UZMAN SİSTEM TEMELLİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YAKLAŞIMI

Cemal GEMCİ

DOKTORA TEZİ
ELEKTRONİK VE BİLGİSAYAR EĞİTİMİ ANABİLİM DALI

GAZİ ÜNİVERSİTESİ
BİLİŞİM ENSTİTÜSÜ

NİSAN 2010
ANKARA

Cemal GEMCİ tarafından hazırlanan "UZMAN SİSTEM TEMELLİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YAKLAŞIMI" adlı bu tezin Doktora tezi olarak uygun olduğunu onaylarım.

Prof. Dr. Ömer Faruk BAY
Tez Yöneticisi

Bu çalışma, jürimiz tarafından oy birliği ile Elektronik ve Bilgisayar Eğitimi Anabilim Dalında Doktora tezi olarak kabul edilmiştir.

Başkan : Prof.Dr. A. Ziya AKTAŞ

Üye : Prof.Dr. İnan GÜLER

Üye : Prof.Dr. Ömer Faruk BAY

Üye : Prof.Dr. Şeref SAĞIROĞLU

Üye : Yrd.Doç.Dr. Attila BOSTAN

Tarih : ...../……/……

Bu tez, Gazi Üniversitesi Bilişim Enstitüsü tez yazım kurallarına uygundur.

TEZ BİLDİRİMİ

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca tez yazım kurallarına uygun olarak hazırlanan bu çalışmada orijinal olmayan her türlü kaynağa eksiksiz atıf yapıldığını bildiririm.

(İmza)

Cemal GEMCİ

UZMAN SİSTEM TEMELLİ BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ YAKLAŞIMI

(Doktora Tezi)

Cemal GEMCİ

GAZİ ÜNİVERSİTESİ

BİLİŞİM ENSTİTÜSÜ

Nisan 2010

ÖZET

Ülkemizde günden güne yaygınlaşan bilgi teknolojileri, kullanılırlığı yanında güvenlik ihtiyacını birlikte getirmiştir. Özellikle Avrupa ve Uzak Doğudaki kurum ve kuruluşlar arasında yaygınlaşan ISO 27001 standardına uyumluluk çalışmaları bu konuda yüksek danışmanlık ücretleri ödemeyi veya nitelikli bilişim personeli istihdamını zorunlu kılmaktadır. Bu çalışmada temel bilişim teknolojisi bilgisi ile ISO 27001 standardına uyumluluğu sağlayabilmeye olanak veren uzman sistem tabanlı bir yazılım geliştirilmiştir. Geliştirilen yazılımla nitelikli eleman istihdam sıkıntısı içerisindeki işletmeler yüksek maliyetlerle eleman istihdam etmek veya danışmanlık satın almak zorunda kalmayacaklardır.

Geliştirilen yazılım, standardın karmaşık gereksinimlerini basite indirgeyerek anlaşılırlığı kolaylaştırmakla beraber ISO 27001 standardına uyum için en az yapılması gerekenleri belirlemektedir.

Elde edilen sonuçların doğruluğu ve geçerliliği farklı kuruluşlarda uygulanmış ve farklı baş tetkikçiler tarafından değerlendirilerek belgelendirilmeye uygunlukları kanıtlanmıştır.

Bilim Kodu	**:**	**702.3.006**
Anahtar Kelime	**:**	**Bilgi güvenliği yönetim sistemi, ISO 27001, Uzman sistemler**
Sayfa Adedi	**:**	**106**
Tez Yöneticisi	**:**	**Prof. Dr. Ö.Faruk BAY**

EXPERT SYSTEM BASED INFORMATION SECURITY MANAGEMENT SYSTEM APROACH

(Ph.D. Thesis)

Cemal GEMCİ

GAZI UNIVERSITY

INFORMATICS INSTITUTE

April 2010

ABSTRACT

Information Technologies that are today becoming widespread in our country have also brought some security needs. Efforts to conform to the ISO 27001 standard which are now spreading among the organizations particularly in Europe and in the Far East require either public and private payment of considerable fees to consulting firms or employing qualified IT staff. In this study, an expert system based software has been developed which enables conformance to the ISO 27001 standard by fundamental IT knowledge. By using the developed software, it is expected that enterprises under distress due to scarcity of qualified human resources need not employ highly-paid staff or pay for high consulting fees.

Software that is been developed specifies the standards of compliance with ISO 27001 by simplifying complexity and making its comprehensibility easier.

The results obtained have been implemented at various organizations for accuracy and validity, and result assessed by various head auditors, and proved to have conformed to the certification.

Science Code : 702.3.006
Key Words : Information Security Management System, ISO 27001, Expert Systems
Page Number : 106
Adviser : Prof. Dr. Ö.Faruk BAY

TEŞEKKÜR

Çalışmalarım boyunca değerli yardım ve katkılarıyla beni yönlendiren Hocam Prof. Dr. Ömer Faruk BAY'a yine kıymetli tecrübelerinden faydalandığım hocalarım Prof. Dr. İnan GÜLER ve Prof. Dr. Şeref SAĞIROĞLU'na, ayrıca Bilgisayar Mühendisi Erol SERBEST'e manevi destekleriyle beni hiçbir zaman yalnız bırakmayan sevgili aileme ve bu çalışma esnasında isimlerini burada belirtmediğim çalışma arkadaşlarıma teşekkürü bir borç bilirim.

İÇİNDEKİLER

Sayfa

ÇİZELGELERİN LİSTESİ

Çizelge **Sayfa**

ŞEKİLLERİN LİSTESİ

Şekil **Sayfa**

SİMGELER VE KISALTMALAR

Bu çalışmada kullanılmış bazı simgeler ve kısaltmalar, açıklamaları ile birlikte aşağıda sunulmuştur.

Simgeler	**Açıklama**
?r1	CLIPS' te değişken
Assert	CLIPS' te Ekle komutu

Kısaltmalar	**Açıklama**
ARPA	Advanced Research Project Agency (İleri Araştırma Proje Ajansı)
BGYS	Bilgi Güvenliği Yönetim Sistemi
BSI	British Standards Institude (İngiliz Standartlar Enstitüsü)
CISP	Cardholder Information Security Program (Kart sahibi Bilgi Güvenlik Programı)
COBIT	Control Objectives for Information and Related Technology (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri)
CLIPS	C Language Integration Production System (C Dili Entegrasyon Üretim Sistemi)
CSI	Computer Security Institute (Bilgisayar Güvenliği Enstitüsü)
DTI	The Department of Trade and Industry (Ticaret ve Endüstri Teşkilatı)
GLBA	Gramm-Leach-Bliley Act (Gramm-Leach-Bliley Yasası)
ISMS	Information Security Management System (Bilgi Güvenliği Yönetim Sistemi)

IOC	The Initial Operational Capability Milestone (Temel İşlevsel Yapabilirlik Temel Taşı)
HIPAA	Health Insurance Portability and Account Act (Sağlık Sigortasının Taşınabilirliği ve İzlenebilirliği Yasası)
LCA	Lifecycle Architecture Milestone (Yaşam Dönngüsü Mimarisi Temel Taşı)
PCI DSS	Payment Card Industry Data Security Standard (Kartlı Ödeme Sistemlerinde Veri Güvenliği Standardı)
RUP	Rational Unified Process (Rational Birleşik Süreci)
TSE	Türk Standartları Enstitüsü
SOX	Serbane-Oxley Act (Serbane-Oxley Yasası)
UML	Unified Modeling Language (Birleşik Modelleme Dili)
(ISC)^2	International Information Systems Security Certificate Consortium (Uluslararası Bilgi Sistemleri Güvenlik Sertifikası Konsorsiyumu)

1. GİRİŞ

Bilgi birçok formlarda bulunabilir. Kağıda basılabilir, elektronik ortamda bulunabilir, posta veya elektronik yollar ile gönderilebilir, filmler üzerinde gösterilebilir, sohbetlerde konuşulabilir. Bilgi hangi şekilde olursa olsun, her zaman uygun olarak korunmalıdır.

Bir kuruluşun bilgi sistemi; herhangi bir yönetim seviyesinde istenilen yer ve zamanda bilgi sağlayan sistem olarak tanımlanabilir. Böyle bir sistem bilgisayar sistemleri yardımıyla bilgiyi alabilir, saklayabilir, bulabilir, farklı şekle sokabilir, işleyebilir ve iletebilir [1].

Bilgi önceki zamanlarda söylendiği gibi güç olmaktan çıkmış günümüzde bir varlık halini almıştır. Bilgi ve destek süreçleri, sistemler ve bilgisayar ağları önemli ticari varlıklardır. Bilginin gizliliği, güvenilirliği ve elverişliliği; rekabet gücünü, nakit akışını, karlılığı, yasal yükümlülükleri ve ticari imajı korumak ve sürdürmek için zorunlu ve gerekli olabilir. Giderek işletmeler ve sahip oldukları bilgi sistemleri ve ağları bilgisayar destekli sahtekârlık, casusluk, sabotaj, yıkıcılık, yangın ve sel gibi çok geniş kaynaklardan gelen tehdit ve tehlikelerle karşı karşıyadırlar. İş dünyasında bilişim teknolojilerinin yoğunlukla kullanılmasıyla birlikte bilgisayar virüsleri, bilgisayar korsanları ve hizmet saldırıları gibi yıkıcı kaynaklar daha yaygın, daha hırslı ve daha karmaşık hale gelmeye başlamıştır. Bilgi sistemlerine ve hizmetlerine bağımlılık, işletmelerin güvenlik tehditlerine karşı daha savunmasız olduğu anlamına gelmektedir. Genel ve özel ağların birbiriyle bağlantısı ve bilgi kaynaklarının paylaşımı, erişim denetimini oluşturmadaki zorlukları arttırmaktadır. Dağıtılmış bilgi işleme olan eğilim, merkezi uzman denetimin etkinliğini zayıflatmıştır.

Bilgi sistemleri henüz yeterli güvenlik seviyesinde tasarlanmamıştır. Teknik olanaklar aracılığıyla ulaşılabilen güvenlik sınırlıdır ve uygun yönetim ve yöntemlerle desteklenmelidir. Hangi denetimlerin yer alacağının tanımlanması, özenli planlamayı ve detaylara dikkati gerektirir. Bilgi güvenliği yönetimi tüm işletme çalışanlarının katılımını gerektirir. Aynı zamanda tedarikçilerin, müşterilerin

ve ortakların da katılımına gereksinim duyulur. İşletme dışından uzman tavsiyelere gerek duyulabilir. Bilgi güvenliği denetimleri, eğer şartların ve tasarım aşamasının gereklerinde birleştirilirse çok daha ucuz ve etkili olur.

Günümüzde sadece çalışanlarıyla değil, müşteri, iş ortakları ve hissedarlarıyla birlikte tanımlanan organizasyonlarda, bilginin gizliliği, bütünlüğü ve erişilebilirliğine ilişkin güven ortamının yaratılması, organizasyonun sürekliliği için önem taşımaktadır.

Günümüzde bilişim suçlarının geldiği boyutu açığa kavuşturmak için Amerika Birleşik Devletlerinde Computer Security Institute (CSI) tarafından her yıl hazırlanan "Bilgisayar Suçları ve Güvenlik Gözlemi" (Computer Crime and Security Survey) nin 2009 yılı raporunu özetlersek [2];

Gözlem çalışmasına rastgele seçilen kamu ve özel sektörden toplam 443 kurum ve kuruluşun bilgi güvenlik personeli katılmıştır. Bu kurum ve kuruluşların kullandıkları bilgi güvenlik teknolojileri Çizelge 1.1 de gösterilmiştir.

Çizelge 1.1. Gözlem çalışmasına katılan kurum ve kuruluşların kullandıkları bilgi güvenlik teknolojileri ve kullanım oranları.

Kullanılan teknolojiler	**Kullanım oranı**
Anti-virus software	99,1 %
Anti-spyware software	89,9 %
Application-level firewalls	55,5 %
Biometrics	26,2 %
Data loss prevention / content monitoring	40,9 %
Encryption of data in transit	62,2 %
Endpoint security client software / NAC	42,1 %
Firewalls	97,9 %
Forensics tools	44,8 %
Intrusion detection systems	72,6 %
Intrusion prevention systems	59,1 %
Log management software	53 %
Public Key Infrastructure systems	39,6 %
Server-based access control lists	54,6 %
Smart cards and other one-time tokens	32,6 %
Specialized wireless security systems	32,3 %
Static account / login passwords	42,4 %
Virtualization-specific tools	32 %
Virtual Private Network (VPN)	85,7 %
Vulnerability / patch management tools	65,9 %
Web / URL filtering	60,4 %
Other	3,4 %

Gözlem çalışmasına katılan kurum ve kuruluşların kullanmış oldukları güvenlik teknolojilerine bakıldığında oldukça güvenli oldukları kanısına varılsa da bu kurum ve kuruluşların güvenlik açıklarından dolayı yılda ortalama 285.000 USD para kaybına uğradıkları gözlem raporunda ifade edilmektedir.

İngiltere de Department for Business, Innovation and Skills -BIS (İş, Yenilik ve Beceri Teşkilatı) tarafından Ekim 2007 ile Ocak 2008 tarihleri arasında 1007 küçük ve orta ölçekli işletme üzerinde yapılan anketin sonuçlarına göre bu ticari kuruluşların yıl içerisinde yaşadıkları en kötü bilgi güvenliği vakasından kurtulmak için ortalama 10.000£ ile 20.000£ harcama yaptıkları, bu harcamaların büyük ticari kuruluşlarda ise 90.000£ ile 170.000£ olduğu, bilgi güvenliği açıklarının meydana getirdiği olayları azaltmanın en etkin yolunun bilgi güvenliği standartlarını uyumluluğun yaygınlaştırılması ve bilgi güvenliği farkındalık eğitimlerine yatırım yapılması olduğu belirtilmektedir [3].

Bu raporların da açıkça ortaya koyduğu gibi güvenlik açıklarından dolayı kurum ve kuruluşlar ciddi maddi kayıplara uğramaktadırlar. Bilişim teknolojilerinde gelişmiş ülkelerde bilgi güvenliği kayıpları muhtelif şekillerde ölçülmekte, sonuçları yayınlanmakta ve alınması gereken önlemler devlet tarafından tavsiye edilmektedir.
Bilgi güvenliği konusunda dünyadaki çalışmalara bakıldığında ülkelerin ve sektörlerin farklı uygulamalarda bulundukları gözlemlenmektedir. ABD de bilgi güvenliği ile ilgili kanunlar çıkarıldığı ve ilgili sektörlerin bu kanuni yükümlülükleri yerine getirmelerini belgelendirmeleri istenmektedir. ABD de ki Bilgi güvenliği ile ilgili yasaları ve Avrupa Birliği ülkelerince kabul gören standartlar kısaca özetlenirse;

Serbane-Oxley Act (SOX): 2002 Enron olayından sonra ABD'de ivedilikle çıkarılmış bir yasadır [4]. Bu yasanın amacı borsaya açık şirketlerin açıkladıkları bilgilerin doğruluğu ve güvenilirliğini sağlayarak yatırımcıları korumaktır. Bu kanuna göre şirket yöneticileri ve yönetim kurulu üyeleri finansal raporlar hazırlanırken, yeterli iç denetimleri ve prosedürleri oluşturduklarını ve uyguladıklarını belgelendirmeleri gerekmektedir. Bu konulara uymayan şirket yöneticilerine yasa, hapis cezası öngörmektedir.

Gramm-Leach-Bliley Act (GLBA): Finansal kuruluşların müşteri bilgilerinin güvenliği, bütünlüğü ve kişiye özel olmasını korunmak için düzenlemiştir [5]. Finansal kuruluşların yüksek güvenlik bilincinin diğer endüstri kuruluşlarından daha

fazla olması tarihten beri bilinmektedir. GLBA, bankalar, sigorta şirketleri, güvenlik firmaları, mali müşavirleri ve kredi kartı şirketlerini ilgilendirmektedir. GLBA ‘e göre bu şirketler Temmuz 2002 den önce bu kanuna uyumluluklarını tamamlamak ve yürütmeden sorumlu tarafca denetlenip uyumluluklarını belgelendirmek zorundadırlar. GLBA’e göre finans kuruluşları, yönetici ve yönetim kurulununda dahil bulunduğu risk temelli bilgi güvenliği programı geliştirmeli, tehditlerin risk değerlendirmesi yapılmalı, risk yönetimi ve kontrolleri yöneterek gerekli önlemleri almalı ve yönetim kuruluna rapor etmelidir.

Health Insurance Portability and Accountability Act (HIPAA): HIPAA sağlık hizmeti sağlayan kuruluşların uyması gereken kuralları açıklar. Bu kurallar sağlık hizmeti veren kuruluşların kanunun istediği raporları oluşturan bilgilerin sağlanması ve bu bilgilerin korunmasını zorunlu kılmaktadır. HIPAA uyumluluğunu sağlamak için şirketler bilgilerini muhtemel tehditlere karşı korumak, bütünlüğünü sağlamak, yetkisiz kullanılmalarını, ortaya çıkmalarını önlemek zorundadırlar. Bunun yanında kurum çalışanlarının yetkin ve güvenli olduklarının sağlanması gereklidir. Sağlık hizmeti veren kuruluşlar bütün bunları gerçekleştirebilmek için; erişim kontrolü, konfigürasyon kontrolü, zararlı yazılım tespiti, politika yaptırımı, kullanıcı takibi ve yönetimi, çevre ve haberleşme güvenliğini sağlamakla yükümlüdürler [6].

Payment Card Industry Data Security Standard (PCI DSS) : Kartlı ödeme sistemlerinde veri güvenliğini sağlamak amacıyla uluslararası kabul görmüş ödeme markaları olan American Express, Discover Financial Services, JCB International, MasterCard Worldwide ve Visa Inc. International kurumlarınca oluşturulmuş PCI Komitesi tarafından geliştirilmiştir.

PCI DSS, kartlı ödeme sistemlerinde yeralan kurum ve kuruluşlarda bilgi güvenliğini sağlamak için bilgi sistemlerinde bilgi iletimini, bilgi işleyişini ve bilgi depolamayı esas alan 6 temel kriter baz alınarak oluşturulmuş 12 gereksinim kategorisi ve bu kategorilerin altında yer alan 200’ün üzerindeki kontrolden oluşmaktadır [7].

Control Objectives for Information and Related Technology (COBIT): ISACA (Information Systems Audit and Control Association) ve ITGI (IT Governance Institute) tarafından 1996 yılında geliştirilmiş, Bilgi Teknolojileri Yönetimi için en iyi uygulamalar kümesidir.

COBIT yöneticilere, denetçilere ve Bilgi Teknolojileri (BT) kullanıcılarına iş hedeflerinin bilgi işlem hedeflerine dönüşümünü, bu hedeflere ulaşmak için gerekli kaynakları ve gerçekleştirilen süreçleri bir araya getirirken, aynı zamanda bilgi teknolojileri alt yapılarını da etkin kullanmayı sağlar [8].

ISO IEC 27001 Information Security Management Systems (ISMS) : Avrupa ve Uzak Doğu da ise İngiltere de British Standart Institude un başlattığı çalışma sonucu ortaya çıkan ve International Standart Institude tarafından da standart olarak kabul edilen ISO 27001 standardı günden güne yaygılaşan bir standarttır. Yaygın pratik uygulamalardan oluşturulmuştur. Kurum ve kuruluşlarda bilgi güvenlik yöneticilerine çepeçevre kontrol sağlar.

Bu tez çalışmasının amacı temel bilgisayar bilgisine sahip kullanıcıların kolaylıkla kullanabileceği uzman sistem tabanlı, ISO 27001 standardının gerekliliklerini karşılayacak ve uyumluluk belgelendirmesi için zorunlu dokümanların üretmesini gerçekleştirecek bir yazılım geliştirmektir.

Bu konuda yapılan benzer çalışmalar içerisinde BİGRA risk analiz yöntemi incelenmiştir ancak geliştirilen yazılımda kullanılmamıştır [12]. Bu çalışmada risk analiz yöntemi olarak ISO 27005 standardın dan bir yöntem seçilmiştir [38].

Bullen, Brezilya da yapmış olduğu çalışmada KOBİ lerin sınırlı insan gücü ve finansal kaynak kullanabilmeleri nedenleriyle güvenlik kısıtlamalardan en çok etkilenen kesim olduğunu ve Brezilya için dış kaynak kullanmanın en uygun yöntem olduğunu vurgulamaktadır [13].

Qingxiong Ma ile J. Michael Pearson'un birlikte yapmış oldukları çalışmada organizasyonlar için bilgi varlıklarını korumak için birçok standart bulunduğu, bunların arasında ISO 17799 en güvenilir uluslararası bilgi güvenliği standardı olduğunu belirtmişler ve istatistiksel yöntemlerle kanıtlamışlardır [14].

Uzman sistem kullanan bilgi güvenliği araçları incelendiğinde genellikle uzman sistemlerin risk değerlendirme araçlarında kullanıldıkları görülmektedir. RiskPac özellikle ABD kamu sektöründe ve birçok özel sektör firması tarafından kullanılan bir araçtır. RiskPack kullanıcıya sorular yönelterek yanıtlar alır ve uzman sistem bilgi tabanında değerlendirerek varlıkların risk analizini yapar [20].

Octave ise kuruluşun iş çevresine göre kritik varlıklarını ve tehditlerini tespit eder, tehditlere neden olabilecek zafiyetleri belirler ve zafiyetlere karşı bir koruma stratejisi geliştirir. Octave'ın tüm süreçlerinde bilgi tabanı kullanılmaktadır [21].
Uzman sistem tabanlı risk değerlendirme araçları olan RiskPac ve Octave ISO 27001, HIPAA, SOX, InfoSec, Cobit gibi risk değerlendirme gereksinimi olan uyumluluk denetimlerinde sıklıkla kullanılmıştır.

Bu tez çalışmasında tehditlere yönelik korumaların seçilmesinde ve ISO 27001 dokümantasyonunun hazırlanmasında uzman sistem kullanılmıştır. Uzman sistemlerin ISO 27001 kurulumu ve dokümantasyon hazırlanmasında kullanılması literatürde bulunmamaktadır.

Bu tez çalışmasında Türkiye de yaygın olarak kullanılan Microsoft Office uygulamaları ile entegre olabilen ve Nesneye Yönelik bir yazılım geliştirme platformu olan Microsoft .NET C# yazılım geliştirme ortamı olarak seçilmiştir. Veri tabanı olarak Microsoft SQL Express Edition kullanılmıştır. Yazılım geliştirme modeli olarak Nesneye Yönelik yazılım geliştirmeye uygun olan RUP (Rational Unified Process) Model seçilmiş tüm modelleme UML ile gerçekleştirilmiştir.

Uzman sistem geliştirilirken kabuk program kullanılmıştır. Uzman sistem kabuk programı olarak Microsoft .NET platformu için gereken .dll leri bulunan ve ileri zincirlemeyi destekleyen CLIPS kabuk programı tercih edilmiştir.

Bu tez çalışması altı bölümden oluşmaktadır. Birinci giriş bölümünde yapılan çalışmanın hedefleri, literatür araştırmasının özeti, metod ve materyaller özetlenmektedir. İkinci bölümde, "Bilgi Güvenliği" başlığı altında bilgi güvenliğinin tarihi, bilgi güvenliği standartları, ISO 27001 standartının ayrıntıları ve detaylı literatür taraması anlatılmıştır. Üçüncü bölümde metot ve materyaller anlatılmıştır. Dördüncü bölümde tasarım ve gerçekleştirmenin nasıl yapıldığı anlatılmıştır. Bulgular ve yorum başlığı ile beşinci bölümde çalışmanın sonucunda elde edilen bulgular yorumlanmıştır. Altıncı ve son bölüm olan sonuçlar bölümünde ise çalışmanın sonuçları irdelenmiştir.

2. BİLGİ GÜVENLİĞİ

2.1. Bilgi Güvenliği ve ISO 27001 Standardının Tarihçesi

Bilgisayar çağının başlamasıyla birlikte donanımlar, mainframe bilgisayarlar olarak görünmeye başladı. Büyük sistemler odaları kaplıyordu. Yazılımcılar bu büyük sistemlere komutlarını delikli kartlar yardımıyla yaptırıyorlardı. Bu zamanlarda yerel alan ağları henüz yoktu ve bu mainframeler izole olarak çalışmaktaydılar. Bu sistemler arasında iletişim manyetik teyb'e kopyalanmış verilerin diğer sisteme aktarılması ile mümkün oluyordu. Bu nedenle sistemlerin ve manyetik teyp medyalarının fiziksel güvenliği bilgi güvenliğini oluşturmakta idi diğer bir deyişle bilgi güvenliği fiziksel güvenlik ile özdeş halde idi.

1960 lı yıllarda mainframeler gittikçe yaygınlaşıyor ve soğuk savaşın etkisiyle askeri alanlarda çoğunlukla kullanılıyordu. Zamanla, bu sistemlerde yapılan işler kritik olmaya ve fiziksel olarak farklı yerlerde bulunan sistemlerden bilgi akışı zorunlu olmaya başladı. Artık manyetik teyplerin postayla gönderilmesi yeterli olmuyordu. Bu durumu anlayan Department of Defense's Advanced Research Project Agency (ARPA) ARPANET adında bir projenin finansmanını sağladı. Bu projenin hedefi farklı yerlerdeki mainframeler arasında güvenilir, sağlam, veri akışını sağlayacak network yapısının sağlanmasıydı. Bugünkü internetin habercisi olan ARPANET ilk kez uzak bilgisayarların sakladığı verileri işleme olanağı sağladı.

Bilgisayarlara uzaktan erişim bilgi güvenliğinin fiziksel güvenlik ile özdeş olduğu düşüncesini sona erdirdi. ARPANET'in kullanımının arttıkça birçok güvenlik açığının olduğu ortaya çıktı. Uzak bilgisayarda bilgi güvenliği politikaları yetersizdi, bazen de hiç yoktu. Standartların ve formatların zayıf uygulanmasından dolayı parolaların kırılması kolaydı. Uzak siteye telefonla ulaşmayı yönetmek zordu çünkü erişim numaraları çoğu kez korumasızdı. Bilgisayar sistemlerine saldırılar sıradan olmaya başladı. Öyle ki 1980 lerin ortalarında Los Alamos National Laboratory, the Memorial Sloan-Kettering Cancer Center, AT& T, ve Department of Defense saldırıları halk tarafından çok iyi biliniyordu. Bu dönemde en büyük saldırılardan

birisi network de dolaşan, Unix sistemlerde güvenlik açıklarını ortaya çıkaran ve yeniden dolaşması için kendisini kopyalayan bir solucan idi. Bu saldırı o dönemdeki sistemlerin yaklaşık 1/10 ‘u olan 6000 sisteme aynı anda yayıldı.

Gittikçe büyüyen bu sorunlara tepkiler birçok çevreden farklı forumlarda geldi. 1970 lerin başında de Department of Defense (Savunma Bakanlığı) Rand Report R-609 olarak da bilinen “Bilgisayar Sistemleri için Güvenlik Kontrolleri” başlıklı bir rapor yayınladı. Birçok bakımdan bu rapor bilgi güvenliğinin ilk tohumları sayılmaktadır. Rand raporu bilgi güvenliği konusunu sadece donanımın fiziksel güvenliğinden farklı olarak; veri, kullanıcı ve altyapı güvenliği konularını da ele alması bakımından önemli idi. Rapor bilgi varlığının öneminin tanınması, kullanıcı yetkilerinin bu varlığın güvenliğini sağlamada en önemli unsur olduğunu ve bütün bunların anlık tepkilerle değil kapsamlı, çok seviyeli kurumsal bir planda ele alınması gerekliliğini vurgulaması ile Rand Report bugünkü bilgi güvenliği disiplininin filozof isini oluşturmaktadır.

Güvenlik bakışındaki değişiklikler uygulamalarda da değişiklikleri getirdi. Örneğin, 1960 ların sonunda ortaya çıkan ilk işletim sistemi güvenlik konusunu ilk öncelikli olarak dikkate alan bir yapıda tasarlanmıştı. İşletim sisteminin adı “Multiplexed Information and Computer Service” veya kısaca MULTICS ilk kez güçlü parola koruma ve birçok güvenlik seviyelerinde yetkilendirme sağlamaktaydı. İlginç olan konu MULTICS projesine katkıda bulunan kişilerin geliştirdiği UNIX işletim sistemi 1970 lerde ilk çıktığında bu özelliklere sahip değildi zamanla bu özellikler UNIX işletim sistemine ilave edildi.

1980 lerde kişisel bilgisayarların artan kullanımıyla güvenlik konusu daha da önem kazandı. Kişisel bilgisayarlar insanların çalışma masalarında ve hatta evlerinde kullanılmaya başlandı. Bu başlangıç küçük yerel alan ağlarına bağlanmayı ve daha sonra global internete bağlanmayı sağladı. Örümcek ağı gibi oluşan güvenli veya güvenliksiz networkler açık veya gizli bir şekilde başka bilgisayarlardaki bilgilere erişme çabalarını beraberinde getirdi. Zafiyetler internet kaynaklarındaki bilgilere erişimi ve paylaşımı daha da kolaylaştırdı. 1990 ların başlarında grafik web

browserların kullanımı, network kullanım kolaylıkları ve işletim sistemlerinde grafik kullanıcı arayüzleri moda işler olmakla beraberinde acemi kullanıcıların bilgilerinin tüm dünyaya açmalarına ve meraklı hackerların da birçok araç geliştirmelerine ve bu araçlarla tecrübe kazanmalarına neden oldu. Bu araçlar korunmasız veya zayıf korumalı sistemlerle ve networklerde bulunmakta ve zafiyetlerde ortaya çıkmaktadırlar. Bu süreç ARPANET in kurulumundan günümüze artarak devam etmektedir.

