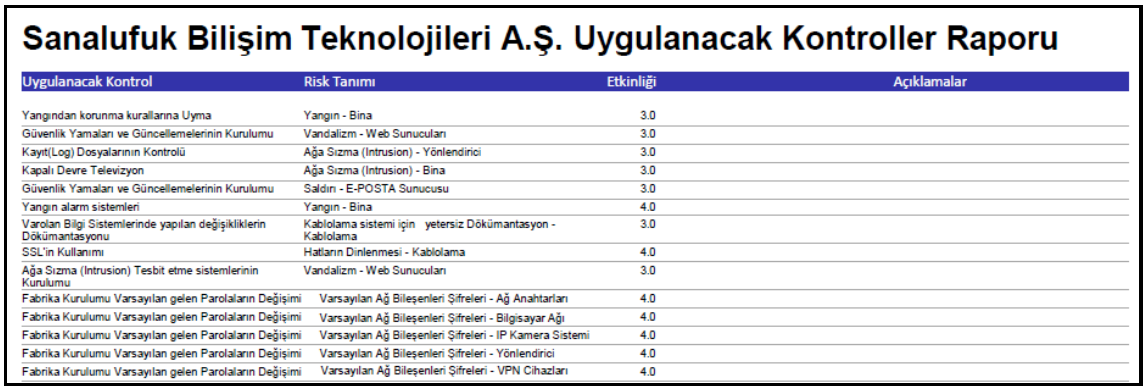
Uygulanacak kontrollerin ve sorumluların belirlenmesi sonucunda uygulanan kontrollerin etkinliğinin ölçülmesi işlemi gerçekleştirilmiş olacaktır. Bu aşamada elde edilen verilerle kurumun mevcut kontrollerin güncelleştirilmesi veya yeni kontrollerin eklenmesi sağlanacaktır. Bu sayede risklerin kabul edilebilecek seviyelere indirilip indirilmediği de analiz edilecektir. Risk yönetim sisteminin ana penceresinde bulunan risk değerlendirme penceresinde uygulanan kontroller güncellenebilmekte veya yeni risk yönetim sistemine yeni eklenen kontroller ilave edilebilmektedir. Ayrıca değerlendirme ile ilgili detaylı rapor alınabilmektedir. Örnek işlem Şekil-49'da gösterilmiştir.

Şekil 49. Risk Değerlendirme İşlemi



Risk değerlendirme kapsamında belirlenen ve uygulanmasına karar verilen kontrollerin raporları risk yönetim sisteminin ana penceresinde bulunan üçüncü adımdaki “Kontrol Raporları” bölümünden alınmaktadır. Kurumun bilgi varlıklarını kullanan tehditlerin sebep olduğu riskleri önlemek maksadıyla kontrol etkinliğinin de belirtildiği bu rapor risk yönetim grubu tarafından değişen şartlar altında sürekli güncel tutularak BGYS süreç yönetim sistemi dökümantasyon kısmında tutulmaktadır. Örnek Kontrol raporu Şekil-50’de özet olarak gösterilmiştir.

Şekil 50. Uygulanacak Kontrol Raporu Örneği



Sanalufuk Bilişim Teknolojileri A.Ş. Uygulanacak Kontroller Raporu

Uygulanacak Kontrol	Risk Tanımı	Etkinliği	Açıklamalar
Yangından korunma kurallarına Uyma	Yangın - Bina	3.0	
Güvenlik Yamaları ve Güncellemelerinin Kurulumu	Vandalizm - Web Sunucuları	3.0	
Kayıt(Log) Dosyalarının Kontrolü	Ağa Sızma (Intrusion) - Yönlendirici	3.0	
Kapalı Devre Televizyon	Ağa Sızma (Intrusion) - Bina	3.0	
Güvenlik Yamaları ve Güncellemelerinin Kurulumu	Saldırı - E-POSTA Sunucusu	3.0	
Yangın alarm sistemleri	Yangın - Bina	4.0	
Varolan Bilgi Sistemlerinde yapılan değişikliklerin Dökümantasyonu	Kablolama sistemi için yetersiz Dökümantasyon - Kablolama	3.0	
SSL'in Kullanımı	Hatların Dinlenmesi - Kablolama	4.0	
Ağa Sızma (Intrusion) Tesbit etme sistemlerinin Kurulumu	Vandalizm - Web Sunucuları	3.0	
Fabrika Kurulumu Varsayılan gelen Parolaların Değişimi	Varsayılan Ağ Bileşenleri Şifreleri - Ağ Anahtarları	4.0	
Fabrika Kurulumu Varsayılan gelen Parolaların Değişimi	Varsayılan Ağ Bileşenleri Şifreleri - Bilgisayar Ağı	4.0	
Fabrika Kurulumu Varsayılan gelen Parolaların Değişimi	Varsayılan Ağ Bileşenleri Şifreleri - IP Kamera Sistemi	4.0	
Fabrika Kurulumu Varsayılan gelen Parolaların Değişimi	Varsayılan Ağ Bileşenleri Şifreleri - Yönlendirici	4.0	
Fabrika Kurulumu Varsayılan gelen Parolaların Değişimi	Varsayılan Ağ Bileşenleri Şifreleri - VPN Cihazları	4.0	

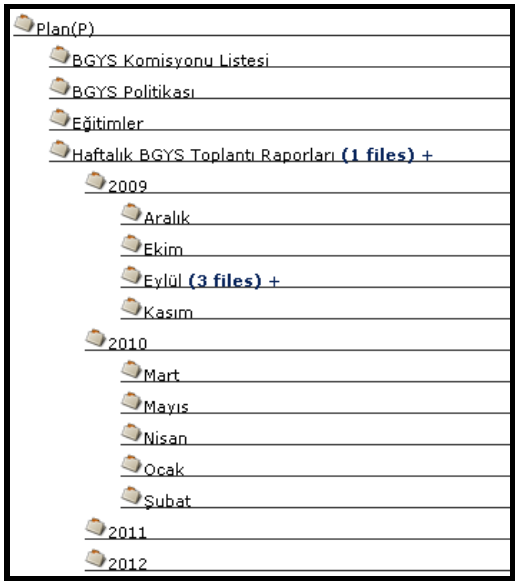
Risk Yönetim sürecinde uygulanan kontroller sonucunda bazı riskler karşısında hiç bir zaman tam güvenlik sağlanmamaktadır. Örneğin kurumsal bilgilerin işlendiği bir bilgisayarın uygulanan kontrollere rağmen hırsızlık riski ile karşı karşıya kalması ihtimali kapsamında risk yönetim grubu kabul edilebilir risk seviyesi altındaki risklerle birlikte yönetimden artık riskler için onay alması gerekmektedir. Senaryoya göre yapılan toplantılarda kabul edilen artık risklerin onayı yönetimden alınarak BGYS süreç yönetim sisteminde dökümantasyon kısmında yayınlanmıştır. Bu dökümanın hazırlanmasındaki amaç, kurum tarafından meydana gelme ihtimali olan söz konusu risklerin göze alındığının yönetim tarafından taahhüt edilmesidir.

Risk yönetim süreci kurum için sürekli devam edecek olan bir döngüdür. Bu kapsamda kurumun değişen ve gelişen bilgi varlıklarına yönelik risklerin de değişebilmesi mümkündür. Bu sebepten kullanılan risk yönetim sisteminin BGYS komisyonu ve risk yönetim grubu çalışmaları kapsamında sürekli güncel tutulması, aynı zamanda sistemin belirli aralıklarla yedeklenmesi de önemlidir. Bu kapsamda risk yönetim grubu, risk yönetim sistemi veritabanının haftalık olarak yedeğini almaktadır.

4.2.2.2.3. Dökümantasyon Analizi

SANALUFUK Bilişim Teknolojileri A.Ş. BGYS komisyonunun BGYS'nin uygulanması için yetki alınması işleminden hemen önce ISO/IEC 27001 BGYS kapsamında ihtiyaç duyacağı dökümantasyonun kontrolünü yapmak maksadıyla doküman analizi görevi tanımlanmıştır. Bu görevin mahiyetinde yapılan toplantıların sonucunda BGYS kapsamında yapılan haftalık BGYS ilerleme toplantılarının sonuçları belirlenen şablonda haftalık olarak hemen toplantının sonrasında sekreterya tarafından hazırlanarak BGYS süreç yönetim sisteminde dökümantasyon bölümünde Şekil-51'de belirtildiği bölümlerde yayınlanmasına karar verilmiştir.

