İSTANBUL KÜLTÜR ÜNİVERSİTESİ★FEN BILIMLERI ENSTITÜSÜ

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ ALTYAPISININ DEĞERLENDİRİLMESİ İÇİN BİR TEST ARACI GELİŞTİRİLMESİ

YÜKSEK LİSANS TEZİ

Mehtap ÇETİNKAYA

Anabilim Dalı: Fen Bilimleri Enstitüsü

Programı: Bilgisayar Mühendisliği

Tez Danışmanı: Yrd. Doç. Dr. Orhan GÖKÇÖL

EYLÜL 2008

TEŞEKKÜRLER

Değerli yardımlarından dolayı, Yrd. Doç. Dr. Orhan GÖKÇÖL'e, Bilgi Güvenliği alanında çalışmam için imkan sağlayan ve desteğini her zaman hissettiğim, Murat LOSTAR'a, eğitim hayatıma önemli katkıları olan Kültür Üniversitesi ve Kültür Okulları kurucusu Akıngüç Ailesi'ne ve Dr. Bahar Akıngüç Günver'e, kıymetli hocam Sayın Erdoğan YILMAZ'a, anket çalışmaları sırasında destek veren tüm arkadaşlarıma ve kurum/şirketlere, maddi ve manevi destekleri ve sonsuz sevgileriyle her zaman yanımda olan aileme, varlığıyla hayatıma anlam katan sevgili Özgür'e sonsuz teşekkürlerimi bir borç bilirim.

İÇİNDEKİLER

KISALTMALAR

BGYS : Bilgi Güvenliği Yönetim Sistemi

BSI : İngiliz Standartlar Enstirüsü (British Standards Institute)

BT : Bilgi Teknolojileri

COBIT : Bilgi Sistemleri Denetim ve Kontrol Birliği (Control Objectives for Information and Related Technology)

DoD : A.B.D. Savunma Bakanlığı (US Department of Defense)

EPL : Ürün Değerlendirme Listesi (Evaluation Product List)

FTP : Dosya Aktarım Protokolü (File Transfer Protocol)

GWS : Google Web Server

IEC : Elektrik Sistemleri Uluslararası Konseyi (International Electrotechnical Commission)

ISACF : Bilgi Sistemleri Denetim ve Kontrol Kurumu (Information System Audit and Control Foundation)

ISO : Uluslararası Standartlar Teşkilatı (International Organization for Standardization)

ITIL : Bilgi Teknolojisi Altyapı Kütüphanesi (Information Technology Infrastructure Library)

PHP : Sunucu uygulamaları geliştirme dili (Personal Home Page)

PUKÖ : Planla – Uygula – Kontrol et – Önlem al

TPEP : Güvenilir Ürün Değerlendirme Programı (Trusted Product Evaluation Program)

TSE : Türk Standartları Enstitüsü

TABLO LİSTESİ

ŞEKİL LİSTESİ

ABSTRACT

In this work a web tool has been developed to detect how a company successfully implement the information security principles. The tool uses the security management principles defined in the ISO/IEC 27001:2007. The development language for the tool is PHP and data collected is stored in a database which is developed in MySQL. Open source instruments have been choosen because of their extensive support and usage.

The web tool collects data about the company and its IT infrastructure, then throughout an inventory, it explores the strong and weak sides of the company in terms of ISO27001 based information security principles. The tool then generates a report showing the status of the company with some advices and numerical indicators showing how that company successfully implements the information security principles. ISO/IEC 27001 divides all of the areas of the information security management into eleven sub-topics which are called as "security areas". The current test tool produces ISO/IEC 27001 compatible evaluation reports and gives a measure on how successful the company's implementation is.

Since the tool collects company information as well as the information security inventory results it is, as a priori, an invaluable instrument to findout the nation-wide information security practices all over the Turkey. It has a basic management interface with which a backoffice user (i.e. admin) can manage the system. The inventory questions and answers and security main categories can be modified throughout a web interface. Additionally, the stored inventories and company information can be listed and searched a great detail.

The tool is tested through the companies which already have a security management system. The test results show that it successfully handles the security and gives correct results. The web tool then applied to 22 companies from different sectors and data were collected and presented.

Keywords – *Information Security, Information Security Management System, ISO 27001*

ÖZET

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

Web tabanlı olarak hazırlanan çevrim içi (online) anket şeklindeki bir envanter sistemi yardımıyla toplanan bilgiler ISO/IEC 27001 ölçütleri çerçevesinde değerlendirilerek, envanteri dolduran kurumun/şirketin (hem kurumsal, hem de her bir çalışanı bazında bireysel) bilgi güvenliği altyapısı ile ilgili çıkarımlarda bulunulmuştur. Ayrıca, sektörel bazda istatistiksel çıkarımlar da yapılarak, ülkemizdeki durumun kendi içinde ve dünyadaki diğer örnekleriyle karşılaştırılması hedeflenmiştir.

Çalışma, "Bilgi Güvenliği Yönetim Sistemi"nin kurum içindeki süreçlere katkısını da ortaya çıkartmaktadır. Çalışmanın son ürünü, Bilgi Güvenliği Yönetim Sistemi altyapısını değerlendirip, raporlayan bir test aracıdır (yazılım sistemi). Bu sistem, aynı zamanda, kendi içinde temel bir yönetim modülüne de sahiptir. Böylece, envanter soruları, yorumlar, bilgi güvenliği temel alanları gibi unsurlar kolayca değiştirilebilir ve yenileri eklenebilir. Envanteri dolduran firmalarla ilgili tüm bilgiler ve envanter yanıtları tüm detayları ile raporlanAbilir.

Bu araç, bilgi güvenliği yönetim sistemini oluşturmuş firmalarla test edilmiş ve güvenilirliği kanıtlanmıştır. Daha sonra, farklı sektörlerden 22 firmaya uygulanmış ve elde edilen sonuçlar listelenmiştir.

Anahtar Kelimeler – *Bilgi Güvenliği, Bilgi Güvenliği Yönetim Sistemi, ISO 27001*

1 GİRİŞ

1.1 Problem Tanımı

Günümüzde kurumlar ve şirketlerde, teknolojik yatırımlara ağırlık verilip, bilgi üretimi ve kullanımında Bilgi Güvenliği'nin sağlanması gibi önemli bir sürecin gözden kaçırıldığı görülmektedir. Genelde, Bilgi Güvenliği, donanım ve yazılım ile sağlanan çözümlerle sağlanmakta ve bunun etkinliği ölçülmemektedir. Bu tez çalışması kapsamında, "Bilgi Güvenliği Yönetim Sistemi" standardı ile tanımlanan "Bilgi Güvenliği" ile ilgili ölçütlerin, ülkemizde kurum/ şirketlerde nasıl karşılandığı ile ilgili web tabanlı bir değerlendirme yazılımı, açık kaynak kodlu araçlar kullanılarak oluşturulmuştur.

Çalışmada izlenen yöntem şu şekildedir :

- ISO/IEC 27001 BGYS irdelenmesi
- Bilgi Güvenliği ölçütlerinin tespit edilmesi
- Envanter hazırlanması
    - Envanter sorularının kontrolü, ölçütleri kapsayıp kapsamadığının belirlenmesi
- Test aracı veri toplama sisteminin geliştirilmesi
    - Envanter veri tabanının geliştirilmesi
    - Web uygulamasının ve arayüzlerin geliştirilmesi
    - Çevrim içi envanter sisteminin uygulamaya eklenmesi
- Test aracı veri değerlendirme uygulamasının geliştirilmesi
- Test aracı raporlama sisteminin geliştirilmesi
- Uygulama

1.2 Bilgi Güvenliği ile İlgili Standartlar

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

Tarihsel evrimi içinde bilgi sistemlerinin güvenliği ve sonrasında Bilgi Güvenliği konusunda pek çok akademik araştırma yapılmış, makaleler yayınlanmış ve ticari ürünler ortaya çıkartılmıştır.

Bilgisayar sistemlerinin güvenliği konusunda yapılan ilk çalışmaların IBM ve A.B.D. Savunma Bakanlığı (US Department of Defense –DoD-) kaynaklı olduğu görülmektedir. 1981 yılında Adalet Bakanlığı (Department of Defense, DoD) National Security Agency'e bilgisayar güvenliğinin sorumluluğunu verdi ve DoD Computer Security Center kuruldu, daha sonra ismi değiştirilerek NCSC (National Computer Security Center) oldu. NCSC daha sonra "Orange Book" olarak ta bilinen ilk DoD Trusted Computer System Evaluation Criteria (TCSEC) kriterini yayınladı. 1985'te DoS Standart (DOD 5200.28-STD) adı altında tekrar yayınlanarak TCSEC kriterinin temelini oluşturmuştur. TCSEC standartı güvenliğin gittikçe arttığı bir sınıflandırma yapısına sahiptir. Her seviye, hem bir önceki seviyenin güvenlik seviyesine hemde bazı ek özelliklere sahiptir [20, 21, 22,32].

İşte üreticilerin ürünleri bu TCSEC kriteri çerçevesinde Trusted Product Evaluation Program (TPEP) programıyla sınıflandırılır ve belli sınıf kodlarını alırlar. TPEP programıyla test edilen ve sonuçlanan ürünler EPL (Evaluation Product List) listesinde yayınlanırlar. TPEP programının ana amacı daha fazla güvenli bilgisayar ürününün geliştirilmesini teşvik etmektir.

DoD çalışmaları daha sonra Bilgi Güvenliği'nin daha fazla ön plana çıktığı 1990'larda, çeşitli firma temelli ya da uluslararası standartlar şekline gelmiştir [20, 21, 22,32].

İngiltere Standartlar Enstitüsü'nün (British Standards Institute (BSI)) yaptığı çalışmalarla, "Bilgi Güvenliği Yönetim Sistemi" deyimi ilk kez 1998 yılında tarafından yayınlanan BS 7799-2 standardında kullanılmıştır. Daha sonra bu standart Uluslararası Standartlar Kurumu ISO tarafından kabul edilmiş ve ISO/IEC 27001:2005* olarak yayınlanmıştır. BSI tarafından yayınlanan bir diğer standart BS 7799-1 ise Bilgi Güvenliği'nin sağlanmasında kullanılacak kontrollerden bahsetmektedir. Bu da yine ISO tarafından kabul edilmiş ve ISO/IEC 27002:2005 olarak yayınlanmıştır. ISO/IEC 27002:2005 bu standardın Temmuz 2007'den itibaren kullanılan ismidir, bu tarihe kadar standart ISO/IEC 17799:2005 olarak adlandırılıyordu. Bilgi güvenliği yönetimi konusunda en yaygın olarak kullanılan standart, "ISO/IEC 27002:2005 Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri" standardıdır. Bu standart, işletmeler içerisinde Bilgi Güvenliği yönetimini başlatmak, gerçekleştirmek, sürdürmek ve iyileştirmek için genel prensipleri ve yönlendirici bilgileri ortaya koyar. ISO/IEC 27002:2005 rehber edinilerek kurulan BGYS'nin belgelendirmesi için "ISO/IEC 27001:2005 Bilgi Güvenliği Yönetim Sistemleri – Gereksinimler" standardı kullanılmaktadır. Bu standart, dokümante edilmiş bir BGYS'ni kurumun tüm iş riskleri bağlamında kurmak, gerçekleştirmek, izlemek, gözden geçirmek, sürdürmek ve iyileştirmek için gereksinimleri kapsamaktadır. İş risklerini karşılamak amacıyla ISO/IEC 27002:2005'te ortaya konan kontrol hedeflerinin kurum içerisinde nasıl uygulanacağı ve denetleneceği ISO/IEC 27001:2005'te belirlenmektedir [35].

Her iki standardın Türkçe hali TSE tarafından sırasıyla TS ISO/IEC 17799:2005 ve TSISO/IEC 27001:2005 isimleri ile yayınlanmıştır. Söz konusu standardın belgelendirmesi konusunda TSE tarafından "TS 13268-1 BGYS Belgelendirmesi İçin Gereksinimler ve Hazırlık Kılavuzu" yayınlanmıştır. ISO/IEC 27001 ve ISO/IEC 27002 standartları BGYS konusunda en temel başvuru kaynaklarıdır. Bu iki standart doğrudan Bilgi Güvenliği konusunu ele alırlar. Teknik ve teknoloji bağımlı standartlar değildirler.

Belli bir ürün veya bilgi teknolojisi ile ilgilenmezler. Hatta bilgi teknolojileri güvenliği dahi bu standartların içerisinde yer almaz. Tek ilgi alanı vardır, o da Bilgi Güvenliği'dir.

Diğer taraftan geliştirilmiş başka standart ve metodojilerde olmuştur. Bunlardan biri de "Control Objectives for Information and Related Technology – COBIT"dir. COBIT, bilgi teknolojileri süreçlerini iş süreçlerinin destekçisi olarak görür ve aralarındaki ilişkileri birebir ortaya koyar. Bu sayede bilgi teknolojileri kaynaklarının iş stratejileri doğrultusunda etkin biçimde kullanılmasına olanak sağlar.

COBIT ilk olarak 1996 yılında Information System Audit and Control Foundation (ISACF) tarafından yayımlanmıştır. Bu metodoloji birçok standardı içinde barındırdığı ve diğer metodolojilerle uyum içinde olduğundan şirketlerin ilişki içinde oldukları iş ortakları, müşteri ve düzenleyici kurumlar tarafından talep edilen bilgi teknolojileri kontrol süreçleri sertifikasyonları denetimlerine hazır olmaya yardımcı olur ve böylece hızlı bir sertifikasyona olanak sağlar [29, 30].

Bir diğer yönetim metodolojisi, "Information Technology Infrastructure Library-ITIL"dir. ITIL, BT servislerini eksiksiz ve en iyi kalitede yönetmek üzere geliştirilmiş servis yönetim metodolojisidir. ITIL, 1987'de İngiltere Ticaret Bakanlığı tarafından geliştirilmiştir. İş süreç yaklaşımı sayesinde ITIL, müşteri, tedarikçi, BT bölümü ve kullanıcıları arasında başarılı bir şekilde iletişim kurulmasını sağlamaktadır. "En iyi uygulamalar / deneyimler" üzerine yapılandırılmış olan ITIL, BT Servis Yönetimi ve dağıtımı süreçleri ile dünyada yaygın olarak kullanılmakta ve kabul görmüş bir standart olarak benimsenmektedir [31]. ITIL, BT servislerini yönetmede ayrıntılı ve yapısal en iyi uygulama örnekleri serisidir

Bir başka standart olan ISO 20000 - BT Hizmet Yönetim Sistemi, hizmet kalitesinin artması, güvenilir kurumsal destek, hizmetler hakkında daha net veriler elde edilmesi, çalışanların işdeki başarısının doğru analiz edilmesi, müşteriler memnuniyeti, doğru hizmet sunulması, hizmet süreçlerinin güvenliğinin sağlanması ve sürekli erişim gibi bir çok faydalar sağlayabilen bir sistemdir [18, 33, 34].

1.3 Tez Yol Haritası

Bu tez çalışmasının birinci bölümünde BGYS tanımlanmış ve çalışmaya konu olan problem hakkında bilgi verilmiştir. Ayrıca, Bilgi Güvenliği konusunda yapılmış standartlardan örnekler sunulmuştur. Tezin ikinci kısmında Bilgi Güvenliği, Bilgi Güvenliği Yönetim Sistemi ve Bilgi Güvenliği yönetiminde bilgisayar destekli modellerin kullanımı anlatılmıştır. Üçüncü kısımda ise, Bilgi Güvenliği Yönetim Sisteminin değerlendirilmesi için geliştirilen modelden bahsedilmiştir. Dördüncü kısımda uygulama detayları ve test aracının alt yapısı ve kullanımına yönelik bilgiler verilmiş, son kısımda sonuçlar değerlendirilerek, gelecekte yapılabilecek çalışmalara yer verilmiştir.

2 BİLGİ GÜVENLİĞİ VE YÖNETİMİ

2.1 Bilgi Güvenliği

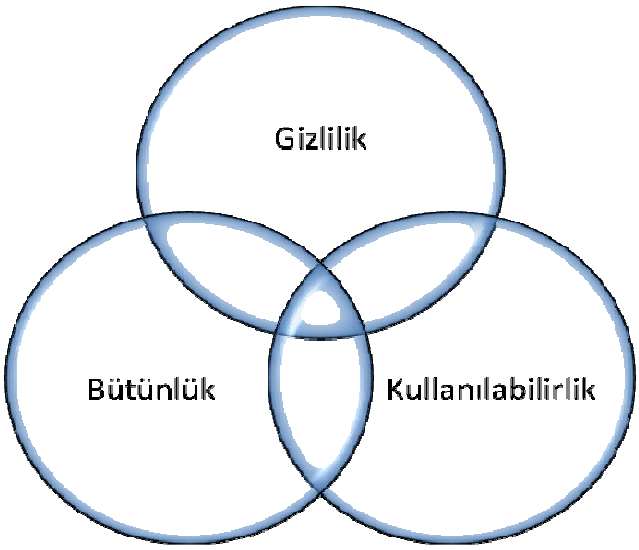
Bilgi, tarih boyunca insanoğlunun düşüncesini, yaşayışını, davranışşnı, gelişimini belirleyen faktörlerin başında gelen büyük bir güç olarak yerini korumuştur. Bilişim teknolojilerinin hızla yaygınlaşmasıyla bilginin yönetilmesi, iş verimliliğinin ve akışlarının hızlandırılması, çalışanlar ve diğer kurumlarla daha hızlı iletişim kurulabilmesi sağlanmış, hayatı kolaylaştırmış, üretilen ve tüketilen bilgilerde de artışlar olmustur. Bunun sonucu olarak, elektronik ortamlarda bilginin işlenmesi, taşınması ve saklanması kolaylaşmış, bilgiye mekandan bağımsız olarak istenilen ortamlardan erişilmesi sağlanmıştır. Günlük yaşantımızda yapmış olduğumuz birçok iş ve işlem ise kolaylıkla ve hızlıca yapılabilir hale gelmiştir [6, 7, 8, 17].

Bilgi, her varlık gibi kurumun bir varlığıdır ve her varlık gibi parasal bir değeri vardır. Fiziksel veya elektronik ortamda bulunan bilginin risklere karşı korunması gerekmektedir. Bilgi Güvenliği kurumun rekabetçi gücünün korunması, para akışının sürekli kılınması, karlılığın artırılması, yasal uyumluluğun sağlanması ve kurumsal imajın zedelenmemesi için gereklidir. Bilgi iletişim ağları genellikle güvenlik değil, işlevsellik göz önünde bulundurularak tasarlanmıştır [12, 2]. Gittikçe daha fazla iş fonksiyonunun bu güvensiz ortamlarda yürüyor olması güvenliğe ihtiyacı artırmaktadır.

Bilgi Güvenliği, kurumların bilgi envanterindeki varlıkların gizliliğini, bütünlüğünü, erişilebilirliğini/kullanılabilirliğini tehdit eden risklerin tanımlanıp, bu konuda risk yönetimi gereklerinin yapılması ve bilgi değerlerini izinsiz erişim, ifşa ve kötüye kullanma, değiştirilme veya zarar ve kayıptan korumak üzere kullanılan işlem ve teknolojilerin toplamıdır [7, 15].

Bilgi Güvenliği'ne olan ihtiyacın neden ortaya çıktığını anlamak için zamanında ve doğru olarak bilgi almanın önemini anlamak gereklidir. Bilgi Güvenliği'nin temel amacı doğru kişinin kısa zamanda doğruluğundan emin olunan bilgiye ulaşımını garanti altına almaktır [25, 26, 27, 28].

Buna göre Bilgi Güvenliği konuları incelenirken, Şekil-2.1'de yer aldığı gibi üç temel bakış açısından ele alınır:



Şekil 2.1: Gizlilik – Bütünlük - Kullanılabilirlik

Gizlilik: Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır (Örneğin; şifreli e-posta gönderimi ile e-postanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir)[3].

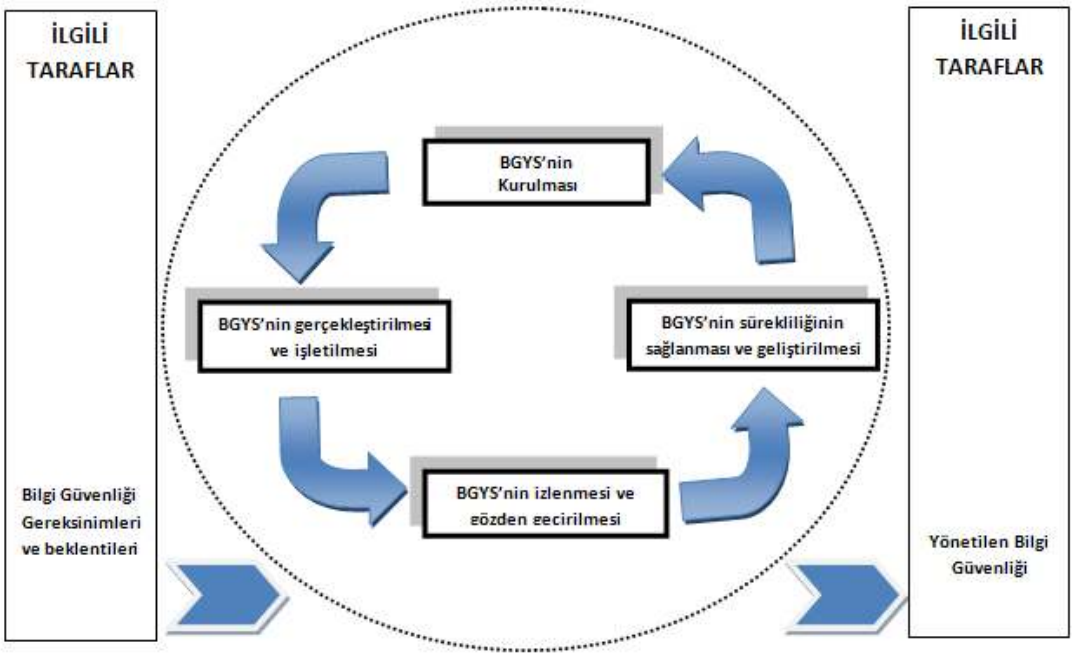
Bütünlük: Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler, çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır (Örneğin; veri tabanında saklanan verilerin özet bilgileri ile birlikte saklanması, dijital imza gibi).

Erişilebilirlik/Kullanılabilirlik: Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Diğer bir ifade ile sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır (Örneğin; sunucuların güç hattı dalgalanmalarından ve güç kesintilerinden etkilenmemesi için kesintisiz güç kaynağı kullanımı gibi).

2.2 Bilgi Güvenliği Yönetimi

Bilgi Güvenliği Yönetim Sistemi (BGYS), kurumun hassas bilgilerini yönetebilmek amacıyla benimsenen sistematik bir yaklaşımdır. Bu sistemin temel amacı hassas bilginin korunmasıdır. Bu sistem çalışanları, iş süreçlerini ve bilgi teknolojileri (BT) sistemlerini kapsar [19]. Geçmiste emek, sermaye ve dogal varlıklar gibi temel üretim faktörlerini yönetmek durumunda olan yöneticiler, günümüzde üretimin temel faktörü durumuna gelen bilgiyi yönetmek durumundadırlar [16]

BGYS standartları kapsamında BGYS'in kurulumu, gerçeklenmesi, işletilmesi, izlenmesi, gözden geçirilmesi, sürdürülmesi ve tekrar gözden geçirilmesi için Şekil 2.2'deki PUKÖ döngüsü (Planla – Uygula – Kontrol et – Önlem al) kullanılmaktadır. PUKÖ döngüsüne ait açıklamaların yer aldığı Tablo 2.1'deki gibi, bu döngüde bir BGYS'nin bilgi güvenliği gereksinimlerini ve ilgili tarafların beklentilerini girdi olarak nasıl aldığını ve gerekli eylem ve işlemler aracılığıyla, bu gereksinimleri ve beklentileri karşılayacak Bilgi Güvenliği sonuçlarını nasıl üretildiği gösterilir [19, 23].