Bilgi güvenliğini sağlamak, teknolojik çözümlerle birlikte sağlam bir güvenlik yönetim sisteminin kurulması ile mümkün olabileceğinin anlaşılmasıyla birlikte tüm dünyada farklı gruplar tarafından çalışmalar başlamıştır. Avrupa da ve Uzak Doğu da yaygın olarak kullanılan ISO 27001 standardı ilk olarak İngiltere de ortaya çıktı. 1992 yılında İngiltere de Ticaret ve Endüstri Bakanlığının "The Department of Trade and Industry (DTI)" önderliğinde belli başlı kurum ve kuruluşların bilişim uzmanları bir araya gelerek güvenlik tecrübelerini aktardıkları "Code of Practice for Information Security Management" hazırladılar. 1995 yılında bu doküman üzerinde değişiklikler yapılarak British Standards Institude (BSI) tarafından BS7799 adı ile yeniden İngiliz Standardı olarak yayınlandı. 1996 yılında ilk destek ve uyumluluk aracı COBRA adıyla pazarlandı. 1999 yılında BS7799 un ilk değişiklik versiyonu temel değişikliklerle yayınlandı. BSI ilk sertifikasyon makamı oldu. 2000 yılında BS7799 yeniden ISO/IEC 17799:2000 adıyla ISO standardı olarak yayınladı. 2001 yılında ISO 17799 toolkit piyasaya sürüldü. 2002 yılında standardın ikinci bölümü BS7799-2:2002 yayınlandı. İkinci bölüm pratik uygulamalar yerine Bilgi Güvenliği Yönetimi tanımlamasıydı ve ISO standartları formasyonunda idi.

15 Haziran 2005 tarihinde ISO/IEC 27002 (2005) *Information technology -- Security techniques -- Code of practice for information security management* standardı yayınlanarak ISO/IEC 17799 (2000) standardının yerini aldı. 14 Ekim 2005 tarihinde ISO/IEC 27001 (2005) *Bilgi Güvenliği Yönetim Sistemi (Information security management systems)* standardı uluslararası bir standart olarak yayınlandı. Bilgi Güvenliği Yönetim Sistemi konusunda yayınlanmış olan bu standart yayım tarihinden itibaren, BS 7799-2 (2002) 'nin yerini almıştır.

ISO 27000 serisinin standartları şunlardır [9];

ISO/IEC 27000 (2009) *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary (Bilgi Teknolojileri-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemi-Genel ve Terimler).*

ISO/IEC 27001 (2005) *Information technology -- Security techniques -- Information security management systems – Requirements (Bilgi Teknolojileri-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemi-Gereksinimler).*

ISO/IEC 27002 (2005) *Information technology -- Security techniques -- Code of practice for information security management (Bilgi Teknolojileri-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemi için Pratik Uygulamalar).*

ISO/IEC 27003 (2010) *Information technology -- Security techniques -- Information security management system implementation guidance (Bilgi Teknolojileri-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemi için Uygulama Rehberi).*

ISO/IEC 27004 (2009) *Information technology -- Security techniques -- Information security management – Measurement (Bilgi Teknolojileri-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemi-Ölçme).*

ISO/IEC 27005 (2008) *Information technology -- Security techniques -- Information security risk management (Bilgi Teknolojileri-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemi Risk Yönetimi).*

ISO/IEC 27006 (2007) *Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems (Bilgi Teknolojileri-Güvenlik Teknikleri-Denetim ve Sertifika Sağlayıcılar için Gereksinimler).*

ISO/IEC CD 27007 *Information technology -- Security techniques -- Guidelines for information security management systems auditing (Bilgi Teknolojileri-Güvenlik Teknikleri-Bilgi Güvenliği Yönetim Sistemi Denetimi için Rehber).* (Henüz yayınlanmadı).

ISO/IEC WD 27008 *Guidance for auditors on ISMS controls (Denetçiler için BGYS kontrolleri Klavuzu)* (Henüz yayınlanmadı).

ISO/IEC NP 27010 *Information security management guidelines for inter-sector communications (Sektörler arası haberleşme için Bilgi Güvenliği Rehberi)* (Henüz yayınlanmadı).

ISO/IEC NP 27011 (2008) *Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002 (Bilgi Teknolojileri-Güvenlik Teknikleri-Telekomünikasyon kuruluşları için ISO 27002 ye göre Bilgi Güvenliği Yönetimi Rehberi).*

Bilgi Güvenliği Yönetim Sistemi (BGYS) tüm yönetim sisteminin ticari risk yaklaşımı, gerçekleştirme, işletme, gözlemleme, idame ettirme ve geliştirmeye dayalı bir parçasıdır. Yönetim sistemi organizasyon, kuruluş yapısı, politikalar, planlanan faaliyetler, sorumluluklar, prosedürler ve kaynakları kapsar. Bilgi güvenliğini kapsamı organizasyonun ve organizasyondaki bilgi kaynaklarının büyüklüğüne bağlıdır. Bilgi güvenliği organizasyonun işletme ve iş kültürünün tümleşik bir parçası olmalıdır. Bilgi güvenliği teknik bir konu olmaktan ziyade temelde yönetimin konusudur. Bilgi güvenliği bir kez yapılacak bir iş olmayıp süreklilik gerektirir. Günümüzde bilgi güvenliğini ihmal ederek faaliyetini sürdüren başarılı hiçbir organizasyon bulunmamaktadır. Bilgi güvenliği için iyi seçilmiş yönetim sistemi kontrolleri, düzgün bir şekilde uygulandığında organizasyonun başarısına olumlu katkılarda bulunurlar [10].

2.2. ISO 27001 Standardının Yapısı

ISO 27001 13 ana başlık altında 133 tane kontrol maddesi bulundurur. Bu kontrol maddelerinin uygulanması ve zorunlu dokümantasyonun standardın istediği şekilde hazırlanması belgelendirme için bir zorunluluktur. ISO 27001 standardının bölümleri aşağıda standartdan özetlenmiştir [11].

2.2.1. BGYS nin kapsam ve sınırlarının belirlenmesi

Kuruluşun ana faaliyet konusuna uygun olarak BGYS kapsamının ve kapsam dışında kalan faaliyetlerinin belirlenmesi gerekmektedir. Kapsam belirlenirken kuruluşun müşteri ve tedarikçilerine ait bilgilerinden kuruluş tarafından yaratılan, kullanılan, gönderilen ve bulundurulan bilgi varlıklarının işleyen, kullanan, gönderen ve bulunduran kuruluş birimleri mutlaka kapsam içerisinde yer almalıdır. Müşteri bilgilerini doğrudan kullanan birimler dışındaki birimler, ilgili birimler olarak değerlendirilmelidirler. Eğer dış kaynak hizmet veya ürün alımı yapılıyorsa dış kaynak sağlayıcıları ise kuruluş dışında ilgili taraflar olarak değerlendirilmelidir.

2.2.2. BGYS politikası belirleme

Kuruluş: İşin, kuruluşun, yerleşim yerinin, varlıklarının ve teknolojisinin özelliklerine göre bir BGYS politikası tanımlamalıdır.

ISO 27001 standardına göre bilgi güvenliği politikası aşağıdaki özelliklere sahip olmalıdır:

i. Kuruluş bilgi güvenliği ile ilgili olarak hedeflerini ortaya koyan için bir çerçeve belirlemeli, prensiplerini ortaya koymalı ve bilgi güvenliğine ilişkin bir eylem için kapsamlı farkındalık yaratmalı,
ii. İş ve yasal ya da mevzuat gerekleri ve sözleşmeye ilişkin güvenlik yükümlülüklerini dikkate almalı,

iii. BGYS kurulumu ve sürdürülmesinin yer alacağı stratejik kurumsal ve risk yönetimini düzenlemeli,
iv. Kurumsal risklerin değerlendirileceği kriterleri kurmalı,
v. Yönetim tarafından onaylanmalıdır.

2.2.3. Kuruluşun risk değerlendirme yaklaşımını tanımlama

Kuruluş organizasyonunun büyüklüğüne ve bilgi varlıklarının çokluğuna, BGYS'ye ve tanımlanmış iş bilgisi güvenliğine, yasal ve düzenleyici gereksinimlere uygun bir risk değerlendirme metodolojisi (risk değerlendirme yaklaşımı) belirlemelidir.

Riskleri kabul etmek için kriterler geliştirme ve kabul edilebilir risk seviyelerini tanımlanmalıdır.

Seçilen risk değerlendirme metodolojisi, risk değerlendirmelerinin karşılaştırılabilir ve yeniden üretilebilir sonuçlar üretmesini sağlamalıdır.

2.2.4. Risklerin tanımlanması

Bilgi güvenliği yönetim sistemi sorumlusu, yukarıda bahsedilen süreç analizi sonuçlarını kullanarak, süreç sahipleriyle eşgüdüm halinde süreç varlıklarını ve sahiplerini belirler.

BGYS kapsamında belirlenen varlıklar için var olan tehditler belirlenir. Tehditler belirlenirken varlığın türü ve yapısı göz önüne alınmalıdır. Bu tehditlere neden olabilecek zafiyetler (açıklıklar) tanımlanmalıdır.

Gizlilik, bütünlük ve erişilebilirlik kayıplarının varlıklar üzerinde olabilecek etkileri tanımlanır. Tüm varlıkların gizlilik bütünlük erişilebilirlik değerlerine göre varlık değerleri belirlenir. Varlık değeri yüksek varlıklar daha çok korunması gereken varlıklardır.

2.2.5. Riskleri çözümleme ve değerlendirme

i. Varlıkların gizliliğine, bütünlüğüne ya da erişilebilirliğine ilişkin oluşan kayıpların olası sonuçlarını dikkate alarak, güvenlik önlemlerinin eksikliğinden kaynaklanabilecek, kuruluş üzerindeki iş etkileri değerlendirilir.
ii. Mevcut tehditler ve zafiyetler ve bu varlıklarla ilişkili etkiler ışığında oluşan güvenlik başarısızlıklarının gerçekçi olasılığını ve gerçekleştirilen mevcut kontroller değerlendirilir.
iii. Risk seviyeleri belirlenir.
iv. Risklerin kabul edilebilir mi olduğunu yoksa riskleri kabul etmek için belirlenen kriterler kullanılarak iyileştirme mi gerektirdiğini belirlemek.

2.2.6. Risklerin işlenmesi için seçenekleri tanımlama ve değerlendirme

Varlıklara yönelik tehditlerin yaratacağı riskleri yok etmek veya azaltmak için uygun kontroller uygulanır.

Kuruluşun politikalarını ve riskleri kabul etme kriterlerini açıkça karşılaması şartıyla, bilerek ve nesnel olarak risklerin kabul edilmesi,

Risklerden kaçınma ve ilişkili iş risklerini diğer taraflara, örneğin, sigorta şirketlerine, tedarikçilere aktarılması ile riskler azaltılır.

Risklerin işlenmesi için kontrol amaçları ve standardın uygun kontrollerini seçme. Kontrol amaçları ve kontroller, risk değerlendirme ve risk işleme süreçlerince tanımlanan gereksinimleri karşılamak için seçilmeli ve gerçekleştirilmelidir.

ISO 27001 Standardının EK-A sında listelenen kontrol amaçları ve kontroller geniş kapsamlı değildir ve ek kontrol amaçları ve kontroller seçilebilir.

2.2.7. Sunulan artık risklere ilişkin yönetim onayı edinme

Risk yönetiminde hedef riskleri yok etmek veya azaltmaktır ancak riskleri azaltmak parasal kaynak gerektirir bu nedenle alınacak önlemler projelendirilir ve bütçelenir. Bu esnada risklerin doğurabilecekleri tehlikeler aşikardır ve yönetimin belirlemiş olduğu risk seviyesinin üzerinde bulunan risklere artık risk denilmekte ve yönetimin onayına sunulmaktadır.

2.2.8. BGYS'yi gerçekleştirmek ve işletmek için yönetim yetkilendirmesi edinme

BGYS kurucak kurum ve kuruluş BGYS yi gerçekleştirmek üzere insan kaynakları görevlendirmesi ve bu personeli yetkilendirmesi gerekir. BGYS sorumluları kurum ve kuruluşların en üst yetkilisi tarafından yetkilendirilir ve yetkilendiren yetkili adına BGYS deki görevlerini yerine getirir.

2.2.9. Uygulanabilirlik bildirgesi hazırlama

Uygulanabilirlik bildirgesi özet olarak ISO 27001 standardının EK-A sında bulunan kontrollerin hangilerinin uygulandığını, uygulanmayan var ise neden uygulanmadığının açıklandığı bir dokümandır. Uygulanabilirlik bildirgesinin hazırlanması bir zorunluluktur.

Aşağıdakileri içeren bir Uygulanabilirlik Bildirgesi hazırlanmalıdır:

i. Seçilen kontrol amaçları ve kontroller ve bunların seçilme nedenleri,
ii. Mevcut gerçekleştirilmiş kontrol amaçları ve
iii. ISO 27001 Standardının EK-A sındaki kontrol amaçları ve kontrollerden herhangi birinin dışarıda bırakılması ve bunların dışarıda bırakılmasının açıklaması.

2.2.10. Dokümantasyon gereksinimleri

Dokümantasyon yönetim kararlarının kayıtlarını içermeli, eylemlerin yönetim kararları ve politikalarına izlenebilir olmasını sağlamalı ve kaydedilen sonuçların yeniden üretilebilir olmasını sağlamalıdır.

Seçilen kontrollerden geriye doğru risk değerlendirme ve risk işleme süreçlerinin sonuçlarına ve sonra da en geride BGYS politikası ve amaçlarına olan ilişkiyi gösterebilmek önemlidir.

BGYS dokümantasyonu aşağıdakileri kapsamalıdır:

i. BGYS politikası (ISO 27001 Madde 4.2.1b) ve kontrol amaçlarının dokümante edilmiş ifadeleri,
ii. BGYS kapsamı (ISO 27001 Madde 4.2.1c),
iii. BGYS'yi destekleyici yöntemler ve kontroller,
iv. Risk değerlendirme metodolojisinin bir tanımı (ISO 27001 Madde 4.2.1c),
v. Risk değerlendirme raporu (ISO 27001 Madde 4.2.1c- 4.2.1g),
vi. Risk işleme planı (ISO 27001 Madde 4.2.2b),
vii. Kuruluş tarafından, bilgi güvenliği süreçlerinin etkin planlanlanmasını, işletilmesini ve kontrolünü sağlamak için ihtiyaç duyulan dokümante edilmiş uygulama esasları (prosedürler) ve kontrollerin etkinliğinin nasıl ölçüleceğini tanımlama (ISO 27001 Madde 4.2.3c)).
viii. Bu standard tarafından gerek duyulan kayıtlar (ISO 27001 Madde 4.3.3) ve
ix. Uygulanabilirlik Bildirgesi.

2.2.11. BGYS iç denetimleri

Kuruluş BGYS iç denetimlerini, BGYS kontrol amaçlarının, kontrollerinin, süreçlerinin ve uygulama esaslarının aşağıdakileri gerçekleştirip gerçekleştirmediğini belirlemek için planlanan aralıklarda yapılmalıdır:

i. Bu standardın gerekleri ve ilgili yasa ya da düzenlemelere uyum,
ii. Tanımlanan bilgi güvenliği gereksinimlerine uyum,
iii. Etkin olarak gerçekleştirilip sürdürüldüğü,
iv. Beklendiği gibi işleyip işlemediği.

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

Denetimlerin planlanması ve gerçekleştirilmesindeki ve sonuçların raporlanması ve kayıtların tutulmasındaki (ISO 27001 Madde 4.3.3) sorumluluklar ve gereksinimler, dokümante edilmiş bir prosedür içinde tanımlanmalıdır.

Denetlenen alandan sorumlu olan yönetim, saptanan uygunsuzlukların ve bunların nedenlerinin giderilmesi için, gereksiz gecikmeler olmaksızın önlemlerin alınmasını sağlamalıdır. İzleme faaliyetleri, alınan önlemlerin doğrulanmasını ve doğrulama sonuçlarının raporlanmasını (ISO 27001 Madde 8) içermelidir.

2.3. Uzman Sistemin Bilgi Güvenliğinde Kullanımı Üzerine Çalışmalar

Bilgi güvenliği konusunda yapılan çalışmalar incelendiğinde;

2003 yılında Gebze İleri teknoloji Enstitüsü Bilgisayar Mühendisliği Ana Bilim Dalında yapılan "Bilgi Güvenliği Risk Analizi (BİGRA) Yöntemi" konulu yüksek lisans tezinde, risk analizi süreçleri içerisinde kullanılan matematiksel ve istatiksel metodlar ile risk analiz yöntemleri anlatılarak bilgi güvenliği risk analizi için yeni bir yöntem önerilmiştir [12]. "Bilgi Güvenliği Risk Analizi" olarak isimlendirilen bu yöntem, günümüz değişen ihtiyaçlarına cevap vermek üzere tasarlanmış hem nitel hem nicel araçları kullanan bir risk analizi yöntemidir. Bilgi güvenliği risk analizi sürecine kurum yöneticilerinin ve kurum çalışanlarının da katılımını sağlayan,

spesifik bir bilgi güvenliği sorunundan kaynaklanan riskleri ortaya koymayı hedeflediğinden dolayı basit bir yapıya indirgenmiş olan BİGRA yöntemi içerisinde temel olarak benzetim ve anket süreçlerini kapsar.

BİGRA yöntemi üç ana adımdan oluşur. İlk adımında riske yol açan bilgi güvenliği sorunu, belirlenmiş kurallar çerçevesinde ortaya konur. İkinci adımda, bilgi güvenliği sorunu için risk modeli kurulur ve model üzerinde benzetim çalıştırılır. Bu aşamada BİGRA yönteminin riski ifade etmek için kullandığı diğer bir metot da durum analizi anketidir. Her iki yöntemin sonucunda risk miktarı ortaya konur. Üçüncü adımda ise benzetim ve anket sonuçları yorumlanır ve risk kontrolü için uygun öneriler getirilir.

"Security in Brasil: Modelling and Predicting Outsourcing Decisions" konulu doktora tezinde James Bullen, günümüzde güvenlik gereksinimlerinin internet ve bilgi teknolojilerinin kullanımını kısıtladığını ve özelliklerde KOBİ lerin sınırlı insan gücü ve finansal kaynak kullanabilmeleri nedenleriyle güvenlik kısıtlamalardan en çok etkilenen kesim olduğunu vurgulamakta, KOBİ ler için bilişim güvenliğini dış kaynaktan sağlamanın (outsource) en uygun yöntem olduğunu, bilişim güvenliğini outsource etmiş 420 KOBİ ler üzerinde yapmış olduğu gözlem çalışmasının sonuçlarını Logistic regression analysis metodu kullanarak KOBİ lerde dış kaynaktan sağlamanın en uygun yöntem olduğunu kanıtlamıştır [13].

Missouri State Universitesi Bilgi Sistemleri bölümünden Qingxiong Ma ile Southern Illinois Universitesi İşletme bölümünden J. Michael Pearson'un birlikte hazırladıkları ve "Communications of the Association for Information Systems (Volume 15, 2005) 577-591" dergisinde yayınlanan makalede organizasyonlar için bilgi varlıklarını korumak için birçok standart ve yol haritası önerildiği bunların arasında ISO 17799 en güvenilir uluslararası bilgi güvenliği standardı olduğunu belirtmişlerdir [14]. Standardın bilgi güvenliğini sağlamak için hem emredici olduğunu hemde organizasyona adapte edilecek prosedürlerin olduğunu ifade etmişlerdir. Bilişim güvenliği professonellerinin ISO 17799 u modern organizasyonlar için bilgi güvenliğini yönetmede en uygun yöntem olduğunu bildirmelerine rağmen şimdiye kadar bu standardın geçerliliğini kanıtlayacak bilinen deneysel bir çalışma

olmadığından yola çıkarak ISO 17799 standardının 36 grupta topladığı soruların benzer veya yanlış anlaşılmalara neden olabilecek olanlarını birleştirerek veya ayırarak 56 soru haline getirmişlerdir. Çalışmaya katkıda bulunacak olan Sertifikalı Bilgi Güvenliği Profesyonellerinden (CISP) International Information Systems Security Certificate Consortium $(ISC)^2$ 'um WEB sayfasında yayınlanan sorulara "Uygulanamaz" dan başlayan ve "Tamamen uygulandı" ile son bulan 5-noktalı Likert skalasında yanıtlamaları istenmiştir. Çalışmaya katılan 3000 CISP den 354 değerlendirmeye alınabilir yanıt elde edilmiştir. Yanıtlama oranı % 11,8 dir.

ISO 17799 da 10 güvenlik boyutu bulunduğundan alınan yanıtlar 10 faktör üzerinden confirmatory factor analysis (onaylayıcı faktör analizi) yapılmıştır.

Analiz çalışmalarının sonunda ISO 17799 standardının 10 güvenlik boyutundan 7 sinin onaylandığı, 3 boyutunun ("personel güvenliği","Fiziksel ve çevre güvenliği","Uyumluluk") onaylanmadığı bunun yanında "Dış kaynak veya iş ortaklarının güvenliği" konusunun eksik olduğu ilave edilmesi gerekliliği ortaya çıkartılmıştır. Bu çalışmanın sonuçları ilgili olan kuruluşlara International Standart Organization (ISO)'ya, Internet Ingineering Task Force (IETF)'ye ve US National Institute of Standards and Techonology (NIST)'e dikkate alınması için gönderilmiştir. Bu çalışmanın önerileri ISO/IEC 2001 (2005) versiyonunda gözönüne alınmıştır.

İngiltere'de yapılan bir çalışmada ise; UCISA (Universities and Colleges Information System Association) Information Security Tool Kit İngiltere nin önde gelen üniversitelerinin (London School of Economics, University of Reading, University of Liverpool, West Midlands RSC. vb) katkılarıyla hazırlanmış ve özellikle üniversitelerin bilgi güvenliklerini oluşturma yolunda standardizasyonun sağlanması ve diğer organizasyonlarında faydalanabileceği bir çalışma yapılarak tamamen BS 7799 standardını esas alan Bilgi Güvenliği Yönetim Sistemi meydana getirmek için bir tool kit oluşturmuşlar ve tüm İngiltere üniversitelerinin kullanımına sunmuşlardır [15].

Vural Y., ve Sağıroğlu Ş., tarafından yapılan çalışmada; kurumsal bilgi güvenliği genel olarak incelenmekte, mevcut çalışmalar özetlemekte, kurumsal bilgi güvenliğinin kurumlarda etkin bir şekilde hayata geçirilmesinin önemi vurgulanmaktadır [16]. Kurumsal bilgi güvenliğinin uygulanmasında önemli bir yer tutan ISO/IEC 27000 serisi standartları kısaca açıklanmakta ve ülkemizde Avrupa Birliği uyum kriterlerinde de adı geçen bu standartların uygulanması konusunda yapılan çalışmaların yetersiz olduğu, bu standardı uygulayan kurum ve kuruluşların sayısının yok denecek kadar az olduğu vurgulanmaktadır.

Callio toolkit : Kanada konuşlu bir firma olan Callio nun ürünü olan Callio tollkit BS 7799 Bilgi Güvenliği Yönetim Sisteminin ve dokümantasyonunun oluşturulmasında kullanıcılara kolaylık sağlayan web üzerinde çalışan bir araçtır. ISO 17799, BS 7799-2, COBIT ve Serbanes-Oxley standartlarınıda destekler ve bu standartlardan soru alışverişi yapabilir [17].

Aşağıdaki fonksiyonları desteklemektedir :

i. ISO 17799 standardına uyumluluk seviyesi,
ii. Şirketin en değerli varlıklarının envanterinin derlenmesi,
iii. BGYS içerisinde süreçlerin ve yapının belirlenmesi,
iv. Varlıklara yönelik risklerin azaltılması,
v. Kontrollerin uygulanmasında senaryolar belirlemek,
vi. Taslak güvenlik politikaları (50 den fazla örnek),
vii. Politika dokümanının hazırlanması ve yönetimi,
viii. Onay bekleyen dokümanların onaylanması veya iptali,
ix. İç tetkik sorularının kişiselleştirilmesi,
x. İç tetkik sorularının içeri alınması veya dışa verilmesi,
xi. BGYS nin BS 7799-2 sertifikasyonu gereksinimlerini karşıladığının doğrulanması,
xii. ISO 17799 standardının 127 maddesinin yönetim çerçevesinde uygulanması, düzenlenmesi ve dokümante edilmesi,

Standard Directs ISO17799 Toolkit : ISO 17799 ve ISO 27001 standartlarını destekleyen temel kaynaklardan birisidir. Aracın içerisinde uygulama ve denetimi destekleyen bölümler bulunmaktadır [18].

Araç beraberinde aşağıdakileri de sağlamaktadır :

i. ISO 17799 ve ISO 27001 standartları,
ii. Belgelendirmeye giden bir rehber/yol haritası,
iii. Denetim listesi,
iv. İş etki analizi (BIA) aracı,
v. Network denetim listesi,
vi. Bilgi güvenliği politikaları,
vii. Felaket kurtarma seti (kontrol listesi ve soruları ile birlikte),
viii. Standardın içeriğini ve çerçevesini yönetim sunumu,
ix. Bilgi Sistemleri ve Bilgi Teknolojileri terimler sözlüğü,

ITGovernance Toolkit: IT Governance kitapları ve kolaylıkları (tool) herhangi bir organizasyonun BGYS ni ilk kez oluşturmalarına rehberlik eder ve destekler. Dünyanın neresinde olursa olsunlar kamu sektöründen, özel sektörden veya gönüllü kuruluşlardan bu kolaylıkları kullananlara zaman ve para tasarrufu sağlar. Geliştirdikleri uygulamayı kitapları ile destekleyen bu İngiliz firması farklı gereksinimlere göre paket çözümler sağlamaktadır. Temelde ISO 17799 a giden bir yol haritası ortaya koyar, kullanıcıların ihtiyaç duyduğu dokümantasyonu hazırlamalarına kolaylık sağlar [19].

Uzman sistem kullanan sistemler günümüzde birçok uygulamada karşımıza çıkmaktadır. Bilgi güvenliği konusunda ise genellikle risk değerlendirme araçlarında kullanıldıkları görülmektedir. Bu araçlardan RiskPac ve OCTAVE en tanınmış olanlarıdır. RiskPac özellikle ABD kamu sektöründe ve birçok özel sektör firması tarafından 1984 yılından beri kullanılan bir araçtır. RiskPack kullanıcıya sorular yönelterek yanıtlar alır ve uzman sistem bilgi tabanında değerlendirerek varlıkların risk analizini yapar [20]. OCTAVE ise kuruluşun iş çevresine göre kritik varlıklarını

ve tehditlerini tespit eder, tehditlere neden olabilecek zafiyetleri belirler ve zafiyetlere karşı bir koruma stratejisi geliştirir. OCTAVE tüm süreçlerinde bilgi tabanı kullanılmaktadır [21].

Uzman sistem tabanlı risk değerlendirme araçları olan RiskPac ve OCTAVE ISO 27001, HIPAA, SOX, InfoSec, Cobit gibi risk değerlendirme gereksinimi olan uyumluluk denetimlerinde sıklıkla kullanılmıştır.

Bu tez çalışmasında tehditlere yönelik korumaların seçilmesinde ve ISO 27001 dokümantasyonunun hazırlanmasında uzman sistem kullanılmıştır. Uzman sistemlerin ISO 27001 kurulumu ve dokümantasyon hazırlanmasında kullanılmasına literatürde rastlanılmamıştır.

3. METODLAR VE MATERYALLER

Bu tez çalışmasında uzman sistem kullanılarak bilgi güvenlik yönetim sistemi kurulmasına yardımcı olmak üzere bir yazılım geliştirilmektedir.

3.1. Yazılım Geliştirme Süreç Modelleri

Yazılım geliştirme süreçleri ile kaliteli bir yazılım ürünü geliştirmek hedeflenir. Proje geliştirme süreci, projede yapılacak faaliyetleri ve bunların sırasını belirler. Süreç modeli, projenin aşamalarını, aşamaların uygulama sıralarını, koşul ve kısıtlamalarını belirler. Uygun olduğu durumlarda süreç modeli kullanılarak proje maliyetini düşürülmesi, yüksek kalitede ürün elde edilmesi, döngü süresinin azaltılması gibi faydalar süreç modellerinin ana hedefidir [22].

Yazılım geliştirme süreç modelleri aşağıda özetlenmiştir.

3.1.1. Şelale (Waterfall) modeli

Yazılım geliştirmede kullanılan en basit modeldir. Büyük ve karamaşık yazılım sürecinin küçük parçalara bölünerek yönetilmesi kolay bir hale dönüştürülmesi ana fikirdir. Model parçalar halindeki süreç aşamaların birbirleriyle ilişkili ancak içiçe olmasını sağlar. Şelale modelinin en büyük avantajı sadeliğidir [22]. İş süreci aşamaları aşağıdaki gibidir [23];

- Fizibilite çalışması
- İhtiyaç analizi ve proje planlaması
- Sistem tasarımı
- Kodlama
- Test ve uyarlama
- Kurulum
- Bakım ve Güncelleme

Fizibilite çalışması: Gerçekleştirilecek projenin emek, para, zaman giderleri göz önüne alınarak gereken faydayı sağlayıp sağlamayacağı incelenerek rapor haline getirilir.