Şekil 51. Haftalık BGYS Toplantı Sonuç Raporları Dökümantasyonu



Dökümantasyon kapsamında alınan kararlardan bir diğeri ise Bilgi Güvenliği eğitim faaliyetleri görevi olarak belirlenmiştir. Eğitimler bilgi sistemlerini kullanan ve yöneten personele verilen eğitimler olarak ikiye ayrılmıştır. Alınan karar gereği, Bilgi güvenliği ve bilgi sistemleri kapsamında bilgi sistem kullanıcılarına ve yöneticilerine verilen veya kurum dışından tedarik edilen eğitimlerin kayıtları BGYS süreç yönetiminde Eğitim Faaliyetleri görevi altındaki ilgili alt göreve kaydedilecek ve eğitimler kapsamında elde edilen dökümanların bir nüshasının BGYS süreç yönetimi sisteminde dökümantasyon kısmında yayınlanacaktır.

Dökümantasyon analizi kapsamında yapılan en önemli çalışmalardan biri BGYS Kalite el kitabı oluşturma çalışmalarıdır. Bu kapsamda BGYS komisyonu tarafından senaryoya

göre daha önce çalıştığı kurumlardaki ISO 9000 Kalite Yönetim Sistemi oluşturulması süreçlerinde Kalite El Kitabı hazırlığında tecrübesi bulunması sebebiyle BGYS komisyonunun Kalite Kontrol Müdürlüğü üyesi görevlendirilmiştir. Konsept açısından BGYS komisyonu kalite birimi üyesini, tüm komisyon üyeleri çalışmalarında destekleyecektir. Senaryoya göre çeşitli yüksek lisans tezleri ve yapılan araştırmalar ve diğer komisyon üyelerinin de desteği ile görev kapsamında verilen süre içerisinde BGYS el kitabı oluşturularak yönetimin onayına sunulmuştur. Yönetimin dökümanı onaylaması sonrasında BGYS el kitabı BGYS süreç yönetiminde Dökümantasyonu bölümünde yayınlanmıştır. BGYS komisyonu değişen ve gelişen olaylara istinaden dökümantasyon analizi görevinin sürekli açık kalmasına karar vermiştir. Bu maksatla ilerleyen zamanlarda ortaya çıkacak dökümantasyon ihtiyaçları bu görev kapsamında yönetilecektir.

4.2.2.2.4. Yönetim Onayı ve Uygulanabilirlik bildirgesinin hazırlanması

SANALUFUK Bilişim Teknolojileri A.Ş. Yönetim kuruluna kurumun Bilgi güvenliğinden sorumlu yönetim kurulu üyesi ve Bilgi İşlem Şube Müdürü tarafından yapılan sunum neticesinde yönetim kurulundan gerekli yetkilendirme alınmıştır. Yönetimin BGYS kurulumu ve işletimi konusunda taahhüt ettiği desteği ve onayını belirten doküman hazırlanarak, Yönetim Kurulu Başkanına imzalatılarak BGYS dökümantasyonuna eklenmiştir.

Yönetimin onayının alınmasından sonra BGYS komisyonu ISO/IEC 27001 standardında belirtilen kontrolleri sıralayarak, söz konusu kontrollerden kurumun BGYS kapsamında uygulananlarını belirleme ve BGYS kapsamı dışında kalan kontrollerin nedenlerini belirten uygulanabilirlik belgesini hazırlama çalışmalarına başlamıştır. BGYS'nin ilk defa uygulandığı kurumlarda idari anlamda uygulanabilirlik belgesinde eksiklikler çıkmaktadır. Fakat Uygulanabilirlik bildirgesi teknik anlamdaki maddeleri genellikle BGYS komisyonu grubunun hazırlamış olduğu dökümantasyon sisteminde detaylı olarak belirtilmiştir. Bu sebepten dolayı Uygulanabilirlik bildirgesi hazırlanırken madde madde uygulanan süreçler analiz edilmelidir. SANALUFUK Bilişim Teknolojileri A.Ş. BGYS komisyonu bu kapsamda ISO/IEC 27001 standardında belirtilen tüm kontrolleri kendi politika ve alt politikaları üzerinden kontrol etmiş ve uygulanan kontrollerin uygulanma nedenleri ile ilgili gerekli sınıflandırmayı yapmıştır.

Bu sınıflandırmaya göre kurum ISO/IEC 27001 standardında belirtilen kontrolleri Yasal ve ISO/IEC 27000 ailesi standartları kapsamındaki gereklilikler, Karşılaşılan ve Örnek alınan süreç ve olaylar, kurumun kendi iç işleyişi kapsamındaki iş gereklilikleri uygulamaları ve Risk Yönetimi sonucunda elde edilen veriler kapsamında uygulamaktadır. Bu sınıflandırma kapsamında ilgili kurum politikalarına atıfta bulunularak hazırlanan uygulanabilirlik belgesi yönetim kuruluna sunulduktan sonra onaylanmasını müteakiben BGYS süreç yönetim sisteminde dökümantasyon kısmında yayımlanmıştır. Hazırlanan uygulanabilirlik bildirgesi özet halinde Şekil-52'de gösterildiği gibidir.

Şekil 52. Uygulanabilirlik bildirgesi Örnek Dökümanı

Uygulanabilirlik Bildirgesi

Kontroller için açıklamalar

YG:Yasal ve Standart kapsamındaki Gereklilikler, **KO**:Karşılaşılan Olaylar, **İG/UU**: İş Gereklilikleri/Uyarlanmış Uygulamalar, **RDS**: Risk Değerlendirmesi Sonuçları