Şekil 2.2: PUKÖ Döngüsü

Tablo 2.1: Planla – Uygula – Kontrol Et – Önlem Al (PUKÖ) Döngüsü

P	**PLANLA** (BGYS'nin Kurulması)	BGYS politikası, amaçlar, hedefler, süreçler ve prosedürlerin geliştirilmesi
U	**UYGULA** **(**BGYS'nin gerçekleştirilmesi ve işletilmesi)	BGYS politikası, kontroller, süreçler ve prosedürlerin gerçekleştirilip işletilmesi
K	**KONTROL ET** (BGYS'nin izlenmesi ve gözden geçirilmesi)	BGYS politikası, amaçlar ve süreç performansının değerlendirilmesi, uygulanabilen yerlerde ölçülmesi ve sonuçların rapor edilmesi
Ö	**ÖNLEM AL** (BGYS'nin sürekliliğinin sağlanması ve iyileştirilmesi)	Yönetimin gözden geçirme sonuçlarına dayalı olarak, düzeltici ve öneleyici faaliyetlerin gerçekleştirilmesi

Bilgi güvenliği yönetimi, başlangıç ve bitiş tarihleri olan bir proje gibi görülmemelidir. Sürekli devam eden bir gelişim süreci olarak düşünülmelidir. PUKÖ döngüsünde gösterildiği gibi faaliyetleri bir döngü içinde durmaksızın sürekli devam etmelidir. PUKÖ döngüsü özet olarak ne yapılacağına karar verilmesi, kararların gerçekleştirilmesi, çalıştığının kontrol edilmesi hedefine uygun çalışmayan kontroller için önlemlerin alınmasıdır [19, 23, 24].

BGYS kurulumu PUKÖ modelinin ilk adımını (Planla) teşkil etmektedir. Yerleşik bir sistemden bahsedebilmek için diğer adımların da uygulanması ve bunların bir döngü içinde yaşaması gerekir. ISO 27001 Bilgi Güvenliği Sistemi kurma aşamaları aşağıdaki gibidir :

• Varlıkların sınıflandırılması
• Gizlilik, bütünlük ve erişebilirlik kriterlerine göre varlıkların değerlendirilmesi
• Risk analizi
• Risk analizi çıktılarına göre uygulanacak kontrolleri belirleme
• Dokümantasyon oluşturma
• Kontrolleri uygulama
• İç tetkik
• Kayıtları tutma
• Yönetimin gözden geçirmesi
• Belgelendirme

BGYS, günümüz iş dünyasında vazgeçilmez hale gelen Bilgi Güvenliği konusunda tüm dünya tarafından kabul görmüş standartlara uygun bir yapı sunmaktadır. BGYS kavramının ve bağlı olduğu standartların doğru anlaşılması bu yapının sağlayacağı faydayı önemli ölçüde arttıracaktır [23].

Bilgi Güvenliği ISO/IEC 27001:2007 EK-A içinde de yer alan aşağıdaki başlıklar içinde şirket ya da kurumun Bilgi Güvenliğini sağlamaya yönelik çalışır.

- Güvenlik politikası
- Bilgi güvenliği organizasyonu
- Varlık yönetimi
- İnsan kaynakları güvenliği
- Fiziksel ve çevresel güvenlik
- Haberleşme ve işletim yönetimi
- Erişim kontrolü
- Bilgi sistemleri edinim, geliştirme ve bakımı
- Bilgi güvenliği ihlal olayı yönetimi
- İş sürekliliği yönetimi
- Uyum

BGYS kurulumunu fazladan bir iş yükü ve gereksiz zaman kaybı olarak görmenin baştan kaybetmek anlamına geleceği bilinmelidir. Bu sistemin vaat ettiklerine ulaşmak için yönetimlere büyük görev ve sorumluluklar düşmektedir.

Kurum/şirktlerde risk analizleri yapılırken çoğunlukla karşılaşılan riskler:

- Yazılımlar için uygulama geliştirme ve test ortamlarının ayrı olarak bulunmaması, canlı sistemle birlikte olması ,
- Bilgi güvenliği sorumluluklarının atanmamış olması,
- Varlık envanteri eksiklikleri,
- Güvenlik olaylarını, zayıflıklarını ve yazılım arızalarını raporlama süreçlerinin olmaması,
- Personel eksikliği,
- Personel eksikliğine bağlı olarak görevlerin ayrılığı prensibinin uygulanamamasıdır.

Kurumların bilgi sistemleri, internet'e bağlı olmanın getirdiği güvenlik risklerine karşı koruma sağlayacak şekilde tasarlanmalı ve yapılandırılmalıdır [9, 10, 11, 12, 14].

2.3 Bilgi Güvenliği Yönetiminde Bilgisayar Destekli Modellerin Kullanımı

Bilgi Güvenliği yönetimi ile ilgili standartlar, firmaların bu alanda atacağı adımları kolaylaştırırken aynı zamanda da kurum/şirket içinde yapılan uygulamaların standarda göre ne başarılılıkta uygulandığının bilinmesi gerekliliğini de beraberinde getirir. Bu noktada "Fark Çözümlemesi (GAP Analizi)" olarak adlandırılan bazı bilgisayar destekli modellerin ve analitik araçların kullanımı Bilgi Güvenliği başarısının ölçülmesinde önem kazanmaktadır. Bu tip araçlar, daha çok ilgili standard uygulayan kurum/şirketlerce kullanılmakta, ancak belli bir standarda bağlı kalmayan ama bilgi güvenliği konusunda bazı şeyler yapan kurum/şirketlere uygulamada zorluklarla karşılaşılabilmektedir.

Ülkemizde yapılan yüksek lisans tezlerinden birinde [4], "Bilgi Güvenliği Yönetim Sistemi" belgelendirilmesinde, firmalara yardımcı olacak ve standardın maddelerinin dökümante edilmesini sağlayan otomatik bir araç (yazılım sistemi) geliştirilmiştir. Bu çalışma, standardın uygulanma adımlarını kolaylaştırmakta ancak standardın hangi başarımda uygulandığını vermemektedir. Ayrıca, BGYS kurmamış firmalara uygulanması da pratik bazı zorluklar getirmektedir.

ISO27001 gibi standartları uygulamak ve uyumlu bir BGYS kurmak parasal açıdan da firmalara (özellikle "KOBİ"lere) ciddi bir yük getirmektedir. İşletmelerin, Bilgi Güvenliği altyapısını ISO27001 uyumlu olarak değerlendiren, buna göre önerilerde bulunan bir araca gereksinim olduğu açıktır ve bu çalışmada böyle bir araç geliştirilmiştir.

3 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİNİN DEĞERLENDİRİLMESİ İÇİN BİR MODEL

3.1 Geliştirme Araçları

Web uygulamaları PHP 5.1 ile geliştirilmiştir. Veritabanı, MySQL kullanılarak ilişkisel bir mimaride tasarımlanmıştır. Geliştirilen yazılım sistemi bir Unix platformunda (FreeBSD) ve Apache web sunucusu ile çalışmaktadır. Hem FreeBSD hem de Apache; yüksek performans, güvenlik, açık kaynak kodlu olmaları, endüstri standard olarak geniş bir kullanım oranına sahip bulunmaları sebebiyle tercih edilmiştir.

3.1.1 PHP

PHP, çoğunlukla dinamik ve interaktif web sayfaları oluşturmak için kullanılan sunucu taraflı bir programlama dilidir. Dil yazım kuralları açısından C ve Perl'e benzer. Çoğu işletim sistemi ve web sunucusu ile birlikte kullanılabilir. PHP, "**P**HP: **H**ypertext **P**reprocessor" anlamına gelen özyineli bir tanımdır. Eski haliyle **P**ersonal **H**ome **P**ages olan PHP, 1993 yılında Rasmus Lerdorf tarafından geliştirilmeye başlamıştır. Daha çok dinamik web içeriği oluşturmak için kullanılan PHP, son zamanlarda, IBM, Oracle ve Zend'in girişimleriyle kurumsal yazılım geliştirme platformu haline getirmeye çalışılmaktadır. 2007 senesinin Kasım ayı itibarıyla tüm dünya çapında 30 milyondan daha fazla alanda kullanılmakta ve bu sayı giderek artmaktadır. 2005 yılı itibariyle **PHP 5** sürümü geliştirilmiş durumdadır. PHP dili, Linux gibi Açık Kaynak Kodlu bir dil olup ücretsiz olarak dağıtılmakta ve geliştirilmektedir.

PHP dosyaları, temel olarak web sunucusunda yer alan metin dosyalarıdır. Web sunucusundan uzantısı *.php olan dosyalar çağrıldığında önce içindeki PHP komutlarını çalıştırır ve HTML'e dönüştürür. Oluşturulan HTML kodlarıda isteği gönderen kullanıcıya web sunucusu aracılığıyla iletilir. PHP derleyicisi dosyadaki

<? ?>

ya da

<?php ?>

etiketlerine rastlayana kadar tüm HTML kodlarını web sunucusuna olduğu gibi gönderir. PHP kodlarının başladığını ve bittiğini belirten etiketler arasındaki komutları işler ve daha sonra web sunucusuna gönderir. PHP kodlarının sonucu düz metin ya da HTML kodları olabilir. PHP'nin en güzel yanlarından biri de PHP ve HTML kodlarının aynı dosyada kullanılabilmesidir.

PHP dil kuralları C programlama dili ile çok benzerlik gösterir. Temel farklar sıralanmak istenirse :

- Tüm değişkenler $ karakteri ile başlar.
- Tüm değişkenler "karakter katarı"dır. Bu haliyle PHP değişken tipini kendi otomatik olarak bulur.
- Farklı veritabanı sistemleri ile çalışabilmek için kendi içinde hazır fonksiyonlar barındırır.
- Web formlarından bilgi almak ve HTML çıktı üretmek için bazı fonksiyonları vardır.

3.1.2 MySQL

MySQL, altı milyondan fazla sistemde yüklü bulunan çoklu iş parçacıklı (multi-threaded), çok kullanıcılı (multi-user), hızlı ve sağlam (robust) bir veritabanı yönetim sistemidir.

UNIX ve Windows'un da dahil olduğu pek çok işletim sistemi için ücretsiz dağıtılmakla birlikte ticari lisans kullanmak isteyenler için de ücretli bir lisans seçeneği de mevcuttur. Linux altında daha hızlı bir performans sergilemektedir. Kaynak kodu açık olan

MySQL'in pek çok platform için çalıştırılabilir ikilik kod halindeki indirilebilir sürümleri de mevcuttur. Ayrıca ODBC sürücüleri de bulunduğu için birçok geliştirme platformunda rahatlıkla kullanılabilmektedir. MySQL, özellikle kendi önbellek sistemiyle, tablolardan bilgi çekme performansı açısından diğer veritabanı yönetim sistemlerine göre daha hızlıdır.

3.1.3 Apache

Apache, açık kaynak kodlu bir web sunucusu programıdır. Windows ve UNIX türevleri dahil bütün işletim sistemlerinde çalışabilir. Genelde her ay yenilenerek yeni sürümleri dağıtılmaktadır. World Wide Web'in genişlemesinde ve yayılmasında anahtar rol oynamıştır. Nisan 1996'dan bugüne Apache İnternet'teki en yaygın web sunucusu olmuştur. Haziran 2008 itibarıyla Netcraft 'ın 172,338,726 web sitesinden bilgi toplayarak yaptığı araştırmaya göre İnternet'teki sitelerin yüzde %49.12'si Apache kullanmaktadır. Google 'ın kendi web sunucusu olan GWS ("Google Web Server") 'ın da geliştirilerek derlenmiş bir Apache olduğu doğrulanmıştır

3.1.4 FreeBSD

FreeBSD x86 Uyumlu, AMD64, IA-64, PC-98 ve UltraSPARC® mimarileri için ileri seviye bir işletim sistemidir. Berkeley'deki Kaliforniya Üniversitesi'nde geliştirilmiş UNIX türevi olan BSD'yi temel almıştır. **FreeBSD** birçok kişi tarafından geliştirilmekte ve devam ettirilmektedir. Ayrıca başka mimariler için geliştirim değişik aşamalardadır. **FreeBSD** ileri seviyede ağ, performans, güvenlik ve uyumluluk özellikleri sunar. Bu özellikler ticari olan bazı işletim sistemlerinde bile bulunmamaktadır. Ayrıca, KDE ve GNOME pencere yöneticileriyle ve ücretsiz ofis uygulamalarıyla son kullanıcı için de uygun bir işletim sistemidir.

3.2 Test Aracı Geliştirilmesi

Test aracı, 11 temel Bilgi Güvenliği alanında işletmelerdeki uygulamaları ortaya çıkartmak için toplam 33 soru barındıran bir envantere sahiptir. Ayrıca, 4 tane de kontrol sorusu sorularak, envanter cevaplarının tutarlılığı sınanmış ve kontrol sorularına hatalı

cevap veren işletmeler için bir "uyarı mesajı" verilmesi sağlanmıştır. 11 temel bilgi güvenliği alanı şunlardır :

- A.5: Güvenlik Politikası
- A.6: Bilgi Güvenliği Organizasyonu
- A.7: Varlık Yönetimi
- A.8: İnsan Kaynakları Güvenliği
- A.9: Fiziksel ve Çevresel Güvenlik
- A.10: Haberleşme ve İşletim Yönetimi
- A.11: Erişim Kontrolü
- A.12: Bilgi Sistemleri Edinim, geliştirme ve bakımı
- A.13: Bilgi Güvenliği İhlal Olayı Yönetimi
- A.14: İş Sürekliliği Yönetimi
- A.15: Uyum

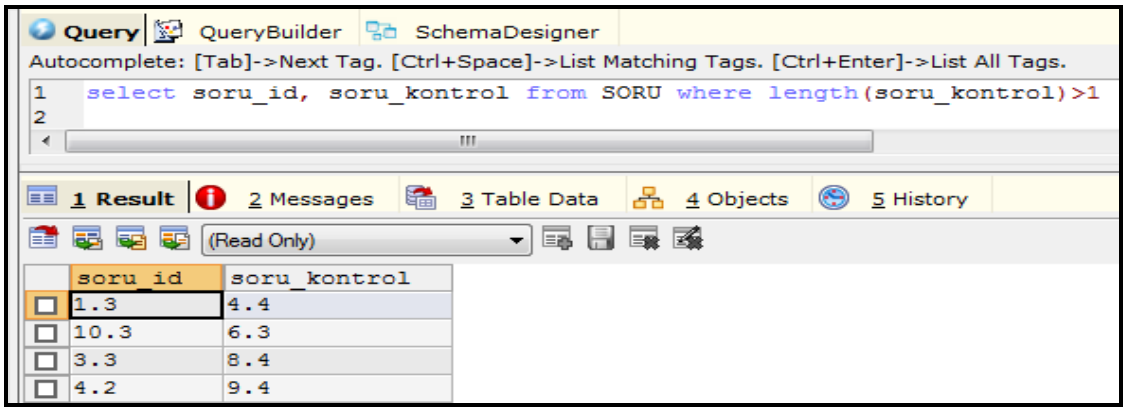
Her bir alanın başındaki numaralar, ISO/IEC 27001:2007 standardında yer alan numaralardır.

Her bir alanla ilgili sorular Şekil 3.1'de ve ilgili kontrol soruları da Şekil 3.2'de verilmektedir. Her başlıkta toplam 3 soru vardır ve eğer varsa, dördüncü soru kontrol sorusudur. Sorular belirlenirken, ana başlıklarla ilgili olarak standartta verilen 133 kontrolden en önemli görünenler alınmış ve envanter sorusu haline getirilmiştir.

Soru No	Başlık No	Soru Metni
1.1	A.5	Kurum/Şirketinizin bir bilgi güvenliği politikası var mı?
1.2	A.5	"Bilgi Güvenliği Politika"nız yönetim tarafından düzenli olarak gözden geçiriliyor mu?
1.3	A.5	Tüm çalışanlarınız ve ilgili dış taraflarla "Bilgi Güvenliği Politikası"nı paylaşıp ve farkındalığı sağladınız mı?
2.1	A.6	Kurum/Şirketinizde "Bilgi Güvenliği" konusunda çalışan var mı?
2.2	A.6	Kurum/şirketinizin çalışmalarında "Bilgi Güvenliği"ne yönelik prosedür, talimat ve sözleşmeler mevcut mu?
2.3	A.6	Organizasyon şemasında "Bilgi Güvenliği"ne yönelik bir yapılanma var mı?
3.1	A.7	"Bilgi Güvenliği" projesi kapsamındaki bölümlerin varlık listeleri gizlilik -bütünlük ve erişilebirlik derecesine göre belirlenmiş midir?
3.2	A.7	Kurum/ şirketinizdeki çalışanlara bilgilerin gizliliği, bütünlüğü ve erişilebirliğine (kullanılabilirliğine) yönelik farkındalığı artırıcı ve bilgilendirici eğitimler verilmekte midir?
3.3	A.7	Varlıkların kabul edilebilir kullanım kuralları tanımlanmış mıdır?
4.1	A.8	İşe alım ve işten çıkışlarda dökümante edilmiş belirli bir yöntem izlenmekte midir?
4.2	A.8	Çalışanın belirlenmiş kurallara uymamaları durumunda işleyen yazılı bir disiplin süreci mevcut mudur?
4.3	A.8	İşten ayrılan kişilerin, erişim yetkilerinin kısıtlanması ve sahip oldukları şirket bilgi- eşyalarını teslim etme şekilleri belli midir?
4.4	A.8	Çalışanlar "Bilgi Güvenliği" konusunda yeterli farkındalığa sahip midir?
5.1	A.9	Kurum/Şirketinizin fiziksel güvenliği kartlı giriş ya da benzeri bir sistemle sağlanmakta mıdır?
5.2	A.9	Kurumunuza gelen ziyaretçiler, ziyaretçi kartı ya da benzeri bir yöntemle takip ediliyor mu?
5.3	A.9	Bilgi Teknolojileri sistemlerinizin (kablomala, donanımlar vb.) güvenli şekilde yerleştirilmesi ve kaldırılmasında düzenli şekilde izlenen çalışma yöntemleri var mıdır?
6.1	A.10	Kurum/şirketinizde uygulamaların (yazılım) geliştirilmesi, test edilmesi ve devreye alınmasında izlenen bir yöntem var mıdır?
6.2	A.10	Üçüncü taraflara (dış taraflar) hizmet sunulan durumlar varsa bunlarla ilgili yapılan sözleşme ve prosedürler mevcut mudur?
6.3	A.10	Donanım ve yazılım ihtiyaçları için planlama yapılmakta mıdır?
6.4	A.10	Bilgiler düzenli olarak (günlük, haftalık, aylık ve yıllık) yedeklenmekte midir?
7.1	A.11	Çalışanların internet kullanımları, çeşitli uygulmaları kullanmaları, ağ üzerindeki hareketlerini takip etmeye yönelik izleme ve loglama yapılmakta mıdır?
7.2	A.11	Çalışan ya da dış kaynakların şirket ağı içindeki erişim yetkileri ve bu yetkileri alma yöntemleri belirlenmiş midir?
7.3	A.11	Çalışanlar bilgisayarlarının başından kalktıklarında oturumlarını kitlemekte midir ya da otomatik olarak bilgisayar oturumları kitlenmekte midir?
8.1	A.12	Çalışanlar gizli ve önemli bilgileri masalarının üzerinde değil kilitli çekmece veya dolaplarda saklamakta mıdırlar?
8.2	A.12	Kurum/şirket içinde kriptografik (şifreleme)kontroller uygulanmakta mıdır (e-imza,ssl vb.)?
8.3	A.12	Teknik açıklıkları kontrol etmek amacıyla, düzenli olarak testler yaptırılmakta mıdır?
8.4	A.12	Harici disk, USB, yazılabilir CD/DVD gibi taşınabilir cihazların ve uygulamaların kullanımına yönelik kurallar belirlenmiş midir?
9.1	A.13	"Bilgi Güvenliği" olaylarının rapor edilmesi için uygun prosedür ve yönetim kanalı var mıdır?
9.2	A.13	Çalışanlar "Bilgi Güvenliği" olaylarını rapor etmek için sorumluluklarının bilincinde ve yeterli farkındalığa sahip midir?
9.3	A.13	"Bilgi Güvenliği"ne yönelik herhangi bir olay çıktığında uygulanacak aksiyonlar belirlenmiş midir?
9.4	A.13	Disiplin dokümanında çalışanların belirlenen kurallara, politika ve prosedürlere uymamaları durumundaki yaptırımlar açıkça belirlenmiş midir?
10.1	A.14	Teçhizat, elektrik kesintileri ve destek hizmetlerindeki arızalardan kaynaklanan diğer bozulmalara karşı korunmakta mıdır?
10.2	A.14	Teçhizatın sürekli kullanılabilirliğini ve bütünlüğünü sağlamak için doğru şekilde bakımı yapılmakta mıdır?
10.3	A.14	Kurum/şirketinizde iş sürekliliğini sağlamaya yönelik planlar var mıdır?
11.1	A.15	Lisanslı yazılımın kullanılması konusunda denetimler yapılmakta mıdır?
11.2	A.15	Tüm sözleşmeler, yasalar ve düzenlemelerle uyum için kriptografik kontroller kullanılmakta mıdır?
11.3	A.15	Kurum/şirketin yasalar karşısında uyması gereken kurallarla ilgili yapılması gerekenler belirlenmiş midir?

Şekil 3.1. Envanter soruları ve ilgili ISO/IEC 27001:2007 ana başlıkları

Kontrol soruları ise şu şekildedir :

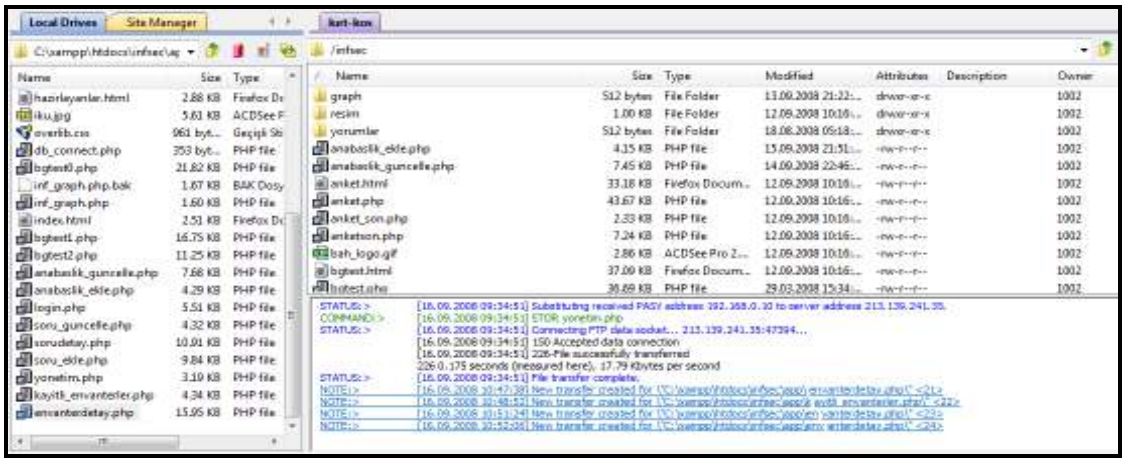


Şekil 3.2. Kontrol soruları

Her bir sorunun 5 puanı vardır. Dolayısıyla, her bir ISO/IEC 27001:2007 ana başlığı için alınabilecek olası puan toplamı 15'tir. Kontrol sorularının puanı yoktur, sadece testin tutarlılığını sınamak için kullanılmaktadır.

