

T.C.  
GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ  
MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ

BİLGİ TEKNOLOJİLERİ SİSTEMLERİNİN  
ORTAK KRİTERLERE UYGUN OLARAK  
GÜVENLİK DEĞERLENDİRMESİ

Mehmet ÇAKIR  
YÜKSEK LİSANS TEZİ  
BİLGİSAYAR MÜHENDİSLİĞİ  
ANABİLİM DALI

TEZ DANIŞMANI  
Yrd. Doç. Dr. İbrahim SOĞUKPINAR

GEBZE  
2004

**T.C.**  
**GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ**  
**MÜHENDİSLİK VE FEN BİLİMLERİ ENSTİTÜSÜ**

**BİLGİ TEKNOLOJİLERİ SİSTEMLERİNİN**  
**ORTAK KRİTERLERE UYGUN OLARAK**  
**GÜVENLİK DEĞERLENDİRMESİ**

**Mehmet ÇAKIR**  
**YÜKSEK LİSANS TEZİ**  
**BİLGİSAYAR MÜHENDİSLİĞİ**  
**ANABİLİM DALI**

**GEBZE**  
**2004**

## ÖZET

Günümüzde organizasyonlar varlıklarını bilgi sistemlerini kullanarak saklamakta, işlemekte ve iletmektedir. Gelişen teknoloji ile birlikte bu varlıklara gerçekleştirilen saldırıların sayısı ve niteliği artmaktadır. Organizasyonların yasal zorunlulukların ve iş gereksinimlerinin sonucu olarak bilgi sistemlerinin güvenliklerine verdikleri önem de artmaktadır. Bunların sonucu olarak BT (Bilgi Teknolojileri) sistemlerinin güvenlik değerlendirmelerinin bağımsız kuruluşlar tarafından ölçülmesi ihtiyacı doğmuştur.

CC (Ortak Kriterler) standardı BT ürünlerinin ve sistemlerinin güvenlik değerlendirmelerinin gerçekleştirilmesi için geliştirilmiş bir standarttır. Standartın kullanımı giderek yaygınlaşmıştır fakat şu anki haliyle yalnızca ürün değerlendirmelerinde kullanılabilmektedir. Çünkü BT sistemlerinde kullanılabilmesi için yeterli değildir.

Bu çalışmada Ortak Kriterler standardının kullanımı ile ilgili bilgi verilmiş, ürün değerlendirmelerinde nasıl kullanıldığı incelenmiştir. Ayrıca sistem değerlendirmeleri için standardın eksikleri ortaya koyulmuş ve bu eksiklerin giderilmesi için çözüm önerileri sunulmuştur. ISO 17799 bilgi sistemlerinin yönetimi için genel prensipler tanımlamıştır. Bu çalışmada standart BT sistemlerinin Ortak Kriterler'e uygun değerlendirilebilmesi için kaynak olarak kullanılmıştır.

Çalışmanın son kısmında BT sisteminin Ortak Kriterler standardına ve önerilen çözümlere uygun olarak nasıl güvenli olarak tasarlanıp gerçekleştirilebileceği ortaya konulmuştur.

## SUMMARY

After the developments on IT sector for fifteen years, nowadays organizations use IT systems in order to store, process and transmit almost all of their assets. Although this development also increased the number and quality of the attacks to this information systems. The mandatory laws about data protection and increase of attacks forced organizations to give more importance to the security of their information systems. As result evaluation of their IT systems by independent third party labs became necessary.

Common Criteria is a standart which is developed for evaluation of IT products and system. The usage of CC is became world wide since 2000, although its current version is just applicable for IT products because it current version is not sufficient for system evaluations.

This study first shows how to conduct evaluations according to CC. After list the deficiencies of the standart for system evaluations and propose solutions for these deficiencies. ISO 17799 is a standard which propose general principals for IT system management. This study used ISO 17799 as a resource for evaluations of IT systems according to CC.

In the last part of this study a methodology is proposed for IT systems. With this methodology it is possible to design and implement an IT system according to CC and evaluate it according to CEM and ISO 17799.

## TEŞEKKÜR

Tez çalışmam boyunca daha ilerisini hedeflememde büyük pay sahibi olan tez danışmanım Sayın Yrd. Doç. Dr. İbrahim Soğukpınar'a teşekkürlerimi sunarım. Tez çalışmamı destekleyen TÜBİTAK-UEKAE Müdürü Sayın Önder Yetiş'e ve proje müdürüm Sayın Mert Üneri'ye teşekkürlerimi sunarım.

# İÇİNDEKİLER DİZİNİ

|                                                                                       | <b><u>Sayfa</u></b> |
|---------------------------------------------------------------------------------------|---------------------|
| ÖZET                                                                                  | iv                  |
| SUMMARY                                                                               | v                   |
| TEŞEKKÜR                                                                              | vi                  |
| İÇİNDEKİLER DİZİNİ                                                                    | vii                 |
| SİMGELER VE KISALTMALAR DİZİNİ                                                        | x                   |
| ŞEKİLLER DİZİNİ                                                                       | xi                  |
| ÇİZELGELER DİZİNİ                                                                     | xii                 |
| <br>                                                                                  |                     |
| 1. GİRİŞ                                                                              | 1                   |
| 1.1. Bilgi Teknolojileri Sistemleri                                                   | 4                   |
| 2. BİLGİ GÜVENLİĞİ ve ORTAK KRİTERLER                                                 | 8                   |
| 2.1. Bilgi Güvenliği [Karabacak, 2003]                                                | 8                   |
| 2.2. Ortak Kriterler                                                                  | 10                  |
| 2.2.1. Tarihçesi                                                                      | 11                  |
| 2.2.2. Kapsamı ve Kullanımı                                                           | 12                  |
| 2.2.3. Değerlendirme Metodolojisi                                                     | 15                  |
| 2.2.4. CCRA ve Ortak Kriterler Yapısı                                                 | 16                  |
| 2.3. Ortak Kriterler’e Uygun Ürün Değerlendirmesi                                     | 17                  |
| 2.3.1. Güvenlik Hedefi Değerlendirmesi                                                | 19                  |
| 2.3.2. EAL1 Değerlendirmesi                                                           | 23                  |
| 2.3.3. EAL2 Değerlendirmesi                                                           | 25                  |
| 2.3.4. EAL3 Değerlendirmesi                                                           | 28                  |
| 2.3.5. EAL4 Değerlendirmesi                                                           | 33                  |
| 2.4. ISO 17799 Bilgi Teknolojisi – Bilgi Güvenliği Yönetimi için Uygulama Prensipleri | 39                  |
| 2.4.1. ISO 17799 Kontrol Objeleri                                                     | 40                  |
| 2.5. COTS Ürünlerinin Değerlendirilmesi                                               | 41                  |
| 2.5.1. V-RATE Değerlendirme Modeli ile COTS Değerlendirmesi                           | 42                  |
| 2.5.1.1. V-RATE Yöntemi [Lipson, 2002]                                                | 43                  |
| 2.5.1.2. Özel Satıcı-Risk Azaltma Teknikleri                                          | 45                  |

|                                                               |    |
|---------------------------------------------------------------|----|
| 2.5.1.3. COTS Ürünlerinin Test Edilmesi                       | 48 |
| 2.5.1.3.1. Beyaz kutu testleri                                | 49 |
| 2.5.1.3.2. Siyah kutu testleri                                | 49 |
| 2.5.1.3.3. Test yöntemleri                                    | 50 |
| 2.5.1.4. Test Yöntemlerinin Değerlendirilmesi                 | 50 |
| 2.5.1.5. V-RATE Metodu & Ortak Kriterler Standardı            | 51 |
| 3. BİLGİ TEKNOLOJİLERİ SİSTEMLERİ GÜVENLİK<br>GEREKSİNİMLERİ  | 53 |
| 3.1. Güvenlik Fonksiyonel Gereksinimleri                      | 53 |
| 3.2. Güvenlik Yönetim Gereksinimleri                          | 54 |
| 3.2.1. Örnek Güvenlik Yönetim Gereksinimleri                  | 60 |
| 3.2.1.1. Erişim Kontrolü Sınıfı                               | 60 |
| 3.2.1.2. Fiziksel Güvenlik ve Ortam Güvenliği Sınıfı          | 61 |
| 3.3. Güvenlik Garanti Gereksinimleri                          | 62 |
| 4. BİLGİ TEKNOLOJİLERİ SİSTEMLERİ GÜVENLİK<br>DEĞERLENDİRMESİ | 65 |
| 4.1. Değerlendirme Süreci                                     | 66 |
| 4.2. Sistemler için Değerlendirme Garanti Düzeyleri           | 67 |
| 4.2.1. Tasnif Dışı Bilgi Ağ Sistemleri                        | 67 |
| 4.2.2. Hassas Bilgi Ağ Sistemleri                             | 68 |
| 4.2.3. Özel Bilgi Ağ Sistemleri                               | 69 |
| 4.2.4. Gizli Bilgi Ağ Sistemleri                              | 71 |
| 4.3. Güvenlik Hedefi'nin Hazırlanması                         | 73 |
| 5. SİSTEMİN GERÇEKLENMESİ VE TESTLER                          | 75 |
| 5.1. Değerlendirme Metodolojisinin Uygulanması                | 75 |
| 5.2. Garantinin Devamının Sağlanması                          | 76 |
| 5.3. Örnek Bir Sistemin Değerlendirilmesi                     | 76 |
| 5.3.1. Ağ Topolojisi [Karabacak, 2002]                        | 77 |
| 5.3.2. Kurumun Varlıkları ve Güvenlik Politikaları            | 78 |
| 5.3.2.1. BT Varlıkları                                        | 78 |
| 5.3.2.2. BT Dışı Varlıklar                                    | 81 |
| 5.3.3. Değerlendirme Yönteminin Uygulanması                   | 82 |

|                                                                       |     |
|-----------------------------------------------------------------------|-----|
| 5.3.3.1. Risk Değerlendirmesi ve Risk Yönetimi [Karabacak, 2002]      | 82  |
| 5.3.3.1.1. Açıklıklar ve Tehditler                                    | 82  |
| 5.3.3.1.2. Güvenlik Önlemleri                                         | 87  |
| 5.3.3.1.3. Varlık Puanlaması                                          | 87  |
| 5.3.3.1.4. Tehdidin Gerçekleşme İhtimali                              | 90  |
| 5.3.3.1.5. Tehdidin Mutlak Etkisi                                     | 91  |
| 5.3.3.1.6. Risk Hesaplanması                                          | 93  |
| 5.3.3.1.7. Risk Yönetimi                                              | 95  |
| 5.3.3.2. Sistemin Güvenlik Hedefinin Oluşturulması                    | 96  |
| 5.3.3.2.1. Kabullenmeler, Tehditler, Riskler ve Güvenlik Politikaları | 96  |
| 5.3.3.2.2. TOE için Güvenlik Amaçları                                 | 100 |
| 5.3.3.2.3. TOE Güvenlik Gereksinimleri                                | 103 |
| 5.3.3.2.4. Gereksinimlere Karşı Tedbirler                             | 109 |
| 5.3.4. Uygulamanın Sonuçları                                          | 111 |
| 5.3.5. Koruma Profili Kullanımı                                       | 113 |
| 6. SONUÇLAR VE ÖNERİLER                                               | 115 |
| KAYNAKLAR                                                             | 118 |
| ÖZGEÇMİŞ                                                              | 120 |
| Ek-1: Tanımlar                                                        |     |