Analiz ve planlama: Mevcut durumun analiz edildiği, isterlerin belirlendiği yazılım sürecinin en kritik aşamasını teşkil eder. Bu aşamada yapılacak bir yanlışın düzeltilmesi insan gücü ve para israfına neden olur.

Sistem Tasarımı: Analiz aşamasında belirlenen gereksinimlere uygun şekilde veri sözlüğü, meta-veri ve veri tabanının tasarlandığı aşamaya tasarım aşaması denir.

Kodlama: Tasarım aşamasında oluşturulan yapıya uygun şekilde yazılımın yapıldığı aşamadır.

Test ve Uyarlama: Geliştirilen yazılımın hata ve eksikliklerini belirlemek amacıyla test edildiği aşamadır. Bu aşamada yazılım yeterli olgunluk seviyesine ulaşana kadar kodlama aşaması arasında git gel yapılarak gereken düzeltmelerin yapılması ve yazılımın istenilen hale gelmesi sağlanır.

Kurulum: Test aşamasından geçerek yeterli olgunluğa ulaşan uygulama yazılımının devreye (kullanıma) alındığı aşamadır. Yazılım farklı lokasyonlara kurulacak ise kurulum ekibinin eğitimi, kullanıcıların eğitimi ve yardım masasının oluşturulması bu aşamada yapılır.

Bakım-Güncelleme: Sistemin iş sürekliliğinin sağlanması için güncellemelerinin yapılması ve bakım planının oluşturulması aşamasıdır.

Şelale modelinin yaygın bir şekilde kullanılmasına rağmen çok önemli kısıtlamaları vardır. Bunlar;

1. Tasarım aşamasın başlamadan önce isterlerin kesin bir şekilde belirlenmesi ve dondurulması gerekmektedir.

2. Belirlenerek dondurulmuş isterlere bağlı olarak donanımın seçilmesi gerekliliği bir kaç yıl süren bir projenin erken aşamalarında donanımın belirlenmesi zorunluluğunu doğurmaktadır.
3. Tüm yazılım bir defada ve proje sonunda elde edilir. Bu durum yanında büyük riskleri getirmektedir. Müşteri projenin sonuna kadar gelişmeler hakkında bilgi sahibi olamaz.
4. Müşterinin isterleri abartmasına neden olur.
5. Doküman esaslı bir süreç olduğundan her aşama sonunda birçok doküman hazırlanmasına neden olur.

3.1.2. Prototip model

Şelale modelinin birinci kısıtlamasını bertaraf etmek için geliştirilmiş bir modeldir. Şelale modelinde analiz safhasında tespit edilen isterlerin tasarım ve kodlama aşamalarına geçmeden önce belirlenme zorunluluğuna karşın prototip model mevcut durumda bilinen isterlere göre prototip in yapılmasını sağlar. Kullanıcı arzulanan sistemin isterlerini daha iyi anlar ve sonuçta daha az değişen oturmuş isterlere göre geliştirilmiş bir yazılım sağlanır. Prototip model manuel sürecin olmadığı veya mevcut sistemin isterlerinin belirlemesi gereken karmaşık ve geniş sistemlerde kullanılır. Bu modelde kullanıcının prototip ile oynayarak sistemin isterlerinin belirlenmesinde gereksiz ve önemli girdileri belirlemesini sağlar. Prototip geliştirildikten sonra kullanıcıya (müşteri) prototipi test etmesi için olanak sağlanır. Kullanıcının geri beslemeleri alınarak doğru olanlar, geliştirilmeye gereksinim duyulan yerler ve yanlış olan yerler belirlenir. Geri beslemeye göre prototip üzerinde geliştirmeye devam edilerek sistem yazılım geliştirilir.

Prototip model;

- Analiz
- Tasarım
- Kodlama
- Test

aşamalarından oluşur.

3.1.3. Döngüsel (Iterative) model

Döngüsel model şelale modelinin üçüncü ve dördüncü kısıtlamalarını bertaraf etmek, şelale modelin ve prototip modelin avantajlarını kullanan bir modeldir. Temel düşünce yazılımın küçük ilavelerle tamamlanmasıdır. Her döngünün sonunda, projenin bazı çıktılar elde edilir. Her döngüde, yazılıma yeni bir özellik eklenir.Bu sayede yazılım kademeli veya artırımsal olarak geliştirilir. Bu model yazılımın yapısına daha uygundur çünkü proje ilerlediği sürece yeni bilgiler ve deneyimler ortaya çıkar ve bu bilgi ve deneyimler projeyi geliştirmek için kullanılabilir [22].

Döngüsel modelde, projenin erken safhalarında elde edilen çıktılar, projenin geç safhalarında değişirse, bu değişiklikler projeye pahalıya mal olmaz. Bu Döngüsel modelin en büyük avantajıdır. Aynı zamanda, döngüsel modeldeki her döngü, projenin çalışanları için bir öğrenme sürecidir [23].

Döngüsel model gereksinimler daha başta olgun olmadığı ve projenin doğası gereği döngüler halinde kademeli olarak geliştirmeye yatkın projelerde kullanılmaya uygundur. Yazılım fonksiyonel olarak bölünmeye uygun olmalıdır. Her parça ayrı olarak ele alınır ve her döngüde yeni bir grup fonksiyon eklenir.

3.1.4. RUP (Rational Unified Process) model

IBM tarafından satın alınan Rational tarafından geliştirilen RUP diğer bir iterative modeldir [24]. Genel bir süreç modeli olmasına rağmen Unified Modeling Language (UML) kullanılarak Nesneye-Yönelik (*Object-Oriented*) yazılım geliştirmek için tasarlanmıştır [25]. RUP yazılım geliştirmeyi her biri tamamen çalışan sistemler olan döngülere bölmeyi öngörür. Genellikle herbir döngü mevcut sisteme (bir önceki döngü) bazı ilaveler sağlamayı hedefleyen ayrı bir proje olarak çalışır. Dört geliştirme aşaması geliştirme döngüsünü oluşturur. Son halini alan bir yazılım ürünü tüm yaşam döngüsü boyunca birçok geliştirme döngüsüne maruz kalır [26].

- Başlangıç (*Inception*) aşaması
- Değerlendirme (*Elaboration*) aşaması
- Yapım (*Construction*) aşaması
- Geçiş (*Transition*) aşaması

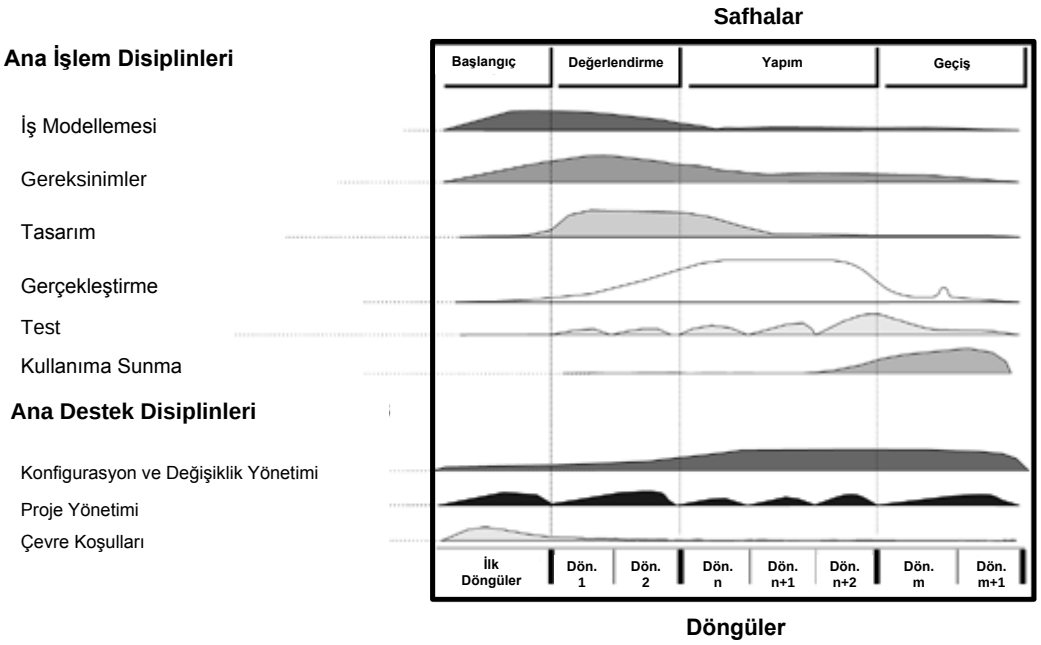
Başlangıç (Inception) aşamasının amacı projenin amaç ve kapsamını ortaya koymaktır. Bu aşamanın sonucunda yaşam döngüsü hedeflerinin kilometre taşları (*Lifecycle Objective Milestone –LCO*) belirlenmiş olur.

Değerlendirme (*Elaboration*) aşamasında ihtiyaç makamının projeyi onaylamasına müteakip detaylı sistem analizine göre sistemin mimarisi tasarlanır. Bu aşama tamamlandığında yaşam döngüsü mimarisi kilometretaşı (*Lifecycle Architecture Milestone - LCA*) tamamlanmış olur. Mimari yapı burada dondurulmuş değildir bu aşamada mimari yapının performansı ve bulundurulabilirliği gibi önemli nitelikleri ve mimari yaklaşım ile kullanılacak teknoloji belirlenir [26].

Yapım (*Construction*) aşaması isterlerin özelliklerini belirlenmesi, mimari konsept ve proje planı ile başlar. Ürünün gerçekleştirilmesi, birim testi ve sistem testi yapım aşamasında gerçekleştirilir. Yapım aşamasının çıktısı ürünün tam bir versiyonudur. Birinci işlevsel Yetenek kilometre taşı (*The Initial Operational Capability Milestone - IOC*) yapım aşamasının sonuç çıktısıdır.

Geçiş (*Transition*) aşaması ürünün geliştirme platformunda kullanıcının operasyonel platformuna aktarıldığı diğer bir deyişle ürünün kullanıcıya teslim edildiği aşamadır. Ürünün, teslim, eğitim ve destek faaliyetlerini içerir. Bu aşamanın sonucunda ürün kullanıma alınır (*product relase*).

Şekil 3.1’ de RUP (Rational Unified Process) Modeli yapısı görülmektedir [24].



Şekil 3.1. RUP modelin yapısı

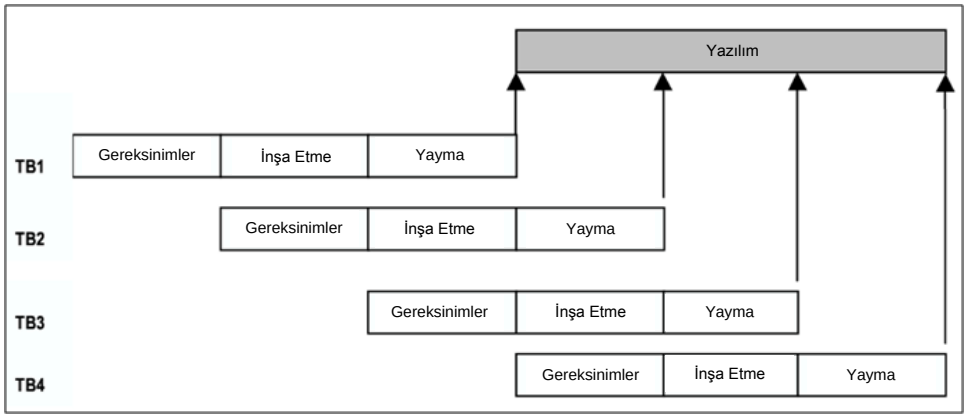
Genel olarak, RUP üst seviyede tekrarlayıcı bir yaklaşım sunmakla beraber yenilemeli bir yaklaşımı da teşvik eden esnek bir süreç modelidir. Aşamalarda projenin gereksinimlerine göre farklı işlerin yapılmasına izin verir [22].

3.1.5. Timeboxing model

Yazılım geliştirmeyi hızlandırmak için farklı döngüler arasında paralellik sağlar. Yeni döngü mevcut döngü tamamlanmadan başlar böylelikle yeni döngü mevcut döngü ile birlikte geliştirilir. Mevcut döngü tamamlanmadan yeni döngüye başlamak ortalama döngü süresini azaltır böylelikle proje süresi azalmış olur. Timeboxing modelinde bir zaman dilimi (döngü) şelale modelinde olduğu gibi aşamalara bölünmüştür . Her aşama döngü içerisinde açıkça belirlenmiş bir görevi yerine getirir ve belirli bir sonuca yöneliktir [22].

Şekil 3.2'de de açıkça görüleceği üzere iki döngü süresinde dört döngü gerçekleştirilmektedir.

Şekil 3.2' de Timeboxing süreç modeli görülmektedir [22].



Şekil 3.2. Timeboxing süreç modeli

3.1.6. Agile süreç modeli

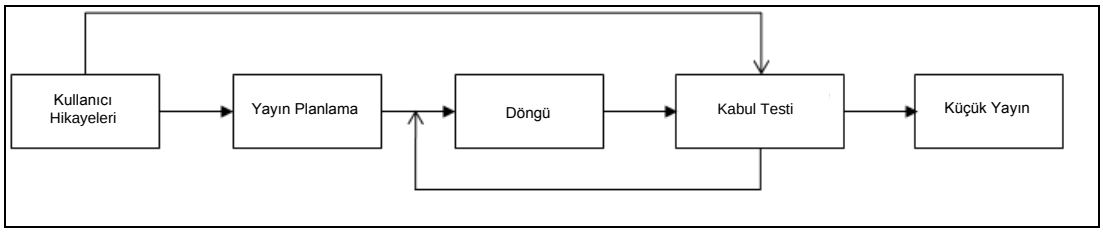
1990 lı yıların başında, diğer doküman ve bürokrasi gerektiren geleneksel süreç modellerinden ve özellikler şelale modelinden farklı geliştirilen bir süreç modeli yaklaşımıdır. Agile yaklaşımı aşağıdaki ortak prensipler üzerine kurulmuştur [22].

- Çalışan yazılım projenin ana ilerleme ölçütüdür.
- Bir projede ilerlemeler, hızlı geliştirilen küçük artırımlar ile elde edilir.
- Geç gelen gereksinim talepleri kolaylıkla karşılanabilir.
- Dokümantasyon yerine yüz-yüze görüşmeler tercih edilir.
- İhtiyaç makamının projeye yakın ilgisi ve sürekli geri beslemesi kaliteli yazılım geliştirmek için gereklidir.
- Olası senaryoya dayalı ayrıntılı tasarım yapmak yerine zaman içerisinde gelişen ve olgunlaşan basit tasarım daha iyi bir yaklaşımdır.
- Ürün teslim tarihleri yetenekli bireylerden oluşmuş güçlü ekipler tarafından karar verilir.

Günümüze kadar bazıları yaygın olarak kullanılan birçok detaylı Agile metodolojisi önerilmiştir. Bunların içerisinden Extreme programming (XP) en yaygın ve iyi bilinen yaklaşımdır. Diğer agile yaklaşımları gibi XP kaçınılmaz değişiklikleri ve yazılım geliştirmenin bu ani değişiklikleri karşılayabilecek bir yapıda olması gerektiğini kabul eder.

Bir extreme yazılımı projesi ihtiyaç makamı ve kullanıcıların sistemden beklentilerini birkaç cümlede anlatan kullanıcı hikayesi (*user stories*) ile başlar. Bu başlangıç geleneksel isterlerin belirlenmesinden detaylar konusunda farklıdır. Yazılım geliştirme ekibi kullanıcı hikayesine göre yazılım geliştirmenin ne kadar süreceğini kabaca kaç hafta olacağını tahmin eder. Bu tahminler ve hikayeler kullanılarak hikayelerin hangi sistem yayınında yapılacağının belirlendiği yayınlama planlaması (*release planning*) yapılır. Sık ve küçük yayınlar arzu edilir.

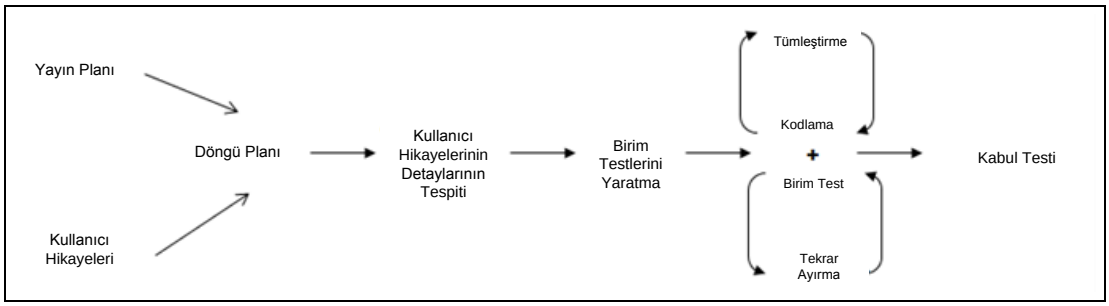
Şekil 3.3' de tüm XP iş süreci görülmektedir [22].



Şekil 3.3. Extreme programming (XP) de iş süreci

Yazılım geliştirme bir haftadan fazla sürmeyen döngüler halinde yapılır. Döngüler hangi hikayenin bu döngüde yapılacağının planlandığı döngü planlaması (*iteration planning*) ile başlar. Yüksek değerli ve yüksek riskli hikayeler yüksek öncelikli kabul edilir ve erken döngülerde geliştirilir.

Şekil 3.4’ de XP de bir döngü görülmektedir [22].



Şekil 3.4. XP de bir döngü

XP ve diğer agile metodları isterlerin sık değiştiği veya değişme olasılığının yüksek olduğu projeler için uygundur.

3.2. Uzman Sistemler

Haberleşme ve iletişim alanındaki gelişmeler, ülkeler arası kurulan iletişim ağları (Internet) dünyayı büyük bir köy haline getirmiştir. Dünyanın herhangi bir yerinde üretilen bilginin sayısal hale getirilerek bilgisayar ortamında saklanması, o bilgiye dünyanın herhangi bir yerinden çok kısa sürede erişimi olanaklı kılmaktadır.

“Bilgi Çağı” ve “Bilgi Toplumu” gibi terimlerin sıklıkla kullanıldığı günümüzde bilginin önemi daha açık bir şekilde ortaya çıkmaktadır. Bilginin önemi arttığı oranda o bilgiye ulaşabilmeyi sağlayan sistemlerin de önemi artmaktadır. Teknolojik gelişmelere paralel olarak bütün iş sektörlerinde bilgisayarlar kullanılmaya başlanmıştır ve her türlü gerekli bilgi bilgisayar ortamında saklanarak istenildiğinde yöneticilere sunulmaktadır. Burada önemli olan bilgilerin toplanması, organize edilmesi ve dağıtılmasıdır. Bir çok organizasyon bilgiyi toplamak, organize etmek ve dağıtmak için bilgisayar destekli bilgi sistemlerini kullanmaktadır. Yönetim bilimleri tabiriyle işletmelerde “Yönetim Bilgi sistemi” kullanımı yaygınlaşmaktadır. Bunun yanı sıra işletmeler “Uzman Sistem” gibi farklı yönetim bilimi tekniklerini kullanmaktadırlar [27].

Turban, uzman sistemleri şu şekilde tanımlamıştır; “Uzman sistem uzmanlığı gerektiren problemleri çözmek için bilgisayar tarafından depolanan insan bilgisini kullanan bir sistemdir. Bu sistemler hem uzman olmayanlar tarafından problemlerin çözümü için kullanılır, hem de uzmanlar tarafından bilgili yardımcılar olarak kullanılır.” Uzman Sistemlerin birçok farklı alandaki zor seviyede sayılabilecek problemleri başarılı bir şekilde çözüme kavuşturması, dikkat çekmelerindeki en önemli unsuru oluşturmuştur [28].

Uzman Sistemler, uzman bir insanın bilgi alanındaki bilgisinin bilgisayara değişik yapılarda aktarılması ve bilgisayarın da benzer şekilde tepki göstermesi yaklaşımı ile çalışır. Bu nedenle uzman sistemler insan bilgisini yoğun biçimde kullanan programlardır. Diğer bir deyişle “Ancak bir uzman insanın çözebileceği karmaşık problemlerin bilgisayar ile çözümüne olanak sağlayan sistemler” olarak tanımlanabilir. Bazen Bilgi-Temelli Sistem veya Bilgi-Temelli Uzman Sistem ifadeleri Uzman Sistem ifadesi yerine kullanılabilir.

Uzman sistem yazılımı geliştirilirken herhangi bir programlama dili yerine, uzman sistem kabuk programı kullanılması zaman ve iş gücünden önemli bir tasarruf sağlar [35].

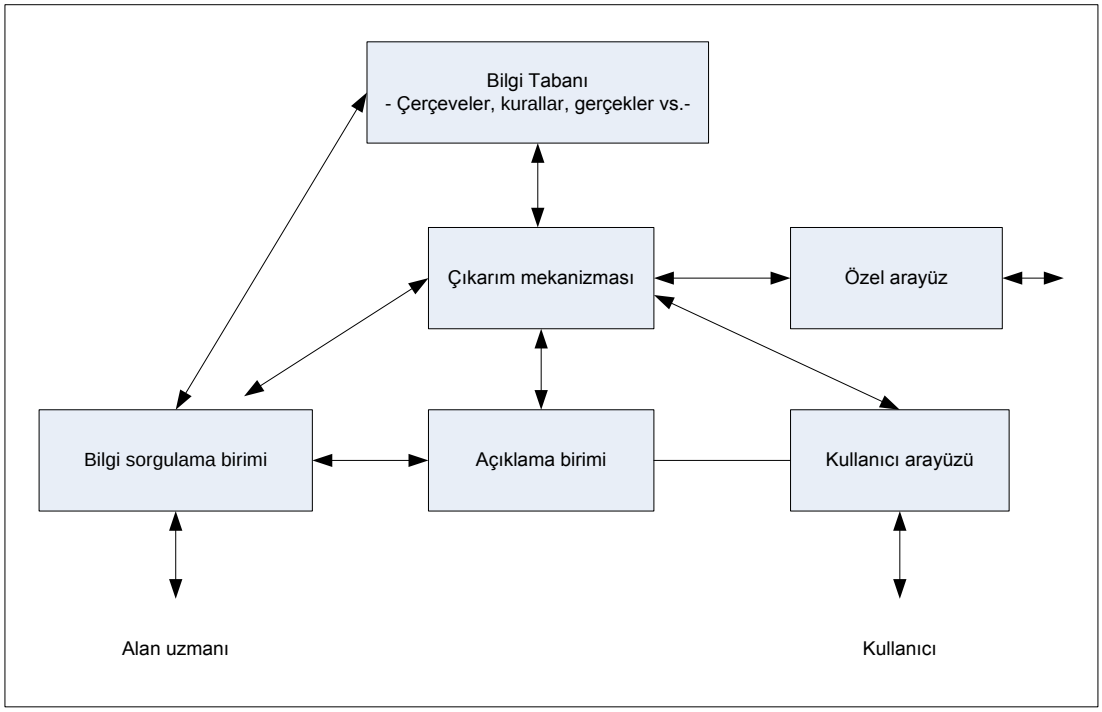
1970’de ilk kez ortaya çıkan Uzman Sistemler, son otuz yıl içerisinde büyük önem kazanmıştır. Uzman Sistemlerin birçok farklı alandaki zor seviyede sayılabilecek problemleri başarılı bir şekilde çözüme kavuşturması, dikkat çekmelerindeki en önemli unsuru oluşturmuştur.

Uzman sistemler karmaşık yapay zeka programlarıdır. Bir sonraki bölümde özetlencek olan tüm teknikler uzman sistemler içerisinde uygulanabilir. Bu teknikler içerisinde alan bilgisinin gösteriminde en yaygın olarak kullanılan teknik üretim kuralları (production rules) dır [29].

3.2.1. Uzman sistemlerin mimari yapısı ve temel bileşenleri

Uzman sistemin temel bileşenleri bilgi tabanı (Knowledge Base), Çıkarım Mekanizması (Inference Engine) ve Kullanıcı Ara yüzü (User Interface) dür. Alan bilgisi uygun formasyonda bilgi tabanında saklanır.

Uzman sistemin mimari yapısı şekil 3.5' de görülmektedir [30].



Şekil 3.5. Uzman sistem mimarisi

3.2.1.1. Bilgi tabanı

Bilgi tabanı problemlerin anlaşılması, formülasyonu ve çözümü için gerekli olan tüm bilgileri içerir. Temel olarak iki çeşit bilgi vardır bunlar; ifade edici bilgi (declarative knowledge) ve işlevsel bilgi (procedural knowledge). İfade edici bilgi veri (data) ve gerçeklerle (facts) gösterilir. İşlevsel bilgi, ifade edici bilgi kullanılarak elde edilen bilgidir. Uzman insanlardan bilgi edinmek ve bu bilgiyi uygun şekile sokmak ve saklamak işlemine bilgi mühendisliği (knowledge engineering) denir [30].

Bilgi tipleri aşağıdaki gibi gösterilir ;

İşlevsel Bilgi (Procedural knowledge)

IF durum THEN işlem
IF satış gün sayısı > 30 THEN ilgili prosedürü kontrol ediniz.

İfade Edici Bilgi (Declarative knowledge)

IF önceki koşul THEN sonraki koşul
IF X ödenebilir bakiye THEN X borçtur.
IF (Y şirketinin borcu = $12,500)
THEN (Y şirketi borca itiraz eder)

3.2.1.2. Bilgi mühendisliği (Knowledge engineering)

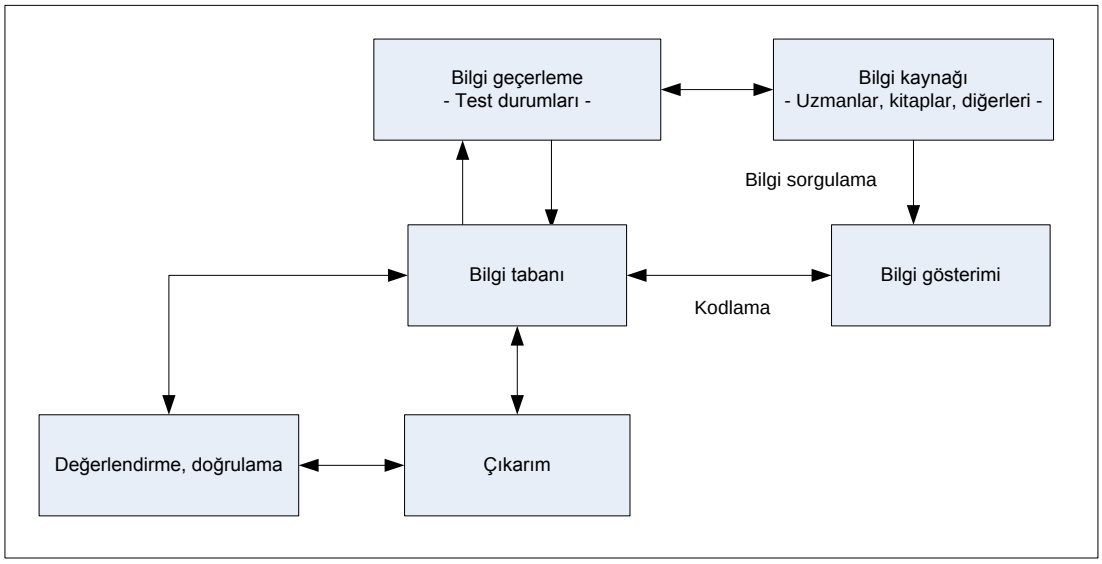
Bilgi mühendisliği ileri seviyede alan uzmanlığı gerektiren karmaşık problemlerin çözümünde bilgisayar sistemlerinin kullanılması ile ilgili bir mühendislik disiplinidir. Bilgi mühendisliğinin ana işlevi bilgi sorgulaması, bilgi gösterimi ve bilgi geçerliliğidir.

Bilgi mühendisliği, yaklaşık yirmi yıl önce prensiplerle, metotlarla ve bilgi toplayan araçlarla ilgili olarak, bilgi tabanı geliştirme maksadıyla yapay zeka nın bir parçası olarak kullanılmaya başladı.

Son zamanlarda bilgi mühendisliği tanımına sadece yapay zeka değil ticaret mühendisliği (business engineering), e-ticaret mühendisliği (e-business engineering), bilgisayar bilmi/mühendisliği (computer science/engineering), yazılım mühendisliği, bilişim teknolojileri ve bilgi yönetimi de dahil olmuştur [31].

Benzer bir tanımlama, Solvberg ve Kung tarafından bilgi sistemleri mühendisliği “information systems engineering” teriminin ortaya atılmasıyla da yapılmıştır [32].

Bilgi mühendisliği süreci Şekil 3.6 da gösterilmiştir [30].



Şekil 3.6. Bilgi Mühendisliği Süreci

3.2.1.3. Bilgi gösterimi

Aşağıdaki metotlarla yapılır.