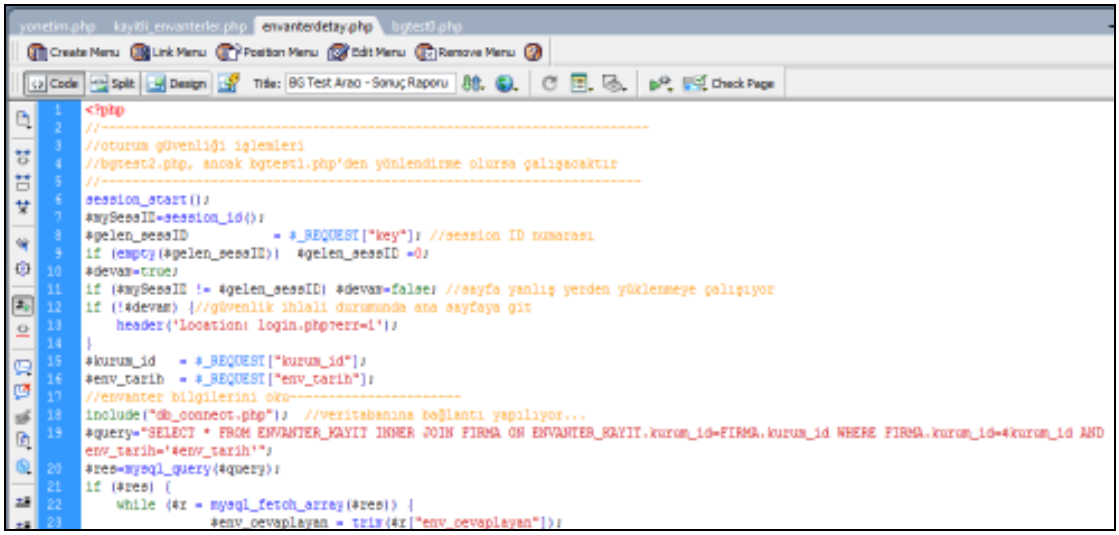
3.3 Uygulama

Uygulama geliştirme bir Windows bilgisayarda yapılmış ve windows altında çalışan bir PHP/MySQL/Apache sistemiyle test edilerek FreeBSD sunucuya FTP ile kopyalanmıştır. Şekil 3.3., böyle bir sistemi göstermektedir ve grafik tabanlı bir FTP istemcisine aittir.

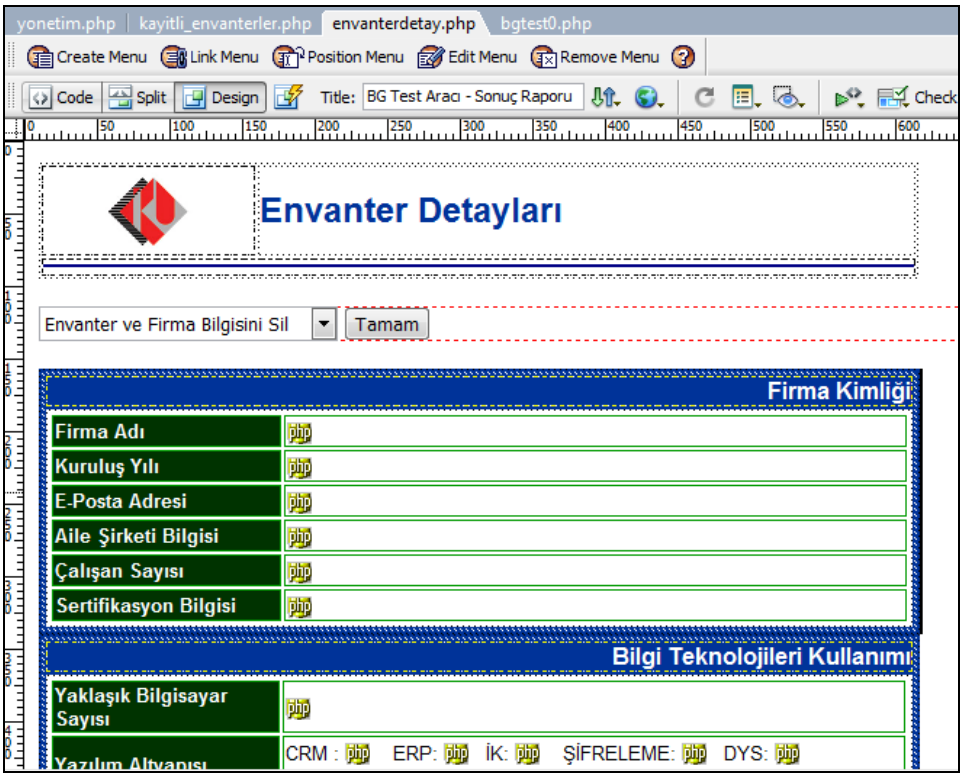


Şekil 3.3. Yerel ve sunucu dosyaları

Web uygulamasını geliştirmede, tasarımda sağladığı kolaylıktan ötürü, bir görsel HTML editor kullanılmıştır. Şeki 3.4 ve Şekil 3.5 sırasıyla PHP kod geliştirme ve grafik arayüz geliştirme ekranlarını göstermektedir.



Şekil 3.4. HTML Editörü, PHP kod geliştirme arayüzü

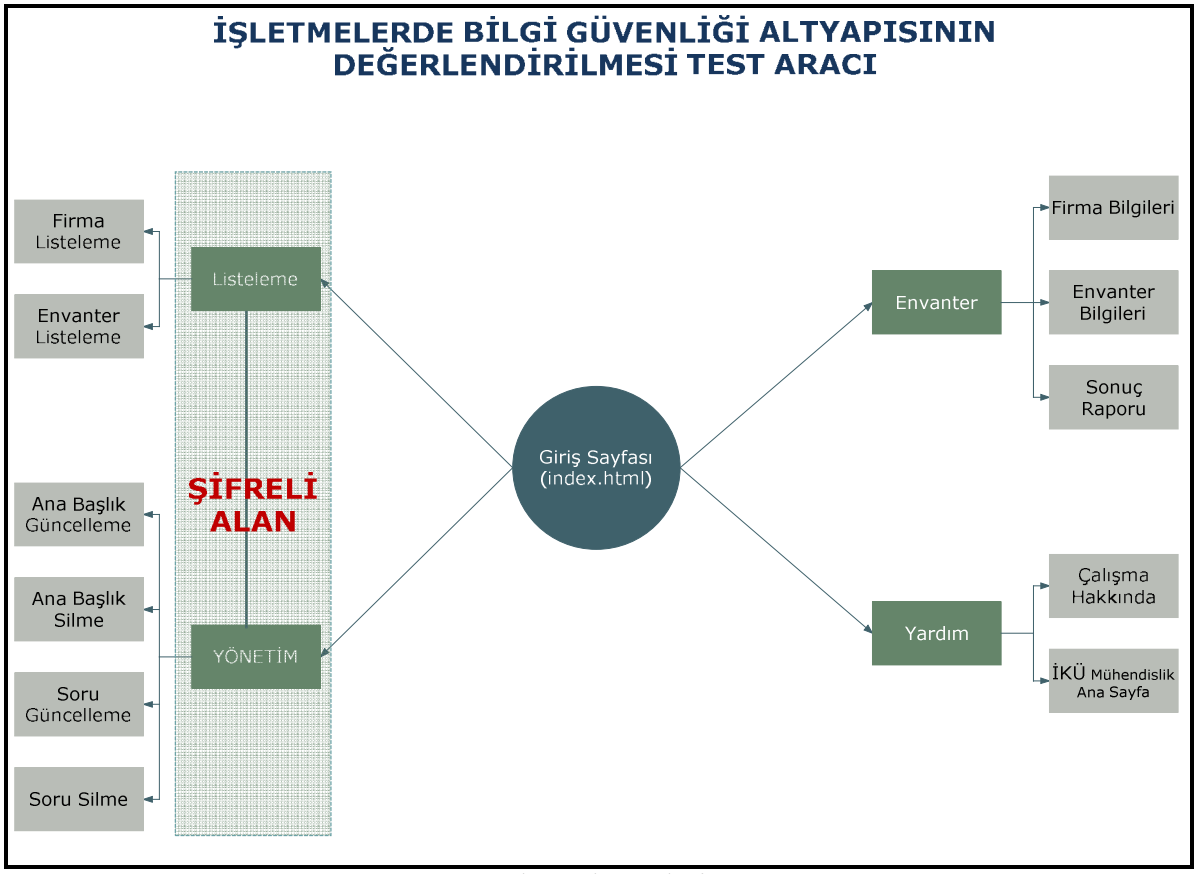


Şekil 3.5. HTML Editörü, web grafik arayüzü geliştirme

4 TEST ARACI GELİŞTİRİLMESİ

4.1 Test Aracı Geliştirmede Kullanılacak Yazılım ve Veritabanı Altyapısı

Şekil 4.1 giriş sayfasından itibaren web uygulama haritasını göstermektedir.



Şekil 4.1. Web uygulaması haritası

Tablo 4.1, web haritasındaki her bir kısıma ait uygulamaların dağılımını göstermektedir.

Tablo 4.1. Test Aracını oluşturan PHP uygulamalarının dağılımı

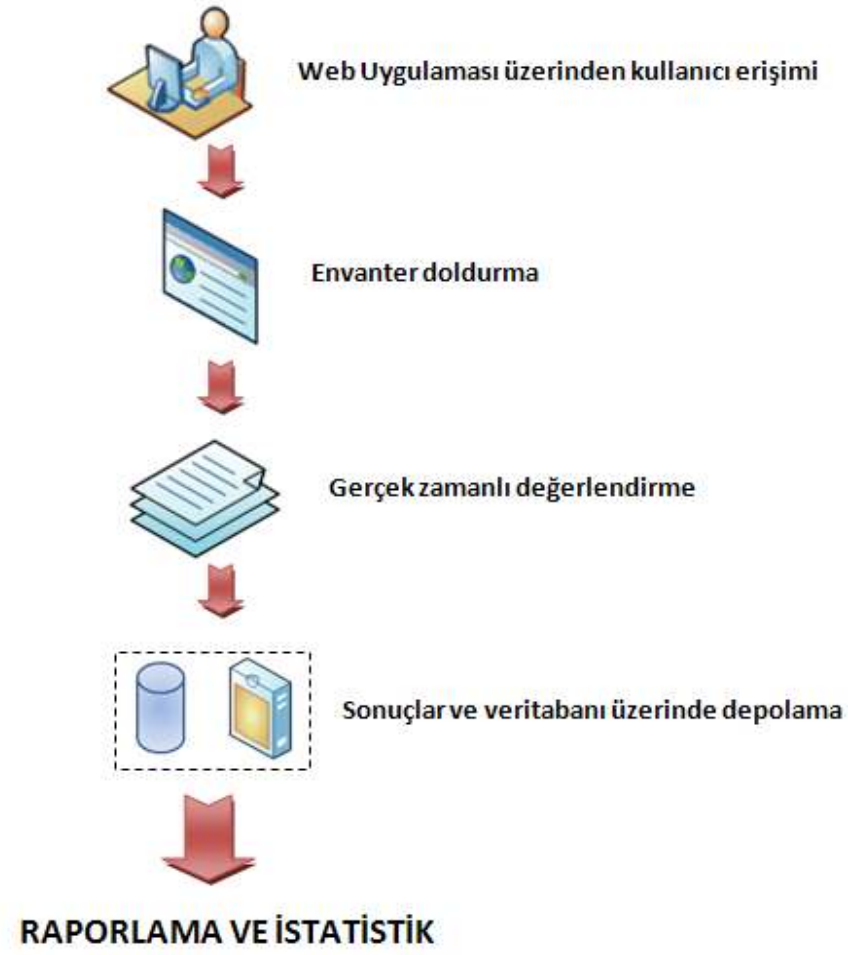
Web Uygulama Alanı	**Uygulama Adı**
Envanter	bgtest0.php : Firma bilgileri ve oturum kontrolü işlemleri bgtest1.php : Envanter uygulaması bgtest2.php : Sonuç raporu
Yönetim	anabaslik_guncelle.php anabaslik_ekle.php soru_guncelle.php soru_ekle.php
Listeleme	kayitli_envanterler.php

Test aracı geliştirmede oturum güvenliğin sağlanması için standart PHP kontrollerinden yararlanılmıştır. Uygulamanın en başında üretilen bir oturum anahtarı, her sayfaya taşınmış ve ilgili sayfada üretilen anahtarla karşılaştırılarak uygulama bütünlüğünün korunup korunmadığı kontrol edilmiştir. Böylece, uygulamanın çalışması sırasında kullanıcılar sisteme en başından giriş yapmak durumundadırlar. Örneğin, envanter doldurmak için önce kurum/şirket bilgilerinin girilmesi gerekmektedir ya da, yönetim araçlarının kullanılabilmesi için önce kullanıcı giriş ekranından giriş yapılması gerekmektedir.

Uygulamanın kullanacağı ilişkisel veritabanı MySQL veritabanı yönetim sisteminde tutulmaktadır.

4.2 Uygulama Akış Diyagramı

Şekil 4.2., test aracına ait fonksiyonel akışı göstermektedir. Uygulama standart bir web istemcisi (internet explorer, firefox vb) kullanılarak çalıştırılmakta ve kullanılmaktadır. Uygulama, "Akıllı Bir Sistem (yarı uzman)"dir ve bunun sebebi değerlendirme puanları, sorular ve kuralların admin tarafından değiştirilebildiği bir test aracı olmasıdır.



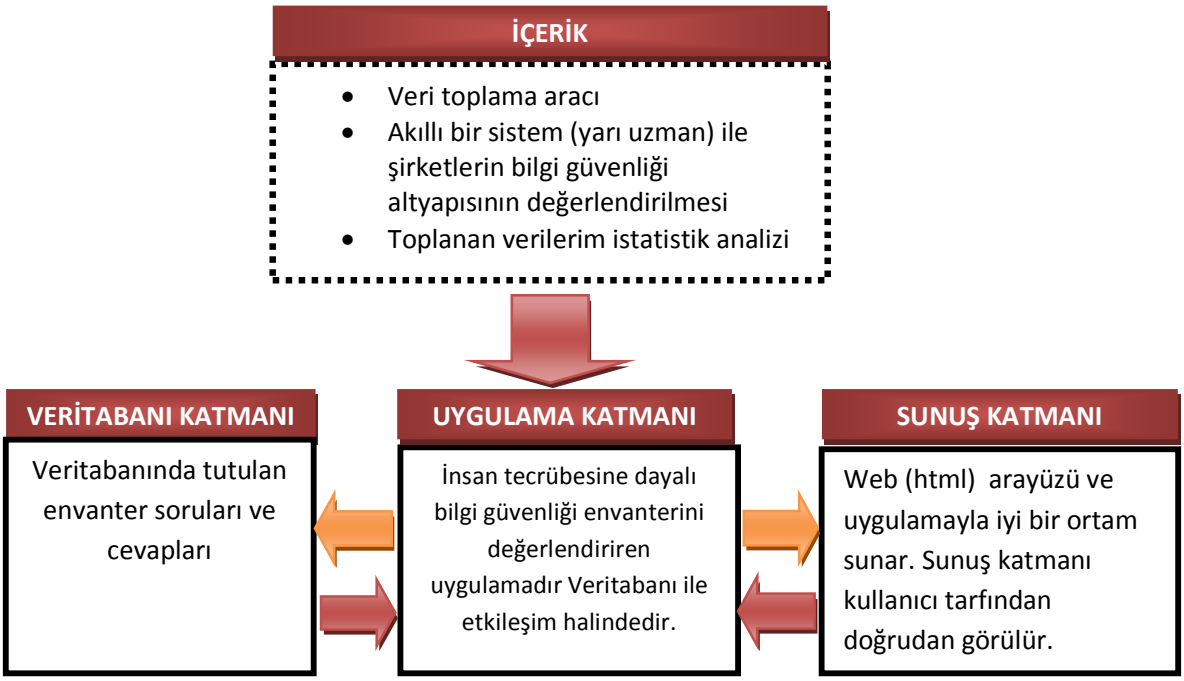
Şekil 4.2: Uygulama Akış Diyagramı

4.3 Uygulama Mimarisi

Test aracı mimarisinin 3 temel katmandan oluştuğu görülmektedir. Bunlar :

- Veritabanı katmanı
- Uygulama Katmanı
- Sunuş Katmanı

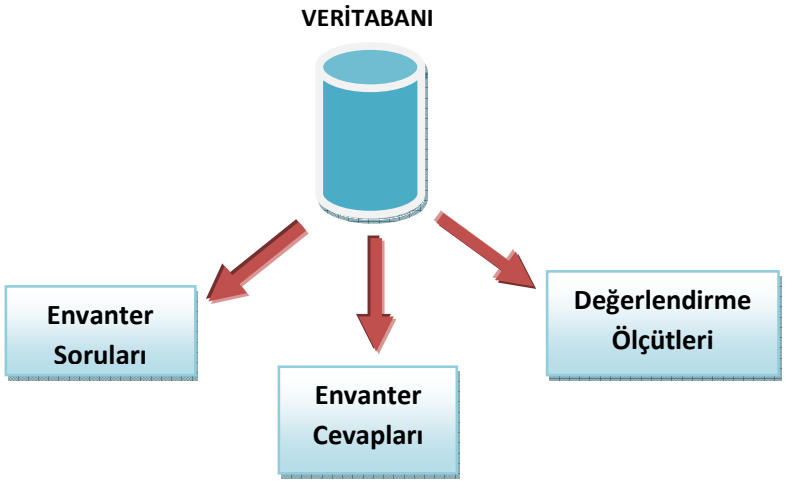
Şekil 4.3., her bir katmanı ve özelliklerini göstermektedir.



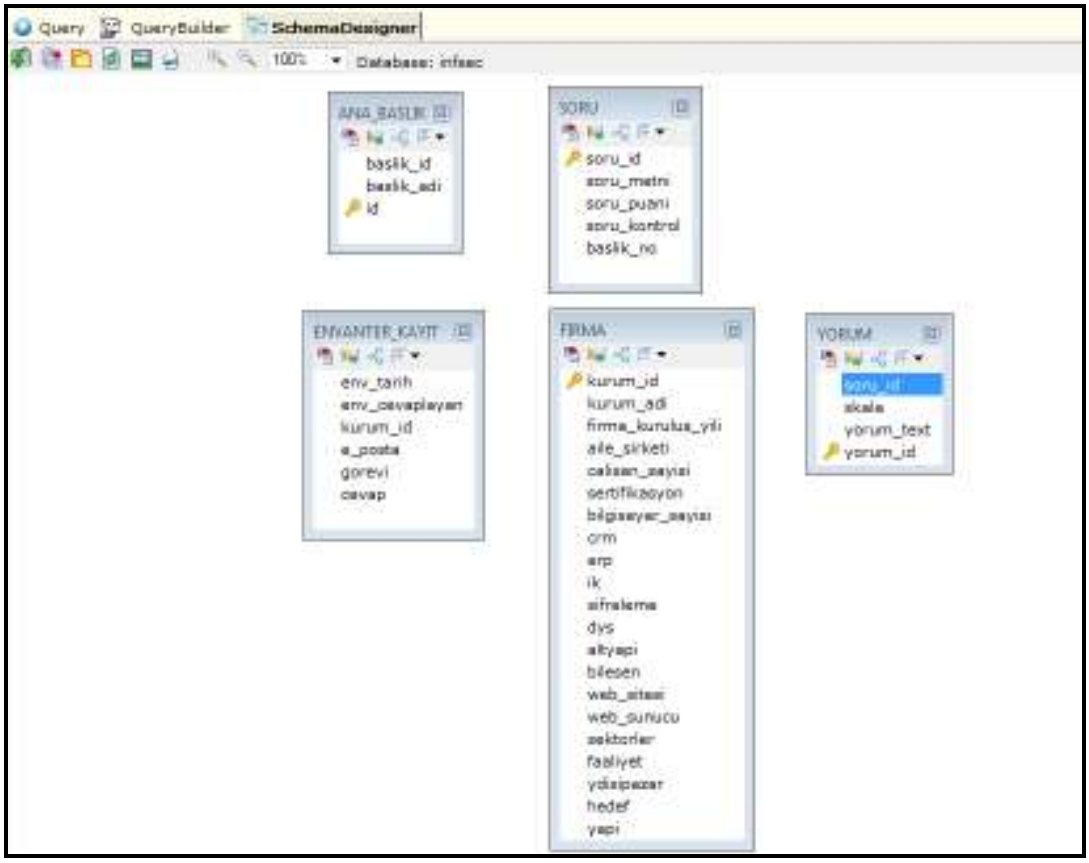
Şekil 4.3: Uygulama Mimarisi

4.4 Veritabanı Tasarımı

Veritabanı, uygulama mimarisindeki katmanlardan birisidir. Hem envanter ile ilgili tüm soru, yorum ve değerlendirme kurallarının; hem de girilen envanterlere ait cevapların tutulduğu bir yapıdır (Şekil 4.4).



Şekil 4.4: Veritabanında tutulan bilgi tipleri



Şekil 4.5: MySQL veritabanı yapısı

Şekil 4.5, MySQL veritabanı yönetim sisteminde tutulan tabloları göstermektedir.

Şekil 4.6, Şekil 4.7, Şekil 4.8, Şekil 4.9 ve Şekil 4.10 ise, veritabanında bulunan tabloların ayrıntılarını göstermektedir.

```
/*Column Information For - infsec.ANA_BASLIK*/
-----------------------------------------------

Field       Type                 Collation          Null    Key     Default  Extra
----------  -------------------  -----------------  ------  ------  -------  --------------
baslik_id   varchar(5)           latin5_turkish_ci  NO
baslik_adi  varchar(255)         latin5_turkish_ci  NO
id          smallint(5) unsigned (NULL)             NO      PRI     (NULL)   auto_increment

/*Index Information For - infsec.ANA_BASLIK*/
-----------------------------------------------

Table       Non_unique  Key_name  Seq_in_index  Column_name  Collation  Cardinality  Sub_part
----------  ----------  --------  ------------  -----------  ---------  -----------  --------
ANA_BASLIK           0  PRIMARY              1  id           A                   11    (NULL)
```

Şekil 4.6: ANA_BASLIK veritabanı tablo yapısı

ENVANTER_KAYIT tablosunda, envantere verilen cevaplar "cevap" alanında tutulmaktadır ve ilerde envanter sorularının artabileceği göz önünde bulundurularak 100 değişken karakter uzunluğunda seçilmiştir. Mevcut uygulamada soru sayısı 37 olduğundan bu alanında uzunluğu 37'dir. Tüm tablo alanlarındaki "VARCHAR" değişken tipleri, ilgili alanın alabileceği en büyük değeri göstermektedir. Veritabanında ise, alanın gerçek değeri ne ise o kadar uzunlukta disk alanı kullanılmaktadır. Envanteri cevaplayan (env_cevaplayan), e-posta adresi (e_posta) ve görevi (görevi) alanları da ortalama kullanımı karşılayabilecek uzunlukta seçilmişlerdir (Şekil 4.7).