## SİMGELER VE KISALTMALAR DİZİNİ

|        |                                                     |
|--------|-----------------------------------------------------|
| BS     | British Standard                                    |
| CC     | Common Criteria                                     |
| CCRA   | Common Criteria Recognition Arrangement             |
| CEM    | Common Evaluation Methodology                       |
| COTS   | Commercial Off The Shelf                            |
| EAL    | Evaluation Assurance Level                          |
| ISO    | International Standards Organization                |
| IT     | Information Technology                              |
| ITSEC  | Information Technology Security Evaluation Criteria |
| PP     | Protection Profile                                  |
| SAR    | Security Assurance Requirements                     |
| SFR    | Security Functional Requirements                    |
| SOF    | Strength of Function                                |
| ST     | Security Target                                     |
| TCSEC  | Trusted Computer Security Evaluation Criteria       |
| TOE    | Target of Evaluation                                |
| V-RATE | Vendor – Risk Assessment and Threat Evaluation      |

## ŞEKİLLER DİZİNİ

| <b><u>Sekil</u></b>                                                     | <b><u>Sayfa</u></b> |
|-------------------------------------------------------------------------|---------------------|
| 1.1. Organizasyon bilgi güvenliği için önerilen yaklaşım                | 3                   |
| 1.2. Değerlendirme hedefi (TOE)                                         | 6                   |
| 2.1. Ortak Kriterler’de güvenliğin sağlanması                           | 14                  |
| 2.2. Ortak Kriterler’e uygun ürün geliştirme adımları [ISO 15408, 1999] | 18                  |
| 2.3. Güvenlik Hedefi dokümanının hazırlanış aşamaları [ISO 15408,1999]  | 19                  |
| 2.4. Güvenlik Hedefi Organizasyonu                                      | 21                  |
| 2.5. Güvenlik Hedefi içeriği [ISO 15408, 1999]                          | 22                  |
| 4.1. Bilgi Teknolojileri sistem değerlendirilmesi süreci                | 67                  |
| 4.2. Güvenlik Hedefi’nin hazırlanması                                   | 74                  |
| 5.1. A şirketi ağ topolojisi                                            | 78                  |

## ÇİZELGELER DİZİNİ

| <b><u>Çizelge</u></b>                                                     | <b><u>Sayfa</u></b> |
|---------------------------------------------------------------------------|---------------------|
| 2.1. EAL1 garanti gereksinimleri                                          | 23                  |
| 2.2. EAL2 garanti gereksinimleri                                          | 25                  |
| 2.3. EAL3 garanti gereksinimleri                                          | 28                  |
| 2.4. EAL4 garanti gereksinimleri                                          | 33                  |
| 2.5. V-RATE Yöntemi                                                       | 43                  |
| 2.6. V-RATE Risk Azaltma Yöntemi                                          | 45                  |
| 3.1. Güvenlik yönetim gereksinimleri [Tabuchi, 2002]                      | 54                  |
| 3.2. Güvenlik garanti gereksinimleri                                      | 63                  |
| 4.1. Tasnif dışı bilgi ağ sistemleri                                      | 68                  |
| 4.2. Hassas bilgi ağ sistemleri                                           | 69                  |
| 4.3. Özel bilgi ağ sistemleri                                             | 70                  |
| 4.4. Gizli bilgi ağ sistemleri                                            | 72                  |
| 5.1. BT Dışı varlıkların değer çizelgesi                                  | 81                  |
| 5.2. Varlık puanlaması değer çizelgesi                                    | 87                  |
| 5.3. Tehdit değer çizelgesi                                               | 90                  |
| 5.4. Tehditlerin mutlak etkilerinin değer çizelgesi                       | 91                  |
| 5.5. Risk hesaplaması değer çizelgesi                                     | 93                  |
| 5.6. Metodoloji uygulandıktan sonra gerçekleştirilen risk değerlendirmesi | 112                 |

# 1 GİRİŞ

Günümüzde şirketler ve büyük organizasyonlar bütün işlemlerini ağ üzerinden gerçekleştirmektedirler. Bu durum organizasyonların bilgi sistemlerinin gizli ve kritik bilgiler taşımasını gerektirmektedir. Dolayısıyla artık kritik güvenli sistemler organizasyonlar için eskiye nazaran çok daha önem taşımaktadırlar. Örneğin artık akıllı kart sistemleri gittikçe daha fazla amaç için kullanılmaya ve e-ticaret ve diğer kritik güvenli internet kullanımı giderek yaygınlaşmaya başlamıştır. Artan bu güvenlik ihtiyacı organizasyonlara sistemlerinin bilgi güvenliği seviyesini ihtiyaçlarının üzerinde ve rakiplerinden daha yukarıda tutmak zorunluluğu getirmiştir. [Ramachandran, 2002]

Ayrıca şirketlerin her türlü gizlilik seviyesine sahip verileri ve kişisel bilgileri gün geçtikçe daha fazla BT sistemleri üzerinde taşınmakta, işletilmekte ve yönetilmektedir. Bu bilgilerin güvenli bir şekilde korunması için BT güvenliği artık çoğu ülkede yasal zorunluluk haline gelmiştir. Özellikle Avrupa Birliği direktifleri aday bir ülke olan Türkiye'yi de yakından ilgilendirmektedir. AB'de bu kapsamda 1995 yılında yayınlanmış Bilgi Koruma Direktifi<sup>1</sup> ve 1998 yılında yayınlanmış Bilgi Koruma Yasası<sup>2</sup> ile kişisel bilgilerin korunmasını organizasyonlar için zorunlu hale getirmiştir. Ayrıca AB direktifleri kapsamında akıllı kart sistemlerinin ve takografların Ortak Kriterler'e uygun olarak değerlendirmeden geçmesi ve sertifikalandırılması da zorunludur. Bütün bu yasal zorunlulukların yanı sıra şirketlerin ticari ilişkilerini düzenlerken dikkat ettikleri en önemli hususlardan biri de kişisel bilgilerin korunmasına verilen önemdir. Şirketler ancak bu şekilde BT'ye dayalı toplumun gelişebileceğine inanmaktadır.

Ortak Kriterler BT ürünlerin ve sistemlerinin güvenliğinin sağlanması ve garanti edilmesi için kullanılmakta olan uluslararası bir standarttır. [Vedder, 1998] CC katalog halinde tanımlamış olduğu Güvenlik Fonksiyonel Gereksinimleri

---

<sup>1</sup> EU Data Protection Directive 1995 Article 17, Kontrol sistemleri ve işlemciler kişisel bilgileri özellikle bilgi ağlar üzerinde iletilirken kazalara, illegal değişikliklere, kayıplara, yetkisiz dağıtımlara ve erişimlere karşı korumak ve yeterli organizasyonel güvenlik tedbirlerini almak zorundadır. [Buzzard, 2003]

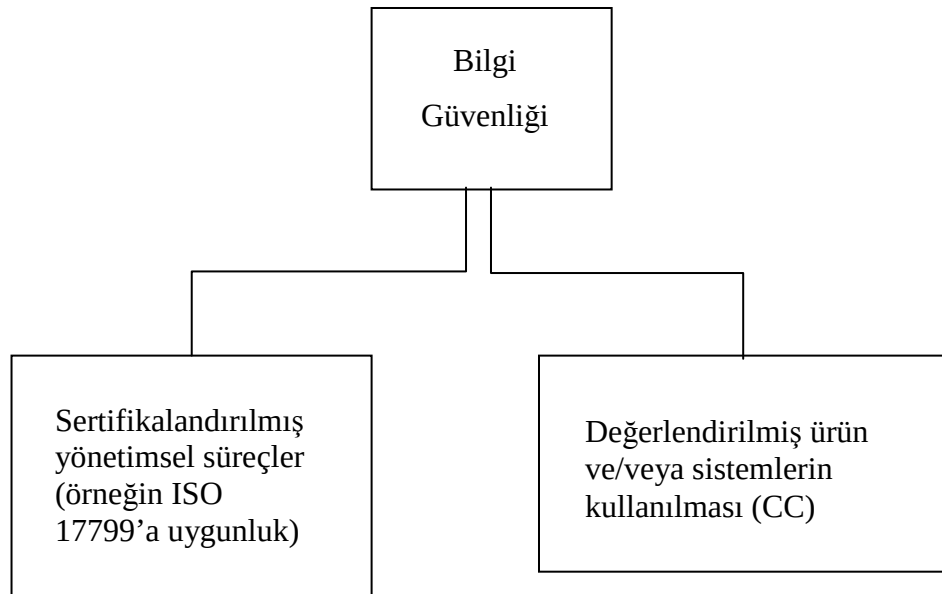
<sup>2</sup> The Data Protection Act 1998 Principle 7, Kişisel bilgilerin işletilmesi ve saklanması sırasında yetkisiz ve illegal erişim ve dağıtımına karşı uygun teknik ve organizasyonel tedbirler alınmalıdır. [Buzzard, 2003]