1. Yüklemsel Analiz (Predicate Calculus)
2. Çerçeveler (Frames)
3. Anlamsal Ağlar (Semantic Networks)
4. Nesne-Nitelik-Değer Üçlüsü (Object-Attribute-Value (O-A-V) Triplets)
5. Üretim Kuralları (Production Rules)
6. Yapay Sinir Ağları (Neural Networks)

Yüklemsel Analiz (Predicate Calculus) : Temel birimi nesne (object) tir. Nesnelerle ilgili cümlelere belirteç adı verilir. Örneğin, mavidir (araba) arabanın mavi olduğuna dair bir savdır.

Predicate calculus bir kelimeyi aşağıdaki formda tanımlar.

- Nesneler seti vardır.
- Her bir nesnenin özellik seti vardır.
- Fonksiyonlar vardır. Verilen nesneleri dikkate alınarak her fonksiyon başka bir nesneyi hesaplar.
- Nesneler arasında tutulabilir bir ilişki vardır.

Çerçeveler (Frames): Gerçekleri (facts) ve ilişkileri temsil eden bir metod sağlar. İlgili nesne ile ilintili tüm bilgileri içeren bir nesne yeri (slot) tanımlar. Slot bir nesnenin değer, ilk değerler, diğer framelerle işaretçiler, kural kümeleri veya prosedürler içeren bileşenidir.

Anlamsal Ağlar (Semantic Networks): Düğüm (Node) adı verilen nesnelerin toplamından oluşan networke semantic adı verilir. Düğümler nesneler ve tanımlarının gösterimi için kullanılır. Bağlantılar (Links) nesneler ve tanımları ilişkilendirmek için kullanılır.

Nesne-Nitelik-Değer Üçlüsü (Object-Attribute-Value (O-A-V) Triplets): Gerçeğe dayalı bilgileri göstermek için yaygın bir yöntemdir. İlk uzman sistem uygulaması olan MYCIN de kullanılmıştır. Nesneler fiziksel veya kavramsal olabilirler. Nitelikler nesneler ile birleşik genel karakteristikler veya özelliklerdir.

Üretim Kuralları (Production Rules): Kurallar ilişkileri göstermeye yarar. Kural tabanlı bilgi gösterimi -IF *kural* THEN *eylem*- yapısındadır. Problem konusu koşula uygun ise eylem gerçekleştirilir.

Yapay Sinir Ağları (Neural Networks): Yapay sinir ağları kullanılarak bilgi gösterimi aşağıdaki faydaları sağlar.

- Hesaplamaya farklı bir yaklaşım getirir.
- Silikon işlemcilere (chips) gömülebilir.
- Eğitimli ve programlanmış değildir.
- Topoloji, hücre özellikleri ve eğitim kuralları belirlenir.

3.2.1.4. Çıkarım mekanizması

Uzman Sistemin beynidir. Bilgi tabanı ve çalışma alanında bulunan bilgiler üzerine düşünmek için bir metodoloji sunan ve sonuçları biçimlendiren bir bilgisayar programıdır. Bir başka deyişle gerçekler ve vaadlerden (promises) sonuç çıkaran mekanizmadır. Burada sistem bilgisinin nasıl kullanılacağı hakkında karar alınır. Başlıca 2 temel görev yerine getirir. Bunlar ;

- Mevcut gerçekler ve kuralları kontrol eder ve mümkün olduğunda yeni gerçekler ekler.
- Hangi çıkarımın yapılacağına karar verir.

Çıkarım başlıca Modus ponens ve Modus tollens olmak üzere iki yöntemle yapılır.

Modus Ponens: Yaygın olarak kullanılan çıkarım stratejisidir, basit muhakeme esaslı ve kolaylıkla anlaşılabilir.

Modus Ponens'in gösterimi;

Sıralı notasyonda $P \rightarrow Q, P \vdash Q$ veya kural formunda $\frac{P \rightarrow Q,\ P}{Q}$ şeklinde mantıksal olarak "IF A THEN B" şeklinde gösterilir.

Örneğin : IF Bugün Pazartesi, THEN işe gideceğim.
Bugün Pazartesidir.
Bu nedenle, İşe gideceğim.

Modus Tollens: Modus Ponens in cevap veremediği eylemin olumsuz olması durumunda kullanılır.

Sıralı notasyonda $P \rightarrow Q,\ \neg Q \vdash \neg P$ veya kural formunda $\frac{P \rightarrow Q,\ \neg Q}{\neg P}$ şeklinde, gösterilir.

Örneğin : IF Köpek hırsız gördüğünde havlar
Köpek gece boyu havlamadı.
Bu nedenle, hırsız gelmedi/yoktu.

Belisizlik Durumunda Çıkarım: Çıkarım mekanizması belirsizlik durumunda eksik bilgi ile de çalışabilmelidir. Belirsizlik derecesi gerçek sayısı ile ilgilidir. İki çıkarım metodu vardır. Bunlar İleri Zincirleme (Forward-Chaining), Geri Zincirleme (Backward Chaining) dir.

İleri Zincirleme: Tüme varım yaklaşımının uygulanmasıdır. Veriye yöneliktir (data-driven). Kullanıcıdan alınan bilgilere kurallar sırasıyla uygulanarak sonuç bulunmaya çalışılır. Kullanıcı ile uzman sistem arasında problem çözümünün sonuna kadar bir etkileşim vardır. Bu etkileşim bilgi tabanındaki kural zinciri içerisinde gerçekleşir.

Basit bir ileri zincirleme örneği aşağıdaki gibidir ;
Kural 1
IF Araba su kaynatırsa THEN Araba arızalanır
Kural 2
Araba arızalanırsa
THEN Masraf çıkarır
VE Eve geç kalırım.

Soru : Arabanın masraf çıkaracağı ve eve geç kalacağınız durum nasıldır?
Olayları başlatan eylem arabanın su kaynatmasıdır.

Geri zincirleme: Tümden gelim yaklaşımının uygulanmasıdır. Diğer bir deyişle sonuca yöneliktir (goal-driven). Sonuç bellidir sebep bulunmaya çalışılır. İşlem, verilen sonuç bulununcaya veya uygulanacak kural kalmayıncaya kadar devam eder.

Kural 1

IF Araba bakımlı değil AND Akü zayıf

THEN Marş motoruna yeterli akım gelmiyor.

Kural 2

IF Marş motoruna yeterli akım gelmiyor

THEN Araba çalışmaz

Verilen gerçekler :

Araba Bakımlı değildir

Akü zayıftır

Soru: Arabanın çalışmaması sonucuna nasıl varılır?

Araba bakımlı değilse ve akü zayıfsa araba çalışmaz.

3.2.1.5. Kullanıcı arabirimi

Uzman Sistemler, kullanıcı ile bilgisayar arasında probleme yönelik iletişimin sağlanması için bir dil işleyici içerir. Bu iletişim, en sağlıklı doğal dil ile yapılır. Kısaca kullanıcı ara birimi kullanıcı ile bilgisayar arasında bir çevirmen rolünü üstlenmiştir. Modern bilgisayar programlarında olduğu gibi, Uzman Sistemlerin de kullanıcının rahat kullanabileceği kolay ve anlaşılır bir arabirimi vardır. Kullanıcı arabiriminin kolay ve anlaşılır olması, sistemin iç çalışmasının akıcı olacağı anlamına gelmez, fakat bu uç kullanıcıların Uzman Sistemi kullanırken sisteme problemlerini rahatça anlatabilmelerini ve sistemin verdiği sonucu da rahatça anlayabilmelerini sağlar.

3.2.1.6. Açıklama birimi

Uzman Sistemleri diğer sistemlerden farklı yapan bir özelliği de açıklama modülünün olmasıdır. Açıklama modülünden kasıt, kullanıcıya çeşitli yardımların verilmesi ve soruların açıklanması olduğu kadar, Uzman Sistemin çıkardığı sonucu nasıl ve neden çıkardığını açıklayabilmesidir. Burada Uzman Sistem karşılıklı soru cevap şeklinde davranışlarını açıklar.

3.2.2. Uzman sistemlerin özellikleri

Bir Uzman Sistem genelde şu özellikleri taşıyacak şekilde tasarlanır:

i. *Yüksek Performans*: Bir Uzman Sistem programı, sorulan sorulara uzman bir insana denk veya daha iyi bir düzeyde cevap verebilmelidir.
ii. *Hızlı Cevap Verme:* Tasarlanan sistemin, sorulan sorulara yönelik bir sonuca makul bir sürede varabilmesi ve hatta uzman bir insandan daha çabuk karar verebilmesi gerekir. Örneğin, bir uzmanın bir saatte sonuca vardığı bir konuda, Uzman Sistemin bir yılda karar vermesi elbette işe yaramaz.
iii. *Güvenilirlik:* Hazırlanan Uzman Sistemin güvenilir olması, hata vermemesi gerekir.
iv. *Anlaşılabilirlik:* Tasarlanan sistemin, bir konuda vardığı sonucun aşamalarını tek tek açıklayabilmesi gerekir. Sonuca nasıl vardığı meçhul olan bir sistemden ziyade, tıpkı bir insan uzman gibi, gerektiğinde vardığı sonucun nedenlerini açıklayabilmelidir.
v. *Esneklik:* Bir Uzman Sistemde kullanmak üzere büyük miktarda bilgi yüklemek gerekir. Bu yüzden bilgi ilave etmek, değiştirmek ve silmek için etkin bir mekanizmanın Uzman Sisteme eklenmesi gerekir. Kural-Tabanlı Sistemlerin (Rule-Based Systems) popüler olmasının önemli nedenlerinden biri, kuralların etkin ve modüler bir biçimde saklanabilme özelliğidir.

3.2.3. CLIPS (C Language Integration Production System) kabuğu (shell)

CLIPS (C Language Integration Production System), 1986 yılında NASA/Lyndon B.Johnson Uzay Merkezinin Yazılım Teknoloji Şubesi (Software Technology Branch -STB-) tarafından geliştirilmiştir. Açık kaynak kodu olarak temin edilebilen bir uzman sistem kabuğudur. CLIPS ileri zincirleme muhakemesi yapar ve bilgi gösteriminde üretim kuralları metodunu kullanır [32].

CLIPS kabuğunun notasyonu LISP programlama diline çok benzerdir. Aşağıda CLIPS kullanılarak bir kural tanımlamasının örneği verilmiştir [34]:

```
(defrule kimdir
(adı ?r1 Ali)
(soyadı ?r1 Yılmaz)
(saç rengi ?r1 Kızıl)
=>
(assert (is-patron ?r1)))
```

?r1 değişken gösterimi için kullanılmıştır, bu durum için bir şahıstır. *Assert* Veritabanına fact (gerçek) atamak için kullanılır, örnekte üç gerçekten bir sonuç üretilmektedir. Şöyle ki eğer şahısın adı Ali, soyadı Yılmaz ve saç rengi kızıl ise bu şahıs patrondur.

Yukarıda ki örneğin başka bir şekilde gösterimi:

```
(assert (adı x Ali))
(assert (soyadı x Yılmaz))
(assert (saç rengi x Kızıl))
(run)
```

Burada (facts) komutu gerçekleri görmek için kullanılır. Veritabanındaki gerçekler aşağıdaki gibi görünür:

CLIPS> (facts)

f-0 (adı x Ali)

f-1 (soyadı x Yılmaz)

f-2 (saç rengi x Kızıl)

f-3 (is-patron x)

4. ÖNERİLEN SİSTEMİN TASARIMI VE GERÇEKLEŞTİRİLMESİ

Bu tez çalışmasında uzman sistem CLIPS kabuğu kullanılarak bilgi güvenlik yönetim sistemi kurulmasını sağlayan bir yazılım geliştirilmiştir.

4.1. Uzman Sistem Yaklaşımının ISO 27001 Bilgi Güvenliği Yönetim Sistemine Uygulanması

Bu tez çalışmasında Türkiye de bilgi teknolojileri kullanımının gün geçtikçe arttığı ve bu konuda bilgi sahibi personelin çok az sayıda istihdam edildiği kurum ve kuruluşlara yönelik ISO 27001 bilgi güvenliği yönetim sisteminin kurulması ve sürdürülmesine ilişkin uzman sistem temelli bir çözüm geliştirilmektedir.

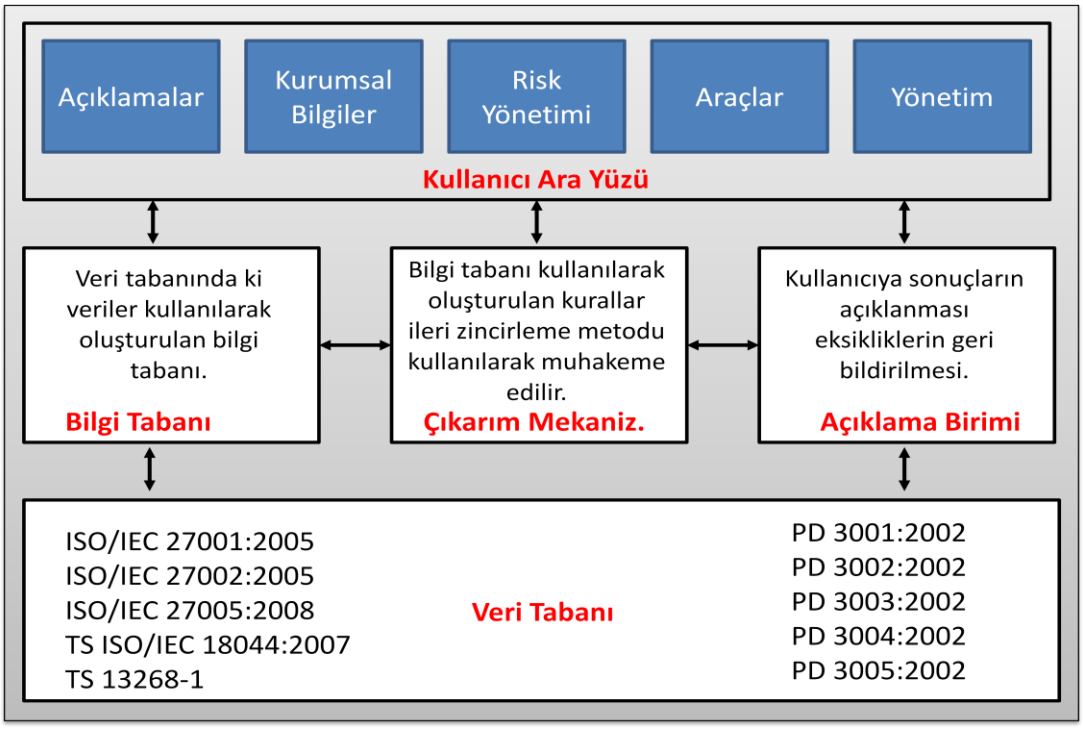
Uygulamanın hedef kullanıcı kitlesi temel bilgisayar bilgisine sahip personel istihdam eden kurum ve kuruluşlardır. Bu nedenle geliştirilen yazılımın kullanımı kolay ve görsel özelliklerin ön planda olduğu bir platformda geliştirilmesi uygun olacaktır. Bu nedenle yazılım geliştirme ortamı olarak kurum ve kuruluşlarda yaygın olarak kullanılan Microsoft Office uygulamaları ile entegre olabilen ve Nesneye Yönelik bir yazılım geliştirme platformu olan Microsoft .NET C# seçilmiştir. Veri tabanı olarak ücretsiz olması nedeniyle Microsoft SQL Express Edition kullanılmıştır. Yazılım geliştirme modeli olarak Nesneye Yönelik yazılım geliştirmeye uygun olan RUP (Rational Unified Process) Model seçilmiş tüm modelleme UML ile gerçekleştirilmiştir.

Uzman sistem geliştirilirken zamandan tasarruf sağlaması ve hata yapma olasılığını azaltması nedenleriyle, uzman sistem kabuk programı kullanılmasının zaman ve emek tasarrufu sağlaması yanısıra yapılabilecek olası programlama hatalarını önleyeceğinde dolayı geliştirilen yazılımda kabuk program kullanılmıştır. Uzman sistem kabuk programı seçilirken C, C++, C#, Java uygulama geliştirme platformlarını destekleyen CLIPS, ACQUIRE gibi kabuk programları incelenmiştir. Ücretsiz olarak temin edilebilmesi, Nesneye Yönelik programlamaya uygun olması, Microsoft .NET platformu ile uyumlu çalışması ve .NET için gereken .dll lerin

bulunması ve özellikle bu tez çalışmasında yoğun olarak kullanılan ileri zincirlemeyi çok iyi desteklemesi nedenleriyle CLIPS kabuk programı bu çalışmada tercih edilmiştir.

ISO 27001 standardına uygun BGYS kurulurken ilgili standartlar kullanılarak bilgi tabanı oluşturulmuştur. Bilgi tabanı oluşturulurken ifade edici bilgi (declarative knowledge) ve işlevsel bilgi (procedural knowledge) birlikte kullanılmıştır. Bilgi tabanı kullanılarak kurallar oluşturulurken bilgi gösterme yöntemlerinden üretim kuralları (production rules) kullanılmış ve CLIPS kabuk programına aktarılmıştır.

Kullanıcıların cevaplaması gereken sorular basit ve kolay anlaşılır şekilde hazırlanmıştır. Çıkarım birimi ileri zincirleme yöntemi kullanılarak hazırlanmıştır. Kullanıcıların vermiş oldukları doğru ve yanlış cevapların nedenleri kendilerine açıklama birimi tarafından bildirilerek kullanıcıların standardın gereklerini yerine getirmeleri sağlanmıştır. Geliştirilen yazılıma Smart ISMS adı verilmiştir. Sistemin mimari yapısı Şekil 3.7. de gösterilmektedir.



Şekil 3.7. Uzman Sistem tabanlı BGYS yaklaşımı mimarisi

Önerilen sistem ISO 27001, ISO 27002 [37], ISO/IEC 27005 [38] ve TS 13268-1 dokümanlarında belirtilen BGYS nin belgelendirilebilmesi için gereken koşulları sağlayacak şekilde geliştirilmiştir [36].

Geliştirilen yazılımda; Açıklamalar modülü, Kurumsal bilgiler modülü, Risk yönetimi modülü, Araçlar modülü ve Yönetim modülü bulunmaktadır.

Açıklamalar Modülü:

Kullanıcılara geliştirilen yazılımı kullanıma başlamadan önce Bilgi Güvenliği Yönetim Sistemi ve Smart ISMS hakkında açıklayıcı bilgi verir.

Kurumsal Bilgiler Modülü:

Smart ISMS içerisinde kullanılan kullanıcı kurum/kuruluş bilgilerinin alındığı, organizyon yapısının belirlendiği ve bilgi güvenliği yönetim sisteminin kapsamının oluşturulduğu modüldür. Ayrıca bu modülde kurum/kuruluşun mevcut durum tespiti kullanıcıya yöneltilen sorulara verilen cevapların, çıkarım mekanizması tarafından ISO 27001 'in EK-A sında bulunan 10 başlık altında 133 adet kontrol maddesi ile mukayese edilirek kurum/kuruluşun tamam ve eksiklikleri tespit edilir. Kullanıcı eksiklikleri tamamlayarak (kullanıcı isterse eksik olarak) bu kontrol maddelerinin organizasyon içerisinde nasıl uygulancağını açıklayan en az 10 prosedür Smart ISMS tarafından hazırlanır ve araçlar modülünde raporlara eklenir.

Risk Yönetimi Modülü:

Süreç esaslı veya doğrudan bilgi varlıklarının envanterinin çıkartıldığı, varlıkların gizlilik, güvenilirlik ve erişilebilirlik değerlerine göre değerlemesinin yapıldığı, varlıkların zafiyet ve tehditlerin tespit edildiği ve varlıkların korumalarının belirlendiği modüldür.

Varlık envanterinin nasıl çıkartılacağı ve bilgi varlıklarının değerlendirilmesinin nasıl yapılacağı ISO/IEC 27005 (2008) Information Security Risk Management dokümanı esaslarına göre yapılır [38].

Kuruluşun kapsam dahilindeki bilgi varlıklarını süreç analizi yaparak belirlenmesi ve bu varlıklara gizlilik, bütünlük, erişilebilirlik değerlerinden oluşan varlık değerinin belirlenmesi bu modülde gerçekleştirilir. Bu tez çalışmasında hedef kullanıcı kitlesi olarak temel bilgisayar bilgisine sahip kişiler göz önüne alındığından, risk değerlendirme anlaşılması ve kullanımı kolay standart bir yaklaşım ile yapılmaktadır.

Çizelge 3.1. Varlık değerlendirme çizelgesi

GİZLİLİK DEĞERİ	**BÜTÜNLÜK DEĞERİ**	**ERİŞİLEBİLİRLİK DEĞERİ**	**AÇIKLAMA**
5	5	5	Çok Yüksek
4	4	4	Yüksek
3	3	3	Orta
2	2	2	Düşük
1	1	1	Çok Düşük

Bu çalışmada **GİZLİLİK, BÜTÜNLÜK ve ERİŞİLEBİLİRLİK** kriterleri eşit ağırlıkta kabul edilir ve aynı öneme sahip olarak değerlendirilir.

Varlık Değeri Formülü:

$$Varlık\ Değeri = Gizlilik_{Değeri}\ x\ Bütünlük_{Değeri}\ x\ Erişilebilirlik_{Değeri}$$

Örneğin: En yüksek Varlık Değeri = 5 x 5 x 5 =125
En düşük Varlık Değeri : 1 x 1 x 1 = 1 dir

Varlıklara yönelik tehditlerin ve zafiyetlerin bu varlıklarla ilişkili etkileri ışığında oluşan güvenlik başarısızlıkları, gerçekçi olma olasılıkları mevcut kontroller göz önünde tutularak belirlenir. Herbir tehdit için olasılık değerleri Çizelge 3.2. esas

alınarak tespit edilir. Keza oluşan güvenlik başarısızlıklarının hasar derecesi Çizelge 3.3. de gösterilmiştir. Değerlendirilen olasılıklar ile belirlenen iş hasarları Risk Değerlendirme Raporu üzerinde varlıklara ait her bir tehdit için ifade edilir.

Çizelge 3.2. Tehdidin olasılık derecesi çizelgesi

OLASILIK DERECESİ	OLASILIK	AÇIKLAMA
5	Çok Yüksek	Tehdit kaçınılmazdır
4	Yüksek	Tehdit sıkça tekrarlanır
3	Orta	Tehdit gerçekleşebilir
2	Düşük	Tehdit nadiren gerçekleşir
1	Çok Düşük	Tehdit yok denecek kadar azdır

Çizelge 3.3. Tehdidin hasar derecesi çizelgesi

HASAR DERECESİ	HASAR	AÇIKLAMA
5	Çok Yüksek	Kurumsal sürekliliği tehlikeye sokacak hasar
4	Yüksek	Faaliyeti itibar kaybına yol açacak kadar kesintiye uğratacak hasar
3	Orta	Faaliyeti önemsiz ölçüde kesintiye uğratacak hasar
2	Düşük	Faaliyeti etkileyen ama kesintiye uğratmayan hasar
1	Çok Düşük	Faaliyeti doğrudan etkilemeyen hasar

Risklerin yok edilmesi veya azaltılması ve değerlendirmesi aşağıdaki önlemler alınarak gerçekleştirilir;

- Uygun kontroller uygulanır,
- Kuruluşun politikalarını ve riskleri kabul etme kriterlerine uygun risklerin kabul edilir,

- Risklerden kaçınılır veya mümkünse tedarikçilere veya sigorta şirketlerine aktarılır.

Risk Seviyesi Formulü:

RİSK SEVİYESİ = VARLIK DEĞERİ x TEHDİDİN OLASILIĞI x İŞ HASARININ DERECESİ

Bu formül sonucunda maksimum Risk değeri 3125, minimum risk değeri ise 1 olmaktadır.

Kabul edilebilir risk değeri tüm değerlerin medyanı alınarak hesaplanır bu durumda;

$$RİSK\ SEVİYESİ_{Kabul\ Edilebilir} = VARLIK\ DEĞERİ_{Ortalama} \times TEHDİDİN\ OLASILIĞI_{Var} \times İŞ\ HASARININ\ DERECESİ_{Yönetim\ Kararı}$$
$$= 3 \times 3 \times 3$$
$$= 27$$

olarak belirlenmiştir.

Bu modülde ISO/IEC 27005 (2008) dokümanına uygun olarak varlıkların tipine göre tehdit zafiyet belirlemesi ve korumaların atanması oluşturulan risk değerlendirme işlemleri bilgi tabanı yardımıyla yapılır.

Araçlar Modülü:

Mevcut durum tespiti menüsünde yaratılan raporların bulunduğu modüldür. Bu modül yardımıyla tüm dokümanlar üzerinde değişiklikler yapılabilir. Bilgi güvenliği politikası ve Smart ISMS tarafından kullanılan risk değerlendirme metodolojisi ile ISO 27001 de zorunlu olarak istenen risk değerlendirme raporu, risk işleme planı, uygulanabilirlik bildirgesi bu modül tarafından hazırlanır. Ayrıca bu modülde kurum/kuruluşun yapması gereken iç denetimler için soru hazırlaması yapılır.

Yönetim Modülü :

Smart ISMS yazılımının yeni kullanıcı ekleme ve şifre değiştirme gibi işlevlerini yerine getiren modüldür.

4.2. Smart ISMS Yazılımının Geliştirilmesi

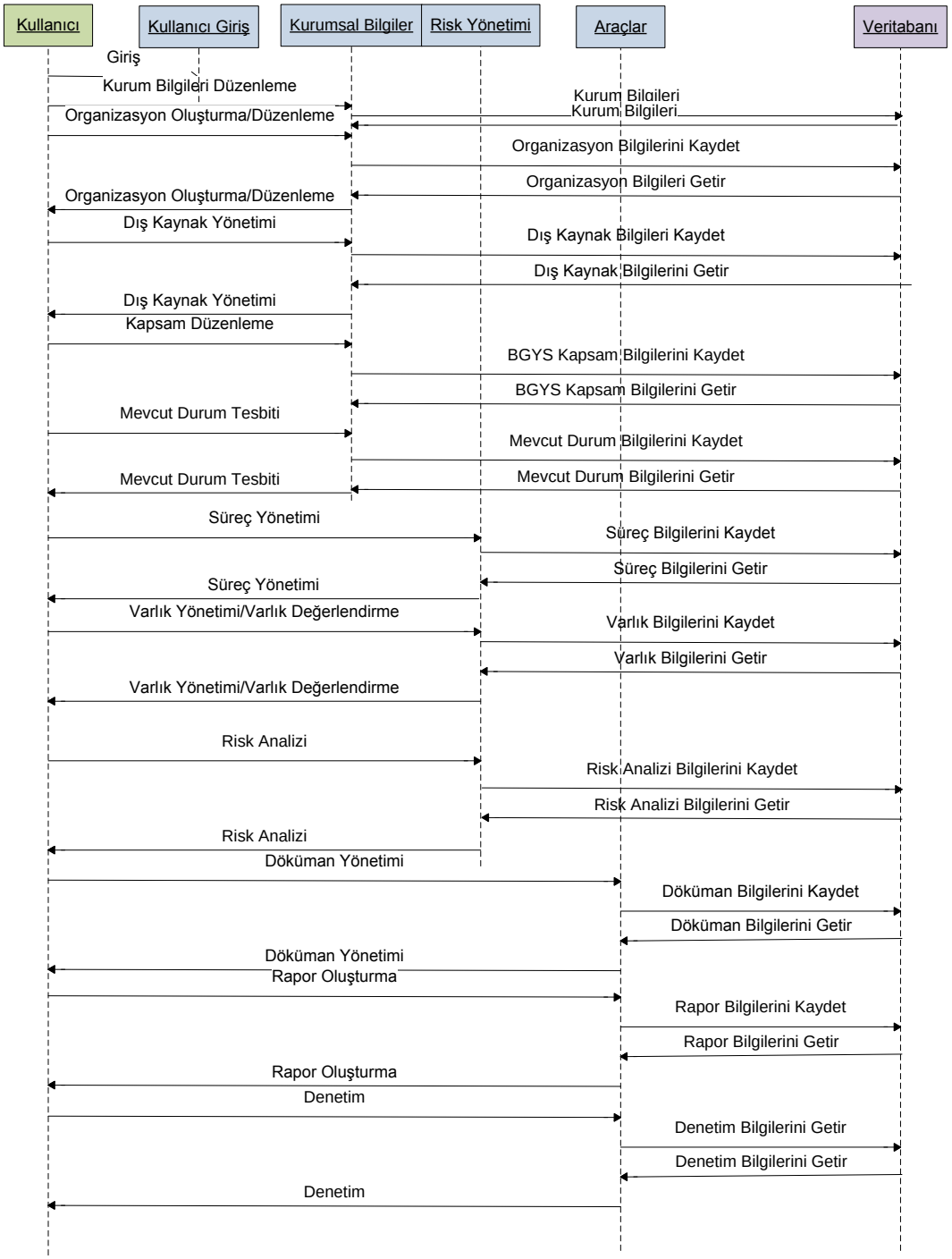
Smart ISMS yazılımı hedef kullanıcı kitlesinin bilgisayar kullanım bilgisi göz önüne alınarak görselliği ön planda tutan ve Nesneye Yönelik bir yazılım geliştirme ortamı olan Microsoft .NET C# platformunda WEB tabanlı olarak geliştirilmiş, veri tabanı olarak Microsoft SQL Express Edition kullanılmıştır.