Düzenlenen Tarih 12.Kas.09

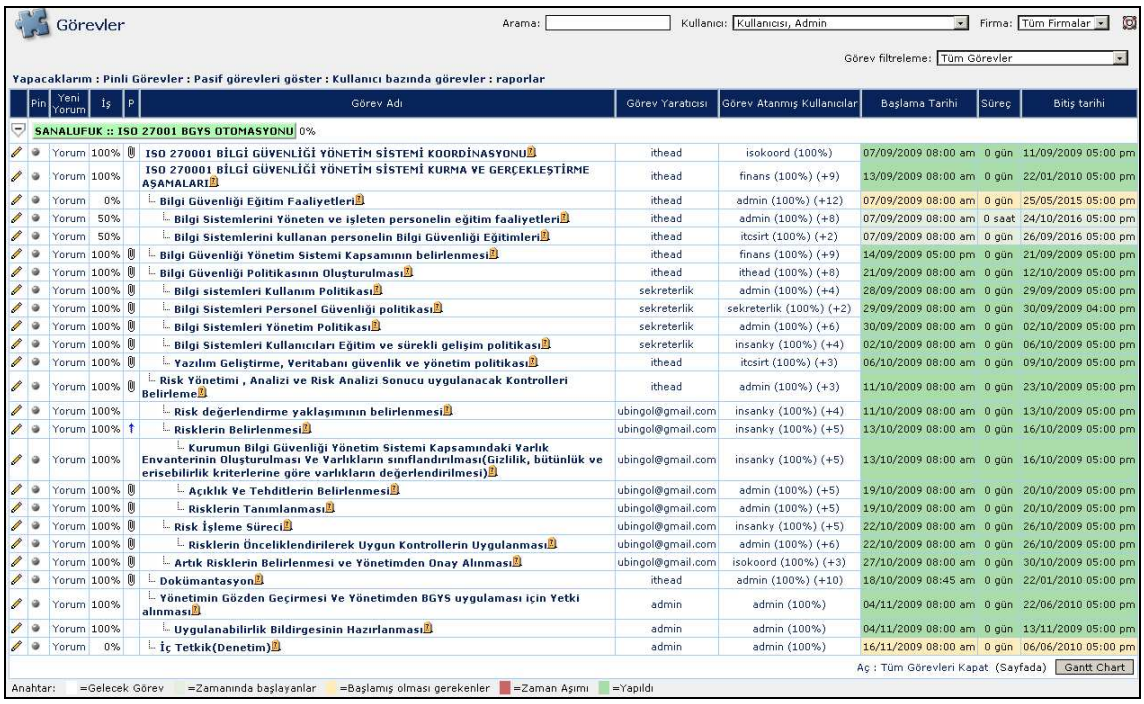
ISO 27001 Kontrolleri			Geçerli Kontroller	Yorumlar(Kapsam Dışı Tutulması gerekçeleri)	Seçilen kontroller ve Kontrol sebepleri				Yorumlar(Uygulamalarla Alakalı)
					YG	KO	İG/UU	RDS	
Konu	Bölüm	Zorunlu Kontroller/Kontroller							
Bilgi Güvenliği Politikası	5,1	Bilgi Güvenliği Politikası							
	5.1.1	Bilgi Güvenliği Politika Dökümanı	■		■				Alt politikalarla Desteklenmektedir.
	5.1.2	Bilgi Güvenliği Politikasını Gözden Geçirme	■		■				Altı ayda bir gözden geçirme yapılacaktır.
Bilgi Güvenliği Organizasyonu	6,1	İç Organizasyon							
	6.1.1	Yönetimin Bilgi Güvenliğine bağlılığı	■		■		■		
	6.1.2	Bilgi Güvenliği Koordinasyonu	■		■		■		Koordinasyon Grubu kurulmuştur.
	6.1.3	Bilgi Güvenliği sorumluluklarının tahsisi	■		■		■		Koordnasyon grubu sorumlulukları dağıtılmıştır.
	6.1.4	Bilgi işleme vasıtaları için yetki süreci	■		■		■		BGYS politikaları
	6.1.5	Gizlilik anlaşmaları	■		■		■		BGYS politikaları
	6.1.6	Otoritelerle iletişim	■		■		■		BGYS politikaları
	6.1.7	Özel ilgi grupları ile iletişim	■		■		■		BGYS politikaları
	6.1.8	Bilgi güvenliğinin bağımsız olarak gözden geçirilmesi	■		■		■		BGYS politikaları
	6,2	Dış taraflar							
	6.2.1	Dış taraflarla ilgili riskleri tanımlama	■			■		■	BGYS politikaları
	6.2.2	Müşterilerle ilgilenirken güvenliği ifade etme	■				■		BGYS politikaları
	6.2.3	Üçüncü taraf anlaşmalarında güvenliği ifade etme	■				■		BGYS politikaları
Varlık Yönetimi	7,1	Varlıkların sorumluluğu							
	7.1.1	Varlıkların envanteri	■		■			■	Risk Yönetim Süreci Faaliyeti
	7.1.2	Varlıkların sahipliği	■		■			■	Risk Yönetim Süreci Faaliyeti
	7.1.3	Varlıkların kabul edilebilir kullanımı	■		■			■	Risk Yönetim Süreci Faaliyeti
	7,2	Bilgi sınıflandırması							
	7.2.1	Sınıflandırma kılavuzu	■		■		■	■	Varlıklar risk Yönetim sürecinde G,B,E şeklinde sınıflandırılarak Varlık değeri
	7.2.2	Bilgi etiketleme ve işleme	■		■		■	■	
İnsan Kaynakları Güvenliği	8,1	İstihdam Öncesi							
	8.1.1	Roller ve sorumluluklar	■		■		■		Bilgi Sistemleri Personel Güvenliği Politikası
	8.1.2	Roller ve sorumluluklar(İzleme)	■		■		■		
	8.1.3	İstihdam koşulları	■		■		■		
	8,2	Çalışma Esnasında							
	8.2.1	Yönetim sorumlulukları	■		■		■		Bilgi Sistemleri Personel Güvenliği Politikası
	8.2.2	Bilgi güvenliği farkındalığı,eğitim ve öğretimi	■		■		■		
	8.2.3	Disiplin prosesi	■		■		■		
	8,3	İstihdamın sonlandırılması veya değiştirilmesi							
	8.3.1	Sonlandırma sorumlulukları	■		■		■		Bilgi Sistemleri Personel Güvenliği Politikası
	8.3.2	Varlıkların iadesi	■		■		■		
	8.3.3	Erişim haklarının kaldırılması	■		■		■		
			■		■				
Fiziksel ve Çevresel Güvenlik	9,1	Güvenli Alanlar							
	9.1.1	Fiziksel güvenlik çevresi	■		■	■	■	■	Bilgi Sistemleri Kullanım Politikası
	9.1.2	Fiziksel güvenlik çevresi	■		■	■	■	■	
	9.1.3	Ofisler, odalar ve olanakları korumaya alma	■		■	■	■	■	
	9.1.4	Dış ve çevresel tehditlere karşı koruma	■		■	■	■	■	Bilgi Sistemleri Kullanım Politikası
	9.1.5	Güvenli alanlarda çalışma	■		■	■	■	■	
	9.1.6	Açık erişim, dağıtım ve yükleme alanları	■		■	■	■	■	
	9,2	Techizat Güvenliği							
	9.2.1	Techizat yerleştirme ve koruma	■		■	■	■	■	Bilgi Sistemleri Kullanım Politikası
	9.2.2	Destek Hizmetleri	■		■	■	■	■	
	9.2.3	Kablolama Güvenliği	■		■	■	■	■	

4.2.3. BGYS'nin gerçekleştirilmesi ve işletilmesi

Kurumun BGYS Komisyonunun Uygulanabilirlik Bildirgesini hazırlayarak yayınlaması ile birlikte kurum için BGYS'nin planlanıp gerçekleştirilmesi işlemi tamamlanmış olmaktadır. Artık kurumun yönetilen bir Bilgi Güvenliği Yönetim Sistemi bulunmaktadır. Uygulanabilirlik Bildirgesinin hazırlanması ile birlikte Süreç yönetim

sisteminde kurumun BGYS kurulum ve gerçekleştirme faaliyetleri kapsamındaki tüm görevleri Şekil-53'de gösterildiği gibi tamamlanmıştır.

Şekil 53. Kurulum İşlem Maddeleri



Şekil-53'de belirtilen ve tamamlanan görevlerden eğitim ve tetkik faaliyetlerinin sürekli geliştirilmesi sebebiyle sözkonusu görevler açık olarak bırakılmıştır. Sonuç olarak fiili olarak eğitim ve tetkik faaliyetleri sürekli icra edilmesi gereken süreçlerdir.

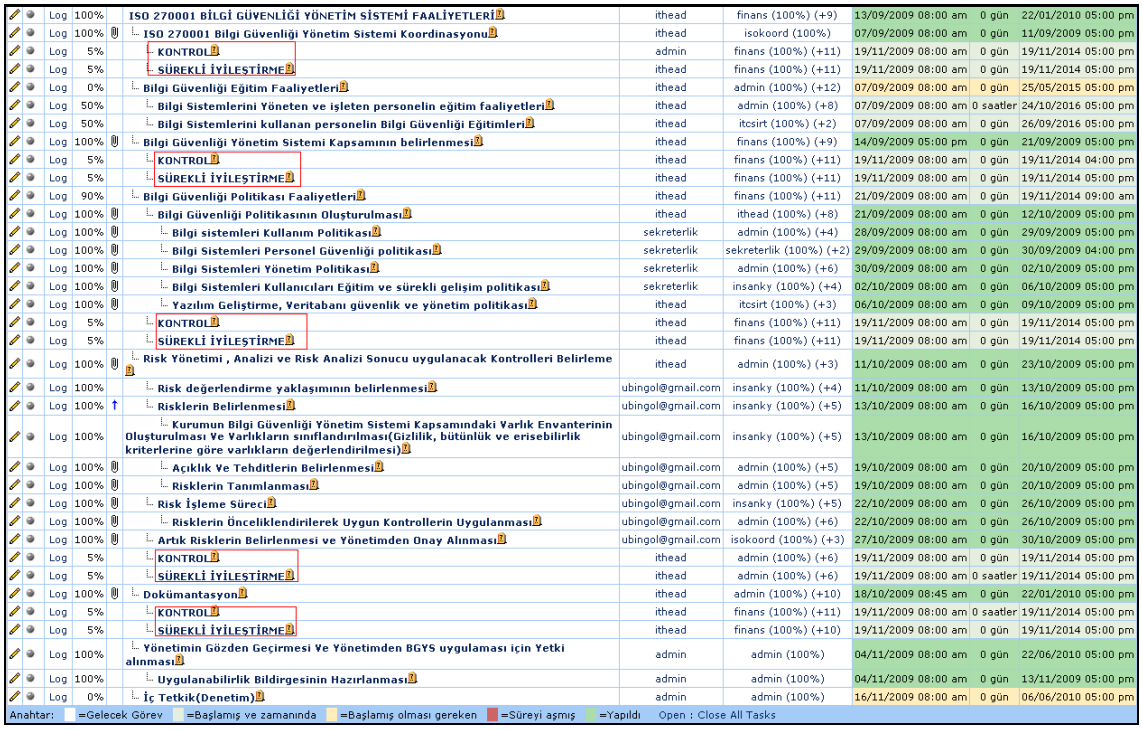
Uygulanabilirlik bildirgesinin hazırlanması ile birlikte kurumun daha önceki bölümlerde anlatıldığı üzere PUKÖ döngüsünün Planlama ve uygulama aşamaları gerçekleştirilmiştir.

4.2.4. BGYS'nin Kontrol ve İyileştirme aşamaları

SANALUFUK Bilişim Teknolojileri A.Ş. BGYS komisyonu kurumun BGYS'ni işletirken PUKÖ döngüsüne göre sürekli kontrol ve iyileştirme çalışmaları icra etmesi gerekir. Bu sebeplerden dolayı BGYS komisyonu kurulum aşamasında yapılan görev tanımlarının tamamında "Sürekli iyileştirme" ve "Kontrol" alt görevleri tanımlanmıştır. Bu kapsamda BGYS ana görev tanımı BGYS Kurma ve Gerçekleştirme Faaliyetleri yerine BGYS Faaliyetleri olarak kabul edilmiştir. Yeni Görev yapılanması Şekil-54'de gösterilmiştir. Süreç yönetim sisteminin herhangi bir bölümünde değişiklik yapılmamış,

mevcut dökümantasyon sistemi korunmuştur. Hiyerarşik sürüm dosyalama sistemine devam edilmiştir.