aracılığıyla ürünlerin veya sistemlerin korumaları gereken varlıklar ve karşılımları gereken tehditler için sağlamaları gereken güvenlik gereksinimlerini tanımlar. Ayrıca Güvenlik Garanti Gereksinimleri kataloğu ile de bu fonksiyonları nasıl uygulayacağını ve sürekliliğini nasıl sağlayacağını garanti edecek gereksinimleri tanımlar. Bu gereksinimler BT ürünleri veya sistemleri için geliştirilen Koruma Profillerinde BT müşterileri tarafından kullanılır ve müşteriler belirli bir ürün için güvenlik ve garanti ihtiyaçlarını belirtir. Üreticiler ise müşterilerin bu ihtiyacına cevap verecek bir ürün geliştirdiklerinde bir Güvenlik Hedefi dokümanı ile bu ihtiyacı karşıladıklarını doğrularlar. Örneğin, ticari bir veritabanı yönetim sistemi için bir koruma profili hazırlanır ve ORACLE bu koruma profilini karşılayan ürünü için güvenlik hedefini hazırlar. Bu yöntemle ve CC kabul edildiği 1998 yılından itibaren gittikçe yaygınlaşan kullanımıyla BT güvenliği alanında ürünlerin veya sistemlerin güvenlik garanti düzeylerinin üçüncü bir bağımsız kuruluş tarafından değerlendirilmesinde standart olarak kullanılmaktadır. [Cugini, 1995] Yapılan bu değerlendirmelerde CC “Güvenlik Garanti Düzeyi” adı verilen ve EAL1’den EAL7’ye kadar değişen yedi adet garanti düzeyi ile ürün ve sistemleri sınıflandırmaktadır. Organizasyonlar son dönemde artan güvenlik ihtiyaçları sebebiyle sistemlerinde mümkün olduğunca CC standardına uygun olarak değerlendirilmiş ve sertifikalandırılmış ürünler kullanmaya yönelmişlerdir. Fakat belirli bir BT ortamına uygun şartlarda değerlendirilmiş bir ürün, organizasyonun sisteminde yerini aldığı anda hala aynı garantiyi sağlamamaktadır. Çünkü söz konusu bir sistemin parçası veya bütünü olduğunda ürünün sağladığı güvenlik fonksiyonları ve geliştirilme güvenliği kadar ürünü kullanan insan kaynağı ve şirketin bilgi sistemleri politikaları da önem kazanmaktadır.

Yöneticiler organizasyonlarının bilgi güvenliği seviyesinin güncel BT trendini takip etmesini ve bu seviyenin rakip firmalar ile karşılaştırılabilmesini garanti etmek isterler. Günümüzde modern organizasyonların BT kaynaklarının başarılı yönetimi bütün güvenlik ihtiyaçlarının yapısal ve hesap verilebilir bir şekilde sağlanmasını gerektirmektedir. Bu yüzden bilgi sistemleri yöneticileri organizasyonlarının bilgi güvenliğini sağlamak için sistemlerinde güvenlik değerlendirmesinden geçmiş sertifikalı ürünler kullanmaktadırlar. Fakat sistemin sertifikalı ürünlerden kurulmuş olması o sistemin bilgi güvenliği seviyesi için tek etken değildir. Çünkü bir kurumda bilgi güvenliğinin ana etmeni kurum çalışanları ve kurumun bilgi güvenliği

politikasıdır.[Dr. Ross, 2002] Ayrıca sistemin bileşenlerinin tek tek değerlendirilmiş olması dahi bütün sistem hakkında bize yeterli bilgiyi vermemekte ve bütün sistemin güvenlik değerlendirilmesinden geçmesi gerekmektedir. Bu durumun farkında olan bilgi güvenliği yöneticileri kurumlarının bilgi güvenliği için bir takım standartlaşmış kılavuz dokümanlar kullanmaktadırlar. Bu dokümanlardan en fazla tanınmış olanı ve kullanılanı İngiliz Standartlarının yayınlamış olduğu ISO 17799 “Bilgi Güvenliği Yönetimi için Uygulama Prensipleri”’dur.[Trcek, 2003] Bir kurumun bu standarda uygun çalışması o kurumda bilgi güvenliği açısından gereken yönetsel süreçlerin yerine getirildiği, kurumun tanımlanmış ve işleyen bir kurumsal güvenlik politikası olduğu anlamına gelmektedir. Kurumlar ihtiyaç duydukları taktirde bu standarda uygunluklarını bağımsız bir kuruluşa denetletip başarılı oldukları taktirde söz konusu standarda uygunluk sertifikalarını alabilmektedirler. Fakat bu sertifika yalnız başına kurumun bilgi güvenliği sistemi seviyesini belirlemede yeterli değildir.

Organizasyonlar için önerilen çözüm bu iki yöntemin yani sistemde değerlendirilmiş ürün kullanılması ile kurumun bilgi güvenliği konusunda yayınlanmış bir standarda uygun yönetilmesinin birlikte kullanılmasıdır. İki yöntem ayrı ayrı kullanıldığında gayet zayıf kalmakla beraber birlikte kullanıldıklarında organizasyonun bilgi güvenliği seviyesinde bir artış gözlenebilmektedir. Şekil 1.1 Organizasyon bilgi güvenliği için önerilen yaklaşım’de bu yöntem temsil etmektedir. [Eloff, 2000]



Şekil 1.1 Organizasyon bilgi güvenliği için önerilen yaklaşım

## 1.1 Bilgi Teknolojileri Sistemleri

Aslında “sistem” kavramı bilim için yeni bir kavram sayılmaktadır. Doğu filozofları dünyayı çok çeşitli bileşenlerden oluşan bir sistem olarak görmektedir, fakat batılılar dünyayı birbirleriyle ilişkisi olan parçalara ayırarak tanımlamaktadır. Sistemin tanımını yapmak, fiziksel ve mantıksal sınırlarını çizmek özellikle BT sistemleri için zordur. Ancak Ortak Kriterler standardında yapılan sistem tanımı ile ve sistemlerin özellikleriyle bu sınırların tanımını yapmak mümkün olmaktadır. Öncelikle sistemler birbirleriyle ilişkide ve iletişimde bulunan bileşenlerden oluşur. Örneğin bilgisayarların iletişiminden yerel alan ağları, yerel alan ağlarının iletişiminden geniş alan şebekeleri oluşmaktadır. Bu ağlar, kullanıcılarına, amaçlarına ve taşıdıkları bilgilere göre sınıflanırlar ve sistemleri oluştururlar. Giriş kısmında da bahsedildiği gibi organizasyonlar bilgilerini gün geçtikçe bilgi teknolojileri sistemleri üzerinde taşımaktadırlar ve bu sistemlerin taşıdıkları bilgilerin sınıflarına uygun olarak güvenliğini sağlamak için yatırımlar yapmaktadırlar. Bu yüzden kriptografi, güvenlik duvarı teknolojileri açık anahtar altyapıları, IDS gibi teknolojiler geliştirildi ve sistemler bu teknolojilerle güçlendirildi. Fakat SecurityFocus gibi web sitelerinin raporlarına bakıldığında güvenlik teknolojileri ne kadar gelişse de saldırıların artarak devam ettiği, ve sistemlerin güvenliğinin tam olarak sağlanamadığı görülmektedir. Bu sonucun başlıca iki sebebi vardır.

Bunlardan ilki teori ile pratiği birbiri ile olan ilişkisidir. Güvenlik teorisi ile ilgili çok fazla çalışma gerçekleştirilmektedir, kriptografi teorisi, güvenlik duvarı ve IDS teorisi, biyometri teorisi gibi. Birçok sistem bu teorilerin en başarılı ürünleri ile donatılmakta fakat pratikte başarısız olmaktadır.

Yogi Berra’nın dediği gibi “Teoride teori ile pratik arasında fark yoktur fakat pratikte vardır.” [Schneier, 2000] Teoriler ideal koşullarda ve laboratuvar koşullarında başarı ile sonuçlanmaktadır ve güvenlik ürünlerinde bu testlerden başarı ile geçmektedir. Fakat gerçek dünya şartlarında bu ürünler sistemlere adapte edildiğinde insan kaynağı ve diğer ortam şartları devreye girdiğinde aynı başarıyı gösterememektedir.

Diğer sebep ise önleme, tespit etme ve tepki verme arasındaki ilişkidir. Güvenli bir sistemde bu üç özelliğinde koordineli bir şekilde uygulanması gerekmektedir. Fakat günümüzde organizasyonlar bilgi teknolojileri sistemlerinin güvenliğinde önleme için kriptografi, güvenlik duvarı ve benzeri ürünleri kullanırken tespit etmek için genellikle hiç, tepki verme ve denetleme içinse neredeyse çok az çaba göstermektedirler.

Bu çalışmada gerçek dünyadaki çalışma ortamında bir bilgi teknolojisi sisteminin taşıdığı bilginin sınıfına göre güvenlik değerlendirmesi için ve önleme, tespit etme ve tepki verme tedbirlerinin uygulandığının onaylanması için Ortak Kriterler standardı ve ISO 17799 standartları temel alınarak bir metodoloji önerilmiştir.

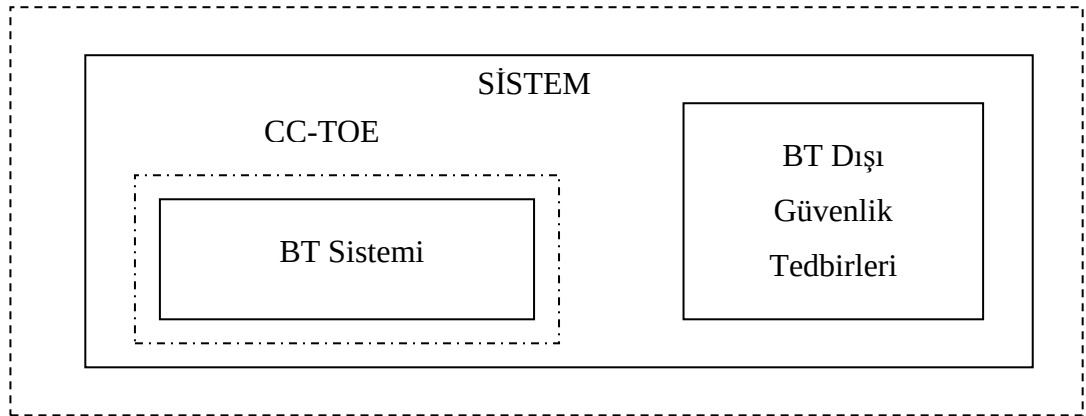
Amiral Garce Hopper'ın dediği gibi “Hayat İkinci Dünya Savaşından önce daha basitti, daha sonra sistemler kullanmaya başladık.”[Schneier, 2000]

İlk olarak bu çalışmada sistemin nasıl algılandığının tanımlanması gerekmektedir. Ortak Kriterler standardı sistemi belli bir çalışma ortamına ve amaca sahip özel bir BT kurulumu olarak tanımlamaktadır. Sistem sadece birden çok ürünün birleşmesinden oluşan bir sonuç değildir. Daha çok bu ürünlerin bilinen ve kontrol edilebilen BT dışı güvenlik tedbirleri<sup>3</sup> ile birleşmesinden oluşmaktadır. Bu çalışmanın konusu olan BT sisteminin fiziksel sınırları **Şekil 1.2. Değerlendirme hedefi (TOE)**'de gösterilmiştir.