Yazılım geliştirme metodu olarak RUP kullanılmış modelleme aracı olarakta UML kullanılmıştır. UML diagramlarından önemli olan Use case, Component diagram, Activity diagram, Class ve Sequence diagramları hazırlanmıştır. Smart ISMS yazılımının UML diagramlarından Sequence diagramı Şekil 3.8 gösterilmiştir.

Geliştirilen yazılımın kullanıcı use case diagramı EK-1 de, Component diagramı EK-2 de, Activity diagramı EK-3 arasında, Class diagramları EK-4 ile EK-7 arasında, Raporlar Class diagramları EK-8 ile EK-10 arasında ve Clips class diagramı EK-11 de gösterilmiştir.

Class ve Object diyagramları statik bilgiyi modeller. Halbuki gerçek zamanlı sistemlerde zaman içinde değişen interaktiviteler bu diyagramlarla gösterilemez. Bu tür zamanla değişen durumları belirtmek için sequence diyagramları kullanılır.

Smart ISMS yazılımının Sequence diagramı Şekil 3.8’ dedir.



Şekil 3.8. Sequence diagram

Alan uzman bilgisi ve ISO 27001, ISO 27002, ISO/IEC 27005 standartları kullanılarak üretim kuralları (production rules) hazırlanmıştır.

Örneğin Risk değerlendime kuralı aşağıdaki gibidir;

IF
Organizasyonun bilgi varlıkları envanteri çıkarılmışmıdır IS TRUE
AND
Bilgi varlıklarının risk değerlendirmesi yapılmışmıdır IS TRUE
AND
Bilgi varlıklarına tehditlere karşı kontroller uygulanarak risk seviyesi azaltılmışmıdır IS TRUE
AND
Yönetim kabul edilebilir risk seviyesini belirlemişmidir IS TRUE
AND
Uygulanabilirlik beyannamesi hazırlanmışmıdır IS TRUE
THEN
Risk değerlendirmesi uygundur.

Hedef kullanıcı kitlesinin bilgisayar bilgisi göz önüne alınarak kolay ve anlaşılır sorular hazırlanarak kurum veya kuruluşun mevcut durum tespiti yapılmıştır. Kullanıcının sorulara verdiği cevaplar çıkarım biriminde muhakeme edilerek kurum veya kuruluşun eksik ve tamam olan güvenlik önlemleri kullanıcıya açıklama birimi tarafından geri bildirimi yapmaktadır.

Örnek: (Fiziksel ve Çevresel Güvenlik)

1. Kuruluşunuza gelen müşterileriniz veya misafirleriniz nasıl karşılanıp içeri girerler? (Birden fazla şık işaretlenebilir)
    a. Girişte güvenlik görevlisi veya resepsiyon görevlisi karşılar ve gideceyi yere kadar refakat eder.
    b. Yolu bilen misafirler kendisi gelir.(--)
    c. Gelenlerin ziyaret maksadı ve kiminle görüşeceği kayıt altına alınır.

d. Gelenlere giriş kartı verilir ve ziyaret süresince görünür şekilde taşımaları istenir.
e. Gişir kartını taşımayanlar uyarılır.
f. Kapımız herkese açıktır isteyen girer.(--)
g. 7/24 güvenlik görevlisi/görevlileri çevresel ve giriş güvenliğini sağlamaktadır.

Bu sorunun Clips de geliştirilmiş kuralı ve açıklamaları:

Clips:

```
(deftemplate Soru1
  (slot f1)
  (slot f2)
  (slot f3)
  (slot f4)
  (slot f5)
  (slot f6)
  (slot f7))

(defrule rule10
  (declare (salience 100))
  (Soru1 (f1 "evet") (f2 "hayir") (f3 "evet") (f4 "evet") (f5 "evet") (f6 "hayir") (f7 "evet"))
  =>
  (printout t "tamam Misafir veya müşterilerin karşılanmasında herhangi bir eksikliğiniz yok. "  crlf))

(defrule rule1a
  (declare (salience 100))
  (Soru1 (f1 "hayir") (f2 ?o) (f3 ?m) (f4 ?k) (f5 ?a) (f6 ?p) (f7 ?c))
  =>
```

```
  (printout t "eksik Girişte güvenlik görevlisi veya resepsiyon görevlisi dışardan gelen kişileri karşılaması ve gideceyi yere kadar refakat etmesi gerekir"  crlf))

(defrule rule1b
  (declare (salience 100))
  (Soru1 (f1 ?n) (f2 ?o) (f3 "hayir") (f4 ?k) (f5 ?a) (f6 ?p) (f7 ?c))
  =>
  (printout t "eksik Gelenlerin ziyaret maksadı ve kiminle görüşeceği kayıt altına alması gerekir"  crlf))

(defrule rule1c
  (declare (salience 100))
  (Soru1 (f1 ?n) (f2 ?o) (f3 ?m) (f4 "hayir") (f5 ?a) (f6 ?p) (f7 ?c))
  =>
  (printout t "eksik Gelenlere giriş kartı verilmesi ve ziyaret süresince görünür şekilde taşımaları istenmesi gerekir."  crlf))

(defrule rule1d
  (declare (salience 100))
  (Soru1 (f1 ?n) (f2 ?o) (f3 ?m) (f4 ?k) (f5 "hayir") (f6 ?p) (f7 ?c))
  =>
  (printout t "eksik Giriş kartını taşımayanların uyarılması gerekir"  crlf))

(defrule rule1e
  (declare (salience 100))
  (Soru1 (f1 ?n) (f2 ?o) (f3 ?m) (f4 ?k) (f5 ?a) (f6 ?p) (f7 "hayir"))
  =>
  (printout t "eksik 7/24 güvenlik görevlisinin/görevlilerinin çevresel ve giriş güvenliğini sağlamasi gerekmektedir."  crlf))

(defrule rule1a2
  (declare (salience 100))
```

```
  (Soru1 (f1 "evet") (f2 ?o) (f3 ?m) (f4 ?k) (f5 ?a) (f6 ?p) (f7 ?c))
  =>
  (printout t "yapildi: Girişte güvenlik görevlisi veya resepsiyon görevlisi dışarıdan gelen kişileri karşılar ve gideceyi yere kadar refakat eder"  crlf))

(defrule rule1b2
  (declare (salience 100))
  (Soru1 (f1 ?n) (f2 ?o) (f3 "evet") (f4 ?k) (f5 ?a) (f6 ?p) (f7 ?c))
  =>
  (printout t "yapildi: Gelenlerin ziyaret maksadi ve kiminle görüşeceği kayıt altına alınır"  crlf))

(defrule rule1c2
  (declare (salience 100))
  (Soru1 (f1 ?n) (f2 ?o) (f3 ?m) (f4 "evet") (f5 ?a) (f6 ?p) (f7 ?c))
  =>
  (printout t "yapildi: Gelenlere giriş kartı verilmesi ve ziyaret süresince görünür şekilde taşımaları istenir."  crlf))

(defrule rule1d2
  (declare (salience 100))
  (Soru1 (f1 ?n) (f2 ?o) (f3 ?m) (f4 ?k) (f5 "evet") (f6 ?p) (f7 ?c))
  =>
  (printout t "yapildi: Giriş kartını taşımayanlar uyarılır."  crlf))

(defrule rule1e
  (declare (salience 100))
  (Soru1 (f1 ?n) (f2 ?o) (f3 ?m) (f4 ?k) (f5 ?a) (f6 ?p) (f7 "evet"))
  =>
  (printout t "yapildi: 7/24 güvenlik görevlisi/görevlileri çevresel ve giriş güvenliğini sağlamaktadır."  crlf))
```

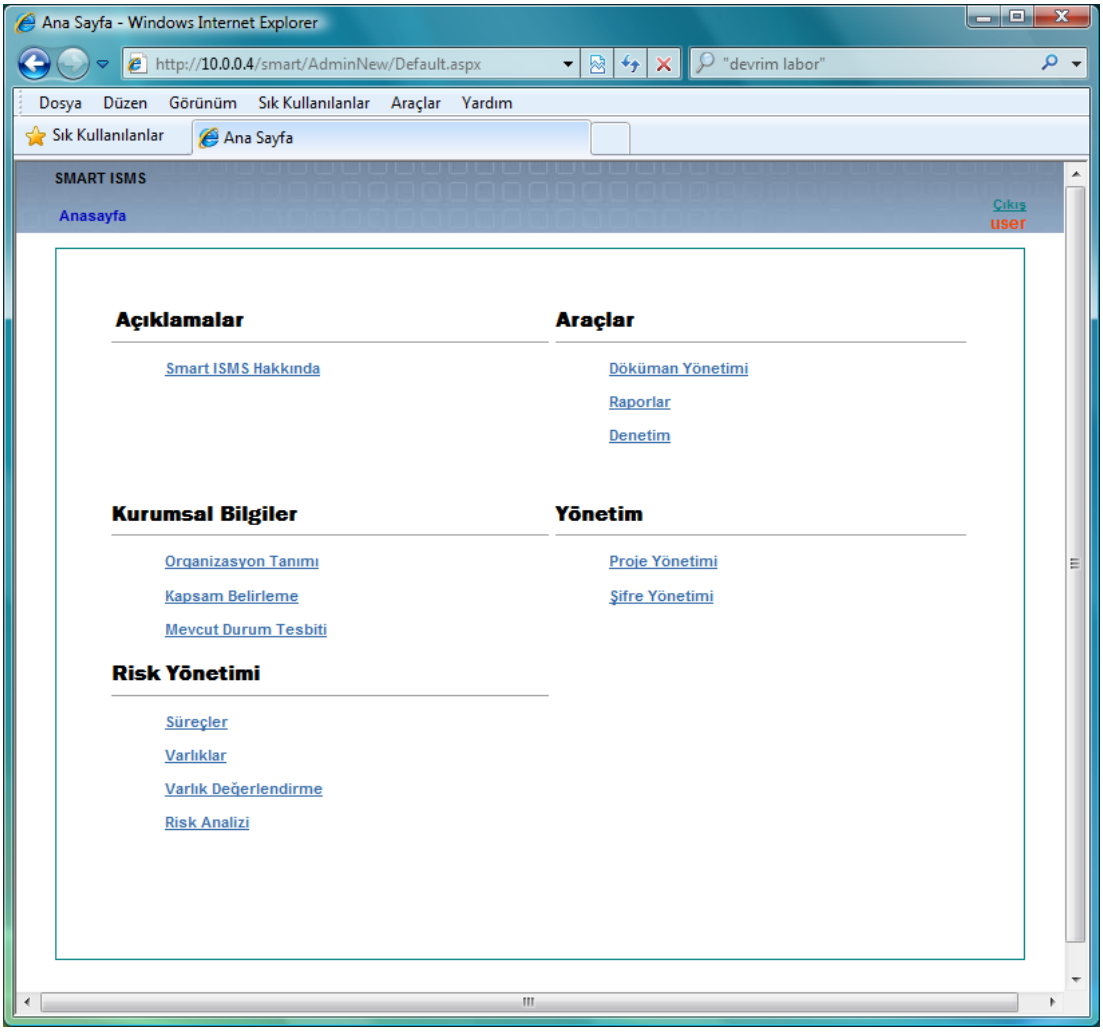
```
(defrule rule1x1
  (declare (salience 200))
  (Soru1 (f1 ?n) (f2 "evet") (f3 ?m) (f4 ?k) (f5 ?a) (f6 ?b) (f7 ?c))
   =>
  (printout t "yanlis: Misafirler yolu bilseler dahi refakatçi ile gelebilir"  crlf))

(defrule rule1x2
  (declare (salience 200))
  (Soru1 (f1 ?n) (f2 ?b) (f3 ?m) (f4 ?k) (f5 ?a) (f6 "evet") (f7 ?c))
   =>
  (printout t "yanlis: Kapimiz herkese açık olsa bile kuruluşunuza gelenle refakatçi
ile birlikte kuruluş içerisinde gezilebilir."  crlf))
```

Programda verilen deffact örneği:

```
(deffacts deneme (Soru1 (f1 "hayir" ) (f2 "evet" ) (f3 "hayir" )  (f4 "hayir") (f5
"hayir" )  (f6 "evet") (f7 "hayir" ))))
```

Çıkarım mekanizması kullanıcının sorulara vermiş olduğu cevapları üretim kuralları aracılığı ile muhakeme ederek eksiklikleri ve yapılanları kullanıcıya geri bildirir. Kullanıcı isterse eksikliklerle birlikte veya eksiklikleri gidererek raporları oluşturabilir. Burada eksikliklerin giderilmesinin kurum veya kuruluşa parasal maliyet getireceği unutulmamalıdır. Burada verilecek karar ISO 27001 standardına göre kuruluşun yönetimi tarafından verilmelidir. Bu maliyeti yıllara sari olarak karşılayacak bir plan yapması önerilmektedir. Smart ISMS tarafından üretilen raporlar Microsoft Office ortamına aktarılabilmekte ve istendiğinde rapor üzerinde değişiklik yapılabilmektedir.

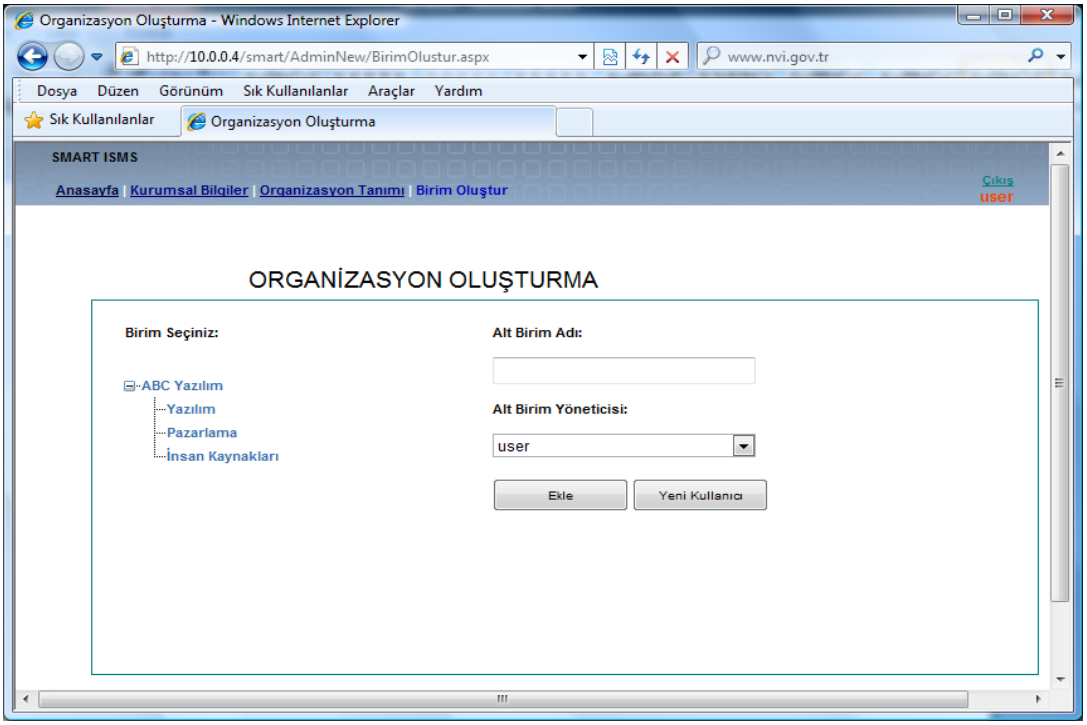
Smart ISMS yazılımının tüm modüllerin ekran görüntüleri ve çıktıları çok uzun olacağından, sadece önemli modüllerin ekran görüntüleri kullanıcı arayüzü ekran görüntüleri Şekil 3.9 ile Şekil 3.19 arasında gösterilmiştir.



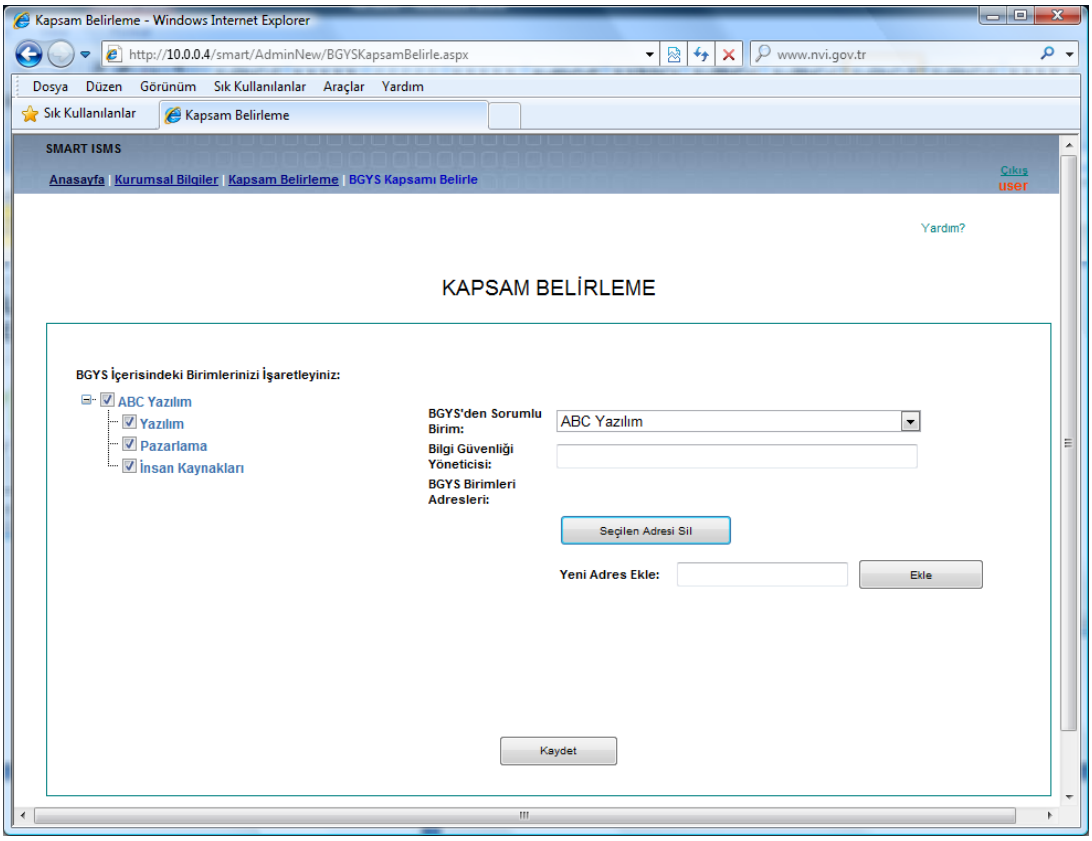
Şekil 3.9. Smart ISMS ana penceresi

Smart ISMS in ana penceresinden tüm modüllere ulaşılabilmektedir.

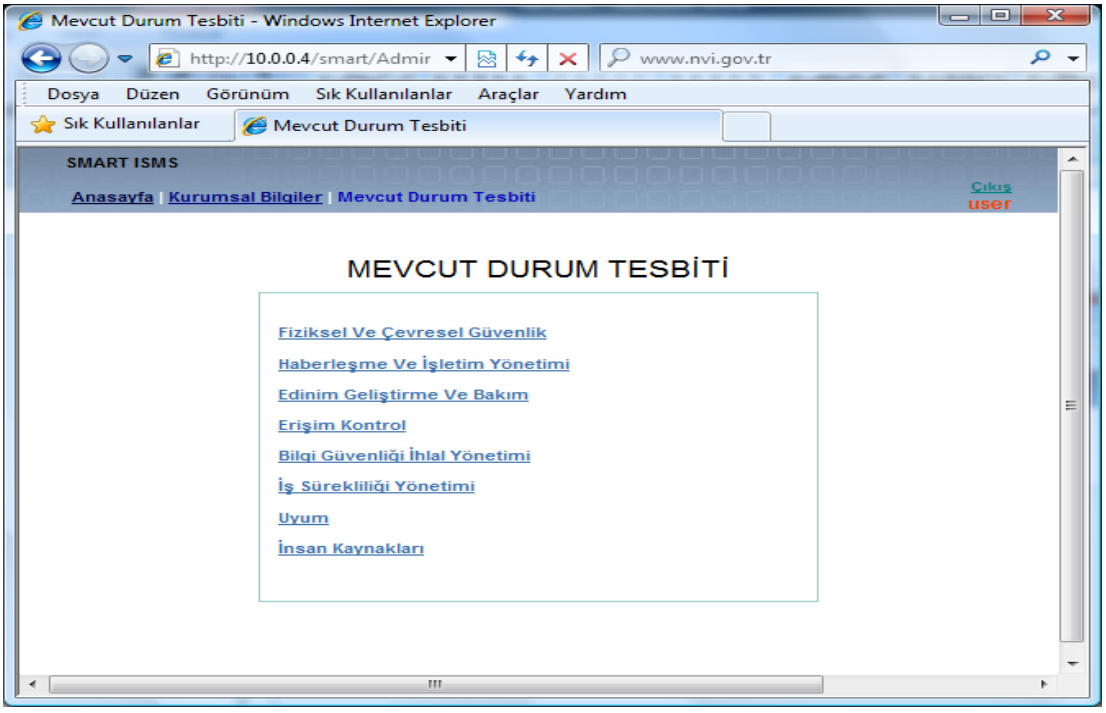
Şekil 3.10. Açıklamalar modülü



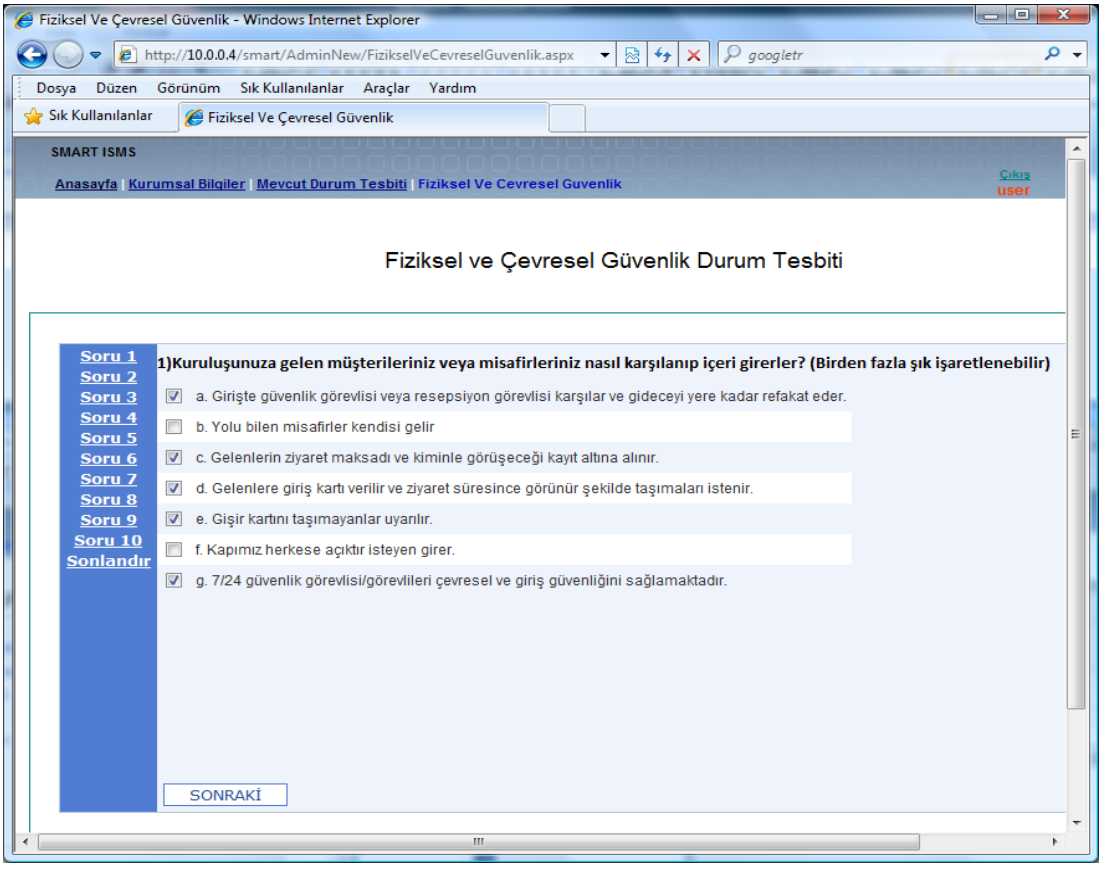
Şekil 3.11. Organizasyon oluşturma penceresi



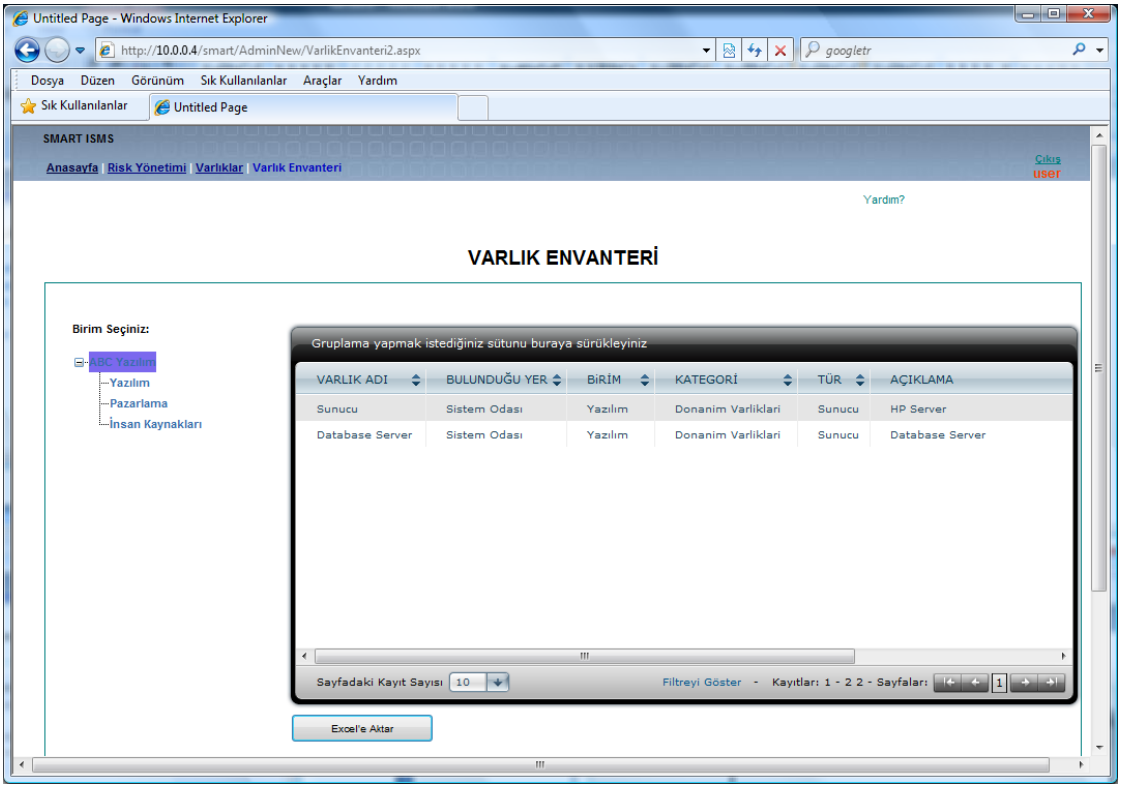
Şekil 3.12. Kapsam belirleme penceresi



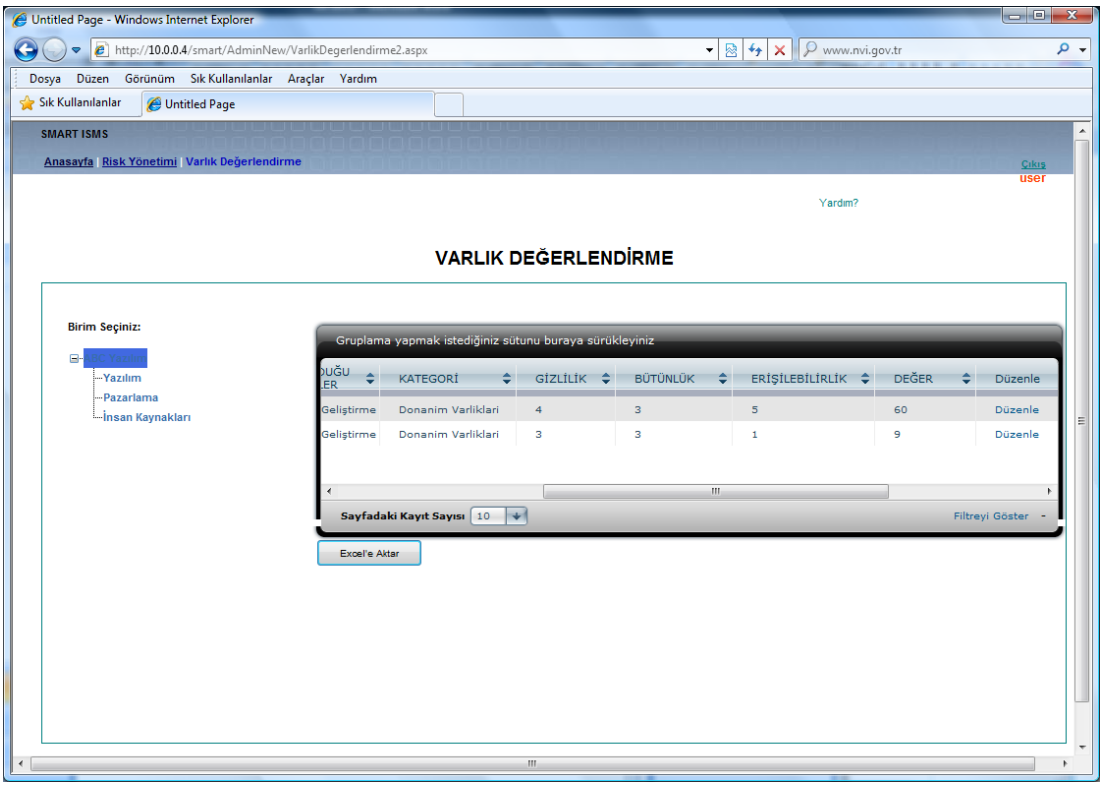
Şekil 3.13. Mevcut durum tespiti penceresi ana menü