Şekil 54. BGYS Süreç Yönetim sistemi Yeni Görev tanımlaması

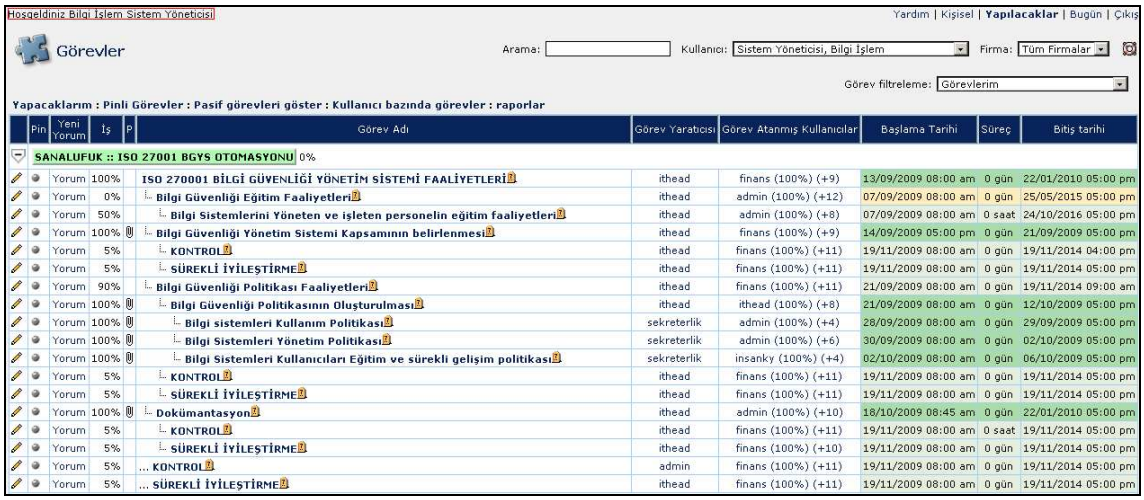


Log	100%		ISO 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ FAALİYETLERİ	ithead	finans (100%) (+9)	13/09/2009 08:00 am	0 gün	22/01/2010 05:00 pm
Log	100%		ISO 27001 Bilgi Güvenliği Yönetim Sistemi Koordinasyonu	ithead	isokoord (100%)	07/09/2009 08:00 am	0 gün	11/09/2009 05:00 pm
Log	5%		KONTROL	admin	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
Log	5%		SÜREKLİ İYİLEŞTİRME	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
Log	0%		Bilgi Güvenliği Eğitim Faaliyetleri	ithead	admin (100%) (+12)	07/09/2009 08:00 am	0 gün	25/05/2015 05:00 pm
Log	50%		Bilgi Sistemlerini Yöneten ve işleten personelin eğitim faaliyetleri	ithead	admin (100%) (+8)	07/09/2009 08:00 am	0 saatler	24/10/2016 05:00 pm
Log	50%		Bilgi Sistemlerini kullanan personelin Bilgi Güvenliği Eğitimleri	ithead	itcsirt (100%) (+2)	07/09/2009 08:00 am	0 gün	26/09/2016 05:00 pm
Log	100%		Bilgi Güvenliği Yönetim Sistemi Kapsamının belirlenmesi	ithead	finans (100%) (+9)	14/09/2009 05:00 pm	0 gün	21/09/2009 05:00 pm
Log	5%		KONTROL	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 04:00 pm
Log	5%		SÜREKLİ İYİLEŞTİRME	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
Log	90%		Bilgi Güvenliği Politikası Faaliyetleri	ithead	finans (100%) (+11)	21/09/2009 08:00 am	0 gün	19/11/2014 09:00 am
Log	100%		Bilgi Güvenliği Politikasının Oluşturulması	ithead	ithead (100%) (+8)	21/09/2009 08:00 am	0 gün	12/10/2009 05:00 pm
Log	100%		Bilgi sistemleri Kullanım Politikası	sekreterlik	admin (100%) (+4)	28/09/2009 08:00 am	0 gün	29/09/2009 05:00 pm
Log	100%		Bilgi Sistemleri Personel Güvenliği politikası	sekreterlik	sekreterlik (100%) (+2)	29/09/2009 08:00 am	0 gün	30/09/2009 04:00 pm
Log	100%		Bilgi Sistemleri Yönetim Politikası	sekreterlik	admin (100%) (+6)	30/09/2009 08:00 am	0 gün	02/10/2009 05:00 pm
Log	100%		Bilgi Sistemleri Kullanıcıları Eğitim ve sürekli gelişim politikası	sekreterlik	insanky (100%) (+4)	02/10/2009 08:00 am	0 gün	06/10/2009 05:00 pm
Log	100%		Yazılım Geliştirme, Veritabanı güvenlik ve yönetim politikası	ithead	itcsirt (100%) (+3)	06/10/2009 08:00 am	0 gün	09/10/2009 05:00 pm
Log	5%		KONTROL	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
Log	5%		SÜREKLİ İYİLEŞTİRME	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
Log	100%		Risk Yönetimi , Analizi ve Risk Analizi Sonucu uygulanacak Kontrolleri Belirleme	ithead	admin (100%) (+3)	11/10/2009 08:00 am	0 gün	23/10/2009 05:00 pm
Log	100%		Risk değerlendirme yaklaşımının belirlenmesi	ubingol@gmail.com	insanky (100%) (+4)	11/10/2009 08:00 am	0 gün	13/10/2009 05:00 pm
Log	100%		Risklerin Belirlenmesi	ubingol@gmail.com	insanky (100%) (+5)	13/10/2009 08:00 am	0 gün	16/10/2009 05:00 pm
Log	100%		Kurumun Bilgi Güvenliği Yönetim Sistemi Kapsamındaki Varlık Envanterinin Oluşturulması Ve Varlıkların sınıflandırılması(Gizlilik, bütünlük ve erisebilirlik kriterlerine göre varlıkların değerlendirilmesi)	ubingol@gmail.com	insanky (100%) (+5)	13/10/2009 08:00 am	0 gün	16/10/2009 05:00 pm
Log	100%		Açıklık Ve Tehditlerin Belirlenmesi	ubingol@gmail.com	admin (100%) (+5)	19/10/2009 08:00 am	0 gün	20/10/2009 05:00 pm
Log	100%		Risklerin Tanımlanması	ubingol@gmail.com	admin (100%) (+5)	19/10/2009 08:00 am	0 gün	20/10/2009 05:00 pm
Log	100%		Risk İşleme Süreci	ubingol@gmail.com	insanky (100%) (+5)	22/10/2009 08:00 am	0 gün	26/10/2009 05:00 pm
Log	100%		Risklerin Önceliklendirilerek Uygun Kontrollerin Uygulanması	ubingol@gmail.com	admin (100%) (+6)	22/10/2009 08:00 am	0 gün	26/10/2009 05:00 pm
Log	100%		Artık Risklerin Belirlenmesi ve Yönetimden Onay Alınması	ubingol@gmail.com	isokoord (100%) (+3)	27/10/2009 08:00 am	0 gün	30/10/2009 05:00 pm
Log	5%		KONTROL	ithead	admin (100%) (+6)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
Log	5%		SÜREKLİ İYİLEŞTİRME	ithead	admin (100%) (+6)	19/11/2009 08:00 am	0 saatler	19/11/2014 05:00 pm
Log	100%		Dokümantasyon	ithead	admin (100%) (+10)	18/10/2009 08:45 am	0 gün	22/01/2010 05:00 pm
Log	5%		KONTROL	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 saatler	19/11/2014 05:00 pm
Log	5%		SÜREKLİ İYİLEŞTİRME	ithead	finans (100%) (+10)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
Log	100%		Yönetimin Gözden Geçirmesi Ve Yönetimden BGYS uygulaması için Yetki alınması	admin	admin (100%)	04/11/2009 08:00 am	0 gün	22/06/2010 05:00 pm
Log	100%		Uygulanabilirlik Bildirgesinin Hazırlanması	admin	admin (100%)	04/11/2009 08:00 am	0 gün	13/11/2009 05:00 pm
Log	0%		İç Tetkik(Denetim)	admin	admin (100%)	16/11/2009 08:00 am	0 gün	06/06/2010 05:00 pm

Anahtar: =Gelecek Görev =Başlamış ve zamanında =Başlamış olması gereken =Süreyi aşmış =Yapıldı Open : Close All Tasks

BGYS komisyonu, faaliyetleri BGYS'nin kontrol edilme iyileştirme aşamalarında Şekil-54'de belirtildiği üzere icra edecektir. Bu kapsamda ilgili görevlerin kontrol ve iyileştirme safhaları görevin atlında "KONTROL" ve "SÜREKLİ İYİLEŞTİRME" şeklinde tanımlanan alt görevler kapsamında belirlenen sorumlulukların yetkileriyle icra edilecektir. Yine göreve atanmış kullanıcılar kendi kullanıcı hesapları ile sisteme giriş yaptıklarında Şekil-55'de belirtildiği gibi sadece kendilerine atanmış görevleri görebileceklerdir.