---

<sup>3</sup> BT dışı güvenlik tedbirleri: Bilgi Teknolojileri ile ilgisi olmayan güvenlik ölçütleri, örn. Fiziksel güvenlik.

## Sis-TOE



Şekil 1.2. Değerlendirme hedefi (TOE)

Ürünlerin güvenlik değerlendirilmesinden geçmesi önemlidir ve güvenli sistemler kurulurken sertifikalandırılmış ve güvenli oldukları bağımsız kuruluşlar tarafından onaylanmış ürünler tercih edilmelidir. Fakat birçok güvenlik sorununun üründen kaynaklanmasının yanı sıra yanlış yamalar yapmak, kötü düzenlenmiş erişim listeleri, güvenlik duvarı kurallarının hatalı tanımlanması ve dosya/dizin yapısındaki bozukluklar gibi sistemlerin gerçek kullanım ortamlarında sistemlerin çıkarabileceği problemlerden de kaynaklandığı bilinmektedir. Ayrıca ağa bağlı bir sistemin güvenlik seviyesinin bu sistemle ilgili diğer ağ bileşenleri ile sıkı bir ilişkisi vardır.

Ortak Kriterler'in ve Ortak Kriterler değerlendirme metodolojisinin sistem değerlendirmeleri için uygulanmasının iki önemli avantajı vardır. Bunlardan ilki değerlendirmelerin tanımlanmış ölçütlere göre gerçekleştirilmesi ve bunun sağladığı kolaylıklardır, diğeri ise değerlendirme sonuçlarının uluslararası ortak tanınmasının getirdiği avantajlardır. BT sistemlerinin Ortak Kriterler değerlendirmesinden geçtiğinin sertifikalandırılması şirketler için pazarda büyük bir üstünlük sağlayacaktır. Çünkü bu sertifikasyon şu an için ABD, Almanya ve İngiltere başta olmak üzere yirmiden fazla ülkede kabul edilmektedir. Bu iki konu Ortak Kriterler standardı içerisinde anlatılmıştır.

Sistemlerin Ortak Kriterler'e uygun olarak değerlendirilmesinin ürün

değerlendirmesinden en büyük farkı, ürün değerlendirmelerinde ürünün kullanılacağı ortamın genel olarak tanımlanması ve detaylı olarak açıklanmamasıdır. Sistem değerlendirmesinde ise gerçek kullanım ortamının mutlaka düşünülmesi gerekmektedir. Bu şartlar altında sistem değerlendirmelerinde dikkat edilmesi gereken konular aşağıdaki gibi olmalıdır;[Tabuchi, 2002]

- a. Sistem değerlendirmelerinde fonksiyonel ve garanti gereksinimlerinin yanı sıra üçüncü bir güvenlik gereksinimi kümesi olarak güvenlik yönetim gereksinimleri oluşturulmalıdır. Sistem güvenliği için bilgi sınıflandırması, personel güvenliği, sistem erişiminin denetlenmesi ve iş devamlılığı yönetimi gibi güvenlik karşıt önlemleri eklenmelidir.
- b. Garanti paketleri sistemlerin geliştirme ve kullanım ortamlarının gereksinimleri baz alınarak düzenlenmelidir. Örneğin karşılanacak gereksinimler COTS (Commercial Off The Shelf) ürünlerinin değerlendirilmesini kapsarsa değerlendirmeler zorlaşacaktır. Ayrıca sızma testleri sistemlerinin güvenlik garantisi için kullanışlı ve uygulanabiliridir. Bu yüzden sistem değerlendirmelerinin varolan EAL'ler (Değerlendirme Garanti Düzeyi) yerine daha esnek, düşük maliyetli ve kısa sürecek garanti düzeylerine ihtiyacı vardır.
- c. Sistemlerin garantisinin devamı için garanti bakım yapısının oluşturulması gerekmektedir. Güvenlik ortamı her gün gerçekleşecek yamalarla değişken bir yapıdadır ve sistemin güvenlik hedefine uygunluğunun sürekli olarak doğrulanması garantinin bakımı ile gerçekleştirilir. Bu yüzden sistemin garantinin bakımının periyodik olarak nasıl gerçekleştirileceği tanımlanmalıdır.

Bu çalışmada Sis-TOE değerlendirme hedefi alınmış ve bu sistem için taşıdığı bilgi sınıfına uygun olarak güvenlik garanti paketleri oluşturulmuştur. Önerilecek yönetim gereksinimleri ile sistemin güvenlik hedefinin nasıl oluşturulması gerektiği ve nasıl değerlendirileceği incelenmiştir. Ayrıca garantinin devamının takip edilmesi için de önerilerde bulunulmuştur.

## 2 BİLGİ GÜVENLİĞİ ve ORTAK KRİTERLER

### 2.1 Bilgi Güvenliği [Karabacak, 2003]

Bilgi ve bilgi güvenliği uluslararası standart olan ISO 17799'da şu şekilde tanımlanmaktadır. “Bilgi, diğer önemli ticari varlıklar gibi, bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken bir varlıktır. Bilgi güvenliği bilgiyi gizliliğini, bütünlüğünü ve süreklilik sağlamak, ve yatırımların dönüşünü en üst seviyeye çıkartmak için geniş tehlike ve tehlike alanlarından korur.”[ISO 17799, 2002]

Varlık, ise risk yönetimi çerçevesinde, ‘korunması gereken her şey’ olarak tanımlanmaktadır. Varlıklar, bilgi sistemlerinde kıymete sahip olan elemanlardır. Bir organizasyonun varlıkları düzgün bir risk yönetimi yapılabilmesi için sınıflandırılmalıdır. Varlık sınıflandırması, donanım, yazılım, veri, politikalar ve prosedürler ile kurum çalışanları şeklinde yapılabilmektedir. Bu beş ana kategoriye girmeyen varlıklar da mevcuttur. Kurumun prestiji buna bir örnektir. Bir kurumun web sayfasının kırılması web sunumcu varlığından çok kurumun prestiji varlığına zarar verebilir.

Bu varlık kategorilerine aşağıdaki gibi örnekler verilebilir:

Donanım varlıkları bilgisayarlar, yazıcılar, alt yapı elemanları şeklinde sıralanabilir. Yazılım varlıkları ise bu donanımların üstünde çalışan her türlü programlardır. İşletim sistemleri, uygulama yazılımları ve iletişim protokolleri yazılım varlıklarına örnektir. Veri varlıklarına örnek ise tüm taşınır ve taşınmaz medyalar üzerindeki kullanıcı ve kurum bilgileridir. Politika ve prosedürler bir kurumun bilgi güvenliği yasalarıdır. Kurumun güvenliği bu politika ve prosedürler baz alınarak sağlanır. Kurum çalışanları önemli bir varlık kategorisidir. Bir kurumdaki bilgi sistemlerini yöneten ya da kullanan öğelerdir. Kurum hakkında en doğru ve en yeni bilgiye sahiptirler.

Bilgi Teknolojileri güvenliğinden bahsedilirken kast edilen tüm bu varlıkların

tehditlere karşı korunması, bilgilerin ise gizlilik, bütünlük ve süreklilik özelliklerinin sağlanmasıdır.

Tehdit kavramını incelerken ilk olarak üzerinde durulması gereken konu açıklıklardır. Açıklık, bir varlığı tehditlere karşı korumasız hale getiren kusurlar olarak tanımlanabilir. Tehditler bu açıklıkları kullanarak bilgi teknolojileri varlıklarına zarar verebilir.

Tehditler bir varlıktaki açıklıkları kullanarak varlığa kısmen ya da tamamen zarar veren etkenlere verilen addır. Tehditler doğal tehditler, kasıtsız ve kasıtlı tehditler olarak üçe ayrılabilir.

Bilgi Teknolojileri sistemlerinde, güvenlik mekanizmalarının koruması gereken üç ana güvenlik amacı, gizlilik, bütünlük ve sürekliliktir.<sup>4</sup> Tehdit, bu üç elementten en az birine zarar veren ya da verme ihtimali bulunan etkenlerdir. Tehdidin sonucunda, para, üretim, güven ve verimlilik kayıpları olur.

Tehditlerin verdiği zararı sıfırlamak ya da azaltmak amacıyla alınan tedbirlere karşı önlem denir. Güvenlik yamaları, güvenilir ürünler kullanılması, güvenlik politikalarının yazılması ve uygulanması, konfigürasyon düzenlemeleri, tasarım, güvenlik yazılımları, yeni donanımların alınması, eğitimler, kişilere sorumluluk yükleme, gözetleme ve denetleme karşı önlem içerisinde sayılabilir. Sonuç olarak bütün bu örnekler tehdidin zararını azaltan faktörlerdir.

Karşı önlem sadece açıklığın kapatılmasını önermez. Açıklığın kapatılması yanında, varlığın değerinin düşürülmesi ya da tehdidin azaltılması da karşı önlemlerdir. Sonuç olarak, bu üç tip karşı önlemin amacı tehdidin verdiği zararı azaltmak yani riski düşürmektir. Açıklığı azaltmaya örnek olarak yazılım yamaları verilebilir, varlığın değerinin düşürülmesine örnek şifrelemedir. Tehdidin azaltılmasına örnek ise, kurum çalışanlarının eğitilmesidir. Kurum çalışanları kurumdaki yazılım ve donanım varlıkları için birer kasıtsız tehdit olabildiğinden dolayı eğitim bu tehdidi düşürecektir.