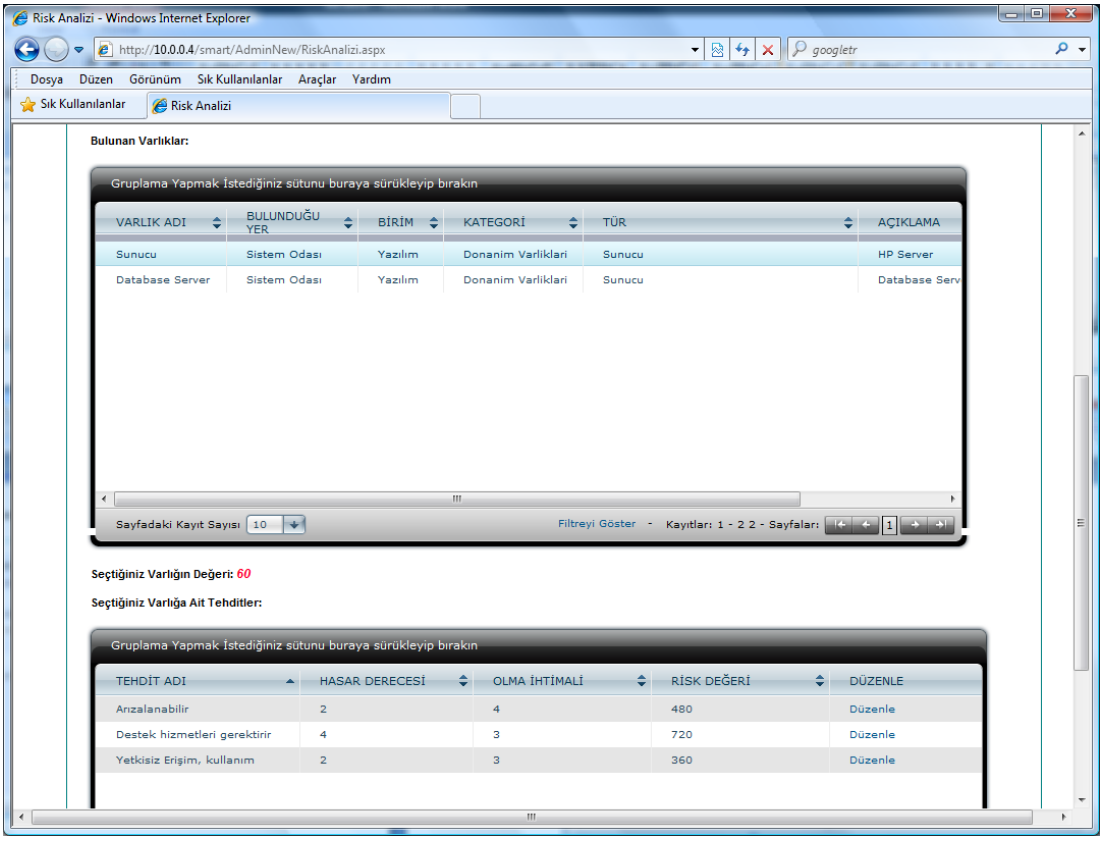
Şekil 3.14. Mevcut durum tespiti penceresi



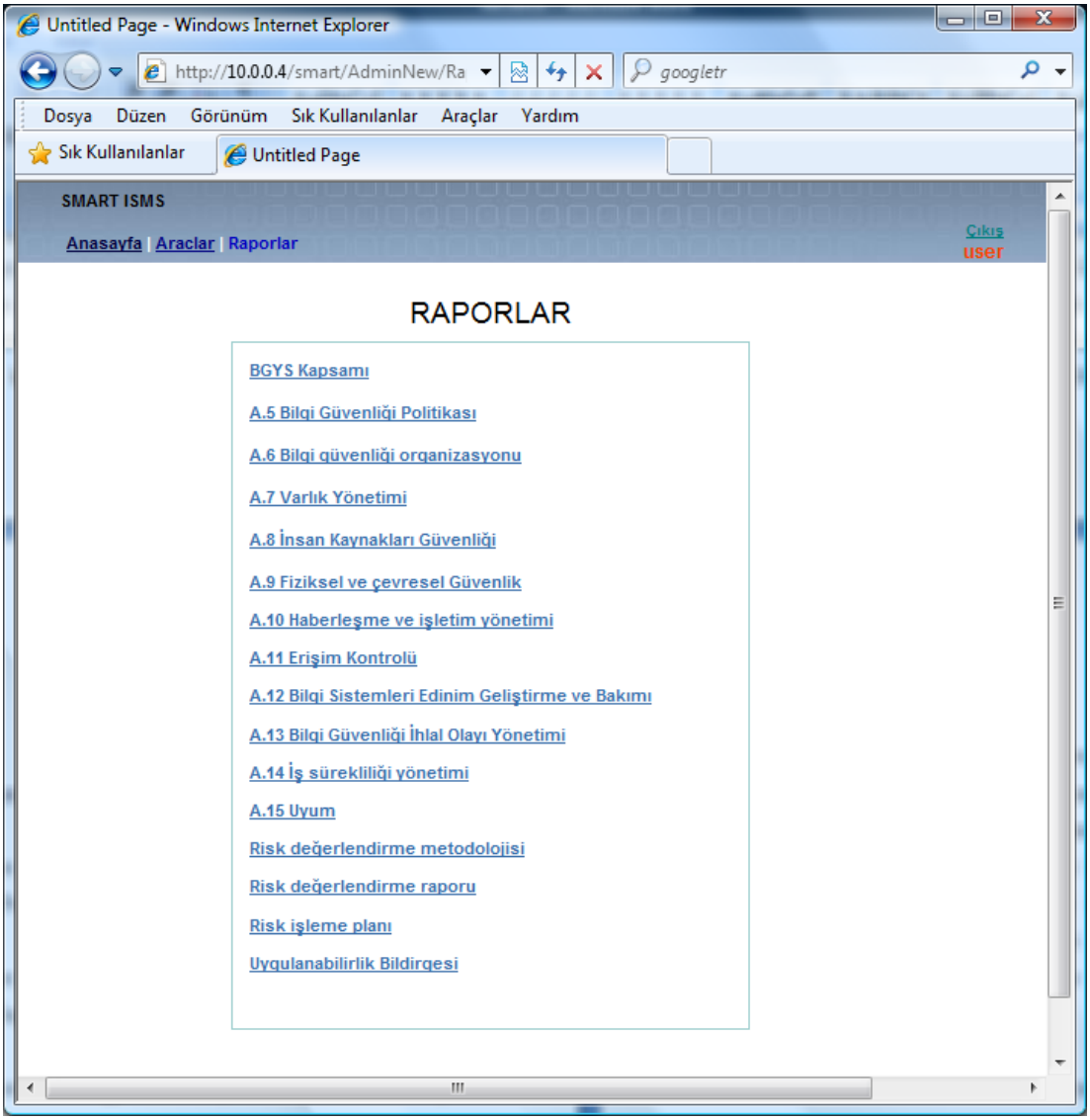
Şekil 3.15. Varlık envanteri penceresi



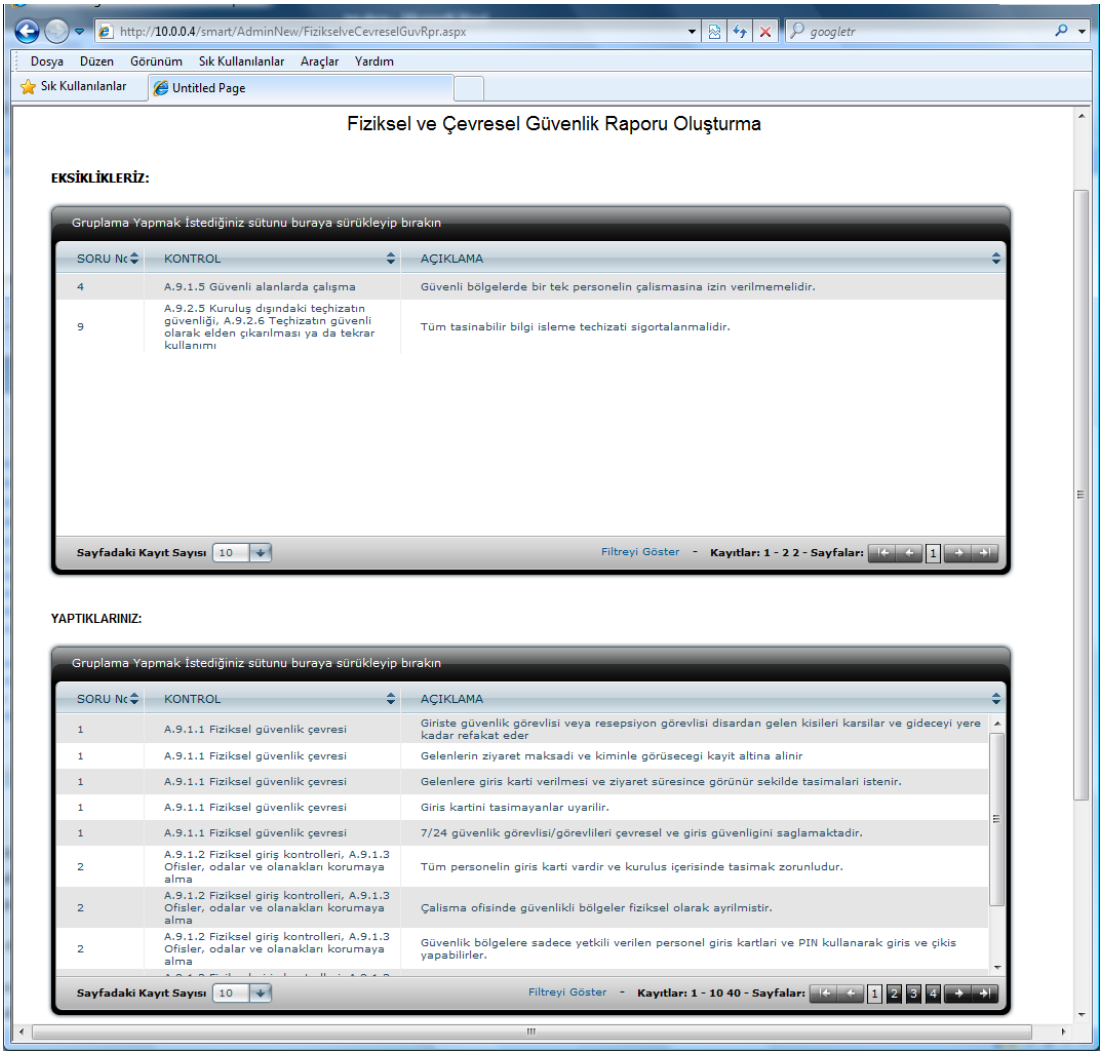
Şekil 3.16. Varlık değerlendirme penceresi



Şekil 3.17. Risk analizi penceresi



Şekil 3.18. Raporlar menüsü



Şekil 3.19. Fiziksel ve çevresel güvenlik raporu oluşturma penceresi

5. BULGULAR VE YORUM

5.1. Denetim Esasları

ISO 27001 Bilgi Güvenliği Yönetim Sistemi belgelendirme denetimi iki aşamada yapılmaktadır;

- Birinci aşama dokümantasyon denetimi
- İkinci aşama uygulama ve kanıt denetimidir

Birinci aşama denetimin bir hedefi, belgelendirme kuruluşunun, kuruluşun güvenlik politika ve hedefleri kapsamındaki BGYS'nin anlaşılmasını ve risk yönetim yaklaşımını ortaya konulmasını sağlamaktır. Bu denetim aşaması, aynı zamanda ikinci aşama denetimin planlanmasına odaklanılmayı sağlar ve kuruluşun denetim için ne kadar hazır olduğunun da kontrol edilmesi için de bir fırsat sunar.

Birinci aşama denetimi, ikinci aşama denetimin başlamasından önce tamamlanması gereken bir belge gözden geçirme sürecini içerir. Denetçinin, kuruluşun en azından risk belirleme raporu, riski ortadan kaldırma planı ve Uygulanabilirlik Belgesi ile BGYS'nin diğer önemli belgelerini kapsayan BGYS'nin tasarımı ve gerçekleştirmesiyle ilgili belgeleri gözden geçirmesi gerekir. Birinci aşama denetimin sonuçlarını içeren bir yazılı rapor hazırlanmalıdır. Bu raporda verilen bulgular, İkinci aşama denetime geçilmesi için doğru zamanın gelip gelmediğine karar verilmesi için kullanılır. Bir sonraki denetim aşamasına geçerken, belgelendirme kuruluşu, hangi ilave belgelerin, ilave bilgilerin ve kayıtların ikinci aşama denetim sırasında ayrıntılı inceleme için gerekli olabileceği hususunda kuruluşu bilgilendirir [39].

Birinci aşama denetimde aşağıdakiler kontrol edilir;

- BGYS kapsamı,
- BGYS'yi destekleyici prosedürler ve kontroller,

  - A.5 Bilgi Güvenliği 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 işletim 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
- Risk değerlendirme metodolojisinin bir tanımı,
- Risk değerlendirme raporu,
- Risk işleme planı,
- Kuruluş tarafından, bilgi güvenliği süreçlerinin etkin planlanmasını, işletilmesini ve kontrolünü sağlamak için ihtiyaç duyulan belgelenmiş süreçler ve kontrollerin etkinliğinin nasıl ölçüleceğini tanımlama,
- Uygulanabilirlik Bildirgesi.

2'nci aşama denetim şu hususları içerir:

a) Kuruluşun kendi politikalarına, hedeflerine ve prosedürlerine göre hareket ettiğinin teyidi,

b) BGYS'nin ISO 27001 standardında geçen gereksinimlerin tümüne uyduğunun ve BGYS'nin kuruluşun politik hedeflerini elde ettiğinin teyidi.

İkinci aşama denetimi özellikle kuruluşun aşağıdakileri nasıl yerine getirdiğiyle ilgilidir:

c) Risklerle ilgili bilgi güvenliğinin belirlenmesi ve kendi BGYS'nin nihai tasarımı,

- Kuruluşun risk belirleme yaklaşımının tanımlanması
- Risklerin tanımlanması
- Risklerin analiz edilmesi ve değerlendirilmesi
- Risklerin ortadan kaldırılması seçeneklerinin tanımlanması
- Risklerin ortadan kaldırılması için kontrol hedeflerinin ve kontrol tedbirlerinin seçimi
- Bir Uygulanabilirlik Belgesi'nin hazırlanması

d) Bu süreçten elde edilen hedeflerin kontrol edilmesi,

e) Hedefler göz önünde bulundurularak performansın izlenmesi, ölçülmesi, rapor edilmesi ve gözden geçirilmesi. Bu husus, süreçlerin uygulandığının ve en azından ISO 27001'de geçen hususların aşağıdakilerde kullanıldığının kontrolünü de içermelidir:

- BGYS'nin gerçekleştirilmesi ve işletilmesi (ISO 27001 Madde 4.2.2),
- BGYS İç denetimleri (ISO 27001 Madde 6),
- BGYS Yönetiminin gözden geçirilmesi (ISO 27001 Madde 7),
- BGYS İyileştirme (ISO 27001 Madde 8),

f) Güvenlik ve yönetim gözden geçirmeleri. Bu husus, süreçlerin yerinde olduğu ve en azından ISO 27001'de geçen hususların aşağıdakilerde kullanıldığının kontrolünü de içermelidir:

- BGYS'nin izlenmesi ve gözden geçirilmesi (ISO 27001 Madde 4.2.3),
- BGYS iç denetimleri (ISO 27001 Madde 6),
- BGYS'nin yönetiminin gözden geçirilmesi (ISO 27001 Madde 7),

g) Bilgi güvenliği politikası için yönetim sorumluluğu. Bu husus, süreçlerin yerinde olduğu ve en azından ISO 27001'de geçen hususların aşağıdakilerde kullanıldığının kontrolünü de içermelidir:

- BGYS'nin izlenmesi ve gözden geçirilmesi (ISO 27001 Madde 4.2.2),
- Yönetim sorumluluğu (ISO 27001 Madde 5),
- BGYS'nin yönetiminin gözden geçirilmesi (ISO 27001 Madde 6),

h) Aşağıda belirtilenlerle arasındaki denetim bağlantısı (ISO 27001 standardının 4 ila 7'nci maddelerinde belirtilen çeşitli faaliyetler, süreçler ve sonuçlar arasındaki bağlantıların gösterilmesini de içermelidir).

- BGYS'nin kapsamı ve politikası,
- BGYS'nin bilgi güvenliği risk belirlemelerinin sonuçları,
- BGYS ve iş hedefleri,
- Sorumluluklar,
- Programlar,
- BGYS prosedürleri,
- BGYS performans verisi, hedefleri, ölçümleri,
- BGYS'nin güvenlik gözden geçirmeleri.

5.2. Uygulama Sonuçları

Bu tez çalışmasında geliştirilen Smart ISMS küçük ve orta ölçekli iki şirkette kullanılarak test edilmiştir.

Şirket-1 profili :

DST Danışmanlık ve Destek Ltd. Şirketi Ankara konuşlu Bilgi Sistemleri konusunda danışmanlık, kurulum ve destek hizmetleri sağlayan bir şirkettir. Şirkette 8 personel çalışmaktadır.

Kullanıcı-1 profili :

Bu çalışmada bilgi sistemleri konusunda temel seviyede bilgi sahibi lise mezunu bir kullanıcı tarafından Smart ISMS kullanılarak şirket için BGYS çalışması yapılmıştır. Şirketin ana faliyet konusu bilgi sistemleri olduğundan kullanıcı, şirketin çalışan diğer personelinden güvenlik konusunda teknik destek almıştır.

Kullanıcı personel çalışma öncesinde ISO 27001 standardını okuyarak BGYS nin yapısı ve uygulaması hakkında bilgi sahibi olmuştur.

BGYS nin kurulması ve dokümantasyonu Smart ISMS yazılımı kullanılarak gerçekleştirilmiştir. Tüm BGYS araçlarında olduğu gibi doküman haline gelen BGYS belgelerinin uygulanması kuruluşun kendi sorumluluğundadır.

Şirket-2 profili :

OSKO Yapı Ltd. Şirketi Ankara konuşlu Alüminyum imalatı ve inşaat konuşunda faaliyet gösteren bir şirkettir. Şirkette 38 personel çalışmaktadır. Firmanın ISO 9001 belgesi bulunmaktadır. Firmada bilgi sistemleri konusunda uzman personel bulunmamakta firma bilgi sistemleri konusunda dış kaynaklı destek almaktadır.

Kullanıcı-2 profili :

Bu çalışmada firmanın bilgi sistemleri konusunda temel seviyede bilgi sahibi meslek lisesi (muhasebe) mezunu bir kullanıcı tarafından Smart ISMS kullanılarak şirket için BGYS çalışması yapılmıştır. Kullanıcı Firmanın kalite yönetiminde sorumlu kişidir ve ISO 9001 konusunda tecrübelidir.

Kullanıcı personel çalışma öncesinde ISO 27001 standardını okuyarak BGYS nin yapısı ve uygulaması hakkında bilgi sahibi olmuştur.

BGYS nin kurulması ve dokümantasyonu Smart ISMS yazılımı kullanılarak gerçekleştirilmiştir. Tüm BGYS araçlarında olduğu gibi dokümante edilen BGYS nin uygulanması kuruluşun kendi sorumluluğundadır.

Her iki kuruluşun BGYS kurulumu ve dokümantasyonu International Register of Certificated Auditors (IRCA) kayıtlı farklı iki baştetkikçi tarafından incelenmiştir. Gizlilik nedenleriyle firmaların varlık envanterleri, risk değerlendirmeleri (tehditleri ve zafiyetleri) ve dokümantasyonları bu tez çalışmasına konulmamıştır ancak tetkikçilerin denetim raporları sırasıyla EK-11 ve EK-12 de sunulmuştur.

Bu tez çalışmasında geliştirilen Smart ISMS yazılımı ile Callio Secura yazılımı mukayese edilmiştir. Callio Secura yazılımı bir Kanada firması olan Callio Technologies in bir ürünüdür. BGYS konusunda farklı büyüklüklerdeki kuruluşlar ile özellikle kolay kullanımı ve yönetimiyle de KOBİ ler tarafından en çok tercih edilen yazılımdır [17]. Bu nedenle bu tez çalışmasında geliştirilen Smart ISMS yazılımı ile Callio Secura yazılımı mukayese edilmiştir. Mukayese sonuçları EK-13 de sunulmuştur.

Callio Secura ingilizce, fransızca, ispanyolca ve çince dillerinde versiyonları ve dünya çapında 1000 den fazla KOBİ kullanıcısı bulunmaktadır. Callio uzmanları tarafından geliştirilen Callio Secura yazılımı, birçok fonksiyonel kolaylıkları, kullanım kolaylığı sağlayan kullanıcı arayüzü ve esnekliği ile ISO 27001 uyumluluğu ve sertifikasyonu isteyen kullanıcılara kaçınılmaz bir yol gösterici olmuştur.

İkinci versiyonunda çok kullanıcılı Web uygulaması halini alan Callio Secura büyük kuruluşlar için de uygun bir araç halini almıştır. Callio Secura ISO 27001 yanı sıra sorular yüklenerek COBIT, HIPAA ve Sarbanes & Oxley kurmak ve işletmek isteyen kuruluşlar için de kullanılabilen bir araçtır.

Callio Secura nın kapsamlı bilgi güvenliği yönetim sistemi aracı olmasını sağlayan temel özellikler aşağıdadır:

- ISO 27001 uyumluluğunun seviyesinin tespiti
- Kuruluşun önemli bilgi varlıkları envanterinin çıkarılması,
- Gap analizi yapılması
- Bilgi varlıklarına yönelik risklerin azaltılması
- Örnek bilgi güvenliği politikaları (50 den fazla örnek)
- Politika dokümanının yönetilmesi
- Bütçe yönetimi
- Dokümanların onaylanmasının yönetimi
- Standartların ithal edilmesi
- Oluşturulan BGYS nin ISO 27002 ye uygunluğunun belirlenmesi
- ISO 27001 standardının kontrollerinin dokümante edilmesi

5.3. Sonuçların yorumlanması

Geliştirilen Smart ISMS yazılımı iki farklı kuruluşta, farklı eğitim seviyesinde kişiler tarafından uygulanmış ve farklı iki denetçi tarafından denetlenmiştir. Denetim sonuçları irdelendiğinde her iki denetçi de dokümantasyon üzerinde belgelendirmeye engel teşkil edecek büyük eksiklikler bulmamıştır.

Literatürde risk yönetimi konusunda birçok uzman sistem uygulaması bulunmakta iken bu çalışmada risk yönetimi ve dokümantasyonun hazırlanmasında uzman sistem uygulaması yapılmıştır. Risk yönetimi ISO 27005 standardına uygun bir risk yönetimi metodu seçilerek Smart ISMS yazılımda kullanılmıştır.

Smart ISMS'i diğer benzer uygulamalardan farklı kılan tarafı ISO 27001 belgelendirmesi için gerekli olan tüm dokümantasyonun yazılım tarafından hazırlanabilmesidir.

Uygulama görsel özellikleri fazla olması ve kullanım kolaylığı sağlaması hedeflenerek, kullanıcıların fare yardıımıyla kolaylıkla kullanabileceği bir uygulama olmasına özen gösterilmiştir.

Bu tez çalışmasında geliştirilen yazılımın uygulamasının yapıldığı firmaların kullanıcıları ile bir kamu kurumunda Smart ISMS Programının kullanımına ilişkin bir kullanıcı anketi yapılmıştır. Kullanıcıların Smart ISMS yazılımının kullanımına ilişkin görüşlerini belirlemek için 5'li Likert tipi bir anket uygulanmıştır. Ölçekledirmede bireyler, her bir maddeyle ilgili yanıtlarını, standart bir anahtar çerçevesinde belirtmişlerdir. Buna göre kişilerin programa karşı görüşlerini ifade eden cümleye ne düzeyde katıldıkları, tümüyle katılma veya hiç katılmama arasında, tercihen beşli bir seçeneğe göre cevap alınarak belirlenmiştir. Her maddeye verilecek cevap kodları 1 ile 5 arasında değişmektedir. Buna göre en olumlu madde 5, en olumsuz madde de 1 olarak alınmıştır. Ölçeklerde yer alan aralıklar eşit olarak (4/5) belirlenmiştir. Seçenekler sıralı biçimde sıralı sayısal değerlerle puanlandırılmıştır (1, 2, 3, 4, 5).

Çizelge 5.1. Smart ISMS Kullanıcı anket seçeneklerine ait sınırlar

Seçenek		**Sınırı**
Çok Kötü	(1)	1,00 – 1,80
Kötü	(2)	1,81 – 2,60
Kısmen İyi	(3)	2,61 – 3,40
İyi	(4)	3,41 – 4,20
Çok İyi	(5)	4,21 – 5,00

Toplanan anket sonuçları SPSS 11.0 (Statistical Packet for The Social Science) paket programından yararlanılmıştır. Denek kullanıcıların programın kullanım kolaylığı görüşlerinin belirlenmesinde aritmetik ortalama ($\bar{x}$) ve standart sapma (*ss*) kullanılmıştır.

EK-14 de Smart ISMS Programının kullanımına ilişkin kullanıcı anketi soruları, EK-15 de Smart ISMS Programının kullanımına ilişkin kullanıcı anketi sunulan sonuçları görülmektedir. Anket sonuçlarına göre Smart ISMS temel bilgisayar kullanım bilgisine sahip kişiler tarafından kolaylıkla kullanılabilen ve bir yazılım olduğu görülmektedir.

6. SONUÇ VE ÖNERİLER

Uzman Sistem temelli bilgi güvenliği yönetim sistemi Smart ISMS, kurum ve kuruluşların, özellikle de ekonominin temel direkleri olarak nitelendirilen KOBİ lerin nitelikli eleman istihdamı ya da yüksek maliyetli danışmanlık hizmeti almaksızın, temel bilişim teknolojisi bilgisiyle, kurumsal bilgi güvenlik yönetim sisteminin ISO 27001 standardına uygun olarak kurulması, işletilmesi ve sürdürülmesine olanak sağlamaktadır.

Bu çalışmada sunulan çözüm sayesinde kurum, kuruluş, KOBİ yöneticisi veya çalışanı, organizasyonu için ISO 27001'e uygun kurumsal bilgi güvenliği yönetim sisteminin oluşturulmasını uzman sistem yardımıyla kolayca gerçekleştirebilecek ve sürekliliğini sağlayabilecektir.

Smart ISMS yazılımı yardımıyla organizasyonların iş ve üretim süreçlerine uygun olarak kurumsal bilgi güvenlik yönetim sistemi gereksinimleri bir uzman sistem yardımıyla belirlenecek, firma yöneticileri bu gereksinimlerin bir kısmını kendileri, bir kısmını da gerekli önlemlerin tedariki yapılarak yerine getirilebilecektir. Bu da kurum, kuruluş ve özellikle küçük işletmelere büyük ekonomik kazançlar sağlayacaktır.

Tez çalışmasında geliştirilen uzman sistem tabanlı bilgi güvenliği yönetim sistemi Smart ISMS yazılımı, ülkemizde bilgi güvenliği konusunda geliştirilen ilk uzman sistem tabanlı yazılımdır.

Uygulama sonunda kullanıcılara uygulanan anket sonuçlarına göre Smart ISMS yazılımının temel bilişim teknolojileri bilgisi ile kolaylıkla kullanılabildiği kanıtlanmıştır.

Dünya da yaygın olarak kullanılan Callio aracı ile yapılan karşılaştırma sonucunda her ikisininde de risk analizinin yapabildiği ancak Smart ISMS in dokümantasyon hazırlamada daha etkin, güçlü ve kullanışlı bir araç olduğu ortaya konmuştur.

Müteakip çalışmalarda kuruluşun tüm bilişim sistemini denetleyen, bölümler halinde çalışmalar yapılabilir. Diğer güvenlik standartlarına uygun değişiklikler yapılarak ISO 27001 den farklı standartlarla da çalışması sağlanabilir.

KAYNAKLAR

1. Aktaş, A. Z., "Structured Analysis & Design of Information Systems", ***Prentice-Hall International Editions***, New Jersey, 1-2 (1987).

2. Computer Security Institute, "14th Annual CSI Computer Crime and Security Survey", ***Executive Summary, New York,*** 6-10 (2009).