Şekil 55. Bilgi İşlem Sistem Yöneticisi Atanmış Görevler



Hoşgeldiniz Bilgi İşlem Sistem Yöneticisi

Yardım | Kişisel | **Yapılacaklar** | Bugün | Çıkış

Görevler

Arama: Kullanıcı: Sistem Yöneticisi, Bilgi İşlem Firma: Tüm Firmalar

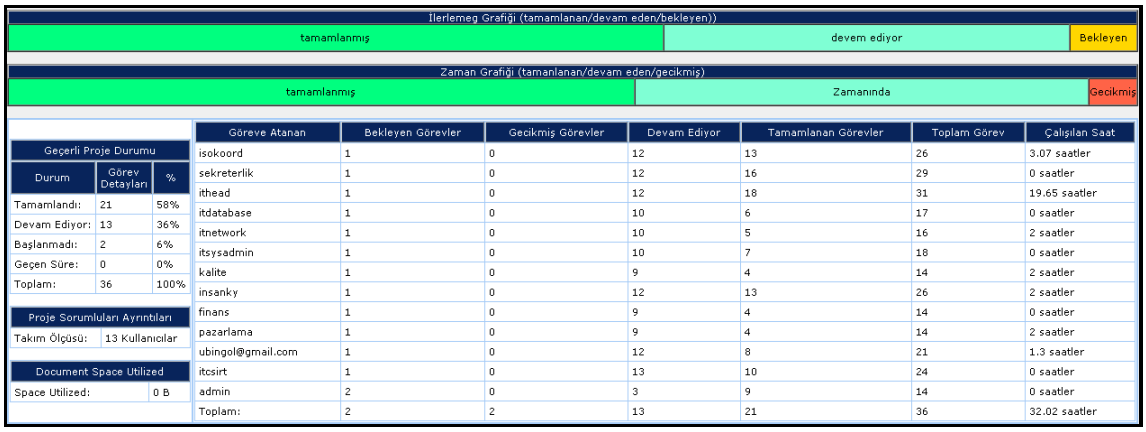
Görev filtreleme: Görevlerim

Yapacaklarım : Pinli Görevler : Pasif görevleri göster : Kullanıcı bazında görevler : raporlar

Pin	Yeni Yorum	İş	P	Görev Adı	Görev Yaratıcısı	Görev Atanmış Kullanıcılar	Başlama Tarihi	Süreç	Bitiş tarihi
				SANALUFUK :: ISO 27001 BGYS OTOMASYONU 0%					
	Yorum	100%		ISO 270001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ FAALİYETLERİ	ithead	finans (100%) (+9)	13/09/2009 08:00 am	0 gün	22/01/2010 05:00 pm
	Yorum	0%		Bilgi Güvenliği Eğitim Faaliyetleri	ithead	admin (100%) (+12)	07/09/2009 08:00 am	0 gün	25/05/2015 05:00 pm
	Yorum	50%		Bilgi Sistemlerini Yöneten ve işleten personelin eğitim faaliyetleri	ithead	admin (100%) (+8)	07/09/2009 08:00 am	0 saat	24/10/2016 05:00 pm
	Yorum	100%		Bilgi Güvenliği Yönetim Sistemi Kapsamının belirlenmesi	ithead	finans (100%) (+9)	14/09/2009 05:00 pm	0 gün	21/09/2009 05:00 pm
	Yorum	5%		KONTROL	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 04:00 pm
	Yorum	5%		SÜREKLİ İYİLEŞTİRME	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
	Yorum	90%		Bilgi Güvenliği Politikası Faaliyetleri	ithead	finans (100%) (+11)	21/09/2009 08:00 am	0 gün	19/11/2014 09:00 am
	Yorum	100%		Bilgi Güvenliği Politikasının Oluşturulması	ithead	ithead (100%) (+8)	21/09/2009 08:00 am	0 gün	12/10/2009 05:00 pm
	Yorum	100%		Bilgi sistemleri Kullanım Politikası	sekreterlik	admin (100%) (+4)	28/09/2009 08:00 am	0 gün	29/09/2009 05:00 pm
	Yorum	100%		Bilgi Sistemleri Yönetim Politikası	sekreterlik	admin (100%) (+6)	30/09/2009 08:00 am	0 gün	02/10/2009 05:00 pm
	Yorum	100%		Bilgi Sistemleri Kullanıcıları Eğitim ve sürekli gelişim politikası	sekreterlik	insanky (100%) (+4)	02/10/2009 08:00 am	0 gün	06/10/2009 05:00 pm
	Yorum	5%		KONTROL	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
	Yorum	5%		SÜREKLİ İYİLEŞTİRME	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
	Yorum	100%		Dokümantasyon	ithead	admin (100%) (+10)	18/10/2009 08:45 am	0 gün	22/01/2010 05:00 pm
	Yorum	5%		KONTROL	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 saat	19/11/2014 05:00 pm
	Yorum	5%		SÜREKLİ İYİLEŞTİRME	ithead	finans (100%) (+10)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
	Yorum	5%		... KONTROL	admin	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm
	Yorum	5%		... SÜREKLİ İYİLEŞTİRME	ithead	finans (100%) (+11)	19/11/2009 08:00 am	0 gün	19/11/2014 05:00 pm

Görev tanımlarının yeniden düzenlenmesi işleminden sonra Süreç Yönetim sistemi istatistikler toplanıp Şekil-56'da gösterildiği şekliyle kullanıcı bazında incelenip doküman haline getirilerek sistemin dökümantasyon kısmında yayımlanmıştır. Ayrıca BGYS faaliyeti süreci görev bazında GANTT Grafiğine dökülerek dökümantasyon kısmında yayınlanmıştır.

Şekil 56. BGYS Süreç Yönetim Sistemi İstatistikleri



İlerlemeg Grafiği (tamamlanan/devam eden/bekleyen))

tamamlanmış | devem ediyor | Bekleyen

Zaman Grafiği (tamanlanan/devam eden/gecikmiş)

tamamlanmış | Zamanında | Gecikmiş

Geçerli Proje Durumu

Durum	Görev Detayları	%
Tamamlandı:	21	58%
Devam Ediyor:	13	36%
Başlanmadı:	2	6%
Geçen Süre:	0	0%
Toplam:	36	100%

Proje Sorumluları Ayrıntıları

Takım Ölçüsü:	13 Kullanıcılar

Document Space Utilized

Space Utilized:	0 B

Göreve Atanan	Bekleyen Görevler	Gecikmiş Görevler	Devam Ediyor	Tamamlanan Görevler	Toplam Görev	Çalışılan Saat
isokoord	1	0	12	13	26	3.07 saatler
sekreterlik	1	0	12	16	29	0 saatler
ithead	1	0	12	18	31	19.65 saatler
itdatabase	1	0	10	6	17	0 saatler
itnetwork	1	0	10	5	16	2 saatler
itsysadmin	1	0	10	7	18	0 saatler
kalite	1	0	9	4	14	2 saatler
insanky	1	0	12	13	26	2 saatler
finans	1	0	9	4	14	0 saatler
pazarlama	1	0	9	4	14	2 saatler
ubingol@gmail.com	1	0	12	8	21	1.3 saatler
itcsirt	1	0	13	10	24	0 saatler
admin	2	0	3	9	14	0 saatler
Toplam:	2	2	13	21	36	32.02 saatler

BGYS süreci SANALUFUK firmasında bilfiil kurulmuş ve işletilmeye başlanmıştır. Bu kapsamda kullanıcı yönetimi ve görev yönetimi güncel gelişmelere göre yeniden düzenlenebilmektedir. Ayrıca BGYS komisyonu içerisindeki personelin değişikliği ihtimaline karşılık sistem yöneticisi tarafından kullanıcı yönetim faaliyetleri düzenlenebilir.