---

<sup>4</sup> confidentiality, integrity, availability

Tehditler bilgi güvenliğinin üç temel amacına karşı yapılmaktadır. Bu güvenlik amaçları aşağıdaki gibidir:

*Gizlilik:* Kişisel gizlilik ve tescilli bilgiler de dahil olmak üzere bilgiye erişimin ve bilginin dağıtımının üzerindeki yetkili kısıtlamaların korunması ve bilgiye sadece yetkili erişimin garanti edilmesidir.

*Bütünlük:* Bilginin kaynağının inkar edilememesinin ve doğrulanmasının sağlanması, ve bilginin uygunsuz bir şekilde değiştirilmesine veya yok edilmesine karşı korunmasıdır.

*Süreklilik:* Bilgiye zamanında ve güvenilir bir ulaşımın sağlanması ve bilginin kullanılabilirliğinin sürekliliğinin sağlanmasıdır.

Özet olarak bilgi güvenliği organizasyonların varlıklarının açıklıklardan kaynaklanan tehditlere karşı güvenlik amaçlarının sağlanması ile korunmasıdır.

## 2.2 Ortak Kriterler

Bu bölümde ilk olarak Ortak Kriterler standardının tarihçesinden bahsedilmiştir. Ardından standardın kapsamının ve kullanımının gösterileceği bölümde Ortak Kriterler detaylarıyla incelenmiştir. Bir sonraki bölümde ise standardın nasıl uygulandığı, standarda uygun test metodolojilerinin nasıl gerçekleştirildiği belirtilmiş ve son olarak Common Criteria Recognition Arrangement (CCRA) ve Ortak Kriterler yapısı anlatılmıştır.

Ortak Kriterler birbirleriyle ilişkili üç ayrı bölümden oluşmaktadır.

**Bölüm 1, Giriş ve Genel Model,** Ortak Kriterler'e giriş niteliğindedir. Bu bölüm BT güvenlik değerlendirmelerinin temel konsept ve prensiplerini tanımlar niteliktedir ve genel bir değerlendirme modeli sunmaktadır. Bölüm aynı zamanda BT güvenlik hedeflerinin oluşturulması, BT güvenlik gereksinimlerinin seçilmesi ve tanımlanması, ve ürünlerin veya sistemlerin üst düzey spesifikasyonlarının yazılması konusunda bilgiler içermektedir. Ayrıca standardın bütün bölümlerinin bütün potansiyel kullanıcılar için nasıl kullanılacağı bu bölümde tanımlanmaktadır.

**Bölüm 2, Güvenlik Fonksiyonel Gereksinimleri**, değerlendirme hedefinin güvenlik fonksiyonel gereksinimlerinin standart bir dille anlatılabilmesini sağlamak için tanımlanmış olan güvenlik fonksiyonel bileşenleri kümesi bu bölümde listelenmektedir. Standardın ikinci bölümü fonksiyonel bileşenlerini, ailelerini ve sınıflarını kataloglar halinde tanımlamaktadır.

**Bölüm 3, Güvenlik Garanti Gereksinimleri**, değerlendirme hedefinin güvenlik garanti gereksinimlerinin standart bir dille anlatılabilmesini sağlamak için tanımlanmış olan güvenlik garanti bileşenleri kümesi bu bölümde listelenmektedir. Standardın üçüncü bölümü garanti bileşenlerini, ailelerini ve sınıflarını kataloglar halinde tanımlamaktadır. Bu bölüm aynı zamanda Koruma Profillerinin ve Güvenlik Hedeflerinin değerlendirme kriterlerini ve değerlendirme garanti seviyelerini oluşturan garanti bileşenlerini de içermektedir. [ISO 15408, 1999]

Ortak Kriterler'in bu üç bölümünün desteklenmesi açısından teknik gerekçeleri ve kılavuz dokümanlarını da içeren dokümanlar yayınlanmıştır<sup>5</sup>.

### 2.2.1 Tarihçesi

Bilgi Teknolojileri kullanıcıları arasında yapılan araştırmalar göstermektedir ki bu kullanıcılar satın aldıkları ürün için satıcının garanti ettiği güvenlik düzeyine güvenmek istemiyorlar. Aynı zamanda bu ürünlerin güvenlik testlerini kendileri de yapmak istemiyorlar. Çözüm olarak bağımsız bir üçüncü şahsın, BT ürünlerini analiz etmesini ve testler aracılığıyla güvenlik garanti düzeyini belirlemesini istiyorlar. Bu gereksinim ülkelerin kabul ettiği güvenlik kriterlerine uygun olarak testler yapan laboratuvarların kurulmasını sağlamıştır. Bu test laboratuvarları önceleri her ülkede o ülkenin kabul ettiği güvenlik kriterlerini kullanarak testler yapmaktaydılar. Amerika'da Savunma Bakanlığının hazırladığı TCSEC yani Trusted Computer Security kullanılırken, Avrupa ülkeleri TCSEC'i temel alarak ITSEC'i yani Information Technology Security kullanmaya başladılar. Bu iki standart devletlerin kullanacakları BT ürünleri için yeterli olmaktaydı. Fakat BT ürünlerinin ülkeler arasındaki ticareti artmaya başladıkça ortak bir kritere ihtiyaç duyuldu.

---

<sup>5</sup> [www.commoncriteriaportal.org](http://www.commoncriteriaportal.org)

Çünkü farklı ülkelerde ürününü satan bir üretici için hem ITSEC sertifikası hem de TCSEC sertifikası almak uzun sürmekte ve masraflı olmaktadır. Bunun yanı sıra TCSEC ve ITSEC standartları askeri projeler için geliştirilmişti ve özel sektörün ihtiyaçlarına cevap verebilecek nitelikte değildi. Bu sebeplerden dolayı ülkeler ortak bir standart geliştirmek için çalışmaya başladılar. CC bu çalışmalar sonucunda geliştirildi. [Donaldson, 2002]

İlk olarak ABD'nin TCSEC, Avrupa'nın ITSEC ve Kanada'nın CTCPEC standartları birleştirilerek 1996 yılının Ocak ayında ilk versiyon yayınlandı. Bu versiyonun geliştirilmesi için ABD, Kanada, İngiltere, Almanya, Fransa, Avustralya ve Yeni Zelanda ülkeleri çalışmıştır. [List, 1997] Mayıs 1998'de yapılan değişikliklerin ardından 2.0 versiyonu yayınlandı ve aynı yılın Haziran ayında ISO Ortak Kriterler'i ISO 15408 numarasıyla uluslararası standart olarak kabul etti. Son olarak ağustos ayında yapılan değişikliklerin ardından şu anki versiyonu yani v2.1 yayınlandı. Halen geliştirilmekte olan standardın 2004 yılında yapılan değişikliklerin onaylanmasının ardından yeni bir versiyonu daha çıkarılacaktır.

Görüldüğü üzere Ortak Kriterler halen geliştirme aşamasında olan çok yeni bir standarttır. Bu standardı tanıyan ülkelerin sayısı her geçen gün artmakta ve BT güvenliği alanında uluslararası geçerliliği olan bir standart olma yolunda hızla ilerlemektedir.

## 2.2.2 Kapsamı ve Kullanımı

Ortak Kriterler'in iki temel kullanımı vardır. Bunlardan ilki ulusal ve uluslararası sınırlarda yapılan değerlendirmeler arasında karşılaştırılabilirlik sağlamasıdır. Yani iki farklı ürünün fonksiyonlarının Ortak Kriterler'e uygun değerlendirmesinin sonuçları birbirleri ile kolayca karşılaştırılabilir. Bunun nedeni, değerlendirmeler sırasında ürünün karşıladığı özelliklerin Ortak Kriterler'de tanımlanmış geniş kapsamlı, kendi içinde tutarlı, belirli bağımlılıklara ve hiyerarşik bir yapıya sahip fonksiyonel gereksinimlerle (SFRs) gösterilmesidir. Bu gereksinimler Ortak Kriterler'in ikinci kitabında yer almaktadır. Ortak Kriterler'in diğer bir faydası da kullanıcılara ihtiyaç duydukları garanti gereksinimlerini ürünün

yerine getirdiğinin garantisini sağlamasıdır. Bu garanti Ortak Kriterler'in üçüncü kitabında tanımlanan kendi içinde tutarlı ve bağımlılıkları olan güvenlik garanti gereksinimlerinden (SARs) hangilerinin ürün tarafından karşılandığının ve hangilerinin karşılanmadığının incelenmesi sonucunda sağlanır. [Shi, 2001]

Ortak Kriterler'in teoride tüketiciler, ürün geliştiriciler, değerlendiriciler ve sponsorlar olmak üzere 4 temel kullanıcısı vardır. Fakat ürün geliştiriciler genelde sponsorluk işini de yaptıkları için üç tip kullanımdan bahsedebiliriz.

Tüketiciler; Ortak Kriterler'i istedikleri güvenlik özelliklerini sağlayan ürünler talep edebilmeleri için rehber olarak kullanırlar. Ayrıca sertifikalı ürün kütüphanesinden faydalanıp isteklerini karşılayan ürün olup olmadığını kontrol edebilirler.

Ürün geliştiriciler; ürünün tasarımından piyasaya çıkışına kadar olan süreci boyunca gerekli güvenlik özelliklerini sağlaması için Ortak Kriterler'i rehber olarak kullanabilirler.

Değerlendiriciler; BT ürünlerini Ortak Kriterler standardına göre değerlendirirken temel kaynak olarak kullanırlar.

Sponsorların yapması gereken ürün değerlendirmesi esnasında geliştirici ile değerlendirici arasında ki iletişimi sağlamak ve değerlendirme sürecine maddi olarak sponsor olmaktır. Fakat başta da belirtildiği gibi sponsorluk işini de genelde ürün geliştiriciler yapmaktadır.