1 Result | 2 Messages | 3 Table Data | 4 Objects | 5 History

```
/*Column Information For - infsec.ENVANTER_KAYIT*/
-------------------------------------------------

Field           Type              Collation          Null    Key     Default  Extra
--------------  ----------------  -----------------  ------  ------  -------  -----
env_tarih       datetime          (NULL)             NO
env_cevaplayan  varchar(40)       latin5_turkish_ci  YES             (NULL)
kurum_id        int(10) unsigned  (NULL)             NO      MUL
e_posta         varchar(45)       latin5_turkish_ci  YES             (NULL)
gorevi          varchar(50)       latin5_turkish_ci  YES             (NULL)
cevap           varchar(100)      latin5_turkish_ci  YES             (NULL)

/*Index Information For - infsec.ENVANTER_KAYIT*/
-------------------------------------------------
```

Şekil 4.7: ENVANTER_KAYIT veritabanı tablo yapısı

Envanter yanıtlanmadan önce doldurulması gereken firma ve sektörel bilgiler alanlarına göre gruplandırılarak karakter alanları oluşturulmuş ve veritabanında bu şekilde tutulmuştur. Böylece, daha fazla değişkenin daha az alanla ifade edilebilmesi sağlanmıştır. Her bir değişkenden sonra "|" karakteri konularak değerler birbirlerinden ayrılmıştır. Bunlar :

- Çalışan sayısı : beyaz_yaka|mavi_yaka (örneğin, beyaz yakalı çalışan 120, mavi yakalı çalışan 208 kişi ise, bu durumda çalışan sayısı alanının değeri **"120|208"** olacaktır.
- Sertifikasyon
- CRM

- ERP
- İK
- Döküman Yönetim Sistemi (DYS)
- Altyapı
- Bileşen
- Sektörler
- Faaliyet
- Hedef
- Yapı

Her bir grup envanterde ilgili alana karşılık gelmektedir. Şekil 4.8, veritabanında bu alanların saklanma biçimleri için örnek bir durumu yansıtmaktadır.

```
/*Column Information For - infsec.FIRMA*/
----------------------------------------
```

Field	Type	Collation	Null	Key
kurum_id	smallint(5) unsigned	(NULL)	NO	PRI
kurum_adi	varchar(100)	latin5_turkish_ci	NO	
firma_kurulus_yili	year(4)	(NULL)	YES	
aile_sirketi	enum('0','1','2','3')	latin5_turkish_ci	NO	
calisan_sayisi	varchar(10)	latin5_turkish_ci	NO	
sertifikasyon	varchar(100)	latin5_turkish_ci	NO	
bilgisayar_sayisi	int(10) unsigned	(NULL)	NO	
crm	varchar(150)	latin5_turkish_ci	NO	
erp	varchar(150)	latin5_turkish_ci	NO	
ik	varchar(150)	latin5_turkish_ci	NO	
sifreleme	enum('0','1')	latin5_turkish_ci	NO	
dys	varchar(150)	latin5_turkish_ci	NO	
altyapi	varchar(50)	latin5_turkish_ci	NO	
bilesen	varchar(100)	latin5_turkish_ci	NO	
web_sitesi	enum('0','1','2','3','4','5','6')	latin5_turkish_ci	NO	
web_sunucu	enum('0','1')	latin5_turkish_ci	YES	
sektorler	varchar(50)	latin5_turkish_ci	YES	
faaliyet	varchar(40)	latin5_turkish_ci	YES	
ydisipazar	int(11)	(NULL)	NO	
hedef	varchar(3)	latin5_turkish_ci	NO	
yapi	varchar(3)	latin5_turkish_ci	NO	

```
/*Index Information For - infsec.FIRMA*/
----------------------------------------
```

Table	Non_unique	Key_name	Seq_in_index	Column_name	Collation	Cardinality	Sub_part
FIRMA	0	PRIMARY	1	kurum_id	A	37	(NULL)

firma_kur	aile_sirketi	calisan_sayisi	sertifikasyon	bilgisayar_	crm	erp	ik	sifrelen	dys	altyapi
2006	0	100|500	1|1|1|0|0|0|1|-|-	1000	1|-	1|-	1|-	1	1|-	1|1|1|1|1
2006	0	10|300	0|0|0|0|0|0|0|-|-	130	1|-	0|-	1|-	0	0|-	0|1|1|0|0
2005	0	2|5	1|0|0|0|0|0|0|-|-	10	0|-	0|-	0|-	0	0|-	1|0|1|1|0
2005	1	20|50	1|1|0|0|0|0|0|-|-	20	0|-	0|-	0|-	0	0|-	0|1|0|1|0
2004	0	100|500	1|1|1|0|0|0|0|-|-	1000	1|-	1|-	1|-	1	1|-	1|1|1|1|1
2002	0	15|1	1|0|0|0|0|0|0|-|-	16	0|-	0|-	0|-	0	0|-	0|1|0|0|1
2002	0	10|1	0|0|0|0|0|0|0|-|-	7	0|-	0|-	0|-	0	0|-	0|0|0|0|0
2001	1	3500|0	1|0|0|0|0|0|0|-|-	0	1|-	1|-	1|-	1	1|-	1|1|1|0|1
2000	1	60|10	1|0|0|0|0|0|0|-|-	60	0|-	0|-	1|-	0	0|-	0|1|1|0|0

bilesen	web_s	web_s	sektorler	faaliyet	ydisi	hede	yapi
1|1|1|1|1|1|1|-|1|0-|0-	6	1	0|0|0|0|0|0|1|0|0|0|0|0-	1|1|1|1|0-	0	1|1	1|1
0|1|1|0|0|0|1-|0|0-|0-	2	1	0|0|0|0|0|1|0|0|0|0|0|0-	0|1|0|0|0-	0	1|1	1|0
0|1|0|0|0|0|0-|0|0-|0-	0		0|0|0|0|0|0|1|0|0|0|0|0-	0|1|0|0|0-	0	1|1	1|0
0|0|1|0|0|0|0-|0|0-|0-	0		1|0|0|0|0|0|0|0|0|0|0|0-	1|0|0|0|0-	0	1|1	1|0

Şekil 4.8: FIRMA veritabanı tablo yapısı

```
/*Column Information For - infsec.SORU*/
----------------------------------------

Field         Type                  Collation          Null    Key     Default
------------  --------------------  -----------------  ------  ------  -------
soru_id       varchar(5)            latin5_turkish_ci  NO      PRI
soru_metni    varchar(255)          latin5_turkish_ci  NO
soru_puani    smallint(5) unsigned  (NULL)             NO              5
soru_kontrol  varchar(5)            latin5_turkish_ci  NO
baslik_no     smallint(5) unsigned  (NULL)             NO      MUL

/*Index Information For - infsec.SORU*/
----------------------------------------

Table   Non_unique  Key_name  Seq_in_index  Column_name  Collation  Cardinality
------  ----------  --------  ------------  -----------  ---------  -----------
SORU             0  PRIMARY              1  soru_id      A                   37
```

Şekil 4.9: SORU veritabanı tablo yapısı

```
/*Column Information For - infsec.YORUM*/
----------------------------------------

Field       Type                  Collation          Null    Key     Default  Extra
----------  --------------------  -----------------  ------  ------  -------  --------
soru_id     varchar(5)            latin5_turkish_ci  NO
skala       smallint(5) unsigned  (NULL)             NO
yorum_text  text                  latin5_turkish_ci  NO
yorum_id    smallint(5) unsigned  (NULL)             NO      PRI     (NULL)   auto_inc

/*Index Information For - infsec.YORUM*/
----------------------------------------

Table   Non_unique  Key_name  Seq_in_index  Column_name  Collation  Cardinality  Sub_p
------  ----------  --------  ------------  -----------  ---------  -----------  -----
YORUM            0  PRIMARY              1  yorum_id     A                  197    (NU
```

Şekil 4.10: YORUM veritabanı tablo yapısı

4.5 Envanter Uygulaması

Envanter uygulaması 4 bölümden oluşmaktadır. Bunlardan birincisi "Giriş" kullanıcıların giriş yapacakları bölümdür. Burada şirket/kuruma ait bilgiler girildikten sonra test alanına geçilip Bilgi Güvenliği'ne yönelik, standart EK-1 A'da da yer alan başlık ve alt başlıkları içerecek ve kurum/şirketlerin altyapısını inceleyecek sorular yer almaktadır. Soruların cevabı "evet", "hayır" ve "cevap yok" şeklinde sınıflandırılmıştır. Soruya verilen cevap "evet" ise 5 ayrı dereceve değerlendirme yapılır. Bunlar:

- 5: Çok İyi
- 4: İyi,
- 3: Orta
- 2: Az
- 1: Yetersiz

Sorular cevaplandıktan sonra "Değerlendir" butonuna basılarak değerlendirme sonuç ekranı ile karşılaşılır. Anket içinde yer alan sorulardan bazıları kullanıcının anketi doldurabilecek yeterlilikte olup olmadığını anlamaya yöneliktir. Belirlenen bazı sorulara verilen cevaplarla kontrol yapılmakta olup, kullanıcının bu sorulara verdiği cevaplarda tutarsızlık olması durumunda değerlendirme ekranında "tutarsızlık olduğu" belirtilmektedir. Değerlendirme ekranında sorulara verilen cevaplar doğrultusunda Bilgi Güvenliği ana başlıklarnda uyumluluk durumları gösterilmiş, uyumluluk durumu doğrultusunda grafiksel gösterime ve ardından da her bir ana başlık için yorumlara yer verilmiştir. Her bir cevabın yorumu ayrı olup, "evet" cevaplarında derecelendirmeye göre iyileştirilmesi gereken ya da mevcut durum doğrultusunda yorum yapılırken, cevabın "hayır" ve "cevap yok" olması durumunda yapılması gerekenlere yönelik tavsiyelerde bulunulmaktadır.

"Çalışma Hakkında"bağlacında, "İşletmelerde Bilgi Güvenliği Altyapısının Değerlendirilmesinde Test Aracı" tezine yönelik bilgilendirme yapılmıştır.

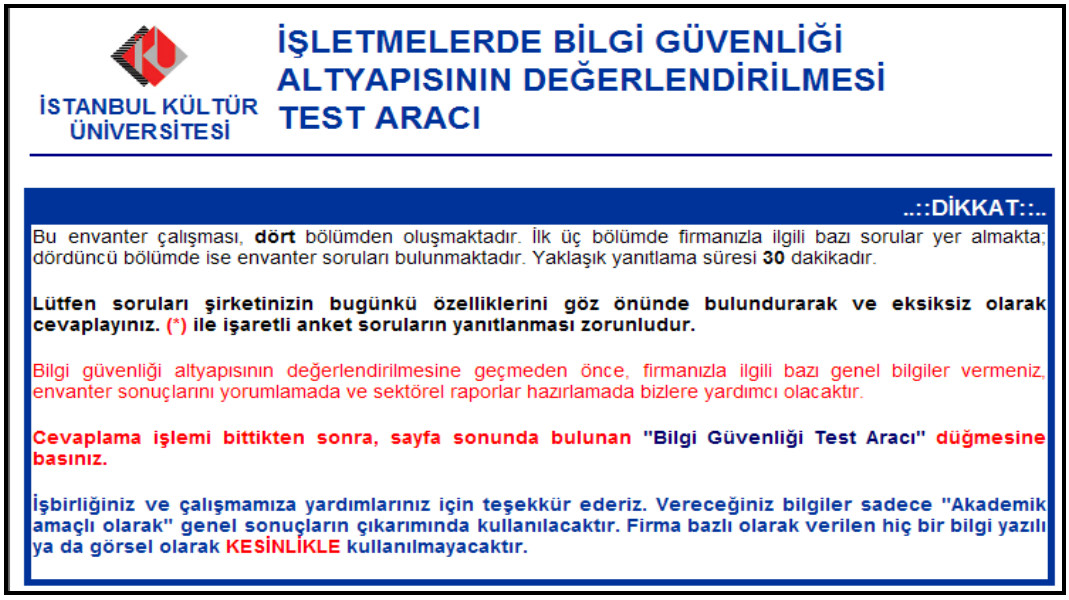
"Test Aracı Yönetimi" bağlacında ise, yönetici alanı bulunmaktadır. Yönetici alanında test aracında yer alan sorular, ana başlıklar , değerlendirme kriterleri ile ilgili takip ve değişiklikler yapılabilmektedir.

"İKÜ-Mühendislik Mimarlık Fakültesi, Bilgisayar Mühendisliği" bağlacında tezin yapıldığı üniversitenin web sayfasına yönledirme yapılmıştır.

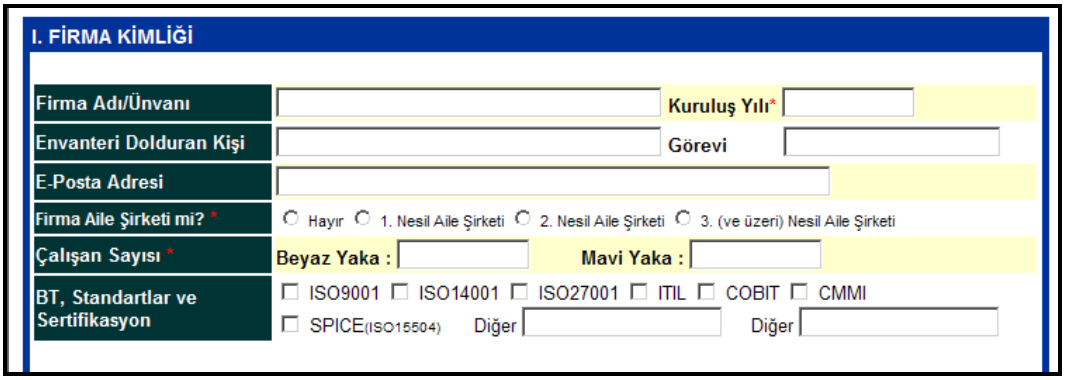
Şekil 4.11., uygulama giriş ana sayfasını göstermektedir. Kullanıcılar, "Giriş" i seçerek envanter uygulamasını çalıştırmaktadırlar.

Şekil 4.11: Uygulama Web Giriş Arayüzü

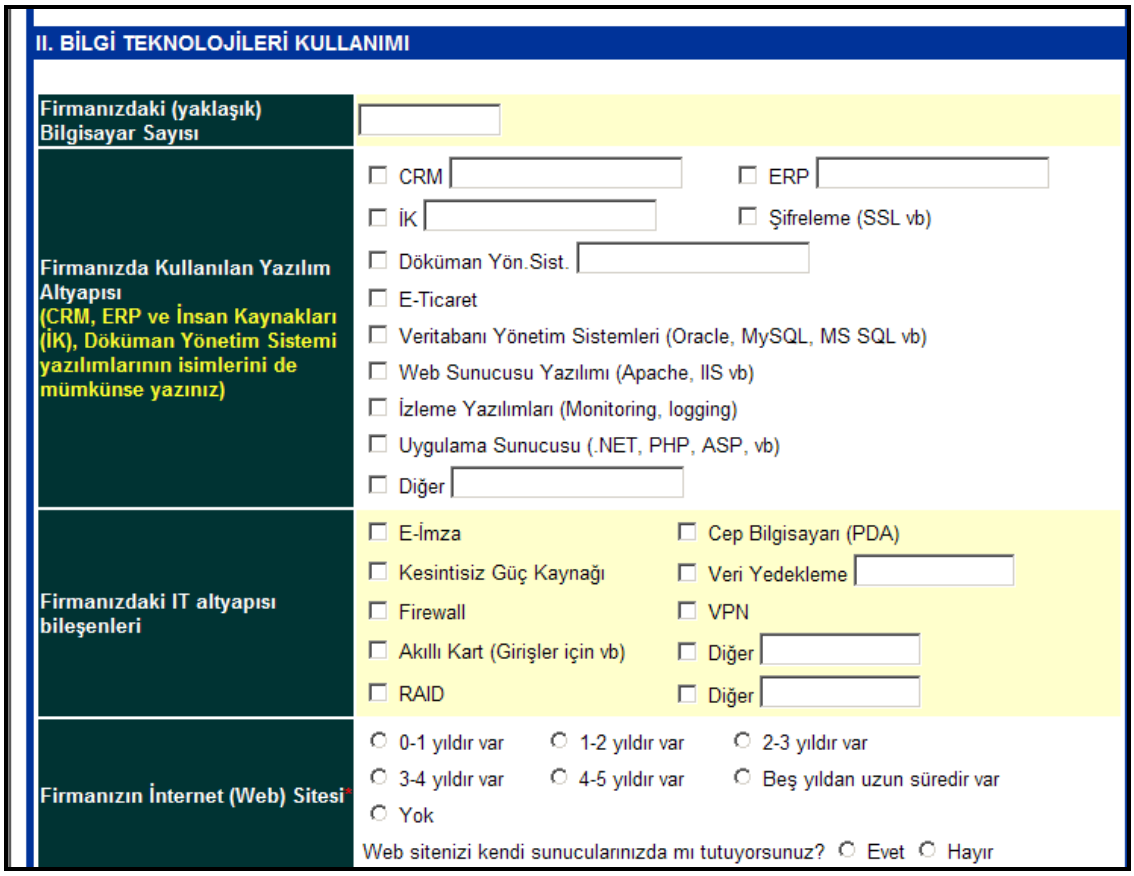
Şekil 4.12, "Giriş" seçildiğinde ilk gelen ekranı göstermektedir. Şekil 4.12, Şekil 4.13, Şekil 4.14 ve Şekil 4.15 envanter uygulamasına geçmeden önce doldurulması gereken firma bilgilerinin olduğu ektandır.



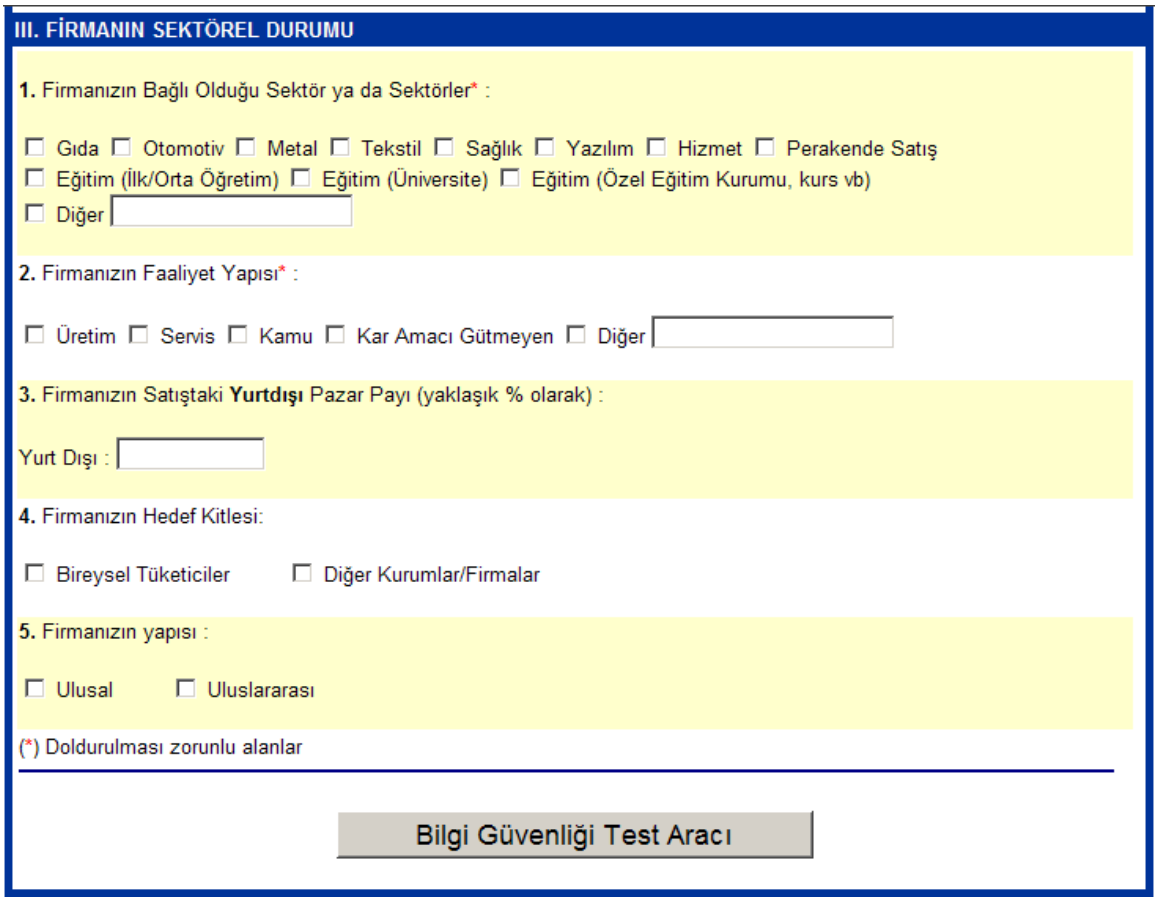
Şekil 4.12: Uygulama Web Anket Değerlendirme Arayüzü -1



Şekil 4.13: Uygulama Web Anket Değerlendirme Arayüzü -2



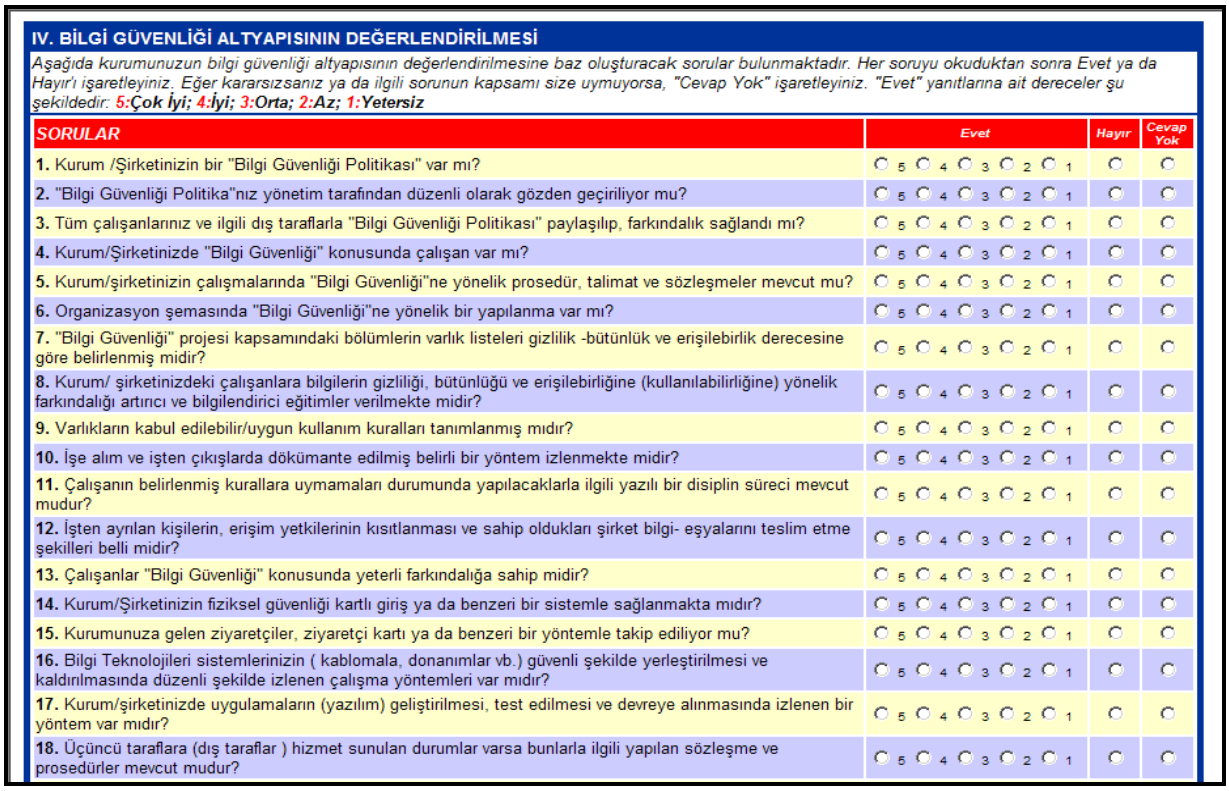
Şekil 4.14: Uygulama Web Anket Değerlendirme Arayüzü -3



Şekil 4.15: Uygulama Web Anket Değerlendirme Arayüzü -4

Firma bilgileri girildikten sonra envanterin uygulanacağı uygulama ekranına gelinir. Şekil 4.16, Şekil 4.17 ve şekil 4.18 envanter uygulama ekranlarını göstermektedir.