3. UK Dept for Business Enterprise & Ragulatory Reform, "2008 Information Security Breaches Survey" ***BERR Technical Report 2008, London,*** 2-3 (2009).

4. USA Congress, "Serbanes-Oxley Act of 2002", ***H.R.3763***, ***Washington,*** 1-65 (2002).

5. USA Congress, "Gramm-Leach-Bliley Act" ***GLBA P.L. 106-102***, ***Washington,*** 1-145 (1999).

6. USA Congress, "Health Insurance Portability and Accountability Act of 1996", ***HIPAA P.L. 104-191***, ***Washington,*** 1-64 (1996).

7. PCI Security Standards Council, "Payment Card Industry Data Security Standard", ***PCI DSS V1.2***, ***Wakefield***, 1-32 (2009).

8. Information Systems Audit and Control Association, "Control Objectives for Information and Related Technology", ***ISACA COBIT V4.1***, ***Illinois,*** 1-164 (2009).

9. International Organization for Standardization, "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary", ***ISO/IEC 27000, Cenevre***, 3-19 (2009).

10. Peltier, T.R., "Preparing for ISO 17799", ***Information Systems Security***, 11(6): 21-28 (2003).

11. International Organization for Standardization, "ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems – Requirements", ***ISO/IEC 27001, Cenevre***, 3-30 (2005).

12. Karabacak, B., "Bilgi güvenliği risk analizi (BİGRA) metodu", Yüksek Lisans Tezi, ***Gebze Yüksek Teknoloji Enstitüsü***, Gebze, 129-133 (2003).

13. Bullen, J.I., "Security in Brasil: Modelling and Predicting Outsourcing Decisions", Doktora tezi, ***Campella University***, Minneapolis, 114-121 (2004).

14. Qingxiong, M., Pearson J.M., "ISO 17799: Best Practice in Information Security Management?", ***Communications of the Association for Information Systems ,*** 15(32): 577-591 (2005).

15. Geoff, C., "UCISA Information Security Toolkit 2.0", ***Information Press***, Oxfordshire, 7-13 (2005).

16. Vural, Y., Sağıroğlu, Ş., "Kurumsal Bilgi Güvenliği ve Standartları Üzerine Bir İnceleme", ***Gazi Üniv. Müh. Mim. Fak. Der.,*** 23 (2), 507-522 (2008).

17. Callio, "Callio Secura 17799", ***Secura***, ***Quebec***, 1-2(2010)

18. British Standard Institude, "ISO 27000 Toolkit", ***Standard Direct 27000 Toolkit***, ***London***, 1-3 (2010).

19. Calder, A., Watkins, S., "IT Governance: A Manager's Guide to Data Security and ISO 27001 / ISO 27002", ***Kogan Page***, London, 165-178 (2008)

20. Cpacs LLC, "RiskPAC Overview", ***Cpacs Riskpac, Southbury,*** 1-6 (2008).

21. Alberts, C., Dorofee, A., "Managing Information Security Risks: The OCTAVE Approach", ***Addison-Wesley,*** Boston, 169-190 (2003).

22. Jalote, P., "A Concise Introduction to Software Engineering", ***Springer,*** London, 13-28 (2008).

23. Bıçakçı, M., "Aviyonik yazılım projeleri için uygun yazılım geliştirme metodolojisini belirleme", ***Yazılım Kalitesi ve Yazılım Geliştirme Araçları Sempozyumu,*** İstanbul, 1-6 (2008).

24. Kruchten, P., "The Rational Unified Process An Introduction 3th ed.", ***Addison- Wesley***, Boston, 132-164 (2003).

25. Boogs, W., Boogs M., "Mastering UML with Rational Rose 2002", ***Sybex***, San Francisco, 61-381 (2002).

26. Stephen, T. A., "The Art of Software Architecture: Design Methods and Techniques", ***John Wiley & Sons***, Indianapolis, 113-130 (2003).

27. Winstanley, G., "Artificial Intelligence in Engineering", ***John Wiley & Sons***, Chichester, 245-321 (1991).

28. Turban, E., Frenzel L.E., "Expert Systems and Applied Artificial Intelligence", ***MacMillan***, California, 427-533 (1992).

29. Rich, E., Knight, K., "Artificial Intelligence 2th Ed.", ***McGraw-Hill***, New York, 547-557 (1991).

30. Venkatasubramanian V., "Expert Systems: Principles and Applications", in the ***Proceedings of the International Workshop on Control Systems Frontiers for the Petroleum, Power and Water Production Industries, Kuwait Foundation for Advancement of Science***, Kuwait, 1-27 (2000).

31. Aktaş Z., Çetin, S., "Rebirth of a discipline: Knowledge Engineering", ***Başkent Üniversitesi, Ankara,*** 15-19 (2010).

32. Solvberg, A., Kung, D. C., "Information Systems Engineering:An Introduction", ***Springer***, New York, 221-316 (1993).

33. Lenanun, S., "The Development of Expert System Shell for Slope Stability Analysis", ***Joint Study of Global Sharing of Digital Assets of Scientific and Cultural Information***, 115-123 (2000).

34. Coppin, B., "Artificial Intelligence Illuminated", ***Jones And Bartlett Publishers***, Sudbury, 241-261 (2004).

35. Salim, M.D., "A Method for Evaluating Expert System Shells for Classroom Instruction", ***Journal of Industrial Technology***, Volume 19 (1): 1-11 (2002)

36. Türk Standartları Enstitüsü, TS "13268-1, Bilgi Güvenliği Yönetim Sistemi Belgelendirmesi İçin Gereksinimler ve Hazırlık Klavuzu",***TSE 13268-1***, ***Ankara,*** 1-30 (2007).

37. International Organization for Standardization, "ISO/IEC 27002:2005 Information technology -- Security techniques – Code of practice for Information security management", ***ISO 27002, Cenevre,*** 1-115 (2005).

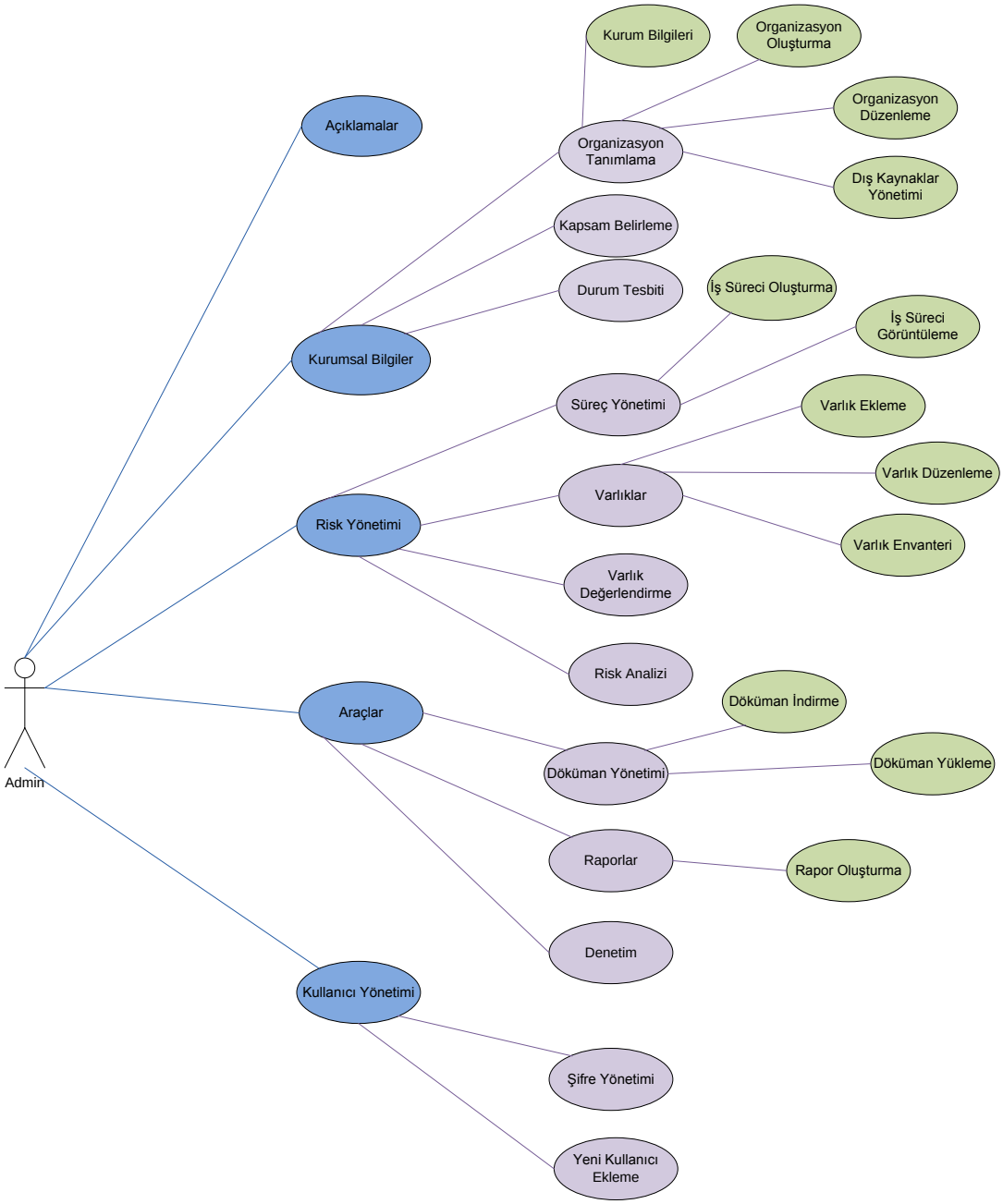
38. International Organization for Standardization, "ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management", ***ISO 27005, Cenevre,*** 1-55 (2008).

39. Türk Standartları Enstitüsü, "TS 13268-4, Bilgi Güvenliği Yönetim Sistemi Denetimlerinin gerçekleştirilmesi ve denetlenmesi", ***TSE TS 13268-4, Ankara,*** 1-94 (2009).

EKLER

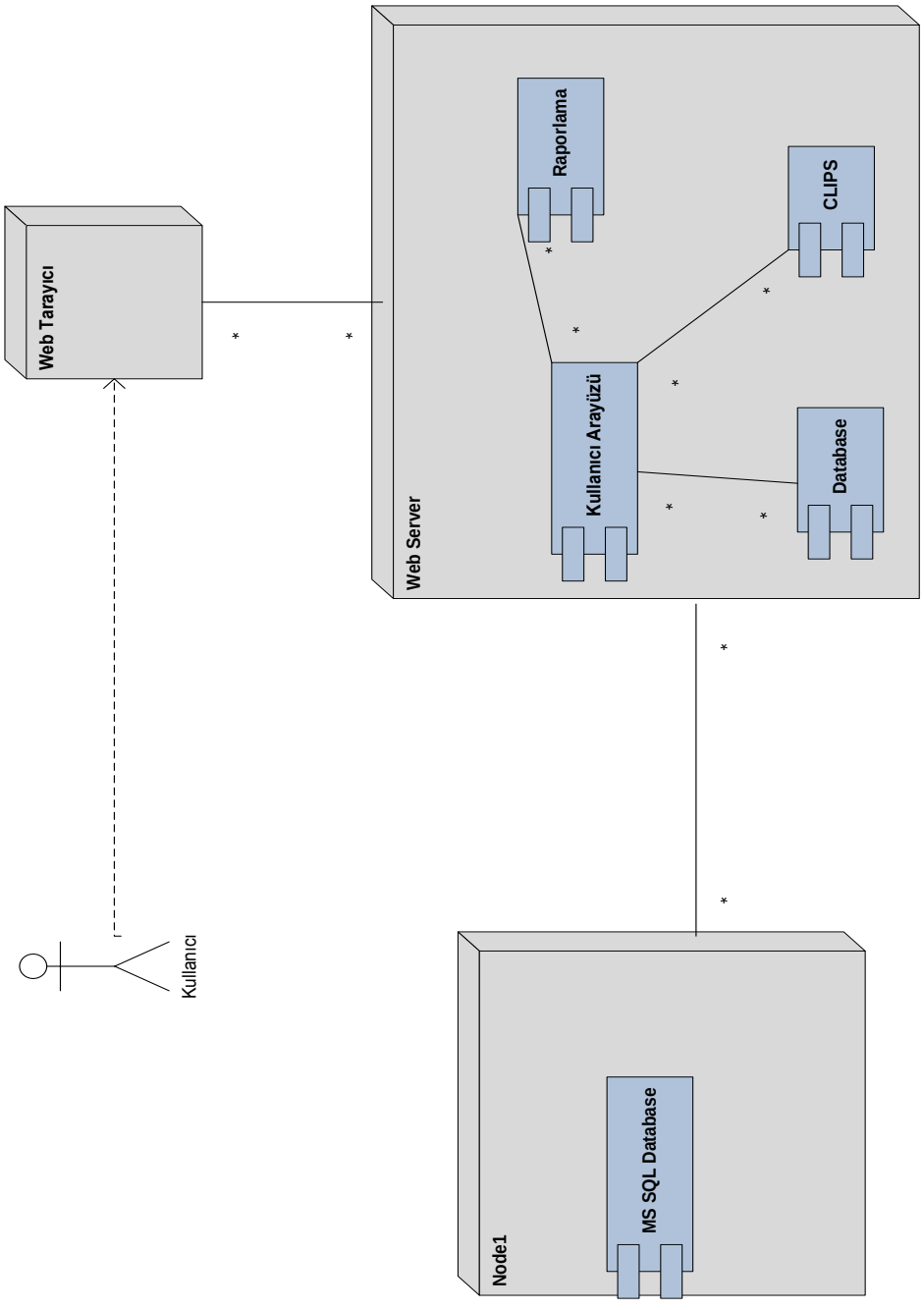
EK-1. Smart ISMS kullanıcı use case diagramı

Programımızın davranışının bir kullanıcı gözüyle incelenmesi Use Case diyagramlarıyla yapılır. Gerçek dünyada insanların kullanacağı bir sistemde bu diyagramlar büyük önem taşırlar.



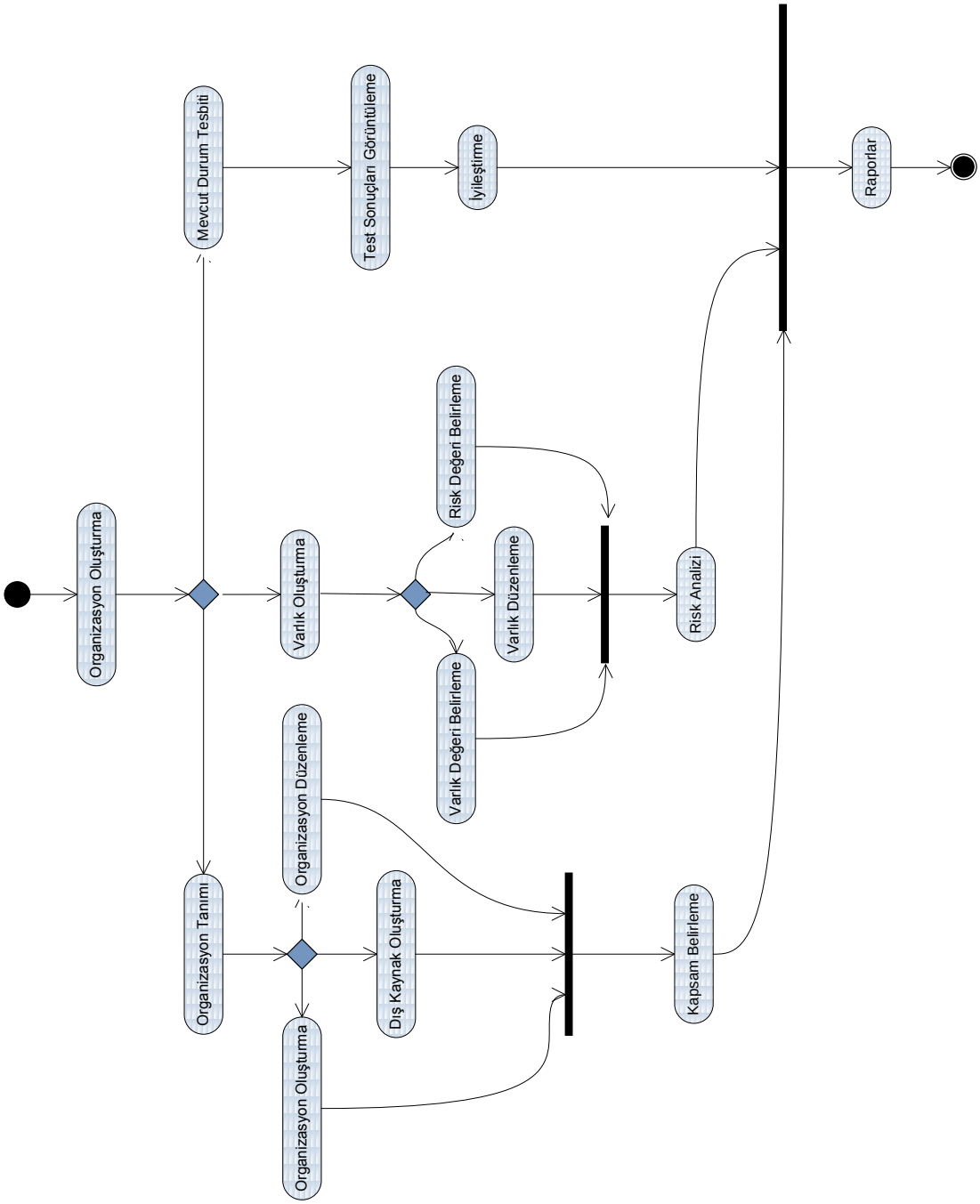
EK-2. Smart ISMS component diagram

Özellikle birden çok geliştiricinin yürüttüğü veya birden çok modülü olan projelerde sistemi component dediğimiz parçalara ayırmak, geliştirmeyi kolaylaştırır. Bu tür modellemeler Component Diyagramlarıyla yapılır.



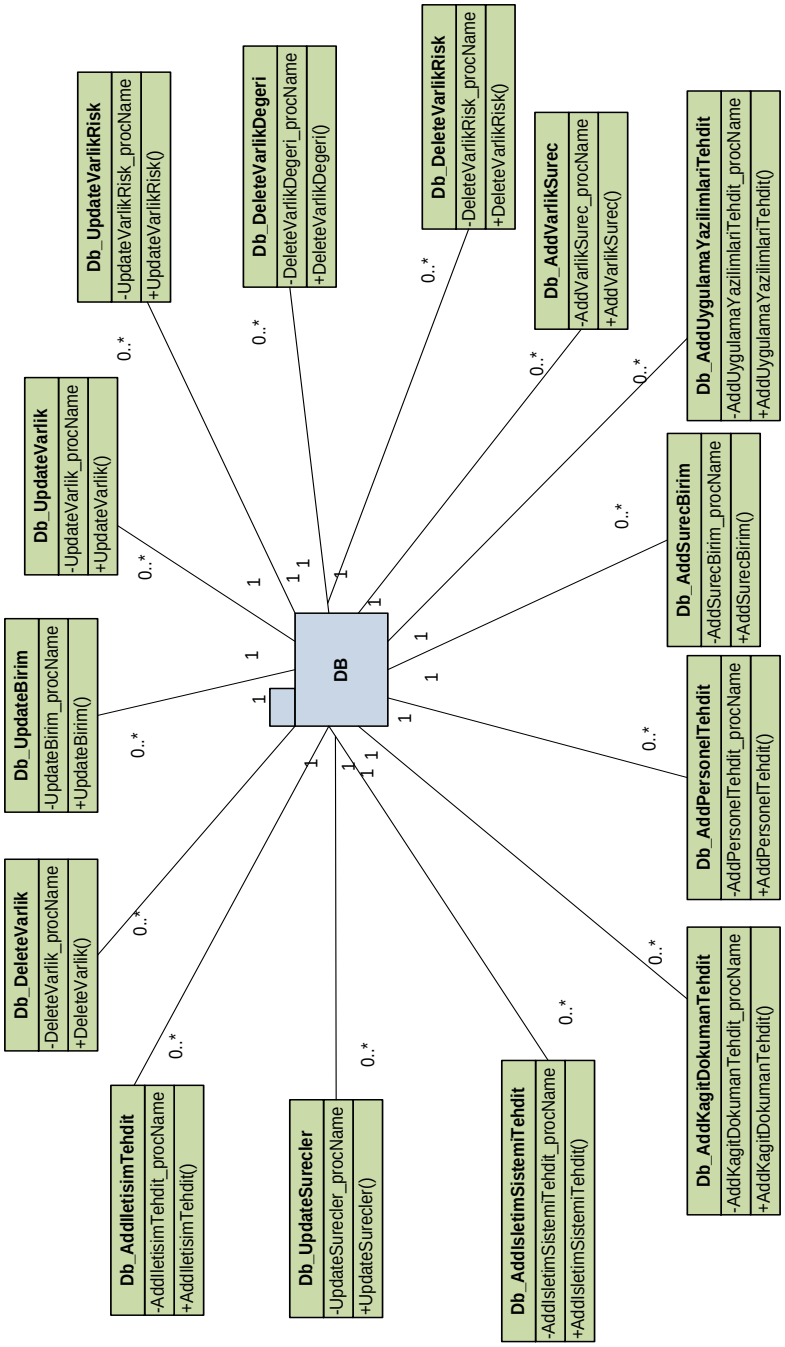
EK-3. Smart ISMS activity diagram

Bir nesnesinin durumu zamanla kullanıcı tarafından ya da nesnenin kendi içsel işlevleri tarafından değişebilir. Bu değişim activity diyagramlarıyla gösterilir.

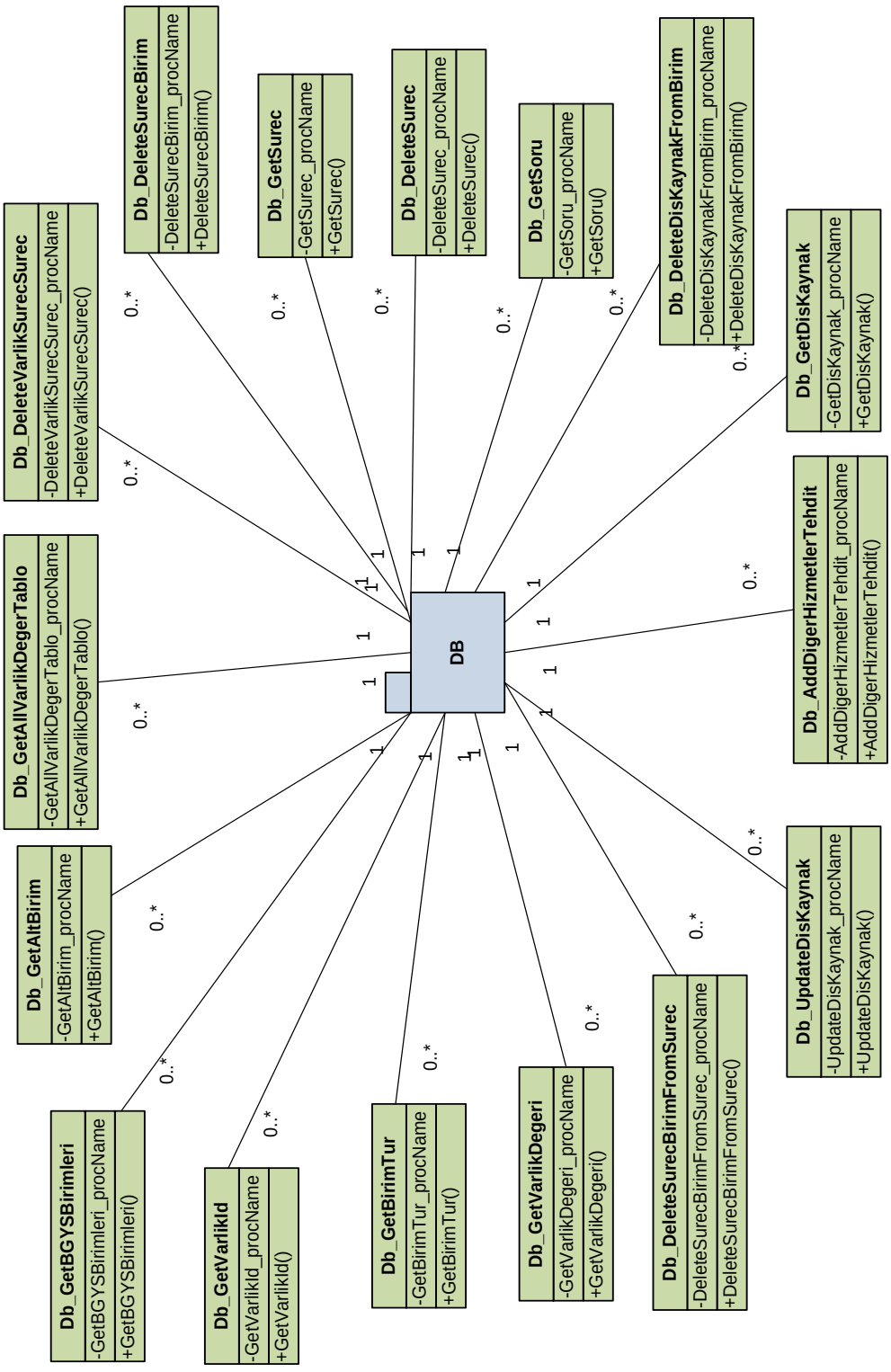


EK-4. Smart ISMS class diagram-I

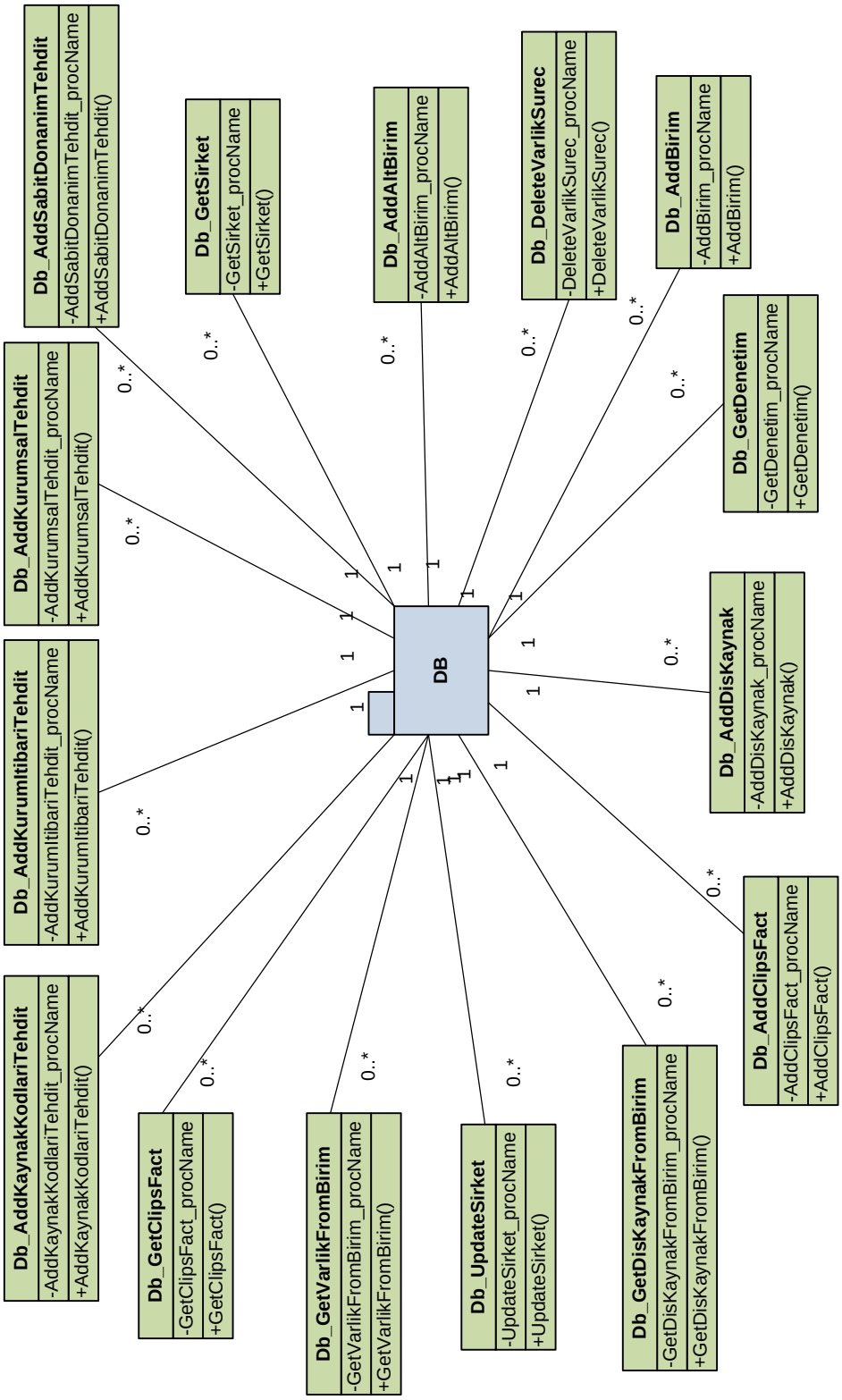
UML modellemesinde class diagramları, sistemin sınıflarını (class), özelliklerini (attribute) ve sınıflar arasındaki ilişkileri gösterir. Smart ISMS yazılımının class diagramları EK-4 ile EK-10 arasında gösterilmiştir.