SONUÇ VE ÖNERİLER

Sonuçlar

Kurumların ISO 27001 Bilgi Güvenliği Kalite Yönetim Sistemini uygularken bu sistemi kurma, işletme ve iyileştirme faaliyetlerini yönetebileceği bir süreç yönetim ve risk yönetimi otomasyonun oluşturulmasını hedefleyen bu çalışmada aşağıdaki sorulara yanıt aranmıştır.

a) Özellikle KOBİ'lerin BGYS sürecini kurma ve işletme aşamalarında mutlaka danışmanlık ve ticari yazılım desteği almaları gerekli midir?
b) Bu maksatla küçük işletmelerin BGYS sürecini yönetmek için Açık Kaynak Kodlu Mimari ile tasarlanan veya tasarlanmış olan ücretsiz yazılımlar kullanılabilir mi?

Bu kapsamda kurumların konu hakkında uzmanlaşmış firmalardan imkanları dahilinde danışmanlık almaları ve ticari yazılımlardan faydalanmaları tercih edilen seçenektir. Fakat konuya maliyetler açısından bakacak olursak, küçük firmaların başlangıçta bu tip belgeleri hak etmek için yüksek danışmanlık ücretleri veya ticari yazılım kullanmaları pek mümkün değildir. Öte yandan KOBİ'ler üretim alanlarındaki faaliyetlerini genişletip büyüme hedefini gerçekleştirmek için ISO 9001 veya ISO 27001 gibi kalite yönetim sistemlerini işletmelerine uygulamalıdır. Günümüzde bu tip belgelendirmelere hak kazanan küçük işletmelerin üretim faaliyetlerindeki başarılarının artması yanında çeşitli kuruluşlar tarafından da mali olarak desteklendikleri görülmektedir. Ticari yazılım sistemlerine ve danışmanlıklara alternatif olarak uygulanacak yöntemde en düşük maliyet, en yüksek etkinlik hedeflenmektedir. Bu sebepten kurumların sadece uluslararası lisanslara bağlı kalmak koşuluyla ISO 27001 BGYS sürecini en düşük maliyetlerle gerçekleştireceği bir açık kaynak BGYS süreç yönetim sistemi ve risk yönetim sistemi otomasyonunun tercih edilecek yöntem olduğu belirlenmiştir. Geliştirilmeye açık olan bu tip yazılımlarla işletmeler tamamen otomasyonu kendilerine göre yeniden düzenleyebilirler. Böylece sistemdeki bir probleme ticari destek yerine herhangi bir anda müdahale edilebilmektedir. Üstelik otomasyon yazılımların platform bağımsız olarak çalışabilmesi de kurumları işletim sistemi maliyetlerinden de kurtarmaktadır. Bu sayede söz konusu ihtiyaçlar için gerekli maliyetler diğer ihtiyaçlarda değerlendirilebilir. Ayrıca kötü niyetli olunmasa da kaynak kodu satın alınamayan yazılımların kurumun bilgi varlıklarının yönetimi esnasında kullanımı da

tartışmalıdır. Açık Kaynak Kodu sayesinde kurumlar ISO 27001 gibi kendileri için hayati önemi sahip bilgi varlıklarının yönetiminde kullanılan yazılımların tamamının kontrolünü sağlarlar.

Bu çalışmanın özellikle üçüncü bölümünde AKK bir otomasyon mimarisi oluşturulmaya çalışılmıştır. Ve çalışma neticesinde elde edilen otomasyon ile işletmelerin orta düzey bir bilgisayar bilgisi bulunan bir personel ile bu tip bir otomasyonu elde edebileceği görülmüştür. Böylece küçük işletmelerin teknik anlamda bir maliyet problemi bu yolla giderilebilecektir. Ayrıca internet ortamında aynı platformda çalışan birçok geliştirici ile görüş alışverişi yapılabileceği ve bunun da kurumların kendi sistemlerine ekleyerek otomasyonlarını geliştirebileceği de açıktır. Böylelikle kurumlar ücretsiz olarak teknik danışmanlık ve destek alabilmektedir. Ayrıca ilave yazılım destek maliyeti de ortadan kalkmaktadır. Bu ilavelere ek olarak bu kapsamda yeniden düzenlenen süreç yönetim sistemi ve risk yönetim sistemi yazılımları işletim sistemi bağımsız olmaları sebebiyle yine kurumun kullandığı açık kaynak kodlu bir işletim sistemi üzerinde rahatlıkla çalışabilmektedir. Ayrıca bu sistemler için ihtiyaç duyulan donanım ihtiyaçlarının da düşük olması KOBİ'ler açısından da olumlu sonuçlar doğurmaktadır.

Çalışmanın dördüncü bölümünde tamamen hayali bir kurumda bu kapsamda düzenlenen AKK yazılımlarla BGYS kurularak etkin bir şekilde işletilmeye başlanmıştır. Süreç Yönetim sistemi otomasyonu ile hiyerarşik bir düzenleme yapılmış, BGYS ile ilgili tüm kayıtların tutulması sağlanmıştır. Ayrıca kullanıcı bazında yetkilendirme yapılarak görevli personelin görevlerini sadece kendi yetkilendirildiği alan üzerinde gerçekleştirmesi sağlanmıştır. Dolayısıyla BGYS komisyonunun kendi içerisinde dahi bilgi güvenliği faaliyeti icra edilmiştir. Risk Yönetim Sistemi yazılımı sayesinde kurumun bilgi varlıklarına yönelik risklerin yönetimi ve raporlaması sağlanmış ayrıca konu ile ilgili karar vericilere yardımcı olacak bir karar destek platformu oluşturulmuştur. Oluşturulan raporlar süreç yönetim sistemine aktarılarak belgelendirme faaliyeti kapsamında risk yönetimi dokümantasyonu olarak yerlerini almıştır. Dördüncü bölümde yapılan çalışmalar çok düşük bir işlemci ve fiziksel bellek'e sahip bir bilgisayar üzerinde test edilmiştir. Olumlu sonuçlar alınmıştır. Böylece donanım ihtiyaçları da düşük seviyede karşılanmıştır. Ayrıca bu yazılımların AKK bir işletim sistemi üzerinde çalıştığı da görülmüştür. Bu sayede işletim sistemi maliyeti de

çözülmüştür. Süreç yönetim sistemi yazılımının web tabanlı olması sayesinde geniş alan ağı üzerinden çalışabilirliği de test edilmiş ve internet üzerinden de çalıştığı görülmüştür. Ayrıca sistemin organizasyon farklılıklarına göre yeniden düzenlenebilmesi de önemlidir. Bu kapsamda farklı kurumlarda rahatlıkla BGYS sürecinin yönetimi sağlanabilmektedir. Ayrıca aynı kurumda iki farklı BGYS uygulama ihtiyacına istinaden birden fazla BGYS sürecini yönetmek mümkündür. Sistemin işletilmesi ile birlikte eşzamanlı yedekleme testleri yapılmış, olası sistem arızaları durumunda sistemin bir başka bilgisayar üzerinden süratle sistemin yeniden çalıştırılarak veri ve zaman kaybının önlenebileceği tesbit edilmiştir.

Üçüncü bölümde oluşturulup, dördüncü bölümde örnek olarak uygulanan mimari sayesinde kurumların BGYS süreçlerini yönetebilecekleri tamamen AKK benzer bir ISO 27001 otomasyon sistemini internet üzerinden yapılan araştırmalar sayesinde oluşturabilecekleri açıktır. Böylelikle özellikle küçük işletmelerin ISO 27001 süreçlerinde önemli bir tasarruf sağlayarak BGYS sürecini yönetebileceği anlaşılmıştır.

Öneriler

Bu çalışma neticesinde elde edilen sonuçlar özellikle ISO 27001 belgesini almaya hak kazanmak için çalışacak olan küçük işletmeler için bu süreci yönetirken yardımcı olacak ücretsiz tamamen açık kaynak kodlu bir sistemin oluşturulabileceğini göstermiştir. Böylelikle kurumlar önemli bir maliyet kaleminden tasarruf sağlayabileceklerdir. Yalnızca ISO 27001 BGYS süreci değil, bunun yanında kurumların bilgi sistemlerinde açık kaynak kodlu yazılımları kullanmaları gerek maliyet açısından gerekse Bilgi Sistemlerinin güvenliği açısından işletmelere büyük faydalar sağlayacaktır. Çünkü AKK yazılımlar gelişmeye veya geliştirilmeye açıktır. Ve işletmelere üçüncü bölümde kısaca bahsedilen lisansların şartları altında ücretsiz olarak kullanılabilme özelliği sunmaktadır. Aynı zamanda AKK yazılım, kaynak kodlarının tamamen açık olması sebebiyle de kullanılan yazılımların ara katmanda ne işlem yaptığının bilinmesine ve sonuç olarak bilgi güvenliği özelliğinin sağlanmasına yardımcı olmaktadır. Yapılan araştırmalar işletmelerin ve kamu kurumlarının AKK yazılımlara geçiş sürecine başladıklarını veya tamamladıklarını ya da planladıklarını işaret etmektedirler. Bu sebepten özellikle KOBİ'lerin bu tip yazılımlara yönelmesi tavsiye edilmektedir.