Ortak Kriterler üç bölümden oluşmaktadır. Birinci bölüm, Giriş ve Genel Model, Ortak Kriterler'in genel kavramlarını güvenlik hedef ve gereksinimlerinin neler olduğunu tanımlayan bir kılavuздur. Ayrıca Security Target(ST) ve Protection Profile(PP)'ın içeriğide bu bölümde yer alır. İkinci bölüm SFR'ları yani güvenlik fonksiyonel gereksinimlerini listeleyen bir referans kitabıdır. Üçüncü bölüm ise güvenlik garanti fonksiyonlarını listeler. Ayrıca bu bölümde garanti seviyeleri ve bu seviyelerin içermesi gereken garanti aileleri gösterilmektedir.

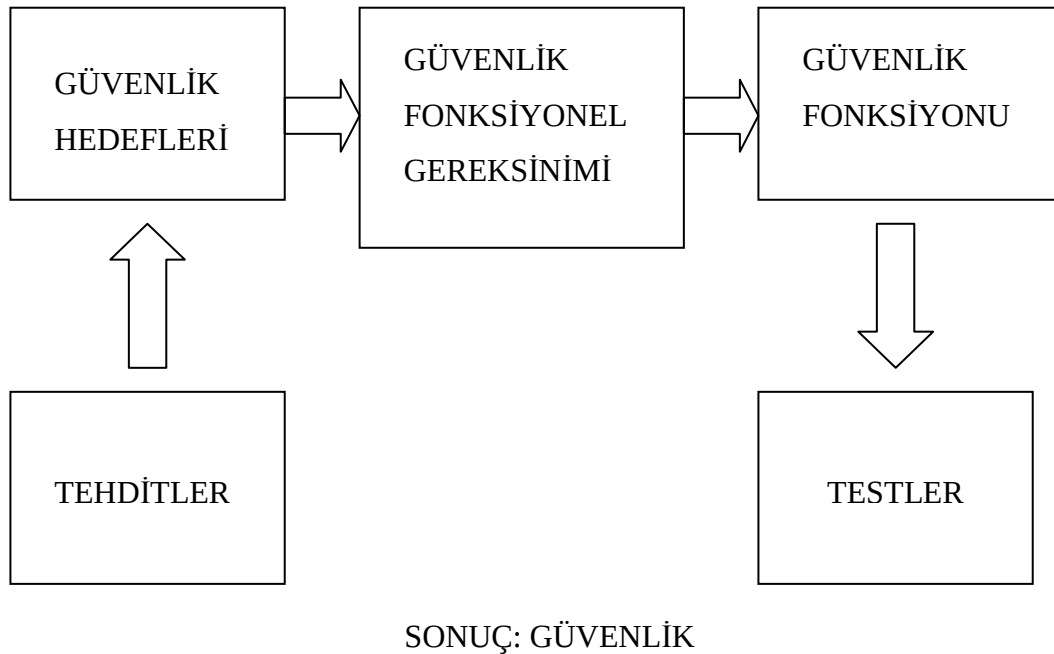
Ortak Kriterler'in iki temel ögesi olan ST ve PP'lerin ve TOE'nin tanımları aşağıdaki gibidir.

**TOE:** (Target of Evaluation) Değerlendirme ögesi olan sistem veya ürüne verilen ismin kısaltmasıdır.

**PP :** (Protection Profile) Bir TOE sınıfı için üründen bağımsız olarak, istenen güvenlik gereksinimlerinin tanımlandığı dokümana verilen isimdir.

**ST:** (Security Target) Ürüne bağımlı olarak yazılan ve ürünün güvenlik özelliklerinin tanımlandığı dokümandır.

PP ve ST'ler Ortak Kriterler değerlendirmelerinin temel öğeleridir. PP'ler müşteriler tarafından yazılır ve ihtiyaç duyulan bir BT ürünü için gereksinimler belirtilir. ST'ler ise ürünü geliştiren firma tarafından ürün Ortak Kriterler değerlendirmesine girmeden önce hazırlanan ve ürünün hangi güvenlik özelliklerini ve hangi güvenlik seviyesini garanti ettiğinin belirtildiği dokümandır. İkisi de eşleştirme mantığı kullanılarak hazırlanır. **Şekil 2.1 Ortak Kriterler'de güvenliğin sağlanması**'de bu eşleştirme mantığını açıklamaktadır.



Şekil 2.1 Ortak Kriterler'de güvenliğin sağlanması

Bu dokümanlarda ilk olarak ürüne olabilecek tehditler, politikalar ve kabullenmeler çıkartılır ve ortam tanımlandıktan sonra tehditleri ve politikaları karşılamak için güvenlik amaçları belirlenir. Bu güvenlik amaçları gerçekleştirmek için gerekli fonksiyonel gereksinimler Ortak Kriterler'in ikinci bölümü kullanılarak hazırlanır. Daha sonra fonksiyonel gereksinimleri ürünün hangi fonksiyonlarının nasıl yerine getirdiği dokümante edilir. Bu güvenlik fonksiyonlarının tehditleri karşılayıp karşılamadığı kontrol edilir ve eğer karşılıyorsa ürünün iddia ettiği güvenliği sağladığı sonucuna varılabilir. Değerlendirici bir ST'yi veya PP'yi incelerken bütün bu eşleştirmelerin doğruluğunu kontrol eder. Ayrıca spesifik bir ürün, ST'si ile birlikte değerlendirirken bütün fonksiyonların çalışıp çalışmadığını ve bütün tehditlerin karşılanıp karşılanmadığını kontrol eder. Sonuç olarak ürün değerlendirici testlerinden geçmişse iddia ettiği güvenliği sağladığına karar verilir. Bir sonraki aşama ürünün iddia ettiği garanti seviyesine uygunluğunu incelemektir.

### 2.2.3 Değerlendirme Metodolojisi

Ortak Kriterler standardına uygun olarak değerlendirme yapılabilmesi için standardı hazırlayan ülkeler birde değerlendirme metodolojisi hazırlamışlardır. CEM (Common Evaluation Methodology) adı verilen bu kılavuz PP, ST ve TOE değerlendirmelerinin nasıl yapılacağını adım adım anlatmaktadır. Değerlendirmeyi yapan laboratuvar bu metodolojiye uygun davranmak zorundadır. Aksi halde yaptığı değerlendirmelerin uluslararası geçerliliği olmaz.

Ürünün ST'si değerlendirilip onaylandıktan sonra TOE değerlendirilmeye başlanır. Standarda göre yedi farklı değerlendirme seviyesi vardır. EAL1 ve EAL2 düşük garanti seviyeleridir. EAL3 ve EAL4 orta düzeyde garanti sağlayan ürünlere verilen seviyelerdir. EAL5 ve EAL6 yüksek derecede garanti veren seviyelerdir. EAL7 ise tam anlamıyla dört dörtlük garanti düzeyi sağlar. ST yazılırken üretici talip olduğu garanti düzeyini ve ürünün sağladığı garanti gereksinimlerini belirtir. Değerlendiricinin kontrol etmesi gereken sağlanan garanti gereksinimlerinin talip olunan garanti düzeyi için yeterli olup olmadığını ve bu gereksinimlerin doğruluğunu kontrol etmektir. [CEM, 1999]

Değerlendirici TOE'nin değerlendirilmesi sırasında birtakım dokümanları üreticiden talep eder. Bunlara değerlendirme delilleri adı verilir. Üretici bu dokümanları değerlendiriciye sağlamak zorundadır.

Metodolojiye uygun olarak değerlendirilen ürün değerlendirme teknik raporu ile birlikte ürüne uluslararası Ortak Kriterler sertifikasını verecek olan sertifikasyon kurumuna gönderilir.

#### **2.2.4 CCRA ve Ortak Kriterler Yapısı**

Standardı oluşturan ülkeler birde karşılıklı tanıma sözleşmesi imzalamışlardır. Bu sözleşmenin amacı bu ülkelerden herhangi birinde yapılan değerlendirmenin diğer ülkeler tarafından da tanınmasını sağlamaktır. Sözleşmeyi iki şekilde imzalamak mümkündür. Bunlardan ilki sözleşmeyi sertifika müşterisi olarak imzalamaktır. CCRA'i (Common Criteria Recognition Arrangement) sertifika müşterisi olarak imzalayan ülkenin uluslararası tanınabilecek sertifika üretme yetkisi yoktur, ülke sadece bu yetkiye sahip diğer ülkelerin sertifikalarına müşteri olabilmektedir.[Olthoff, 2000] 1999 yılından itibaren CCRA'yi bu şekilde imzalayan ülke sayısı onikiyi bulmuştur. Diğer bir imzalama seçeneği de sertifika üreticisi olarak imzalamaktır. Bu durumda ülke Ortak Kriterler değerlendirmeleri yapabilmekte ve ürettiği sertifikalar üye ülkelere tanınmaktadır. CCRA sözleşmesini sertifika üreticisi olarak imzalayabilmek için ülkede kurulmuş ve çalışan bir Ortak Kriterler yapısını göstermek mecburiyeti vardır. Ortak Kriterler yapısının temel taşı sertifikasyon kurumudur. Bu kurum değerlendirmeleri yapacak olan bağımsız laboratuarlara değerlendirme lisanslarını verir ve bütün değerlendirmeler sırasında denetleme görevini yerine getirir. Ayrıca değerlendirme sonucunda değerlendirme teknik raporunu inceler ve başarılı ürünlere Ortak Kriterler sertifikalarını verir. Sertifikasyon kurumu ülkenin güvencesiyle devlete bağlı bir kurumun altında çalışır. Kurumun ürettiği bütün sertifikalardan ülke sorumludur. Sertifikasyon kurumu ülkede Ortak Kriterler yapısını oluşturmaya başlar. Lisans verme prosedürleri de dahil olmak üzere Ortak Kriterler değerlendirmeleri için gerekli bütün prosedürleri tanımlar ve şeffaf olarak çalışır. Yapının diğer önemli bölümü de bağımsız test laboratuvarlarıdır. Sertifikasyon kurumunun denetiminde

çalışırlar ve çalıştıkları yapının bütün kurallarına uyma zorunlulukları vardır. Genel olarak Ortak Kriterler yapısı dendiğinde sertifikasyon kurumu, bağımsız laboratuvarlar ve bu kurumlar arasındaki ilişkiler anlaşılabilir. [Kondakçı, 2003]