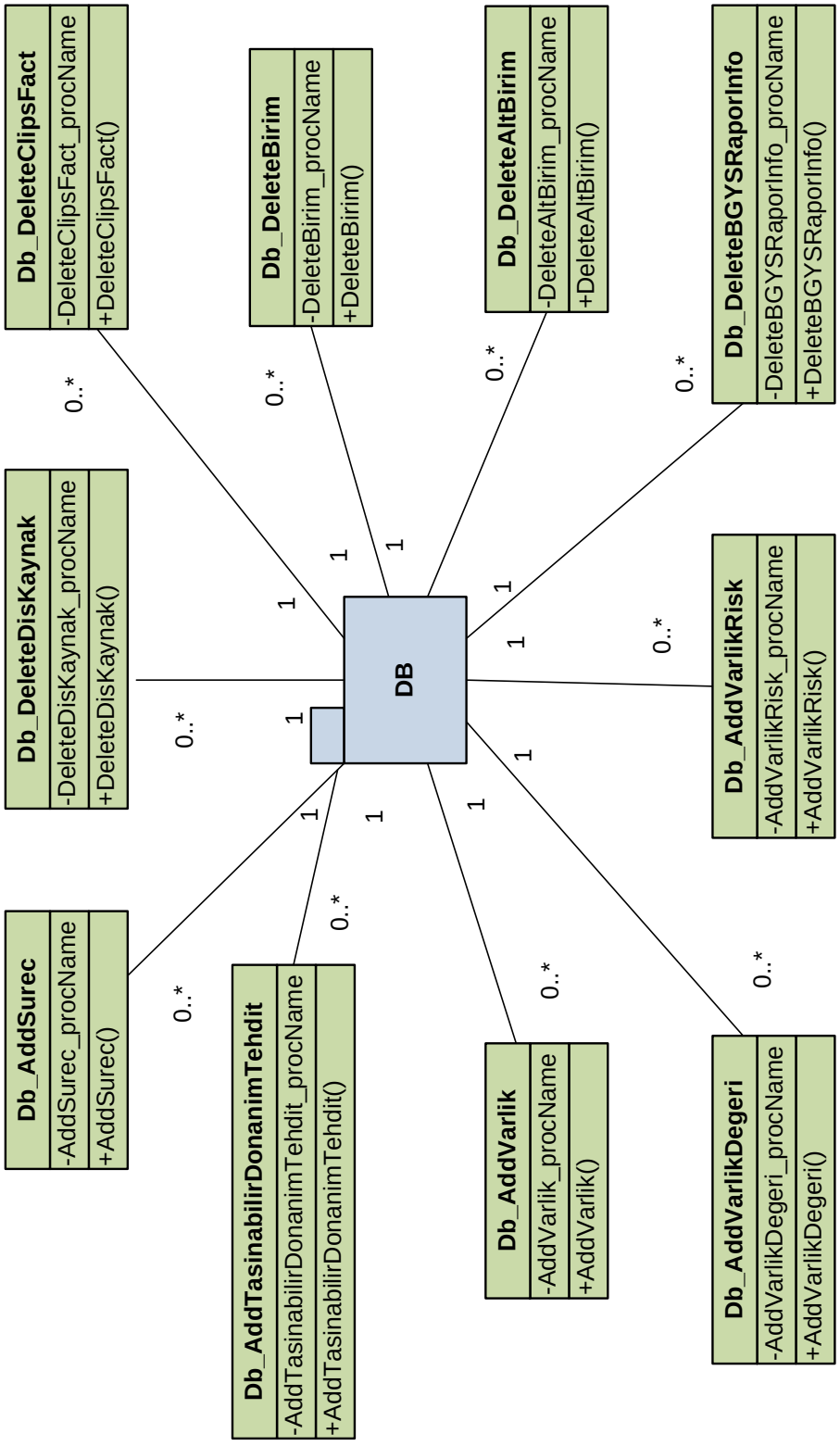
EK-5. Smart ISMS class diagram-II



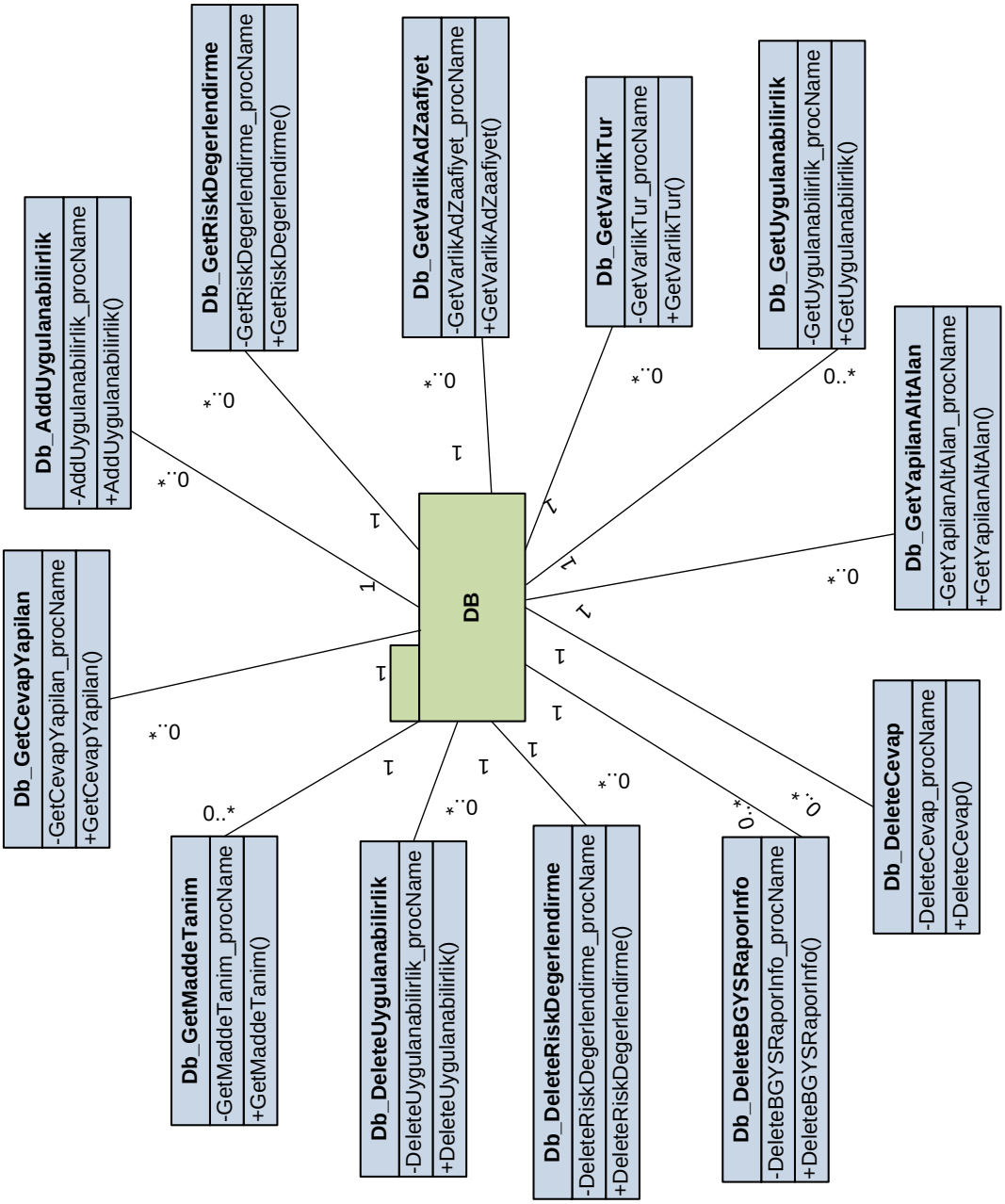
EK-6. Smart ISMS class diagram-III



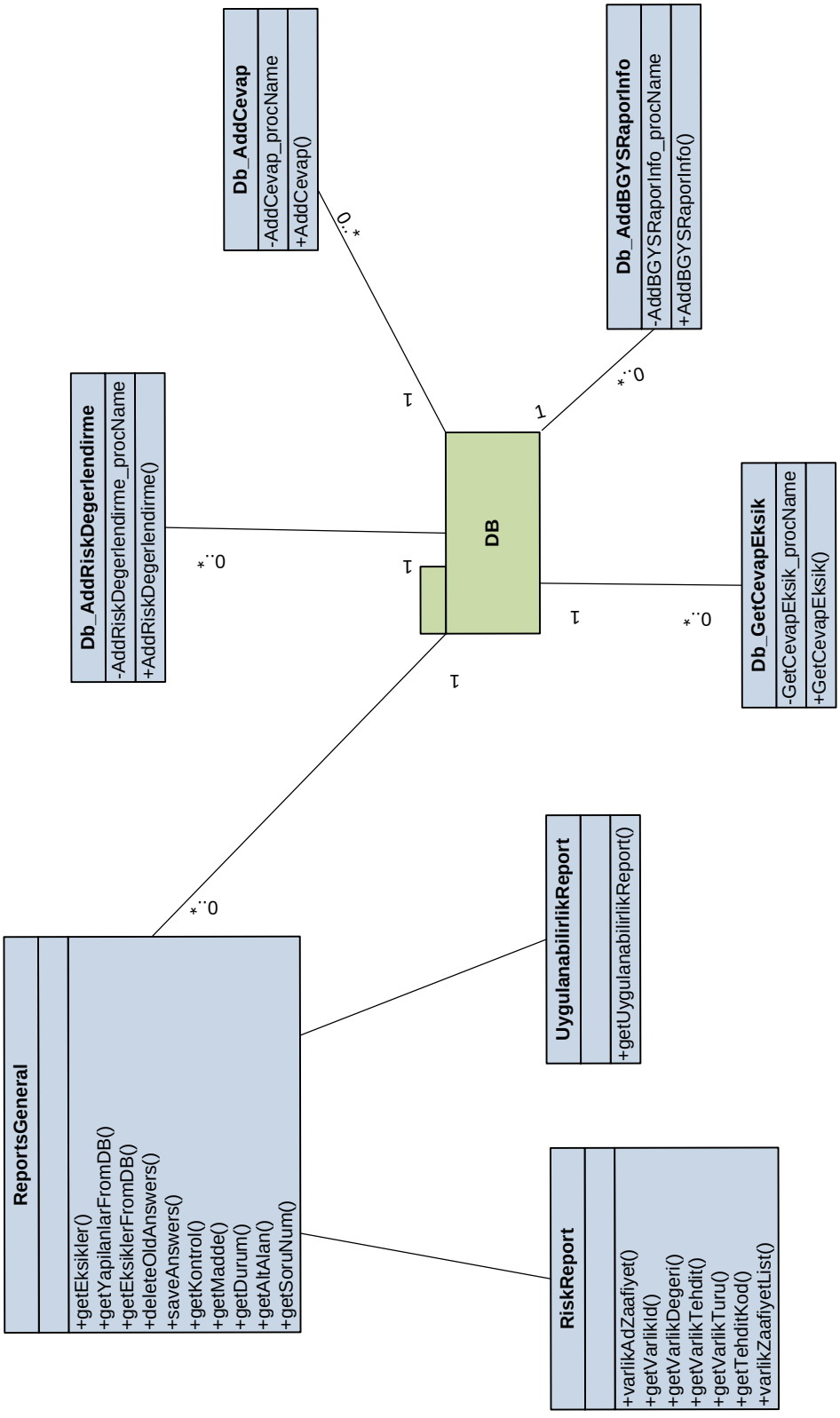
EK-7. Smart ISMS class diagram-IV



EK-8. Raporlar class diagram-I



EK-9. Raporlar class diagram-II



EK-10. Clips class diagram

EK-11. DST Danışmanlık ve Destek Hizmetleri Ltd. Şti. ISO 27001 bilgi güvenliği yönetim sistemi denetim raporu

DST Danışmanlık ve Destek Hizmetleri Ltd.Şti.'nin 4 Mayıs 2009 günü ISO 27001 belgelendirmesi denetimi yapılmıştır. Dokümanlar üzerinde yapılan ön denetim (Birinci Aşama Denetimi) sonucu kuruluşun dokümanlarının incelendiği, majör bir eksiklik bulunmadığı, kuruluşun istediği takdirde uygulama denetimine (İkinci Aşama) girilebilecek seviyede hazır olduğu tespit edilmiştir, Dokümanlarda yazılanların uygulamasının tetkikine müteakip belgelendirilebileceği kanaatine varılmıştır.

Ön denetimde kontrol edilen dokümanlar aşağıdadır;

- BGYS kapsamı,
- BGYS Politikası,
- BGYS'yi destekleyici prosedürler ve kontroller,
    - A.5 Bilgi Güvenliği 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
- Risk değerlendirme metodolojisi,

- Risk değerlendirme raporu,
- Risk işleme planı,
- Kuruluş tarafından, bilgi güvenliği süreçlerinin etkin planlanlanmasını, işletilmesini ve kontrolünü sağlamak için ihtiyaç duyulan dokümante edilmiş prosedürler ve kontrollerin etkinliğinin nasıl ölçüleceğini tanımlama,
- Uygulanabilirlik Bildirgesi.

Burak Dayıoğlu
Baş Tetkikçi (CISA, CISSP)

EK-12. OSKO Yapı Ltd.Şti. ISO 27001 bilgi güvenliği yönetim sistemi denetim raporu

OSKO Yapı Ltd.Şti.'nin 12 Eylül 2009 günü dokümanlar üzerinde yapılan ön denetimi (Birinci Aşama Denetimi) sonucu kuruluşun dokümanlar üzerinden Uygulama denetimine (İkinci Aşama) hazır olduğu, dokümanlarda yazılanların uygulamasının tetkikine müteakip belgelendirilebileceği kanaatine varılmıştır.

Ön denetimde kontrol edilen dokümanlar aşağıdadır;

- BGYS kapsamı,
- BGYS Politikası,
- BGYS'yi destekleyici prosedürler ve kontroller,
    - A.5 Bilgi Güvenliği 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
- Risk değerlendirme metodolojisi,
- Risk değerlendirme raporu,
- Risk işleme planı,
- Kuruluş tarafından, bilgi güvenliği süreçlerinin etkin planlanlanmasını, işletilmesini ve kontrolünü sağlamak için ihtiyaç duyulan dokümante edilmiş prosedürler ve kontrollerin etkinliğinin nasıl ölçüleceğini tanımlama,
- Uygulanabilirlik Bildirgesi.

ISO 27001 Standardının Kontrolleri ile Kuruluşun dokümanları kontrol edilmiş ve kanıtları firmaya sunulmuştur.

A.Gürkan ODABAŞI
Baş Tetkikçi (CISA, CISSP)

EK-13. CALLIO-SMART ISMS mukayese tablosu

Özellikler	Callio	Smart ISMS
Genel Bilgilendirme	Callio Secura nın metodolojisi Proje tanımlama BGYS tanımı Risk Değerlendirmesi Risk iyileştirme Eğitim ve farkındalık Denetime hazırlık Denetim Kontrol ve Sürekli iyileştirme Konularında bilgi verilmektedir.	Var
Politika Hazırlama	Kullanıcının kendisinin hazırlaması istenmekte.	Smart ISMS yardımıyla hazırlanmaktadır.
Kapsam Belirleme	Kullanıcının kendisinin hazırlaması istenmekte.	Smart ISMS yardımıyla hazırlanmaktadır.
Bilgi Güvenliği Organizasyonu	Kullanıcının kendisinin hazırlaması istenmekte.	Smart ISMS yardımıyla hazırlanmaktadır.
Risk Değerlendirme Metodolojisinin Belirlenmesi	Var	Var
Varlıkların belirlenmesi	Süreç tabanlı varlık belirlenmekte.	Süreç tabanlı varlık belirlenmekte.
Varlık değerlendirmesinin yapılması	Varlıkların Gizlilik-Bütünlük-Erişilebilirlik değerleri N/A	Varlıkların Gizlilik-Bütünlük-Erişilebilirlik değerleri Çok Düşük

Özellikler	Callio	Smart ISMS
	Low Medium High Olarak değerlendirilmektedir.	Düşük Orta Yüksek Çok Yüksek Olarak değerlendirilmektedir.
Varlıkların zafiyetlerini tanımlama	ISO 13335-3 e göre Zafiyetler tanımlanır. Zafiyetlerin varlıklara atanması kullanıcı tarafından yapılır.	ISO 27005' e göre Zafiyetler tanımlanır. Varlık kategorisine göre zafiyetler Smart ISMS tarafından uzman sistem kullanılarak belirlenir. Kullanıcı isterse ekleme çıkarma yapabilir
Varlıklar için tehditleri tanımlama	ISO 13335-3 e göre tehditler tanımlanır. Tehditlerin varlıklara atanması kullanıcı tarafından yapılır.	ISO 27005' e göre tehditler tanımlanır. Varlık kategorisine göre tehditler Smart ISMS tarafından belirlenir. Kullanıcı isterse ekleme çıkarma yapabilir
Risk Değerlendirmesinin yapılması	Değerlendirme kullanıcı tarafından yapılıyor	Değerlendirme kullanıcı tarafından yapılıyor
Risklere karşı korumaların seçilmesi	ISO/IEC 27001 ekindeki korumalardan kullanıcı tarafından seçiliyor	Smart ISMS tarafından Uzman sistem yardımıyla seçilmekte, kullanıcı isterse ekleme çıkarma yapabilmektedir.
GAP Analizi yapılması	Kullanıcı tarafından yapılıyor	Smart ISMS tarafından yapılmaktadır.
Artık risklere ilişkin yönetimin onayının hazırlanması	Kullanıcı tarafından yapılıyor	Smart ISMS tarafından yapılmaktadır.
Uygulanabilirlik bildirgesinin	Kullanıcı tarafından yapılıyor	Smart ISMS tarafından yapılmaktadır.

Özellikler	Callio	Smart ISMS
hazırlanması		
Mevcut durum tespiti	ISO/IEC 27001 standart maddeleri kontrol listesi olarak kullanılmakta kullanıcının verdiği yanıtlara göre mevcut durumun standarda uygunluğu belirlenmekte, uygunluk kararı kullanıcı tarafından verilmektedir.	Uzman sistem tarafından kullanıcı arayüzü yardımıyla sorulan kolay anlaşılır sorulara verilen cevaplara göre ISO/IEC 27001 standardına uygunluk uzman sistem tarafından belirlenmekte, eksiklikler açıklanmaktadır.
İnsan Kaynakları Güvenliği Prosedürünün Hazırlanması	Kullanıcı tarafından yapılıyor	Durum tespiti sonucunda eksiklikler ve uygunluklar uzman sistem tarafından belirlenerek "insan kaynakları güvenliği prosedürü" Smart ISMS tarafından hazırlanır. Kullanıcı prosedür üzerinde düzeltme yapabilir.
Fiziksel ve Çevresel Güvenlik Prosedürünün Hazırlanması	Kullanıcı tarafından yapılıyor	Durum tespiti sonucunda eksiklikler ve uygunluklar uzman sistem tarafından belirlenerek "Fiziksel ve Çevresel Güvenlik prosedürü" Smart ISMS tarafından hazırlanır. Kullanıcı prosedür üzerinde düzeltme yapabilir.
Haberleşme ve İşletim Yönetimi Prosedürünün Hazırlanması	Kullanıcı tarafından yapılıyor	Durum tespiti sonucunda eksiklikler ve uygunluklar uzman sistem tarafından belirlenerek "Haberleşme ve İşletim Yönetimi prosedürü" Smart ISMS tarafından hazırlanır. Kullanıcı prosedür

Özellikler	Callio	Smart ISMS
		üzerinde düzeltme yapabilir.
Erişim Kontrolü Prosedürünün Hazırlanması	Kullanıcı tarafından yapılıyor	Durum tespiti sonucunda eksiklikler ve uygunluklar uzman sistem tarafından belirlenerek "Erişim Kontrolü prosedürü" Smart ISMS tarafından hazırlanır. Kullanıcı prosedür üzerinde düzeltme yapabilir.
Bilgi Sistemleri Edinim, Geliştirme ve Bakım Prosedürünün Hazırlanması	Kullanıcı tarafından yapılıyor	Durum tespiti sonucunda eksiklikler ve uygunluklar uzman sistem tarafından belirlenerek "Bilgi Sistemleri Edinim, Geliştirme ve Bakım prosedürü" Smart ISMS tarafından hazırlanır. Kullanıcı prosedür üzerinde düzeltme yapabilir.
Bilgi Güvenliği İhlal Olayı Yönetimi Prosedürünün Hazırlanması	Kullanıcı tarafından yapılıyor	Durum tespiti sonucunda eksiklikler ve uygunluklar uzman sistem tarafından belirlenerek "Bilgi Güvenliği İhlal Olayı Yönetimi prosedürü" Smart ISMS tarafından hazırlanır. Kullanıcı prosedür üzerinde düzeltme yapabilir.
İş Sürekliliği Prosedürünün Hazırlanması	Kullanıcı tarafından yapılıyor	Durum tespiti sonucunda eksiklikler ve uygunluklar uzman sistem tarafından belirlenerek "İş Sürekliliği prosedürü" Smart ISMS tarafından hazırlanır. Kullanıcı prosedür üzerinde düzeltme yapabilir.
Yasal Gereklere Uyum Prosedürünün	Kullanıcı tarafından yapılıyor	Durum tespiti sonucunda eksiklikler ve

Özellikler	Callio	Smart ISMS
Hazırlanması		uygunluklar uzman sistem tarafından belirlenerek “Yasal Gereklere Uyum prosedürü” Smart ISMS tarafından hazırlanır. Kullanıcı prosedür üzerinde düzeltme yapabilir.
BGYS'nin izlenmesi ve gözden geçirilmesi	Kullanıcı tarafından yapılıyor	Smart ISMS tarafından hazırlanmaktadır.
İç denetimin yapılması	Denetim hazırlıklarının kontrolü yapılabilmekte	Smart ISMS tarafından hazırlanmaktadır.

EK-14. Smart ISMS programı kullanımına ilişkin kullanıcı anketi

Açıklama : Aşağıdaki sorulara 1 (En düşük) ile 5 (En yüksek) arasında bir puan veriniz.

1. Bilgisayar konularına hakimiyetiniz

	1	**2**	**3**	**4**	**5**
Bilişim teknolojileri konusunda bilginiz	○	○	○	○	○
Bilgi güvenliği konusunda bilginiz	○	○	○	○	○
ISO 27001 hakkında bilginiz	○	○	○	○	○
ISO 9001 hakkında bilginiz	○	○	○	○	○
Bilgisayar kullanım seviyeniz	○	○	○	○	○

2. Programın Görsel Tasarımı:

	1	**2**	**3**	**4**	**5**
Renk Uyumu	○	○	○	○	○
Yerleşim Düzeni	○	○	○	○	○
Okunabilirlik	○	○	○	○	○
Çözünürlük	○	○	○	○	○
Menü Tasarımı	○	○	○	○	○
Site tasarımının özgünlüğü	○	○	○	○	○

3. Programın İşlevselliği :

	1	2	3	4	5
Kullanım kolaylığı	○	○	○	○	○
Soruların Anlaşılabilirliği	○	○	○	○	○
Hazırlanan raporların uygunluğu	○	○	○	○	○
Mantıksal İş Akışı	○	○	○	○	○
Kullanım memnuniyeti	○	○	○	○	○
Sıralama ve genel yerleşim planı	○	○	○	○	○

4. Programın Verimliliği

	1	2	3	4	5
Programın işinize katkısı	○	○	○	○	○
Zaman tasarrufu	○	○	○	○	○
Personel tasarrufu	○	○	○	○	○
İş sürekliliğine katkısı	○	○	○	○	○
Hataları önlemesine katkısı	○	○	○	○	○

EK-15. SMART ISMS programı kullanımına ilişkin kullanıcı anketi sonuçları

Ankete toplam katılımcı sayısı 13 dür,

1. Kullanıcıların bilgisayar konularına hakimiyeti.

	1	2	3	4	5	Ortalama	SS
Bilişim teknolojileri konusunda bilginiz	2	5	3	2	1	2,6	2,3
Bilgi güvenliği konusunda bilginiz	3	4	3	2	1	2,5	1,31
ISO 27001 hakkında bilginiz	6	3	2	1	1	2,07	4,65
ISO 9001 hakkında bilginiz	3	4	3	2	1	2,53	1,3
Bilgisayar kullanım seviyeniz	1	2	3	5	2	3,3	2,91

Ankete katılanların bilgisayar kullanım seviyesinin ortanın yarıdan fazlasının genel bilgisayar kullanımı orta düzeyin üzerinde bilgi sahibi oldukları ve Bilişim Teknolojileri konusunda temel bilgi sahibi oldukları görülmektedir. Aynı şekilde anket cevap verenlerin ISO 27001 ve ISO 9001 hakkında temel bilgi sahibi olduğu gözlemlenmektedir.

2. Programın Görsel Tasarımı

	1	2	3	4	5	Ortalama	SS
Renk Uyumu	3	3	2	2	3	2,9	0,41

Yerleşim Düzeni	4	3	3	1	2	2,5	1,35
Okunabilirlik	1	2	6	2	2	3,1	4,11
Çözünürlük	1	2	4	5	1	3,2	3,75
Menü Tasarımı	4	3	4	2	0	2,3	2,91
Site tasarımının özgünlüğü	2	2	4	3	2	3	1

Programın görsel tasarımı ile ilgili sorulan altı soruya kullanıcılardan gelen cevaplar yukarıdaki gibidir. Tabloya göre kullanıcılar programın okunabilirlik ve çözünürlük değerlerini beğenirken, yerleşim düzeni ve menü tasarımı konusunda programı eksik bulmuşlardır. Katılımcıların yarısı renk uyumunu beğenirken yarısı beğenmemiştir. Ayrıca sorulara yanıt veren kullanıcıların büyük bir kısmı sitenin tasarımını özgün bulmuşlardır.

3. Programın İşlevselliği

	1	**2**	**3**	**4**	**5**	**Ortalama**	**SS**
Kullanım kolaylığı	2	1	2	6	2	3,4	4,6
Soruların Anlaşılabilirliği	1	1	4	3	4	3,6	3,54
Hazırlanan raporların uygunluğu	2	2	3	3	3	3,3	0,91
Mantıksal İş Akışı	1	3	4	3	2	3,2	1,75
Kullanım memnuniyeti	1	2	3	4	3	3,5	2,35
Sıralama ve genel yerleşim planı	2	2	3	4	2	3,2	1,25

Soruları cevaplayan kullanıcılar, programın kullanımını genel olarak kolay bulmuşlardır. Mevcut durum değerlendirmesi modülünde yer alan sorular büyük çoğunluk tarafından anlaşılır bulunmuş ve katılımcıların yarıdan fazlası kullanımdan memnun kalmışlardır. Aynı şekilde programdaki mantıksal iş akışı ve bilgilerin yerleşim planında çoğu katılımcı tarafından olumlu bulunmuştur.

4) Programın Verimliliği

	1	**2**	**3**	**4**	**5**	**Ortalama**	**SS**
Programın işinize katkısı	1	2	4	4	2	3,3	2,25
Zaman tasarrufu	0	3	3	4	3	3,5	3,31
Personel tasarrufu	0	1	2	4	6	4,2	9
İş sürekliliğine katkısı	1	1	3	4	4	3,7	3,81
Hataları önlemesine katkısı	1	2	2	5	3	3,5	3,31

Programın Verimliliği konusunda katılımcıların büyük bir bölümü programın kendi şirketlerindeki işlerine katkısını çok olumlu bulmuşlar, zaman ve personel tasarrufu sağladığını belirtmişlerdir. Yapılan değişiklikler merkezi bir yönetim tarafından sürekli gözetlenebileceği için program hatalarını önleme konusunda da gayet başarılı bulunmuştur. Yine katılımcılara göre program, iş sürekliliğine olumlu anlamda bir katkı sağlamaktadır.

ÖZGEÇMİŞ

Kişisel Bilgiler

Soyadı, adı	: GEMCİ, Cemal
Uyruğu	: T.C.
Doğum tarihi ve yeri	: 22.10.1962 Çanakkale
Medeni hali	: Evli
Telefon	: 0 (312) 467 89 58
Faks	: 0 (312) 426 93 13
e-mail	: cemal@cymsoft.com

Eğitim

Derece	Eğitim Birimi	Mezuniyet tarihi
Yüksek lisans	ODTÜ / Bilgisayar Mühendisliği	1995
Lisans	Kara Harp Okulu / Elektronik Bölümü	1985
Lise	Bursa Işıklar Askeri Lisesi	1981

İş Deneyimi

Yıl	Yer	Görev
1992-2004	TSK	Bilgi Sistemleri Yöneticisi
2004-2006	Türktrust A.Ş.	Genel Müdür Yardımcısı
2006-	Cymsoft Ltd. Şti.	Genel Müdür

Yabancı Dil

İngilizce, Fransızca

Yayınlar

1. Gemci, C., An Application with SSADM: Personel Information System for Turkish General Staff (TGS) Yüksek Lisans Tezi, 1995.

2. Gemci, C., BAY, Ö.F., "Yapay Zeka Temelli Bilgi Güvenliği Yönetim Sistemi Yaklaşımı", II. Ağ ve Bilgi Güvenliği Ulusal Sempozyumu, 2008.

Hobiler

Tenis, Basketbol, Kayak