Şekil 4.16: Uygulama Web Anket Değerlendirme Arayüzü -5

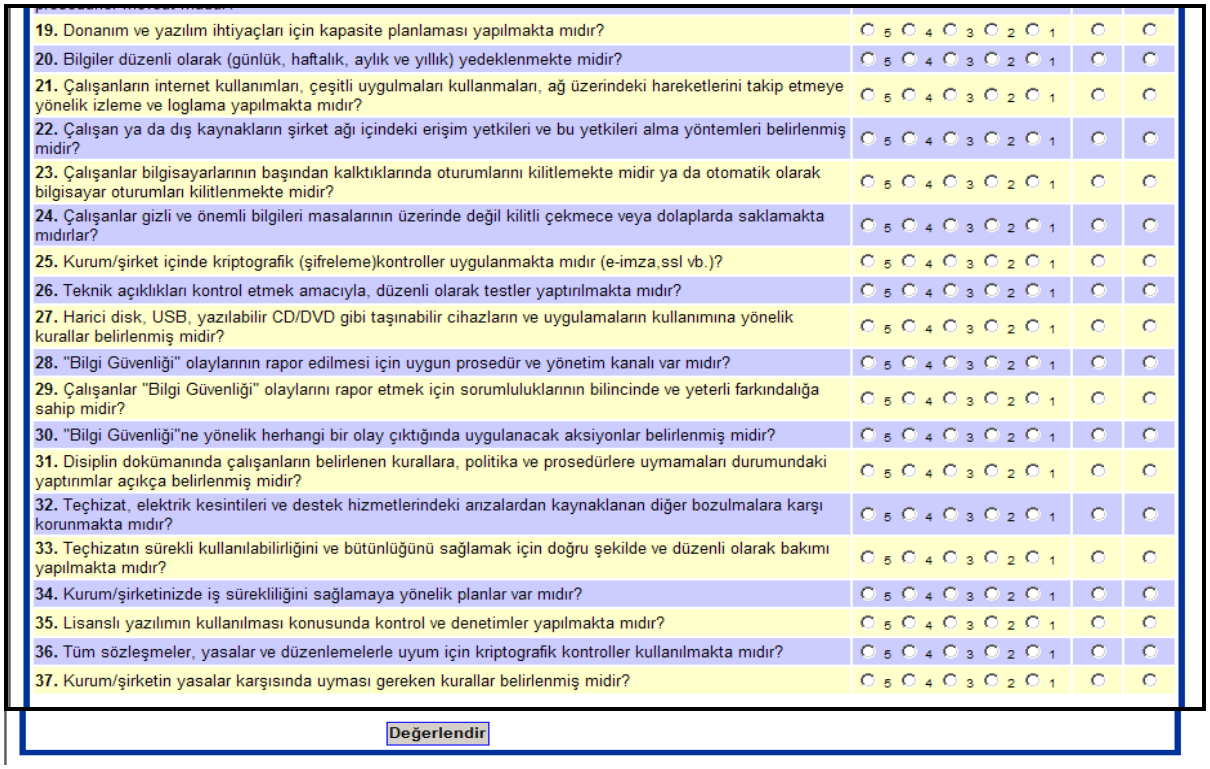


IV. BİLGİ GÜVENLİĞİ ALTYAPISININ DEĞERLENDİRİLMESİ

Aşağıda kurumunuzun bilgi güvenliği altyapısının değerlendirilmesine baz oluşturacak sorular bulunmaktadır. Her soruyu okuduktan sonra Evet ya da Hayır'ı işaretleyiniz. Eğer kararsızsanız ya da ilgili sorunun kapsamı size uymuyorsa, "Cevap Yok" işaretleyiniz. "Evet" yanıtlarına ait dereceler şu şekildedir: 5:Çok İyi; 4:İyi; 3:Orta; 2:Az; 1:Yetersiz

SORULAR	Evet	Hayır	Cevap Yok
1. Kurum /Şirketinizin bir "Bilgi Güvenliği Politikası" var mı?	5 4 3 2 1		
2. "Bilgi Güvenliği Politika"nız yönetim tarafından düzenli olarak gözden geçiriliyor mu?	5 4 3 2 1		
3. Tüm çalışanlarınız ve ilgili dış taraflarla "Bilgi Güvenliği Politikası" paylaşılıp, farkındalık sağlandı mı?	5 4 3 2 1		
4. Kurum/Şirketinizde "Bilgi Güvenliği" konusunda çalışan var mı?	5 4 3 2 1		
5. Kurum/şirketinizin çalışmalarında "Bilgi Güvenliği"ne yönelik prosedür, talimat ve sözleşmeler mevcut mu?	5 4 3 2 1		
6. Organizasyon şemasında "Bilgi Güvenliği"ne yönelik bir yapılanma var mı?	5 4 3 2 1		
7. "Bilgi Güvenliği" projesi kapsamındaki bölümlerin varlık listeleri gizlilik -bütünlük ve erişilebirlik derecesine göre belirlenmiş midir?	5 4 3 2 1		
8. Kurum/ şirketinizdeki çalışanlara bilgilerin gizliliği, bütünlüğü ve erişilebirliğine (kullanılabilirliğine) yönelik farkındalığı artırıcı ve bilgilendirici eğitimler verilmekte midir?	5 4 3 2 1		
9. Varlıkların kabul edilebilir/uygun kullanım kuralları tanımlanmış mıdır?	5 4 3 2 1		
10. İşe alım ve işten çıkışlarda dökümante edilmiş belirli bir yöntem izlenmekte midir?	5 4 3 2 1		
11. Çalışanın belirlenmiş kurallara uymamaları durumunda yapılacaklarla ilgili yazılı bir disiplin süreci mevcut mudur?	5 4 3 2 1		
12. İşten ayrılan kişilerin, erişim yetkilerinin kısıtlanması ve sahip oldukları şirket bilgi- eşyalarını teslim etme şekilleri belli midir?	5 4 3 2 1		
13. Çalışanlar "Bilgi Güvenliği" konusunda yeterli farkındalığa sahip midir?	5 4 3 2 1		
14. Kurum/Şirketinizin fiziksel güvenliği kartlı giriş ya da benzeri bir sistemle sağlanmakta mıdır?	5 4 3 2 1		
15. Kurumunuza gelen ziyaretçiler, ziyaretçi kartı ya da benzeri bir yöntemle takip ediliyor mu?	5 4 3 2 1		
16. Bilgi Teknolojileri sistemlerinizin (kablomala, donanımlar vb.) güvenli şekilde yerleştirilmesi ve kaldırılmasında düzenli şekilde izlenen çalışma yöntemleri var mıdır?	5 4 3 2 1		
17. Kurum/şirketinizde uygulamaların (yazılım) geliştirilmesi, test edilmesi ve devreye alınmasında izlenen bir yöntem var mıdır?	5 4 3 2 1		
18. Üçüncü taraflara (dış taraflar) hizmet sunulan durumlar varsa bunlarla ilgili yapılan sözleşme ve prosedürler mevcut mudur?	5 4 3 2 1		

Şekil 4.17: Uygulama Web Anket Değerlendirme Arayüzü -6



19. Donanım ve yazılım ihtiyaçları için kapasite planlaması yapılmakta mıdır?	5 4 3 2 1		
20. Bilgiler düzenli olarak (günlük, haftalık, aylık ve yıllık) yedeklenmekte midir?	5 4 3 2 1		
21. Çalışanların internet kullanımları, çeşitli uygulmaları kullanmaları, ağ üzerindeki hareketlerini takip etmeye yönelik izleme ve loglama yapılmakta mıdır?	5 4 3 2 1		
22. Çalışan ya da dış kaynakların şirket ağı içindeki erişim yetkileri ve bu yetkileri alma yöntemleri belirlenmiş midir?	5 4 3 2 1		
23. Çalışanlar bilgisayarlarının başından kalktıklarında oturumlarını kilitlemekte midir ya da otomatik olarak bilgisayar oturumları kilitlenmekte midir?	5 4 3 2 1		
24. Çalışanlar gizli ve önemli bilgileri masalarının üzerinde değil kilitli çekmece veya dolaplarda saklamakta mıdırlar?	5 4 3 2 1		
25. Kurum/şirket içinde kriptografik (şifreleme)kontroller uygulanmakta mıdır (e-imza,ssl vb.)?	5 4 3 2 1		
26. Teknik açıklıkları kontrol etmek amacıyla, düzenli olarak testler yaptırılmakta mıdır?	5 4 3 2 1		
27. Harici disk, USB, yazılabilir CD/DVD gibi taşınabilir cihazların ve uygulamaların kullanımına yönelik kurallar belirlenmiş midir?	5 4 3 2 1		
28. "Bilgi Güvenliği" olaylarının rapor edilmesi için uygun prosedür ve yönetim kanalı var mıdır?	5 4 3 2 1		
29. Çalışanlar "Bilgi Güvenliği" olaylarını rapor etmek için sorumluluklarının bilincinde ve yeterli farkındalığa sahip midir?	5 4 3 2 1		
30. "Bilgi Güvenliği"ne yönelik herhangi bir olay çıktığında uygulanacak aksiyonlar belirlenmiş midir?	5 4 3 2 1		
31. Disiplin dokümanında çalışanların belirlenen kurallara, politika ve prosedürlere uymamaları durumundaki yaptırımlar açıkça belirlenmiş midir?	5 4 3 2 1		
32. Teçhizat, elektrik kesintileri ve destek hizmetlerindeki arızalardan kaynaklanan diğer bozulmalara karşı korunmakta mıdır?	5 4 3 2 1		
33. Teçhizatın sürekli kullanılabilirliğini ve bütünlüğünü sağlamak için doğru şekilde ve düzenli olarak bakımı yapılmakta mıdır?	5 4 3 2 1		
34. Kurum/şirketinizde iş sürekliliğini sağlamaya yönelik planlar var mıdır?	5 4 3 2 1		
35. Lisanslı yazılımın kullanılması konusunda kontrol ve denetimler yapılmakta mıdır?	5 4 3 2 1		
36. Tüm sözleşmeler, yasalar ve düzenlemelerle uyum için kriptografik kontroller kullanılmakta mıdır?	5 4 3 2 1		
37. Kurum/şirketin yasalar karşısında uyması gereken kurallar belirlenmiş midir?	5 4 3 2 1		

Değerlendir

Şekil 4.18: Uygulama Web Anket Değerlendirme Arayüzü -7

Envanter uygulama ekranında soruların boş bırakılmamasını sağlamak için gerekli sayfa kontrolleri de bulunmaktadır.

Envanter uygulamasının son aşaması "Değerlendirme" kısmıdır. Burada, kurum/şirketin verdiği bilgilere dayanılarak ISO27001 ana başlıklarına göre bir değerlendirme yapılarak sonuçlar üretilip ekranda sunulmaktadır.

Şekil 4.19, Şekil 4.20, Şekil 4.21, Şekil 4.22, Şekil 4.23, Şekil 4.24, Şekil 4.25 ve Şekil 4.26 değerlendirme sonuç ekranlarını göstermektedir.

Şekil 4.19: Uygulama Web Anket Değerlendirme Arayüzü -8

Envanter yanıtlarının tutarlılığını saptamak için "3.2 Test Aracı Geliştirme" maddesinde de değinildiği gibi, çapraz denetim soruları kullanılmaktadır. Bu çalışma kapsamında, "dört" tane çapraz denetim sorusu kullanılmıştır. Ancak, yeni sorular ve yeni çapraz denetim soruları da envantere eklenebilmektedir. Sistem, çapraz denetim soru sayısından bağımsız olarak çalışabilmektedir.

Firma, Şekil 4.20'deki tablo yardımıyla ISO27001 ana alanlarını ne kadar başarılılıkta karşıladığını görebilir ya da Şekil 4.21'deki grafik yardımıyla izleyebilir. Ayrıca, her bir alt alanla ilgili olarak yapılan değerlendirmeleri de aynı ekranda görebilmektedir.

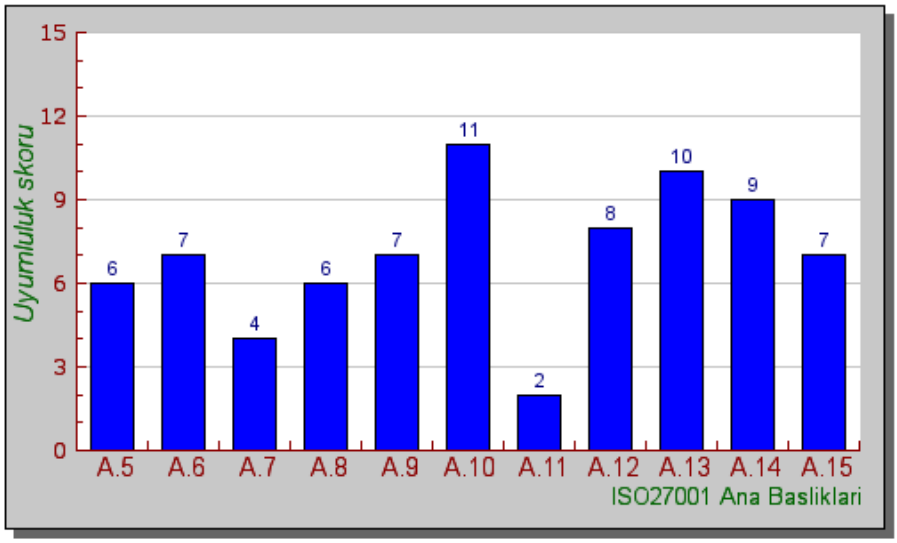
DEĞERLENDİRME

Firma Adı : *deneme*
Tarih : *15/9/2008*

ISO27001 Ana Başlıkları	Uyumluluk Skoru	% Uyumluluk
A.5. Güvenlik Politikası	6/15	40
A.6. Bilgi Güvenliği Organizasyonu	7/15	46.7
A.7. Varlık Yönetimi	4/15	26.7
A.8. İnsan Kaynakları Güvenliği	6/15	40
A.9. Fiziksel ve Çevresel Güvenlik	7/15	46.7
A.10. Haberleşme ve İşletim Yönetimi	11/15	73.3
A.11. Erişim Kontrolü	2/15	13.3
A.12. Bilgi Sistemleri Edinim, Geliştirme ve Bakımı	8/15	53.3
A.13. Bilgi Güvenliği İhlal Olayı Yönetimi	10/15	66.7
A.14. İş Sürekliliği Yönetimi	9/15	60
A.15. Uyum	7/15	46.7
TOPLAM	***77/165***	***46.7***

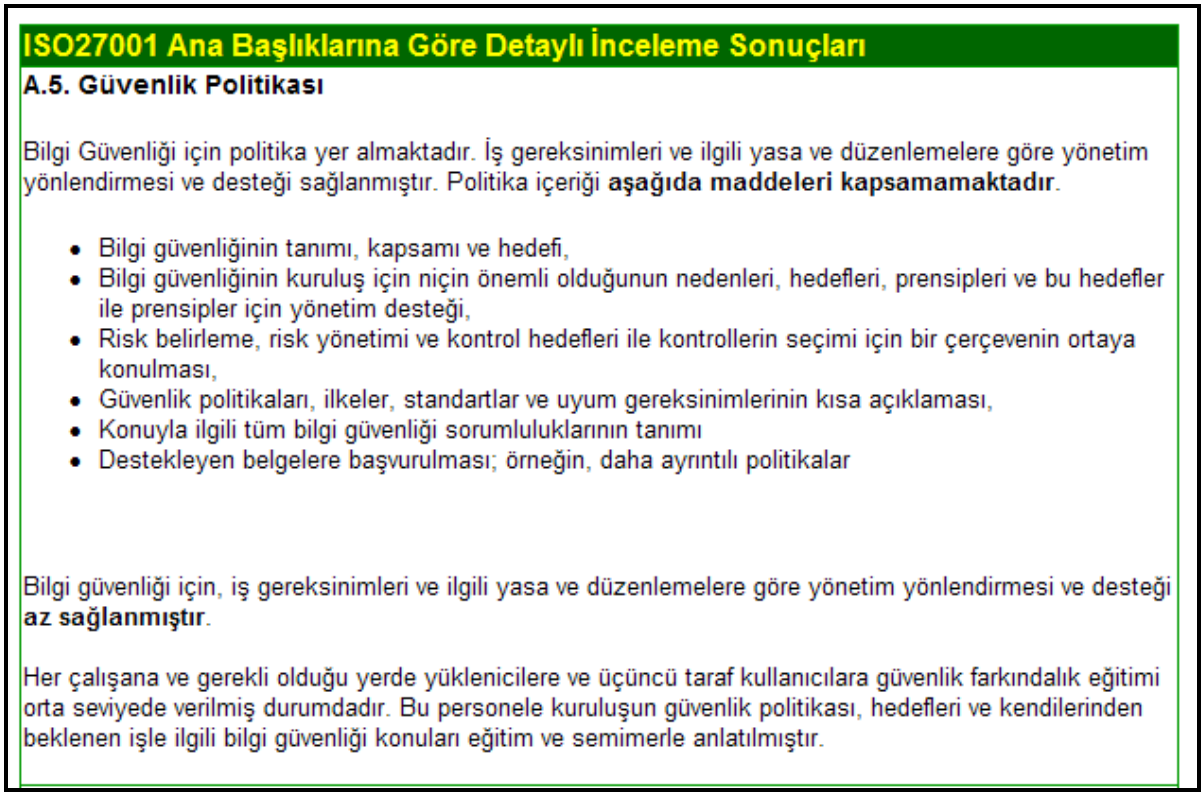
Şekil 4.20: Uygulama Web Anket Değerlendirme Arayüzü -9

Ana başlıklara göre standarda uyumluluk skorlarının dağılımı aşağıda grafiksel olarak gösterilmiştir. Skorun büyük olması, ilgili ana başlığa uyumun yüksek olması anlamına gelir.



ISO27001 ana başlıklarına göre firmanızın detaylı inceleme sonuçları aşağıda verilmektedir. Burada göreceğiniz çıkarımlar sadece "öneri" niteliğinde olup, şirketinizin halihazırdaki Bilgi Güvenliği Yönetim Sistemi altyapısının ISO27001 normlarına göre durumunu değerlendirebilmeniz amaçlanmıştır. ***Bu sonuçların, bir Bilgi Güvenliği uzmanı ile birlikte değerlendirilmesi tavsiye edilir.***

Şekil 4.21: Uygulama Web Anket Değerlendirme Arayüzü -10



Şekil 4.22: Uygulama Web Anket Değerlendirme Arayüzü -11

A.6. Bilgi Güvenliği Organizasyonu

Yönetim kuruluş içinde güvenliği açık yönlendirme, gösterilen bağlılık, açık atama ve bilgi güvenliği sorumluluklarının kabulü ile etkin şekilde desteklenmiştir.

Bilgi Güvenliğine yönelik dokümantasyon çalışması tamamlanmaya çalışılmaktadır.

Bilgi güvenliği faaliyetleri, kuruluşun farklı bölümlerinden uygun rolleri ve iş fonksiyonları olan temsilciler tarafından koordine edilmektedir.Bilgi güvenliği sorumlulukları kısmen tanımlanmıştır.

A.7. Varlık Yönetimi

Kurumsal varlıkların uygun şekilde korumasını sağlanmıştır.Önemli tüm varlıklar için bir sahibin atanması ve atanan bu şahsın varlığın sahibi olması nedeniyle ortaya çıkan vazifelerin ve görevlerin farkında olunması sağlanmıştır. Varlık sınıflandırması ve bu sınıflandırmanın güncellenmesine ilişkin kayıtlar ve varlık sahibinin bu faaliyetlerde gerçekten yer aldığının kanıtlayan dokümanlar bulunmaktadır.Varlığın iş değeri ve iş değerinin kuruluşun iş alanlarındaki önemi hakkında bir değerlendirme yaparak risk belirlenmiştir.Bilgi işleme alınırken, beklenen koruma seviyesi, ihtiyaç ve öncelikleri belirtmek için bilgi sınıflandırılma yapılmıştır.

Tüm personel, güvenlik gereksinimleri ve diğer iş kontrolleri de dahil olmak üzere gerekli politikalar ve yöntemler konusunda eğitilmiştir.Personel aynı zamanda BT ürünleri ve işle ilgili güvenlik yöntemleri kadar çalıştıkları pozisyon itibarıyla bilmeleri gereken paketleri kullanma konusunda da eğitilmişlerdir.

Varlıkların kabul edilebilir kullanım kuralları tanımlanmalı, belgeye dönüştürülmeli ve gerçekleştirilmelidir.

A.8. İnsan Kaynakları Güvenliği

Güvenlik sorumlulukları iş tanımlarında ve çalışma koşullarında istihdam öncesinde yeterince belirtilmelidir.Özellikle hassas görevlerde istihdam edilecek tüm adaylar, yükleniciler ve üçüncü taraf kullanıcıları ciddi bir elemeden geçirilmelidir.Bilgi işlem ünitelerinin çalışanları, yükleniciler ve üçüncü taraf kullanıcılar üstlendikleri güvenlik görev ve sorumluluklarına ilişkin bir anlaşma imzalamalıdır.İstihdamın sonlandırılması ve değişiklik yapılması konusunda yöntemleri ve sorumlulukları belirlenmelidir.

Bu şirket için disiplin süreci yazılı olarak belirtilmiş ve idari personel bu sürecin ayrıntılarını bilmemektedir. Disiplin süreci düzgün şekilde işletilmemektedir.

Şekil 4.23: Uygulama Web Anket Değerlendirme Arayüzü -12

A.8. İnsan Kaynakları Güvenliği

Güvenlik sorumlulukları iş tanımlarında ve çalışma koşullarında istihdam öncesinde yeterince belirtilmelidir.Özellikle hassas görevlerde istihdam edilecek tüm adaylar, yükleniciler ve üçüncü taraf kullanıcıları ciddi bir elemeden geçirilmelidir.Bilgi işlem ünitelerinin çalışanları, yükleniciler ve üçüncü taraf kullanıcılar üstlendikleri güvenlik görev ve sorumluluklarına ilişkin bir anlaşma imzalamalıdır.İstihdamın sonlandırılması ve değişiklik yapılması konusunda yöntemleri ve sorumlulukları belirlenmelidir.

Bu şirket için disiplin süreci yazılı olarak belirtilmiş ve idari personel bu sürecin ayrıntılarını bilmemektedir. Disiplin süreci düzgün şekilde işletilmemektedir.

İstihdamın sonlandırılmasını veya değiştirilmesini gerçekleştirme sorumlulukları açıkça tanımlanmıştır ve uygulanmaktadır.

A.9. Fiziksel ve Çevresel Güvenlik

Güvenli alanlar, yalnız yetkili personelin erişime izin verilmesini sağlamak için uygun giriş kontrolleriyle korunmaktadır.

Ofisler, odalar ve olanaklar için fiziksel güvenlik tasarlanmalı ve uygulanmalıdır.

Veri taşıyan ya da bilgi hizmetlerini destekleyen elektrik ve haberleşme kabloları, kesilme ya da hasarlardan korunmaya çalışılmaktadır.

A.10. Haberleşme ve İşletim Yönetimi

Geliştirme, test ve işletim olanakları, işletilen sisteme yetkisiz erişim veya değişiklik risklerini azaltmak için ayrılmıştır.

Üçüncü taraflarla hizmet sunulan durumlar için sözleşme ve prosedürler mevcuttur.

Bilgi ve yazılımlara ait yedekleme kopyaları alınmakta ve anlaşılan yedekleme politikasına uygun şekilde düzenli olarak test edilmektedir.

Şekil 4.24: Uygulama Web Anket Değerlendirme Arayüzü -13

A.10. Haberleşme ve İşletim Yönetimi

Geliştirme, test ve işletim olanakları, işletilen sisteme yetkisiz erişim veya değişiklik risklerini azaltmak için ayrılmıştır.

Üçüncü taraflarla hizmet sunulan durumlar için sözleşme ve prosedürler mevcuttur.

Bilgi ve yazılımlara ait yedekleme kopyaları alınmakta ve anlaşılan yedekleme politikasına uygun şekilde düzenli olarak test edilmektedir.

A.11. Erişim Kontrolü

Bilgiyi işleyen tüm sistemler için kullanıcıdan bağımsız ve kullanıcı tarafından erişilemeyen bir denetim kaydı tutulmaktadır.

Erişim için iş ve güvenlik gereksinimlerini temel alan bir erişim kontrol politikası kurulmalı, dokümante edilmeli ve gözden geçirilmelidir.

Kağıtlar ve taşınabilir depolama ortamları için bir temiz masa politikası ve bilgi işleme olanakları için bir temiz ekran politikası benimsenmelidir.