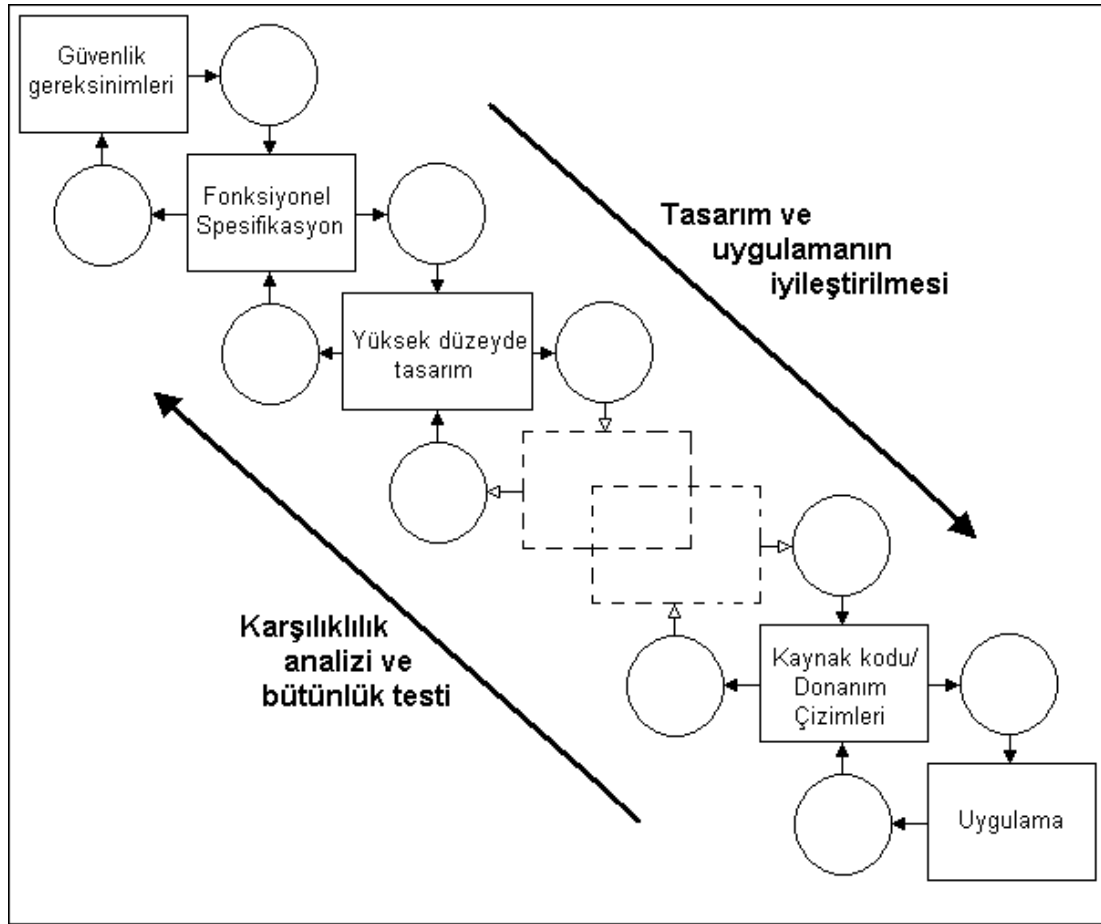
## 2.3 Ortak Kriterler’e Uygun Ürün Değerlendirmesi

Ortak Kriterler standardı güvenlik gereksinimleri göz önüne alınarak ürün geliştirilebilmesi için tasarım aşamasından itibaren uyulması gereken bir metodoloji önermektedir. Ürün değerlendirilmesinde ise bu aşamalar karşılık analizleri ve bütünlük testleri ile doğrulanmakta ve müşterilerin ürün konusunda ihtiyaç duyduğu güvenliğe ve garantiye sahip olmasını sağlamaktadır.

Standardın önerdiği tasarım aşamaları bölüm 2.2.2 de anlatıldığı gibi güvenlik gereksinimlerini tespit ettikten sonra her bir güvenlik gereksinimi için iç ve dış etkileşimleri de içerecek bir fonksiyonel spesifikasyon oluşturmakla başlamaktadır. Ardından bu fonksiyonel spesifikasyonda garanti seviyesine göre biçimsel veya biçimsel olmayan metodlarla tanımlanan güvenlik fonksiyonlarının üst düzey tasarımları hazırlanmalıdır. Bu tasarımın ardından her bir güvenlik fonksiyonunun detaylı bir şekilde tasarımının gösterileceği alt düzey tasarım dokümantasyonu oluşturulmalı ve bu alt düzey tasarıma uygun olarak kaynak kodu ve/veya donanım çizimleri oluşturulmalıdır. Son olarakta bu çizimler uygulanarak ürün geliştirilmelidir.

Ortak Kriterler’e uygun olarak ürün değerlendirme gerçekleştirilirken değerlendiren kurum ürün geliştiriciden bu adımlara uygun olarak tasarımı ve uygulamayı gerçekleştirdiğine dair değerlendirme kanıtları talep etmektedir. Özellikle EAL4 ve üzerindeki garanti seviyelerinde bu adımların tamamına uygun olarak ürün geliştirilmesi gerekmektedir. Fakat EAL3 ve altındaki seviyelerde bu adımlara uygunluk kısmen daha az aranmaktadır.

**Şekil 2.2. Ortak Kriterler’e uygun ürün geliştirme adımları**’de Ortak Kriterler’e uygun olarak ürün geliştirilmesinde ve bu ürünlerin değerlendirme delillerinden olan geliştirme delillerinde gerekli olan adımlar gösterilmektedir.

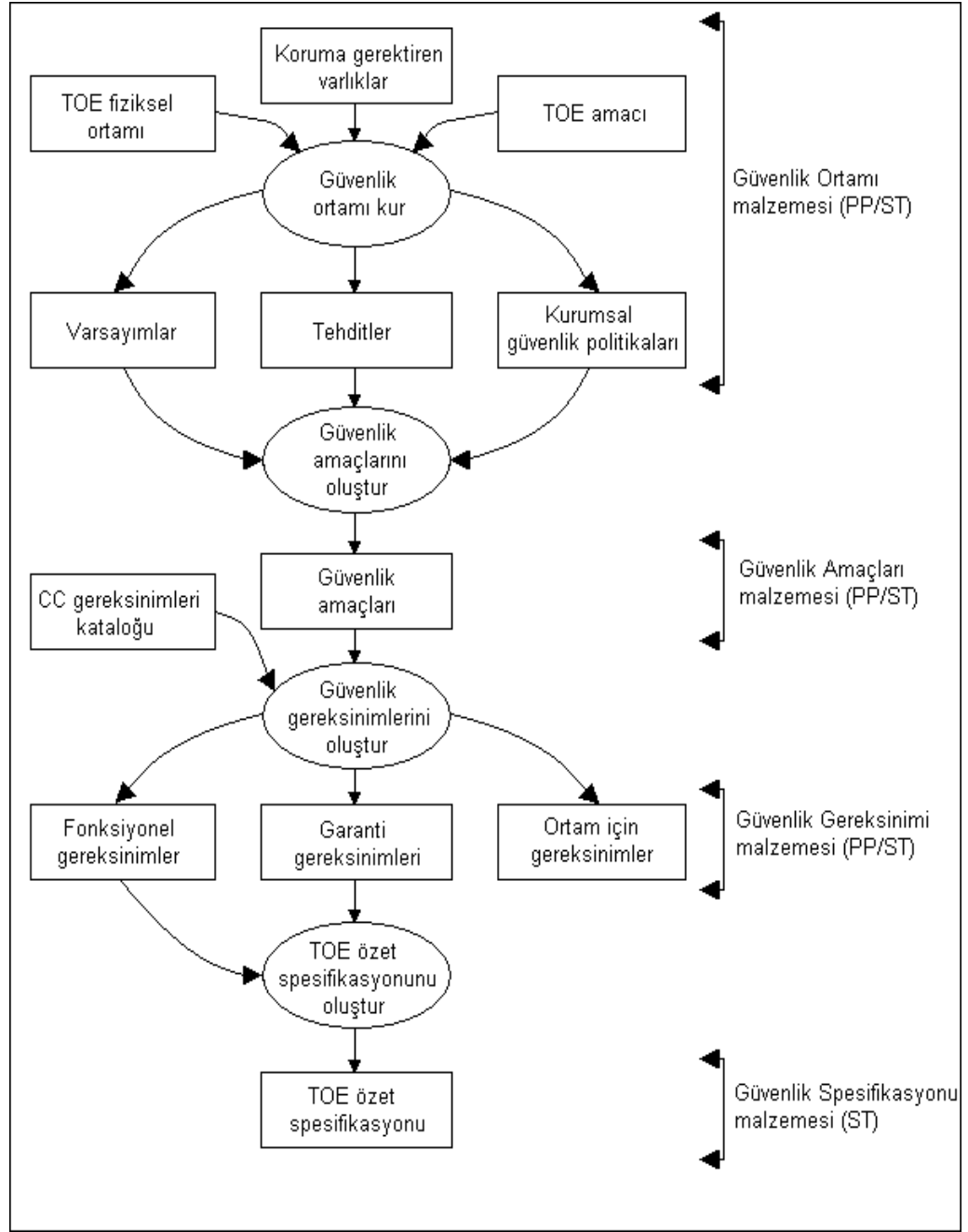


Şekil 2.2. Ortak Kriterler'e uygun ürün geliştirme adımları [ISO 15408, 1999]

Ortak Kriterler'e uygun olarak ürün değerlendirmelerinde gerçekleştirilen ilk adım ürünün Güvenlik Hedefi dokümanının değerlendirilmesi olmaktadır. Güvenlik Hedefi üreticinin geliştirdiği ürün için hazırlaması gereken ve ürünün güvenlik ve garanti özelliklerini tanımladığı dokümandır.