Geçmişten günümüze hayatın en önemli unsurlarından biri olan eğitim, ISO 27001 BGYS sürecinde de son derece hayati bir öneme sahiptir. Sonuç olarak ister ticari

ürünler, ister AKK ürünler, ISO 27001 BGYS sürecinin yönetiminde eğitim olmadan hiçbir fayda sağlamayacaktır. Çalışanlar kurumun bilgi varlıklarının güvenliğini sağlamak için öncelikle bu varlıkların önemini öğrenmek zorundadırlar. Bu husus ise ancak sürekli eğitim faaliyeti ile sağlanabilir. Bu sebepten kurumların ISO 27001 BGYS sürecinde bu sistemleri kullanmadan önce ve sürekli olarak çalışanlara Bilgi Güvenliği Eğitimleri sunmaları tavsiye edilmektedir. Eğitimden yoksun bir BGYS süreci mutlak başarısızlıkla sonuçlanacaktır.

Üçüncü bölümde oluşturulan mimaride BGYS süreç yönetim sisteminin hali hazırda web üzerinden çalışması, olası bir riski sistemin tüm ağ kullanıcılarına açık olarak çalışması riskini ortaya çıkarmaktadır. ISO 27001 dökümanında anlatıldığı üzere bu sorun kabul edilebilir artık bir risktir. Fakat bu sistem kullanılırken IP kısıtlaması ya da IPSEC veya SSL gibi şifreleme metodlarının kullanımı tavsiye edilmektedir. Öte yandan risk yönetim sistemi ise bu değerlendirmelere karşın tek bir bilgisayar üzerinde çalıştırılmalıdır.

Çalışmanın sonucunda kurumların mali imkânları doğrultusunda öncelikli olarak kesinlikle ISO 27001 konusunda uzmanlaşmış danışman kişi veya kurumlardan bu süreçte destek almaları tavsiye edilmektedir. Ayrıca konu ile ilgili Ticari yazılım ürünlerinin kullanımı tamamen kurumların tercihidir. Bu çalışma kapsamında hedef kitle olarak belirlenen küçük işletmelerin tüm bilgi sistemleri varlıklarını yönetmek maksadıyla AKK yazılım mimarisini tercih etmeleri tavsiye edilmektedir.

KAYNAKÇA

"Açık Kaynak Kod Bildirgesi", http://ozguryazilim.pau.edu.tr/iys/_acik-kaynak-kod-bildirgesi.html, 22.02.2010

"Açık Kaynak Kodlu Yazılım (Open Source Software) Nedir?",ODTÜ Bilgisayar Topluluğuhttp://www.cclub.metu.edu.tr/nenedir/Açık+Kaynak+Kodlu+Yazılım+Open+Source+Software)+Nedir%3F, 20.02.2010

ALBAYRAK, H.Oğuz (2008), "Gnu-Linuks Ve Bilişim Dünyasındaki Son Gelişmelerin Türkiye Açısından Önemi", www.yildiz.edu.tr

ARNASON, Sigurjon Thor ve Keith D. Willett (2008), "*How to Achieve 27001 Certification: An Example of Applied Compliance Management*", Auerbach Publications, Boca Raton\FL-ABD

AVCI, Umut ve M. Avcı (2004), "Örgütlerde Bilginin Önemi Ve Bilgi Yönetimi Süreci", *Mevzuat Dergisi*, Yıl 7, Sayı 74, Şubat, s.72-82

BAĞCI, Barış (2007), *Bilgi Teknolojileri Risk Yönetimine Genel Bakış*, http://www.denetimnet.com/Pages/bilgiteknolojileririskyonetimi.aspx,10.11.2009

British Standards Institute, BS ISO/IEC 27002:2005, *Information technology: Security techniques, Code of practice for information security management*, Londra:2007

British Standards Institute, BS ISO/IEC 27005:2008, *Information technology: Security techniques, Information security risk management*, Londra:2008

CALDER, Alan (2006), "*A Business Guide to Information Security*", Kogan Page Limited, Sterling\VA-ABD

CALDER, Alan ve Steve Watkins (2008), "*IT GOVERNANCE A Manager's Guide to Data Security and ISO27001/ISO 27002 4th Edition*", Kogan Page Limited, Philadelphia\PA-ABD

CANBERK, Gürol ve Ş. Sağıroğlu (2006), "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Politeknik Dergisi*, Cilt 9, Sayı 3, s. 165-174.

"Comparison of Oracle, MySQL and PostgreSQL DBMS",http://www-css .fnal.gov/dsg/external/freeware/mysql-vs-pgsql.html, 14.03.2005

COX Phil (2008), "Securing Virtual Environments", *2008 USENIX Annual Technical Conference*, Boston\MA-ABD.

ÇETİNKAYA, Mehtap (2008), *Bilgi Güvenliği Yönetim Sistemi Altyapısının Değerlendirilmesi Maksatlı Araç*, Basılmamış Yüksek Lisans Tezi, Bahçeşehir Üniversitesi Fen Bilimleri Enstitüsü

ÇETİNKAYA, Mehtap (2008), "Kurumlarda Bilgi Güvenliği Yönetim Sistemi'nin Uygulanması", *Çanakkale Onsekiz Mart Üniversitesi Akademik Bilişim 2008 Raporu*, s.511-516.

DİNÇKAN, Ali (2008), TUBİTAK-UEKAE Veri Yedekleme Kılavuzu

DİNÇKAN, Ali (2008), TUBİTAK-UEKAE İş Sürekliliği Yönetim Sistemi Kurulumu Eğitim Dökümanı

DOĞANTİMUR, Fatma (2009), *ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği*, Mesleki Yeterlik Tezi, T.C. Maliye Bakanlığı Strateji Geliştirme Daire Başkanlığı

DORUK, Alpay (2002), *Standards And Practices Necessary To Implement A Successful Security Review Program For Intrusion Management System*, Basılmamış Yüksek Lisans Tezi, İzmir Yüksek Teknoloji Enstitüsü Bilgisayar Mühendisliği Bölümü

DRUCKER, Peter (1994), *"Kapitalist Ötesi Toplum"*,Çev. Belkıs ÇORAKÇI, İnkılap Kitapevi, İstanbul.

DURMUŞ, Gürsoy (2008), Risk Analizi,www.tkgm.gov.tr/turkce/dosyalar/diger%5 Cicerikdetaydh275.pdf , 12.02.2010

"E-Devlete Geçişte Kamu Kurumları İnternet Siteleri", Sayıştay Dergisi (2006), Sayı 62

Elektronik İmza Kanunu (15/04/2004 Tarih ve 5070 Sayılı)

Elektronik Haberleşme Kanunu (05/11/2008 Tarih ve 5809 Sayılı)

Elektronik Haberleşme Güvenliği Yönetmeliği

ERGEN, Gökhan (2007), *Developing An Information Security Management Framework: Case Studies On Registration Office And Computer Center Of A State University*, Basılmamış Yüksek Lisans Tezi, Boğaziçi Üniversitesi Sosyal Bilimler Enstitüsü

ERKAN, Ahmet (2006), *An Automated Tool For İnformation Security Management System*, Basılmamış Yüksek Lisans Tezi, Orta Doğu Teknik Üniversitesi Enformatik Enstitüsü

ESKİYÖRÜK, Doğan (2007), TUBİTAK-UEKAE BGYS Risk Yönetim Süreci Kılavuzu

ESKİYÖRÜK, Doğan (2008), TUBİTAK-UEKAE Bilgi Sistemleri Kabul Edilebilir Kullanım Politikası Oluşturma Kılavuzu

FRISCH, Æleen (2008), "Beyond Shell Scripts: 21st-Century Automation Tools and Techniques", *2008 USENIX Annual Technical Conference*, Boston\MA-ABD.

GALVIN, Peter B. (2008), "Solaris 10 Security Features Workshop (Hands-on)", *2008 USENIX Annual Technical Conference*, Boston\MA-ABD.