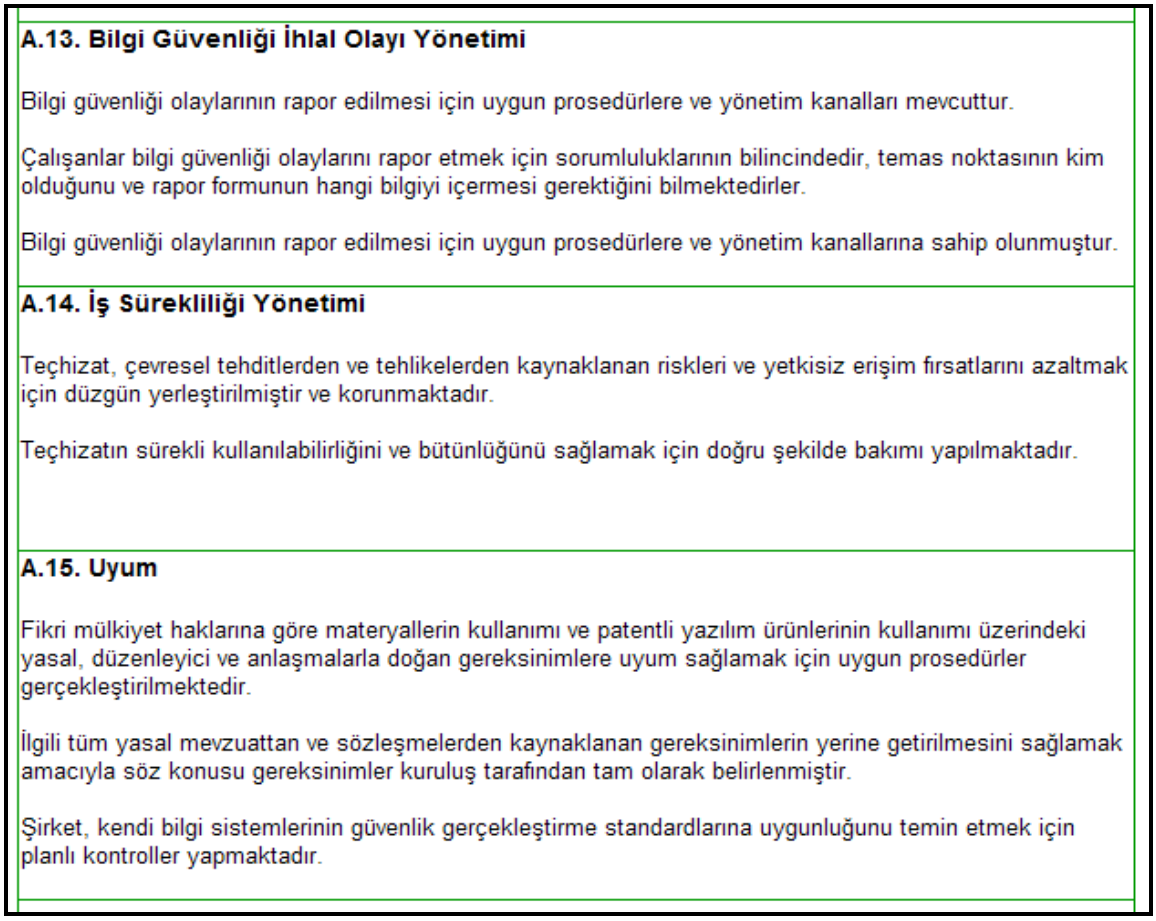
A.12. Bilgi Sistemleri Edinim, Geliştirme ve Bakımı

Kağıtlar ve taşınabilir depolama ortamları için bir temiz masa politikası ve bilgi işleme olanakları için bir temiz ekran politikası benimsenmiştir.

Bilginin korunması için kriptografik kontrollerin kullanımına ilişkin bir politika geliştirilmiştir.

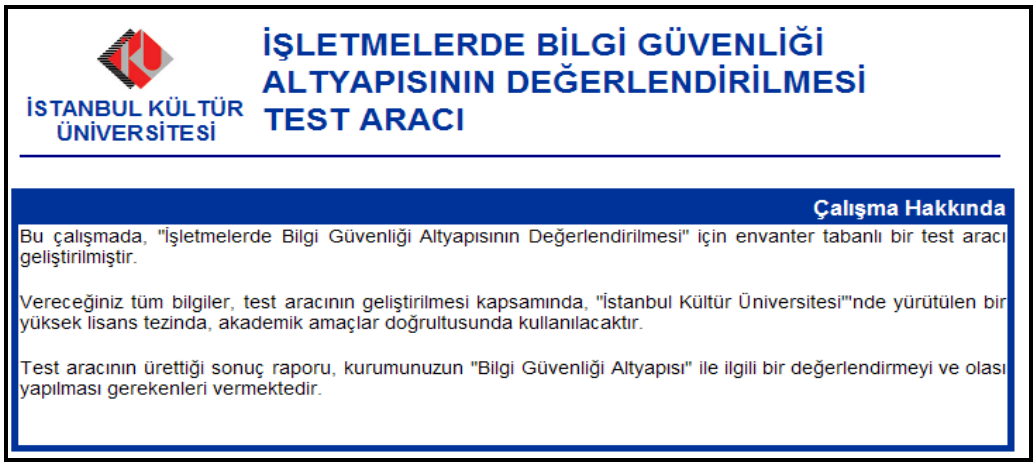
Kuruluş, yayımlanan teknik açıklıklar ve teknik açıklıkları istismar eden saldırılara karşı korunmak için tanımlanmış olan kendi gereksinimler ile ilgili riskleri belirlemeli ve teknik açıklıklar için uygun bir yönetim sürecini hayata geçirmiştir.

Şekil 4.25: Uygulama Web Anket Değerlendirme Arayüzü -14



Şekil 4.26: Uygulama Web Anket Değerlendirme Arayüzü -15

Şekil 4.27 ise, uygulama giriş sayfasında "Çalışma Hakkında" linki seçildiğindegelen kısa bilgi ekranını göstermektedir.

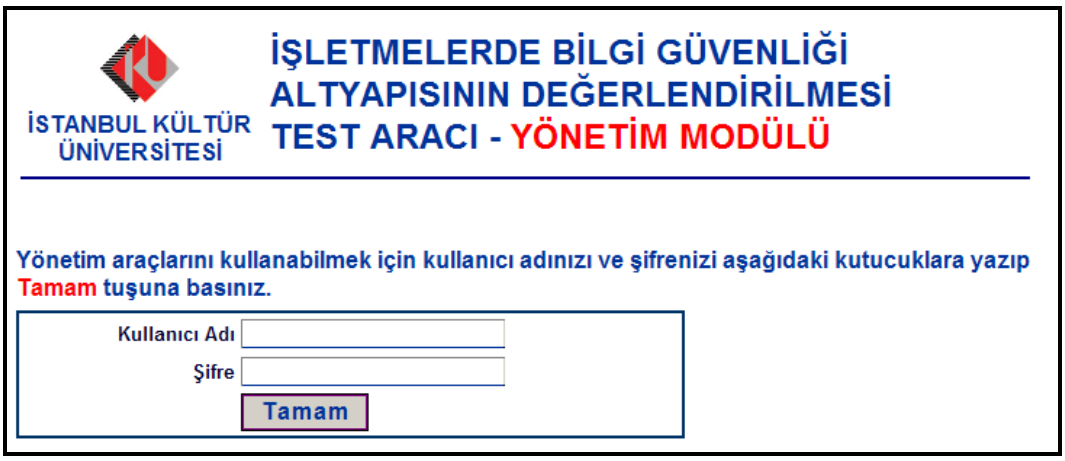


Şekil 4.27: Uygulama Değerlendirme Arayüzü -16

4.6 Test Aracı Yönetim Modülü

Test aracının ana işlevlerinden birisi de, değerlendirme sorularının ve yorumların değiştirilebilir nitelikte olmasıdır. Böylece, değerlendirme ekranlarına, sözgelimi, ISO27001 dışında başka alanlar da eklenebilir ya da mevcutlar değiştirilebilir. Ayrıca, envanter soruları ve yorumları da değiştirilerek test aracının sürekliliği ve güncelliği sağlanmış olacaktır.

Test aracı yönetim modülüne erişimin kısıtlanması için basit bir kullanıcı adı – parola ekranıyla giriş yapılır. Şekil 4.28., ana giriş ekranını göstermektedir.



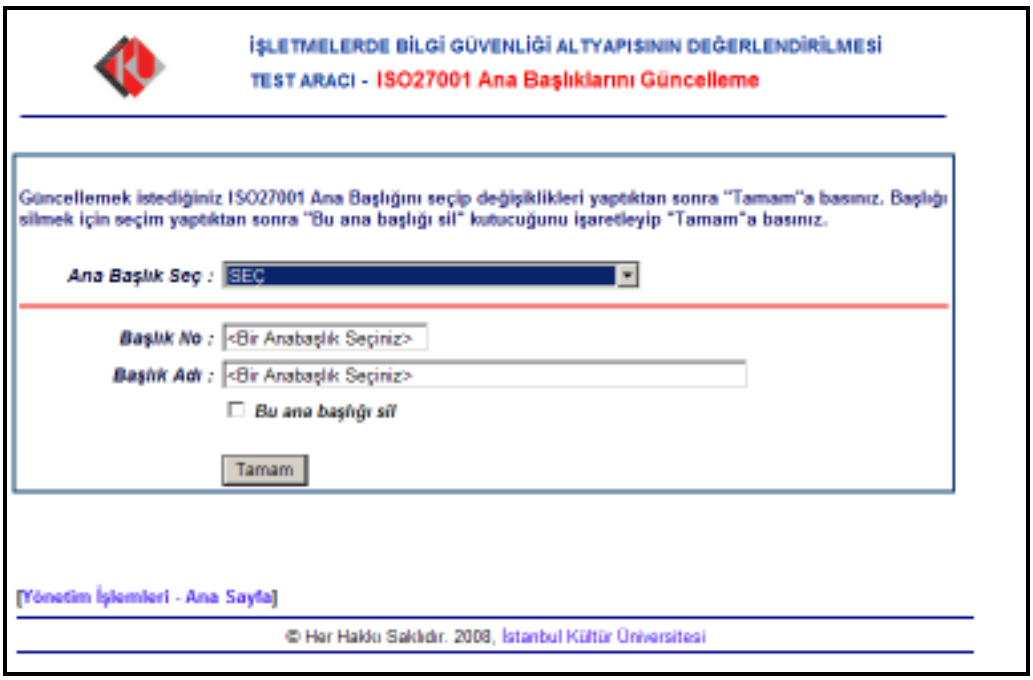
Şekil 4.28: Uygulama Web Anket Değerlendirme Arayüzü -17

Şekil 4.29'da ise, Yönetim Modülü'nün sağladığı araçları göstermektedir. Bunlar :

- Ana başlıkların güncellenmesi (ve silinmesi)
- Yeni ana başlık ekleme
- Envanter sorularını güncelleme (ve silme)
- Sistemde kayıtlı envanterler (listeleme ve silme)

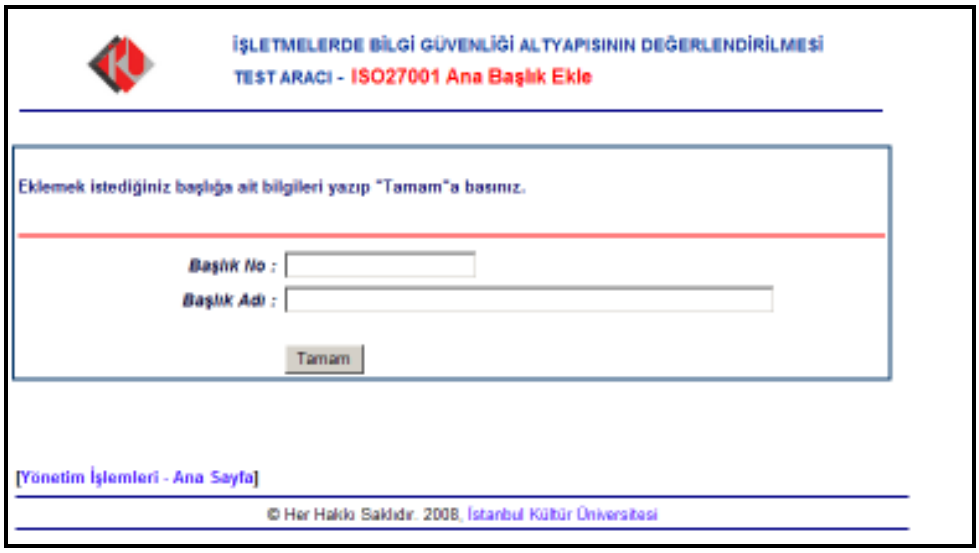
Şekil 4.29: Yönetim İşlemleri

Şekil 4.30, "Ana Başlık Güncelleme ve Silme" ekranını göstermektedir. Güncellenecek/silinecek ana başlık seçilerek işlem gerçekleştirilir.



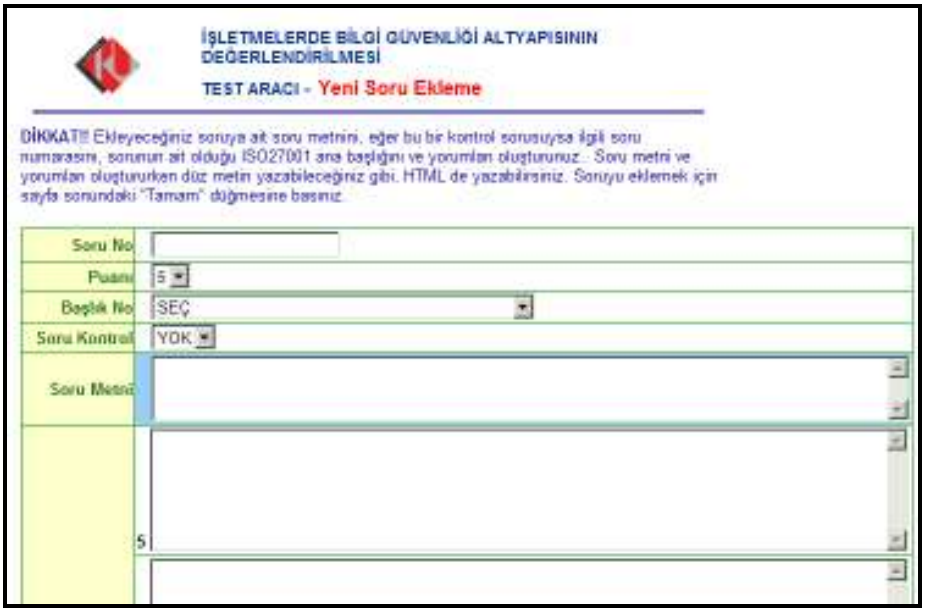
Şekil 4.30: Ana Başlık Güncelleme

Şekil 4.31, ana başlık ekleme seçildiğinde karşılaşılan ekranı göstermektedir.



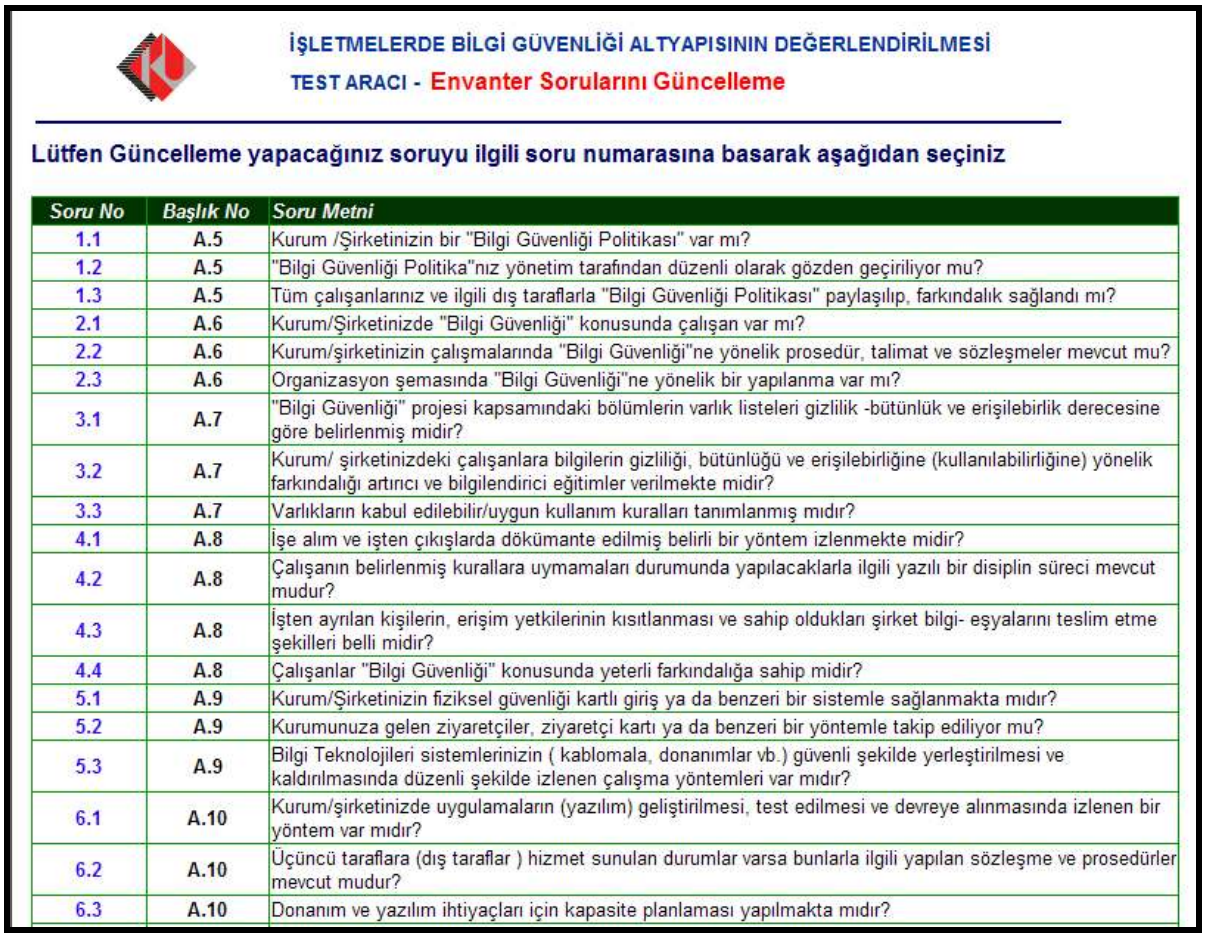
Şekil 4.31: Ana Başlık Ekleme

Şekil 4.32, envantere yeni soru ekleme ekranını göstermektedir.



Şekil 4.32: Yeni Soru Ekleme

Şekil 4.33, güncellemek için seçilecek envanter sorusunun listelendiği ekranı; Şekil 4.34 ve Şekil 4.35 ise soru güncelleme ekranını göstermektedir.



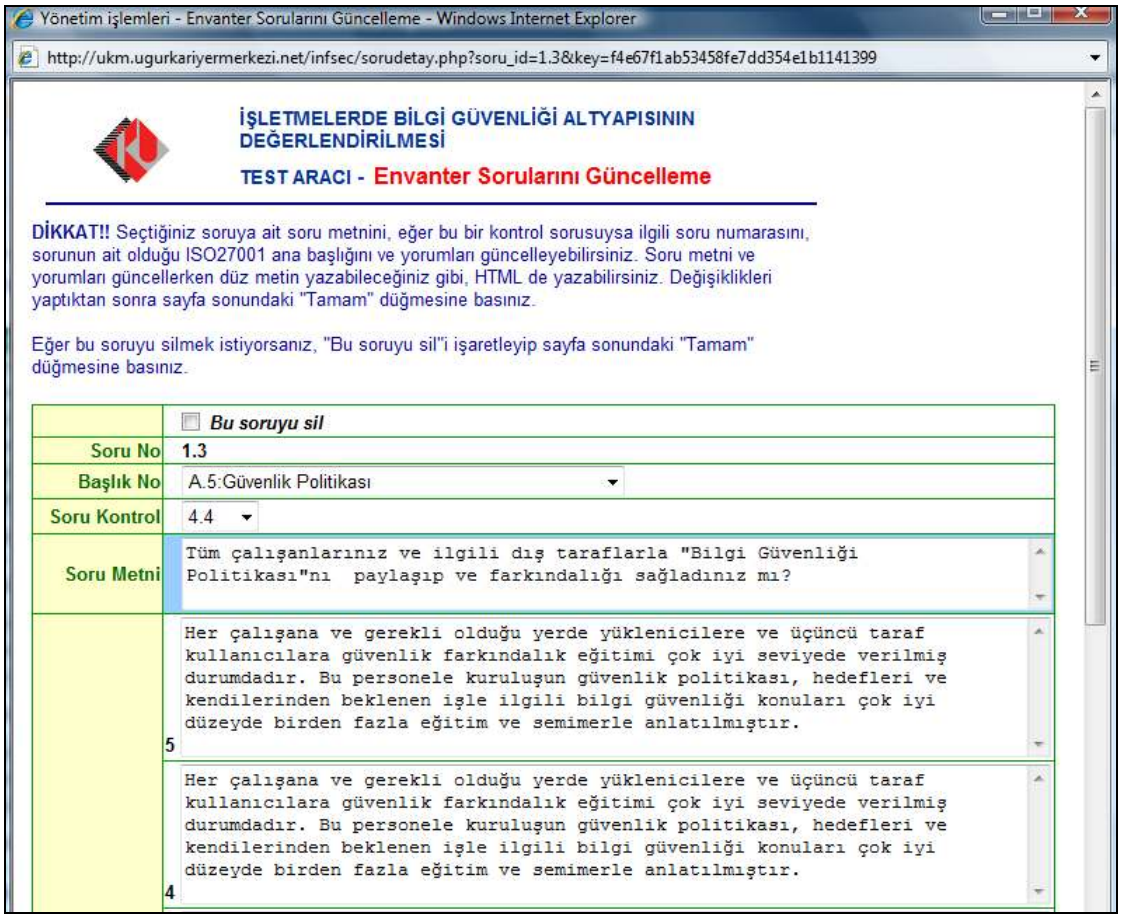
İŞLETMELERDE BİLGİ GÜVENLİĞİ ALTYAPISININ DEĞERLENDİRİLMESİ

TEST ARACI - Envanter Sorularını Güncelleme

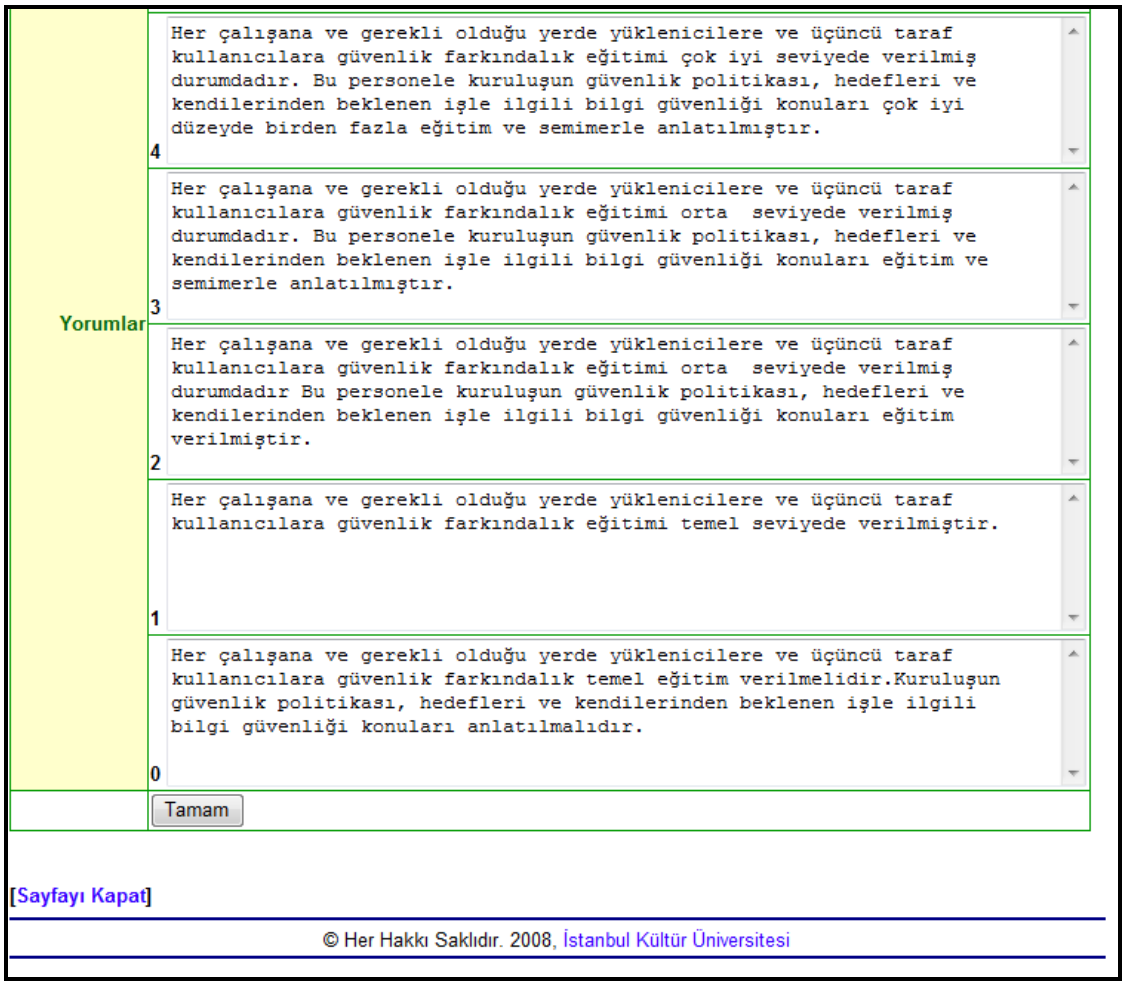
Lütfen Güncelleme yapacağınız soruyu ilgili soru numarasına basarak aşağıdan seçiniz