"GNU felsefesi, lisanslama vs. sıkça sorulan sorular",http://www.belgeler.org/sss/sss-gnu.html, 19.02.2010

"GNU GPLv3 Lisansı (Türkçe)",http://www.phpbbturkiye.net/diger-f79/gnu-gplv3-turkce-t2235.html , 18.02.2010

"GNU GPL (Genel Kamu Lisansı) Sürüm 3 Gayriresmî Çevirisi",http://tr.pardus-wiki.org/GNU_GPL_(Genel_Kamu_Lisansı)_Sürüm_3_Gayrıresmî_Çevirisi 18.02.2010

HINSON, Gary (2003), "*Human factors in information security*", IsecT Ltd., Surrey\İngiltere

ISO/IEC JTC 1 SC 27 - IT Securıty Techniques Çalışma Grupları Tanıtım Dökümanı

İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkındaki 04/05/2007 Tarih ve 5156 Sayılı Kanun

İnternet Ortamında Yapılan Yayınların Düzenlenmesine Dair Usul ve Esaslar Hakkında Yönetmelik

İnternet Toplu Kullanım Sağlayıcıları Hakkında Yönetmelik

KAHRAMAN, Sunay (2006), *Yönetimde Bilgi Güvenlik Sisteminin Yapısı İşleyişi Ve Aselsan A.Ş.'De Uygulaması*, Basılmamış Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü

KARAARSLAN, Enis, A.Teke ve H.Şengonca (2006), "*Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması*", Ege Üniversitesi Uluslararası Bilgisayar Enstitüsü, Bilgisayar Mühendisliği Bölümü

KARABACAK, Bilge (2009) ; "Türkiye'de Bilişim Güvenliğiyle İlgili Yasal Altyapının Analizi", www.bilgiguvenligi.gov.tr

KOÇ, Fatih (2008), TUBİTAK-UEKAE BGYS Varlık Envanteri Oluşturma Ve sınıflandırma kılavuzu

MACİT, İrfan (2005), "Bilişim Nedir ?", Çukurova Üniversitesi Endüstri Mühendisliği Bölümü, http://www.mmf.cu.edu.tr/emb/index.html

NAİR, Güney (2001), "Bilgi'nin Değişen Anlamı Ve Kavram Tartışmaları", *C.Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi*, Cilt 2, Sayı 1, Ocak, s. 329-337.

OLSON, Ingrid M. ve Marshall D. Abrams (2006), "Information Security Policy", Editörler: ABRAMS M.D., JAJODİA S. ve PODELL H.J. *Information Security: An Integrated Collection of Essays*, IEEE Computer Society Press, s 160-169.

OSBORNE, Mark (2006), "*How to Cheat at Managing Information Security*", Syngress Publishing, Rockland\MA-ABD

OTTEKİN, Fikret (2008), TUBİTAK-UEKAE TS ISO/IEC 27001 Denetim Listesi Eğitim Dökümanı

ÖĞÜT, Pelin (2006), *Küreselleşen Dünyada Bilgi Güvenliğine Yönelik Politikalar: Sayısal İmza Teknolojisi Ve Türkiye*, Basılmamış Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü

ÖKMEN, Kemal (2007), Yazılım Telif Hakları Ve Özgür/Açık Kaynak Kodlu Yazılım Kavramları Ders Notu, Çanakkale Onsekiz Mart Üniversitesi Enformatik Bölümü

ÖNDER, Hulusi (2007), *A Security Management System Design*, Basılmamış Yüksek Lisans Tezi, Orta Doğu Teknik Üniversitesi Sosyal Bilimler Enstitüsü

ÖNEL, Dinçer ve A. Dinçkan (2007), TUBİTAK-UEKAE Bilgi Güvenliği Yönetim Sistemi Kurulumu Eğitim Dökümanı

ÖNEL, Dinçer (2007),TUBİTAK-UEKAE Erişim Kontrol Politikası Oluşturma Kılavuzu

ÖNEL, Dinçer (2008), TUBİTAK-UEKAE Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu

ÖZAKTAŞ Haldun ve M. Akgül (2005), "Bilim Camiası, Sivil Toplum ve Kamu, Açık Kaynak Kodlu Yazılımları Tercih Etmelidir", www.tuba.gov.tr , 20.02.2010.

ÖZTÜRK, Günce (2008), TUBİTAK-UEKAE Bilgi Güvenliği Politikası Oluşturma Kılavuzu

PELTIER, Thomas R. (2002), "*Information Security Policies, Procedures, and Standards*", Auerbach Publications, Boca Raton\FL-ABD

PELTIER, Thomas R. (2005), "*Information Security Risk Analysis*", Auerbach Publications, Boca Raton\FL-ABD

PERENDİ, Ünal (2008), TUBİTAK-UEKAE BGYS Kapsamı Belirleme Kılavuzu

PUTHUSEERİ, Vinod Kumar (2006), "ISMS Implementation Guide"

SAĞIROĞLU, Ş., E. Ersoy ve M. Alkan (2007), "Bilgi Güvenliğinin Kurumsal Bazda Uygulanması", *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, s. 200-207

STONEBURNER Gary, A. Goguen ve A. Feringa (2002), "Risk Management Guide for Information Technology Systems", NIST Special Publication 800-30

STRAUB, Detmar W., S. Goodman ve R.L. Baskerville (2008), "*Information Security Policy, Processes, And Practıces*", M.E. Sharpe, Inc., Armonk\NY-ABD

TBD (Türkiye Bilişim Derneği), (2006), "*Bilişim Sistemleri Güvenliği El Kitabı*", TBD Yayınları, Ankara

TBD (Türkiye Bilişim Derneği), (2006), "*Bilişim Teknolojilerinde Risk Yönetimi*", TBD Yayınları, Ankara

TBD (Türkiye Bilişim Derneği), (2006), "E-Devlet Uygulamalarında Güvenlik Ve Güvenilirlik Yaklaşımları", *4. Çalışma Grubu Sonuç Raporu*, Ankara

TBD (Türkiye Bilişim Derneği), (2008), "*Kuruluşlarda Bilgi Güvenliği Yönetim Sisteminin Uygulanmasında ISO/IEC 27001:2005*", TBD Yayınları, Ankara

Telekomünikasyon Kurumu Tarafından Erişim Sağlayıcılara ve Yer Sağlayıcılara Faaliyet Belgesi Verilmesine İlişkin Usul ve Esaslar Hakkında Yönetmelik

Türk Ceza Kanunu (26/09/2004 Tarih ve 5237 Sayılı)

Türk Standardları Enstitüsü, TS ISO/IEC 17799, Bilgi Teknolojisi-Bilgi Güvenligi Yönetimi İçin Uygulama Prensipleri. Ankara: 2002

Türk Standardları Enstitüsü, TS ISO/IEC 27001, Bilgi Teknolojisi, Güvenlik Teknikleri, Bilgi Güvenligi Yönetim Sistemleri, Gereksinimler, Ankara: 2006

VACCA, John (2009), "*Computer and Information Security Handbook*", Morgan Kaufmann Publishers, Burlington\MA-ABD

VURAL, Yılmaz ve Ş. Sağıroğlu (2007), "Kurumsal Bilgi Güvenliği: Güncel Gelişmeler", *Uluslararası Katılımlı Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, s. 191-199

VURAL, Yılmaz ve Ş. Sağıroğlu (2008), "Kurumsal Bilgi Güvenliği Ve Standartları Üzerine Bir İnceleme", *Gazi Üniversitesi Mimarlık ve Mühendislik Dergisi*, Yıl 23, Sayı 2, s. 507-522

WELLING Luke ve L. Thomson (2008), "*PHP ve MYSQL*", Çev., Belgin Eliçioğlu, Alfa Yayınları,İstanbul.

YILDIZ, Bünyamin (2007), *Bilgi Güvenliği Ve E-Devlet Kapsamında Kamu Kurumlarında Bilgi Güvenliği Yönetimi Standartlarının Uygulanması,* Basılmamış Yüksek Lisans Tezi, G.Y.T.E. Sosyal Bilimler Enstitüsü

ÖZGEÇMİŞ

Ufuk BİNGÖL, 04.11.1984 tarihinde Kütahya'da doğdu. İlkokulu Ankara Rauf Orbay İlköğretim Okulu'nda, ortaokulu Ankara Gölbaşı Anadolu Lisesi(Hazırlık,1995-1996) ve Erzurum Anadolu Lisesi'nde, liseyi Deniz Astsubay Hazırlama Okulu'nda tamamladı. 2002 yılında Deniz Kuvvetleri Komutanlığı adına Bilgi Sistemleri Uzmanı (OBİ Astsubayı) yetiştirilmek üzere Kara Kuvvetleri Komutanlığı Muhabere Elektronik Bilgi Sistemleri Okulu ve Eğitim Merkezi Komutanlığında başladığı Sınıf Okulu Eğitimini 2003 yılında bölüm birincisi olarak tamamladı. 2004 yılında Anadolu Üniversitesi İktisat Fakültesi Kamu Yönetimi bölümünde başladığı lisans öğrenimini 2008 yılında tamamladı. 2008 yılında Sakarya Üniversitesi, Sosyal Bilimler Enstitüsü, Çalışma Ekonomisi ve Endüstriyel İlişkiler Anabilim dalı, İnsan Kaynakları Yönetimi ve Endüstriyel İlişkiler Bölümünde yüksek lisans eğitimine başlayan Ufuk BİNGÖL evli olup halen Deniz Kuvvetleri Komutanlığında Bilgi Sistem Uzmanı Astsubay olarak görev yapmaktadır.