Soru No	Başlık No	Soru Metni
1.1	A.5	Kurum /Şirketinizin bir "Bilgi Güvenliği Politikası" var mı?
1.2	A.5	"Bilgi Güvenliği Politika"nız yönetim tarafından düzenli olarak gözden geçiriliyor mu?
1.3	A.5	Tüm çalışanlarınız ve ilgili dış taraflarla "Bilgi Güvenliği Politikası" paylaşılıp, farkındalık sağlandı mı?
2.1	A.6	Kurum/Şirketinizde "Bilgi Güvenliği" konusunda çalışan var mı?
2.2	A.6	Kurum/şirketinizin çalışmalarında "Bilgi Güvenliği"ne yönelik prosedür, talimat ve sözleşmeler mevcut mu?
2.3	A.6	Organizasyon şemasında "Bilgi Güvenliği"ne yönelik bir yapılanma var mı?
3.1	A.7	"Bilgi Güvenliği" projesi kapsamındaki bölümlerin varlık listeleri gizlilik -bütünlük ve erişilebirlik derecesine göre belirlenmiş midir?
3.2	A.7	Kurum/ şirketinizdeki çalışanlara bilgilerin gizliliği, bütünlüğü ve erişilebirliğine (kullanılabilirliğine) yönelik farkındalığı artırıcı ve bilgilendirici eğitimler verilmekte midir?
3.3	A.7	Varlıkların kabul edilebilir/uygun kullanım kuralları tanımlanmış mıdır?
4.1	A.8	İşe alım ve işten çıkışlarda dökümante edilmiş belirli bir yöntem izlenmekte midir?
4.2	A.8	Çalışanın belirlenmiş kurallara uymamaları durumunda yapılacaklarla ilgili yazılı bir disiplin süreci mevcut mudur?
4.3	A.8	İşten ayrılan kişilerin, erişim yetkilerinin kısıtlanması ve sahip oldukları şirket bilgi- eşyalarını teslim etme şekilleri belli midir?
4.4	A.8	Çalışanlar "Bilgi Güvenliği" konusunda yeterli farkındalığa sahip midir?
5.1	A.9	Kurum/Şirketinizin fiziksel güvenliği kartlı giriş ya da benzeri bir sistemle sağlanmakta mıdır?
5.2	A.9	Kurumunuza gelen ziyaretçiler, ziyaretçi kartı ya da benzeri bir yöntemle takip ediliyor mu?
5.3	A.9	Bilgi Teknolojileri sistemlerinizin (kablomala, donanımlar vb.) güvenli şekilde yerleştirilmesi ve kaldırılmasında düzenli şekilde izlenen çalışma yöntemleri var mıdır?
6.1	A.10	Kurum/şirketinizde uygulamaların (yazılım) geliştirilmesi, test edilmesi ve devreye alınmasında izlenen bir yöntem var mıdır?
6.2	A.10	Üçüncü taraflara (dış taraflar) hizmet sunulan durumlar varsa bunlarla ilgili yapılan sözleşme ve prosedürler mevcut mudur?
6.3	A.10	Donanım ve yazılım ihtiyaçları için kapasite planlaması yapılmakta mıdır?

Şekil 4.33: Envanter Sorularını Güncelleme – Soru Seçimi

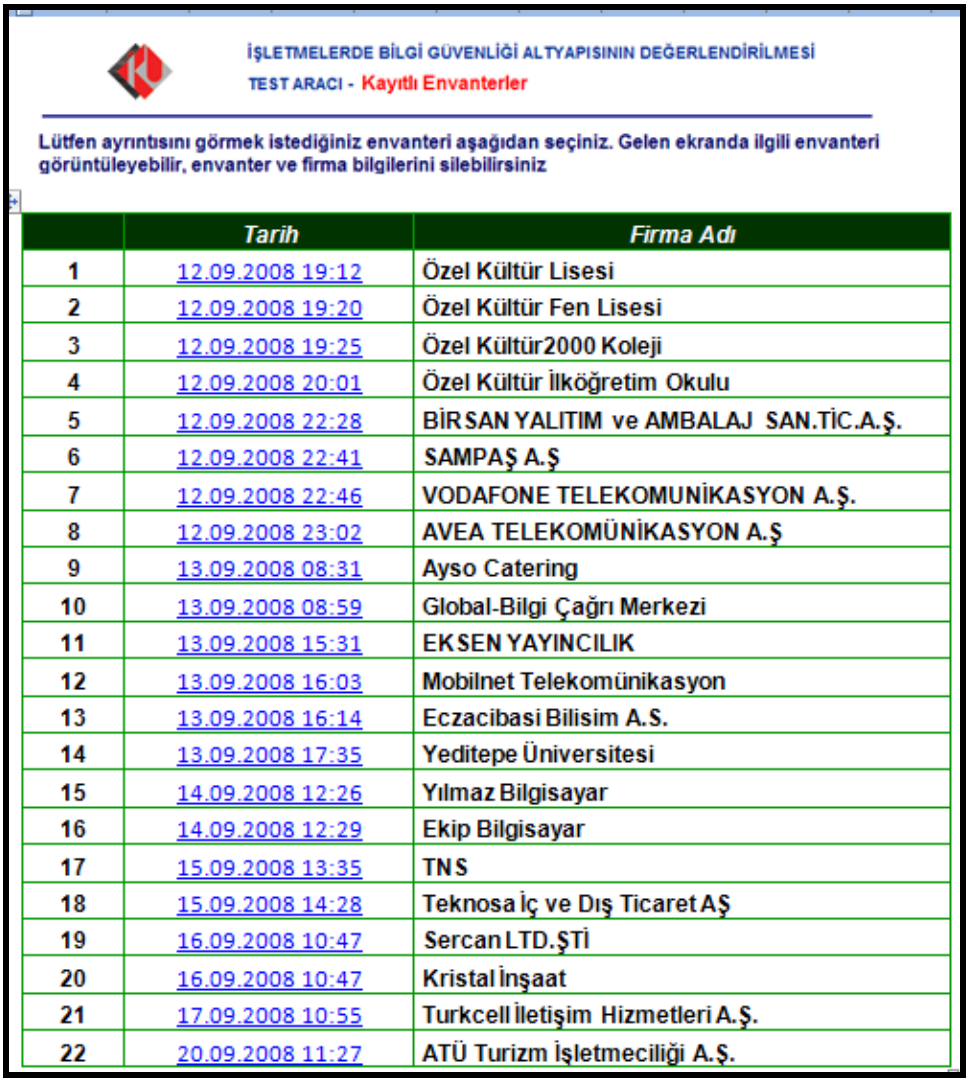


Şekil 4.34: Envanter Sorularını Güncelleme – 1



Şekil 4.35: Envanter Sorularını Güncelleme – 2

Yönetim modülü yardımıyla, ayrıca, kayıtlı envanterler listelenebilmekte ve silinebilmektedir. Şekil 4.36, sisteme kayıtlı envanterleri; Şekil 4.37 ve Şekil 4.38 ise, listeden seçilen bir envantere ait ayrıntılı girişleri ve sonuç raporunu göstermektedir.



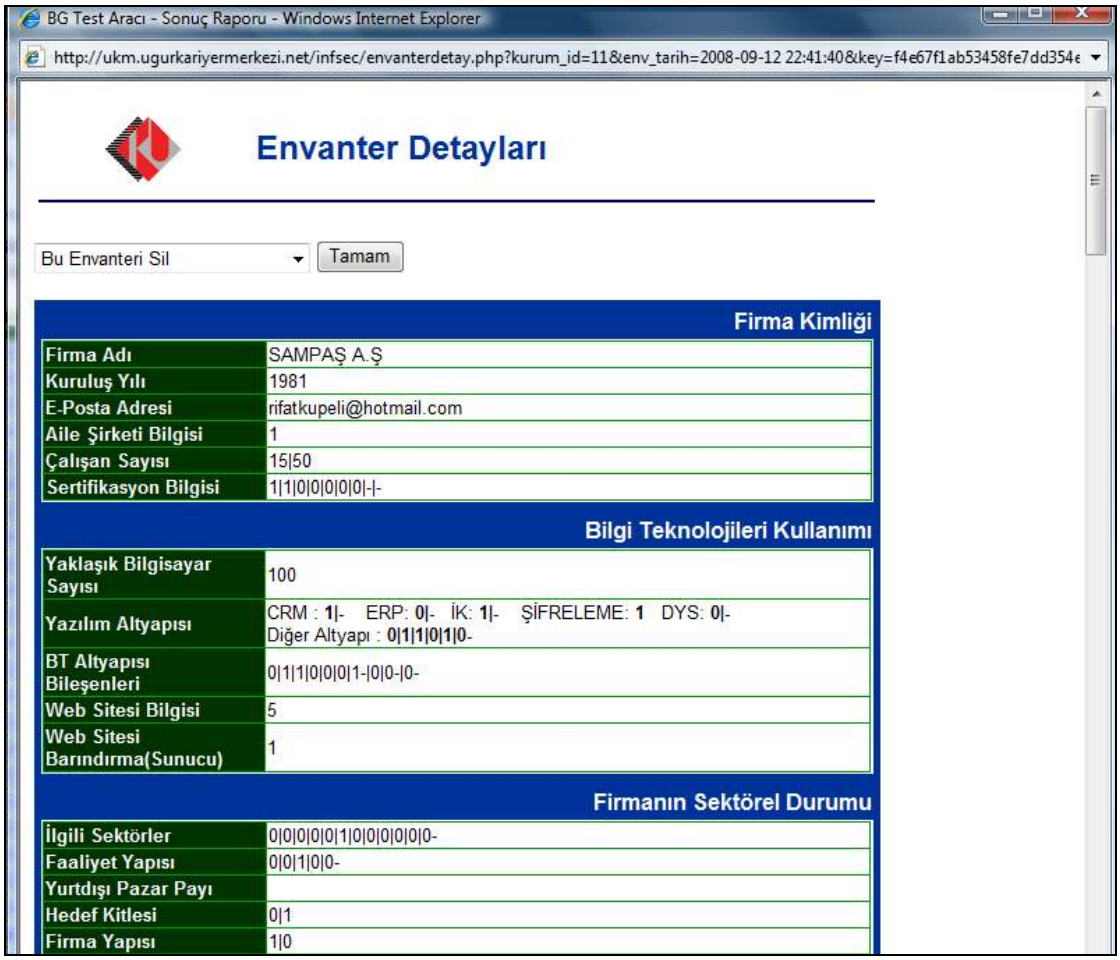
İŞLETMELERDE BİLGİ GÜVENLİĞİ ALTYAPISININ DEĞERLENDİRİLMESİ

TEST ARACI - Kayıtlı Envanterler

Lütfen ayrıntısını görmek istediğiniz envanteri aşağıdan seçiniz. Gelen ekranda ilgili envanteri görüntüleyebilir, envanter ve firma bilgilerini silebilirsiniz

	Tarih	Firma Adı
1	12.09.2008 19:12	Özel Kültür Lisesi
2	12.09.2008 19:20	Özel Kültür Fen Lisesi
3	12.09.2008 19:25	Özel Kültür2000 Koleji
4	12.09.2008 20:01	Özel Kültür İlköğretim Okulu
5	12.09.2008 22:28	BİRSAN YALITIM ve AMBALAJ SAN.TİC.A.Ş.
6	12.09.2008 22:41	SAMPAŞ A.Ş
7	12.09.2008 22:46	VODAFONE TELEKOMUNİKASYON A.Ş.
8	12.09.2008 23:02	AVEA TELEKOMÜNİKASYON A.Ş
9	13.09.2008 08:31	Ayso Catering
10	13.09.2008 08:59	Global-Bilgi Çağrı Merkezi
11	13.09.2008 15:31	EKSEN YAYINCILIK
12	13.09.2008 16:03	Mobilnet Telekomünikasyon
13	13.09.2008 16:14	Eczacibasi Bilisim A.S.
14	13.09.2008 17:35	Yeditepe Üniversitesi
15	14.09.2008 12:26	Yılmaz Bilgisayar
16	14.09.2008 12:29	Ekip Bilgisayar
17	15.09.2008 13:35	TNS
18	15.09.2008 14:28	Teknosa İç ve Dış Ticaret AŞ
19	16.09.2008 10:47	Sercan LTD.ŞTİ
20	16.09.2008 10:47	Kristal İnşaat
21	17.09.2008 10:55	Turkcell İletişim Hizmetleri A.Ş.
22	20.09.2008 11:27	ATÜ Turizm İşletmeciliği A.Ş.

Şekil 4.36: Kayıtlı Envanterler



Şekil 4.37: Seçilen envanterin listelenmesi-1

Doldurulan Envanter İle İlgili Bilgiler

Envanteri Dolduran	RIFAT KÜPELİ
Görevi	YAZILIM DESTEK UZMANI
Envanter Yanıt Katarı	444444433444333333343343343333333333

ENVANTER SONUÇ RAPORU

Envanter Değerlendirme

Firma Adı : *SAMPAŞ A.Ş*

Tarih : *2008-09-12 22:41:40*

ISO27001 Ana Başlıkları	Uyumluluk Skoru	% Uyumluluk
A.5. Güvenlik Politikası	12/15	80
A.6. Bilgi Güvenliği Organizasyonu	12/15	80
A.7. Varlık Yönetimi	9/15	60
A.8. İnsan Kaynakları Güvenliği	9/15	60
A.9. Fiziksel ve Çevresel Güvenlik	10/15	66.7
A.10. Haberleşme ve İşletim Yönetimi	11/15	73.3
A.11. Erişim Kontrolü	9/15	60
A.12. Bilgi Sistemleri Edinim, Geliştirme ve Bakımı	9/15	60
A.13. Bilgi Güvenliği İhlal Olayı Yönetimi	9/15	60
A.14. İş Sürekliliği Yönetimi	12/15	80
A.15. Uyum	10/15	66.7
TOPLAM	***112/165***	***67.9***

Şekil 4.38: Seçilen envanterin listelenmesi-2

5 SONUÇLAR VE TARTIŞMA

5.1 Sonuçlar

Kurumsal Bilgi Güvenligi insan, eğitim, teknoloji gibi birçok faktörün etki ettigi yönetilmesi zorunlu olan karmasık süreçlerden oluşmaktadır. Bu süreçlerin yönetilmesi, güvenlik sistemlerinin uluslararası standartlarda yapılandırılması ve yüksek seviyede bilgi güvenligi sağlanması amacıyla tüm dünyada kurumsal Bilgi Güvenliginin yönetimi konusunda standartlasma çalısmaları hızla sürmektedir.

ISO–27001:2005 standardı ile ülkemizde Türk Standartları Enstitüsü (TSE) tarafından TS ISO/IEC 27001 "Bilgi Güvenligi Yönetim Sistemi" standardı adı altında yayınlanmasıyla birlikte, Bilgi Güvenliği ve belgeleme çalısmaları başlatılmıstır. Bu standart kapsamında kurumsal bilgi varlıklarının güvenliğinin istenilen düzeyde saglanabilmesi amacıyla; gizlilik, bütünlük ve erişilebilirlik/kullanılabilirlik gibi güvenlik unsurlarının kurumlar tarafından sağlanması gerekmektedir [17].

Ülkemizde Bilgi Güvenliği kavramı yeni yaygınlaşmaya başlamış ve birçok firma bu konuda çalışmalar yapmaktadır. Bu tez çalışması kapsamında geliştirilen "**İŞLETMELERDE BİLGİ GÜVENLİĞİ ALTYAPISININ DEĞERLENDİRİLMESİ TEST ARACI",** Eylül 2008 içinde 22 ayrı firmaya uygulanmıştır.Bu kurum/şirketlerden bazıları Bilgi Güvenliği konusunda önemli çalışmalar yapıp, sertifila sahibi iken bir kısmıda Bilgi Güvenliği konusunda hiçbir çalışma yapmamış ancak kendi bünyesinde güvenliği sağlamaya çalışan şirketlerdi. Elde ettiğimiz sonuçlar doğrultusunda Şekil 5.1., uygulama yapılan firmaların listesini ve uygulama tarihlerini göstermektedir.

	Tarih	Firma Adı
1	12.09.2008 19:12	Özel Kültür Lisesi
2	12.09.2008 19:20	Özel Kültür Fen Lisesi
3	12.09.2008 19:25	Özel Kültür2000 Koleji
4	12.09.2008 20:01	Özel Kültür İlköğretim Okulu
5	12.09.2008 22:28	BİRSAN YALITIM ve AMBALAJ SAN.TİC.A.Ş.
6	12.09.2008 22:41	SAMPAŞ A.Ş
7	12.09.2008 22:46	VODAFONE TELEKOMUNİKASYON A.Ş.
8	12.09.2008 23:02	AVEA TELEKOMÜNİKASYON A.Ş
9	13.09.2008 08:31	Ayso Catering
10	13.09.2008 08:59	Global-Bilgi Çağrı Merkezi
11	13.09.2008 15:31	EKSEN YAYINCILIK
12	13.09.2008 16:03	Mobilnet Telekomünikasyon
13	13.09.2008 16:14	Eczacibasi Bilisim A.S.
14	13.09.2008 17:35	Yeditepe Üniversitesi
15	14.09.2008 12:26	Yılmaz Bilgisayar
16	14.09.2008 12:29	Ekip Bilgisayar
17	15.09.2008 13:35	TNS
18	15.09.2008 14:28	Teknosa İç ve Dış Ticaret AŞ
19	16.09.2008 10:47	Sercan LTD.ŞTİ
20	16.09.2008 10:47	Kristal İnşaat
21	17.09.2008 10:55	Turkcell İletişim Hizmetleri A.Ş.
22	20.09.2008 11:27	ATÜ Turizm İşletmeciliği A.Ş.

Şekil 5.1. Uygulama yapılan firmalar

Geliştirilen test aracının doğruluğunu sınamak için, daha önceden Bilgi Güvenliği Yönetim Sistemi altyapısı olan bazı firmalara uygulama yapılmıştır. Şekil 5.2., Vodafone Telekominikasyon; Şekil 5.3. ise Avea Telekominikasyon için elde edilen sonuçları göstermektedir. Her iki firmada da "Bilgi Güvenliği Yönetimi" altyapısı bulunmaktadır ve envanteri dolduran kişiler, ilgili firmaların Bilgi Teknolojilerinden sorumlu kişilerdir.

Elde edilen sonuçlara göre, her iki test firmasında da ana başlıklara gore %100 uyum olduğu ortaya çıkmıştır ve uyumluluk skoru 165 bulunmuştur. Bu sonuçlardan, uygulamanın başarılı bir şekilde çalıştığı sonucuna varılmıştır.

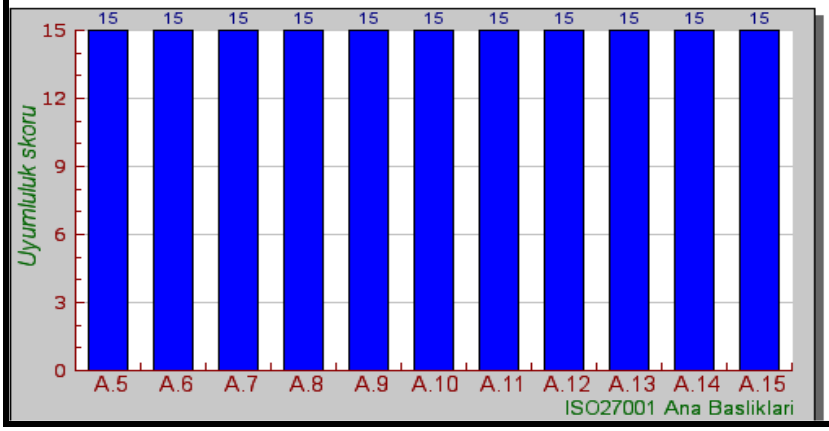
Envanter Değerlendirme

Firma Adı : ***VODAFONE TELEKOMUNİKASYON A.Ş.***

Tarih : ***2008-09-12 22:46:12***

ISO27001 Ana Başlıkları	Uyumluluk Skoru	% Uyumluluk
A.5. Güvenlik Politikası	15/15	100
A.6. Bilgi Güvenliği Organizasyonu	15/15	100
A.7. Varlık Yönetimi	15/15	100
A.8. İnsan Kaynakları Güvenliği	15/15	100
A.9. Fiziksel ve Çevresel Güvenlik	15/15	100
A.10. Haberleşme ve İşletim Yönetimi	15/15	100
A.11. Erişim Kontrolü	15/15	100
A.12. Bilgi Sistemleri Edinim, Geliştirme ve Bakımı	15/15	100
A.13. Bilgi Güvenliği İhlal Olayı Yönetimi	15/15	100
A.14. İş Sürekliliği Yönetimi	15/15	100
A.15. Uyum	15/15	100
TOPLAM	***165/165***	***100***

Ana başlıklara göre standarda uyumluluk skorlarının dağılımı aşağıda grafiksel olarak gösterilmiştir. Skorun büyük olması, ilgili ana başlığa uyumun yüksek olması anlamına gelir.



Şekil 5.2. Test aracının doğruluğunun sınanması-1

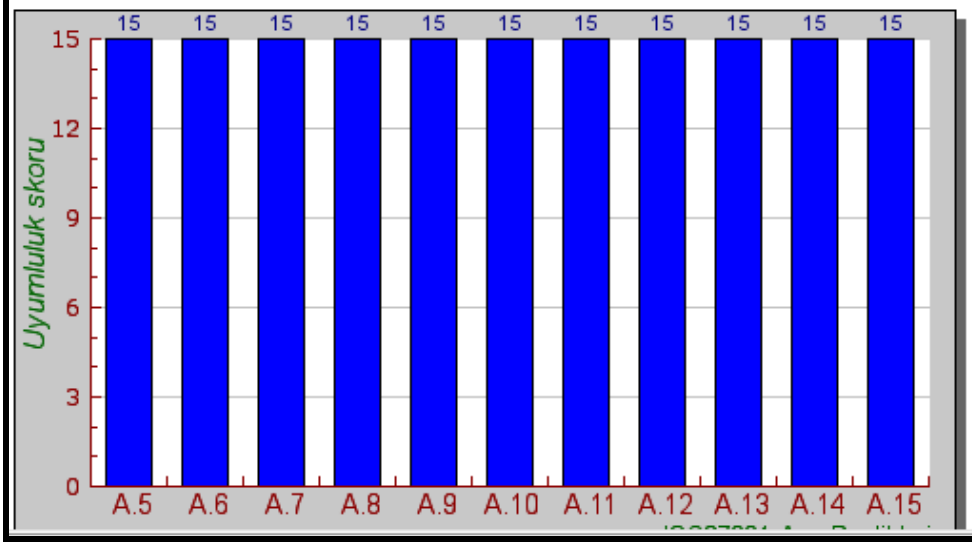
Envanter Değerlendirme

Firma Adı : *AVEA TELEKOMÜNİKASYON A.Ş*

Tarih : *2008-09-12 23:02:14*

ISO27001 Ana Başlıkları	Uyumluluk Skoru	% Uyumluluk
A.5. Güvenlik Politikası	15/15	100
A.6. Bilgi Güvenliği Organizasyonu	15/15	100
A.7. Varlık Yönetimi	15/15	100
A.8. İnsan Kaynakları Güvenliği	15/15	100
A.9. Fiziksel ve Çevresel Güvenlik	15/15	100
A.10. Haberleşme ve İşletim Yönetimi	15/15	100
A.11. Erişim Kontrolü	15/15	100
A.12. Bilgi Sistemleri Edinim, Geliştirme ve Bakımı	15/15	100
A.13. Bilgi Güvenliği İhlal Olayı Yönetimi	15/15	100
A.14. İş Sürekliliği Yönetimi	15/15	100
A.15. Uyum	15/15	100
TOPLAM	***165/165***	***100***

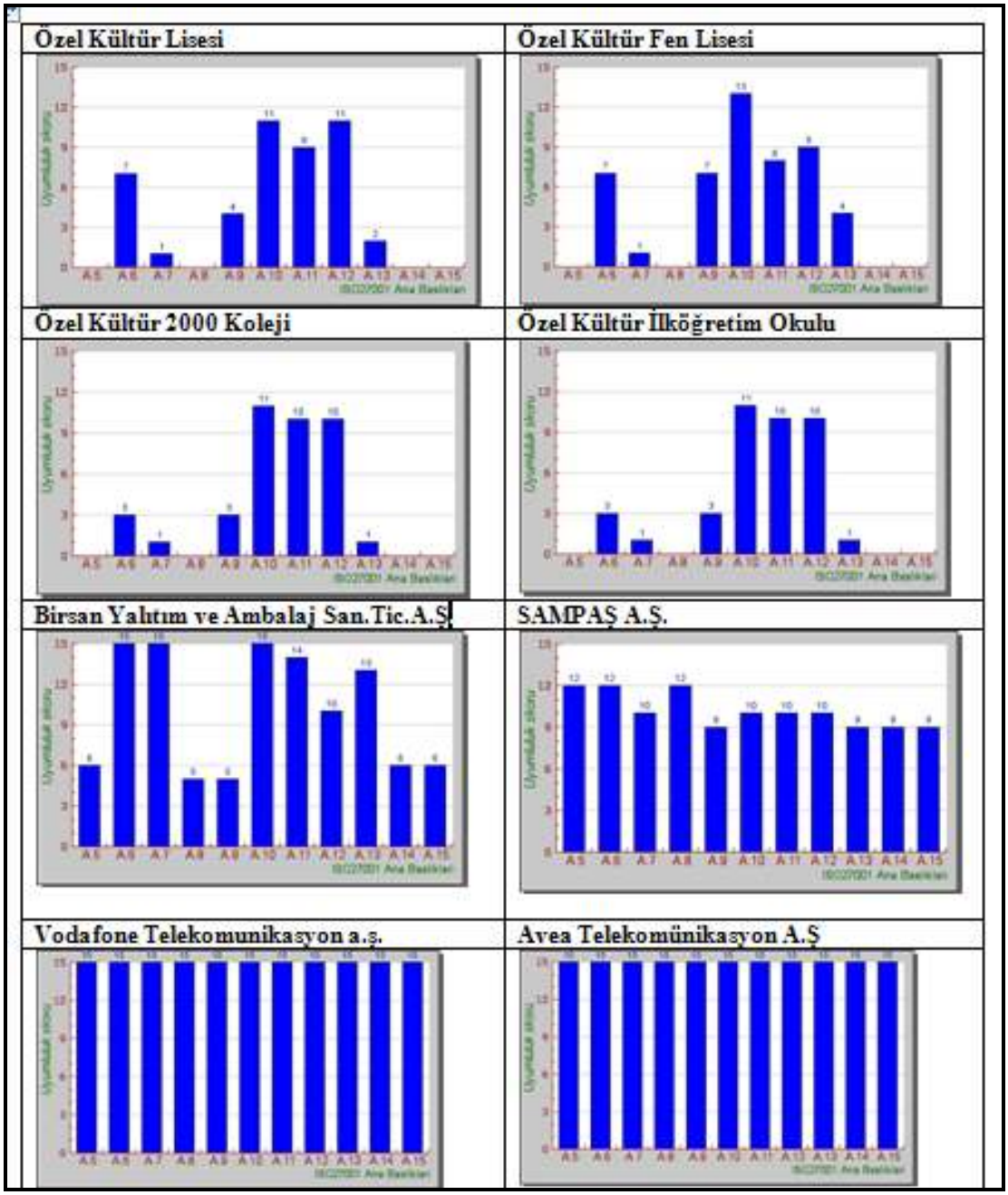
Ana başlıklara göre standarda uyumluluk skorlarının dağılımı aşağıda grafiksel olarak gösterilmiştir
Skorun büyük olması, ilgili ana başlığa uyumun yüksek olması anlamına gelir.



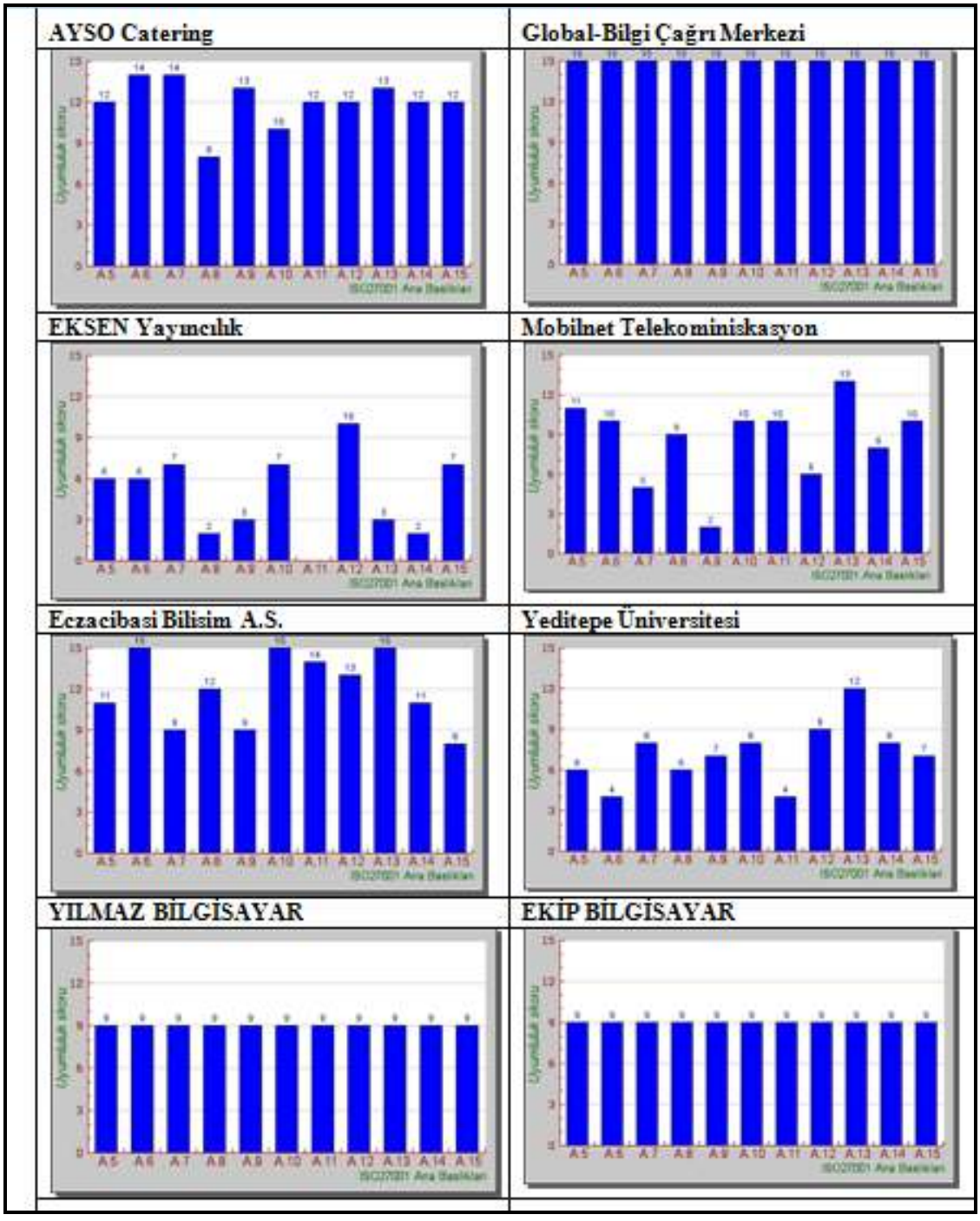
Şekil 5.3. Test aracının doğruluğunun sınanması-2

Şekil 5.4, Şekil 5.5 ve Şekil 5.6 ise, envanter uygulamasını çalıştırıp sonuç raporu üreten ve cevapları tutarlı olan 22 firmaya ait uyumluluk skorlarının dağılımını göstermektedir. Bu firmalar, deneme amaçlı girilen firmalar olmayıp gerçekten envanteri dolduran firmalardır.

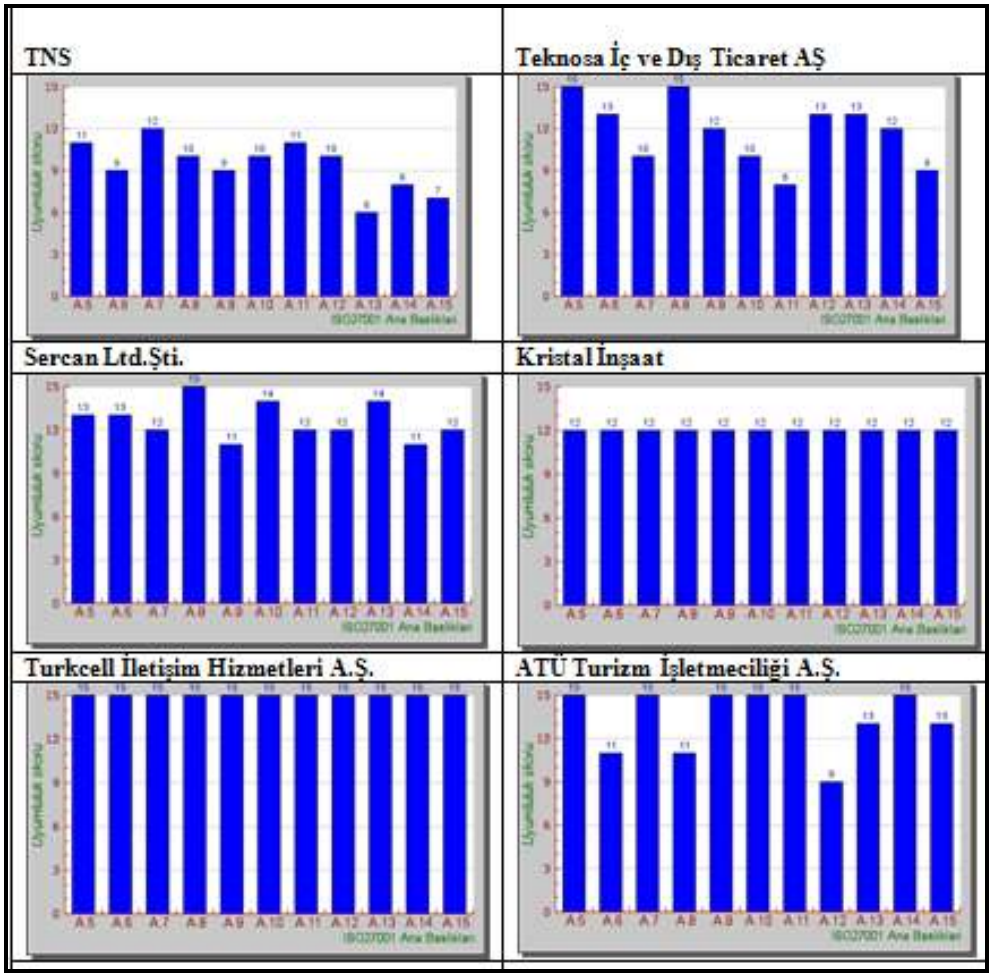
Kısıtlı envanter uygulaması sebebiyle, sonuçlar sektörlere göre gruplanmayıp hepsi aynı şekilde verilmiştir.



Şekil 5.4. Uyumluluk skorlarının dağılımı -1



Şekil 5.5. Uyumluluk skorlarının dağılımı -2



Şekil 5.6. Uyumluluk skorlarının dağılımı -3

Şekil 5.7., envanter dolduran firmaların ortalama uyum skorlarının dağılımını göstermektedir. Şekil 5.4, Şekil 5.5, Şekil 5.6 ve Şekil 5.7 incelendiğinde, ülkemizdeki kurum/şirketlerde genelde aşağıdaki bilgi güvenliği alanlarında uygulama eksikliği bulunduğundan söz edilebilir :

- Uyum
- İş Sürekliliği Yönetimi
- Bilgi Güvenliği İhlal Olayı Yönetimi

Bilgi Güvenliği standartında yer alan ve uygulaması kurum/şirketin faaliyetlerinin devamlılığı açısından oldukça önemli olan "Uyum", "İş Sürekliliği" ve "Bilgi Güvenliği İhlal Olayı Yönetimi" konularında yapılan anket çalışması sonucunda eksiklikler olduğu gözlenmiştir. Diğer alanlarda, özelliklede Bilgi Güvenliği konusund açalışmalar yapan şirketlerde oldukça iyi sonuçlarla karşılaşılmıştır.

ISO27001 Ana Başlıkları	Uyumluluk Skoru	% Uyumluluk
A.5. Güvenlik Politikası	9.51	63.4
A.6. Bilgi Güvenliği Organizasyonu	10.51	70.1
A.7. Varlık Yönetimi	9.61	64.1
A.8. İnsan Kaynakları Güvenliği	9.76	65.1
A.9. Fiziksel ve Çevresel Güvenlik	10.11	67.4
A.10. Haberleşme ve İşletim Yönetimi	10.77	71.8
A.11. Erişim Kontrolü	10.3	68.7
A.12. Bilgi Sistemleri Edinim, Geliştirme ve Bakımı	11.01	73.4
A.13. Bilgi Güvenliği İhlal Olayı Yönetimi	9.04	60.3
A.14. İş Sürekliliği Yönetimi	8.64	57.6
A.15. Uyum	5.93	39.5
TOPLAM	***105.19***	***63.8***

Şekil 5.7. Envanter dolduran firmalara ait ortalama uyum skorları

Sonuç olarak, güvenlik sadece teknoloji problemi olarak degil aynı zamanda insan ve yönetim problemi olarak degerlendirilmelidir [17]. Kurumun stratejik hedeflerini belirleyen en üstseviyedeki yönetim kademelerinin kurumsal bilgi güvenliğinin sağlanması için verecekleri destek ve kurum/şirket içinde oluşacak "Bilgi Güvenliği" konusundaki farkındalık çok önemlidir [1].

5.2 Tartışma

Bu çalışmada, kurumların bilgi güvenliğini hangi başarılılıkta uyguladıklarını saptamak için, ISO/IEC 27001:2007 Bilgi Güvenliği Yönetim Sistemi yaklaşımını esas alan ve açık sistem geliştirme enstrümanları kullanan web tabanlı bir test aracı geliştirilmiştir.

Test aracının güvenilirliği, Bilgi Güvenliği Yönetim Sistemi kurmuş iki ayrı firmanın sonuçları analiz edilerek gösterilmiştir.

Uygulama 22 firmaya denettirilerek kullandırılmış ve sonuçlar alınmıştır. Firmalara yaptırılan uygulamaların "kontrolsüz bir deney ortamı" olduğunu belirtmekte yarar vardır. Bu bakımdan, bu çalışmada, sonuçların genelleştirilerek değerlendirilmesi yerine, test aracının kullanımı daha fazla ön plana çıkartılmıştır.

Geliştirilen test aracına, tüm değerlendirme kriterlerinin sonradan değiştirilebilir nitelikte olması sebebiyle bilgi güvenliği konusundaki ilerde olabilecek olası yeni alanların da dahil edilebilmesi mümkündür.

Firmalar bu test aracını kullanarak kendi bilgi güvenliği yönetim sistemi altyapılarını hızlı bir şekilde değerlendirip hangi alanlarda eksiklikleri olduğunu saptayabilirler. Test aracının başarısı, envanter sorularının içtenlikle yanıtlanmasına bağlıdır.

Gelecekte yapılabilecek çalışmalar açısından, tüm kurum/şirketler ve envanter bilgilerinin merkezi bir veritabanında tutulması sebebiyle, yeterli veri toplandığında, ülke çapında genel ve sektörel bazda analizler yapmak da mümkün olacaktır. Böylece ülkemizdeki sektörlerin karşılaştırılması ve dünyadaki diğer sektörlerlede kıyaslanması mümkün olacaktır. Ayrıca test aracı, farklı standartlarla ilgili sorularında eklenmesi ile diğer standarlara yönelik değerlendirmeler yapılmasıda mümkündür. Daha da ileri çalışmalarda farklı standartların değerlendirilmesi ile aynı konuları içeren standartlar içinde ortak değerlendirmelere gidilebilir.

Envanter sorularının ve yorumların değiştirilebilir nitelikte olması, kurum/şirketlerden alınan veriler doğrultusunda içeriği daha da genişletilebilir. Zaman içinde en ideal soru ve yorumlar elde edilerek, Bilgi Güvenliği konusunda çalışma yapacak olan kurum/şirketlere ön proje aşamasında "Fark Çözümlemesi (GAP Analizi)" şeklinde değerlendirmeler yapılabilir. Aynı zamanda Bilgi güvenliği konusunda çalışan kurum/şirketlerde yaptıkları her yeni adım sonrasında anketi tekrar doldurarak, gelinen durumu takip edebilecektirler.

Son olarak, test aracının ürettiği çıkarımlar sadece "öneri" niteliğinde olup, kuruluşların halihazırdaki Bilgi Güvenliği Yönetim Sistemi altyapısının ISO27001 normlarına göre durumunu değerlendirebilmesi amaçlanmıştır. Bu sonuçların, bir Bilgi Güvenliği uzmanı ile birlikte değerlendirilmesi gerekmektedir.

6 KAYNAKLAR

[1] **Albrechtsen Eirik**., 2007. A qualitative study of users' view on information security, Yüksek Lisans tezi*, Norwagian University of Science and Technology*

[2] **Başhan F**., 2004. İşletmelerin ağ-bilgi sistemlerinde bilgi güvenliğinin yönetimi ve bir uygulama, Yüksek Lisans tezi, *Dumlupınar Üniversitesi*

[3] **Broderick J. S**., 2006. ISMS,Security standaerts and security regulations, Strategic Consulting, Symantec Corporation

[4] **Erkan A**., 2006. An automated tool for information security management system, Yüksek Lisans tezi, *Orta Doğu Teknik Üniversitesi*

[5] **Erkoç K**., 2004. Kriptoloji ve Bilgi Güvenliği, Yüksek Lisans Tezi, *Sakarya Üniversitesi*

[6] **Farn K.J., Lin S.K., Lo C**., 2007. A study on a Taiwan Information System Security Classification and Implementation, Yüksek Lisans tezi, *Loughborough University*

[7] **Furnell S.,** 2006. IFIP Workshop-Information Security Culture,Workshop, *Plymouth University*

[8] **Hu Q., Hart P**., Cooke D., 2007. The role of external and internal influences on information systems security- a neo-institutional perspective, Yüksek Lisans tezi, *Atlantic University*

[9] **Karabacak B**., 2003, Bilgi güvenliği risk analizi (BİGRA) metodu, Yüksek Lisans tezi, *Gebze Yüksek Teknoloji Enstitüsü · Mühendislik ve Fen Bilimleri Enstitüsü*

[10] **Karabacak B., Soğukpınar İ.**, 2006. A quantitative method for ISO 17799 gap analysis*, National Research Institute of Electronics & Cryptology (UEKAE), Gebze Yüksek Teknoloji Enstitüsü*

[11] **Kaya Ö**., 2003. An evaluation of electronic signature policy formation in Turkey (a comparative approach), Yüksek Lisans tezi, *Orta Doğu Teknik Üniversitesi · Enformatik Enstitüsü*

[12] **Kuo M.H**., 2007. An intelligent agent based collaborative information security framework, Yüksek Lisans tezi, *Chaoyang University of Technology*

[13] **Solms B., Solms R**., 2006. From information security to...business security?, *Johannesburg of University and Nelson Mandela Metropolitan University, Computers & Security Volume 24, Issue 4, June 2005, Pages 271-273*

[14] **Terry L. Wiant (2004),** "Information security policy's impact on reporting security incidents", Yüksek Lisans tezi, *Marshall University*

[15] **Öğüt P**., 2006. Küreselleşen dünyada bilgi güvenliğine yönelik politikalar: Sayısal imza teknolojisi ve Türkiye, Yüksek Lisans tezi, *Ankara Üniversitesi*

[16] **Özler İ**., 2007. Bilgi güvenliği ve elektronik imza kavramları: Ekonomik boyutlarının incelenmesi ve elektronik imza uygulamaları, Yüksek Lisans tezi, *Dicle Üniversitesi*

[17] **Vural Y**., 2007. Kurumsal bilgi güvenliği ve sızma (penetrasyon) testleri, Yüksek Lisans tezi, *Gazi Üniversitesi*

[18] **Yıldız B.,** 2007. Bilgi güvenliği ve e-devlet kapsamında kamu kurumlarında bilgi güvenliği yönetimi standartlarının uygulanması,Yüksek Lisans tezi, *Gazi Üniversitesi*

[19] **TS ISO/IEC 27001***, 2006.* Bilgi teknolojisi – Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri – *Gereksinimler, Türk Standartları Enstitüsü, Ankara*

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

[21] **Information Systems (MAIS) Acquisition Programs**,1996. Authorized by DoD 5000.1, *Defense Acquisition*,

[22] **DoD 5200.1-I**, 1995. DoD Index of Security Classification Guides*, authorized by DoD Directive 5200.1.*

[23] **http://www.tse.gov.tr/,** *Türk Standartları Enstitüsü*

[24] **http://www.tubitak.gov.tr/,** *Türkiye Bilimsel Araştırma Merkezi*

[25] **http://www.sans.org/,** *SANS is the most trusted & by far the largest source for information security training, certification & research in the world*

[26] **http://www.google.com/,** *Google Product Search*

[27] **http://www.bilgiguvenligi.org/,** *Bilgi Güvenliği Platformu*

[28] **http://www.bilgiguvenligi.gov.tr/,** *Ulusual Bilgi Güvenliği Web Sitesi*

[29] **http://www.isaca.org/,** *Serving IT Governance Professionals*

[30] **http://www.cobit.org/,** *COBIT Web Site*

[31] **http://www.itil-officialsite.com/**, *Information Technologies Infrastructure Library*

[32] **http://www.defenselink.mil/,** *United States Department of Defence*

[33] **http://www.infratech.com.tr/,** *ISO 20000 Danışmanlık*

[34] **http://www.isoiec20000certification.com/,** *IS0 20000 Sertification*

[35] **http://www.bsi-turkey.com/,** *BSI, dünya üzerinde 100'ü aşkın ülkede standartları yükseltiyor*