Bu doküman oluşturulurken ilk olarak ürünün koruması gereken varlıklar, TOE'nin fiziksel ortamı ve TOE'nin amacı göz önüne alınarak güvenlik ortamı tanımlanmalıdır. Sonraki adımda ise bu güvenlik ortamına olabilecek tehditler, bu ortam ile ilgili kabullenmeler ve organizasyonel güvenlik politikaları ürün geliştiricisi tarafından belirlenmelidir. Ortam ile ilgili tehditlerin, kabullenmelerin ve organizasyonel kurum politikalarının tespit edilmesinin ardından güvenlik amaçları ve bu amaçları karşılayabilmek için güvenlik fonksiyonel gereksinimleri ile güvenlik garanti gereksinimleri ve ortak için gereksinimler çıkartılmalıdır. Son olarak bütün bu gereksinimlerin karşılanabilmesi için ürün spesifikasyonu çıkartılır ve bu adımlar arasındaki eşleştirmelerin gerekçeleri belirtilir. **Şekil 2.3. Güvenlik Hedefi**

**dokümanının hazırlanış aşamaları**'de Güvenlik Hedefi dokümanının hazırlanış aşamaları adım adım gösterilmektedir.



Şekil 2.3. Güvenlik Hedefi dokümanının hazırlanış aşamaları [ISO 15408, 1999]

### 2.3.1 Güvenlik Hedefi Değerlendirmesi

Bu yapının oluşturulmasındaki adımlar aşağıdaki gibidir;

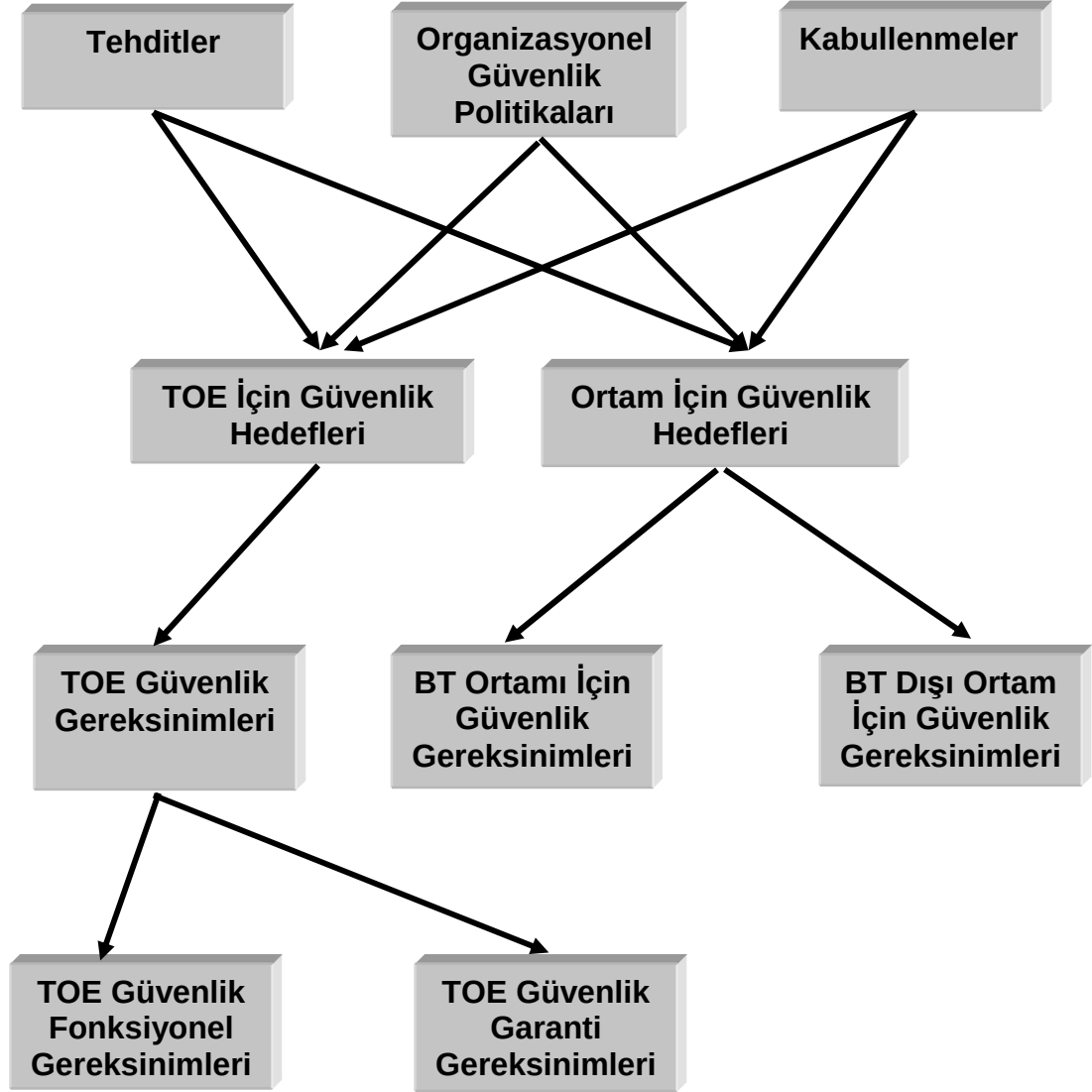
1. Ürünün çalıştığı ortamın tanımlanması gerekmektedir. Bu tanımlamalarda cevap verilmesi gereken sorular bulunmaktadır.

Bunlardan bazıları;

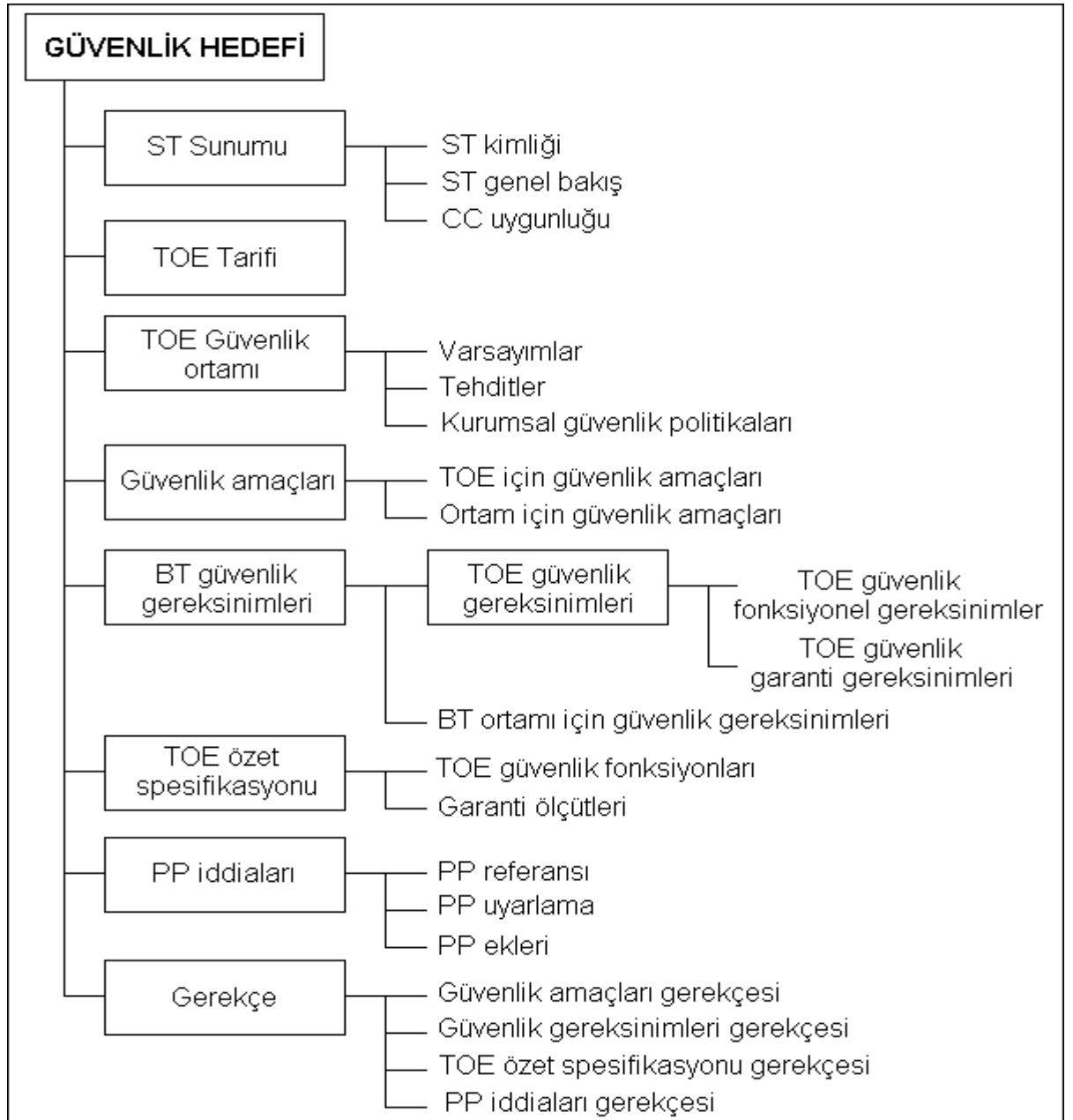
- a. Ürünün koruma sağlaması gereken varlıklara karşı ne gibi tehditler bulunmaktadır?
  - b. Bu ortam hakkında ne gibi kabullenmeler yapılabilir?
  - c. Ortamda geçerli olan politikalardan (kanunlar veya kurumsal politikalar) hangilerine ürünün uyması gerekmektedir.
2. Varlıkların korunması gereken tehditlerin karşılanması için spesifik amaçların belirlenmesi gerekmektedir. Amaçlar belirlenmiş tehditlerin basit olarak olumsuz karşılıkları olmamalı, uygulanabilir ve istenen sonuçları verebilir nitelikte olmalıdır. ST'nin kapsamı bu aşamada belirginleşmektedir. Amaçlar, TOE (değerlendirilen ürün) tarafından karşılanacak olanlar, BT ve BT dışı ortam tarafından karşılanacak olanlar ve bu ikisinin bileşimi sonucu karşılanacak olanlar olmak üzere üç kısma ayrılır.
  3. Ürün için, ve ortamdaki diğer BT ürünleri için tespit edilmiş her bir güvenlik amacını karşılayacak fonksiyonelliği belirlemek için Ortak Kriter standardının ikinci bölümünde bulunan Güvenlik Fonksiyonel Gereksinimleri kataloğu kullanılmalıdır. Standardın ikinci bölümündeki genel gereksinimlerin yetersiz kaldığı durumlarda standardın tanımladığı işlemler yapılmalıdır. Ayrıca ihtiyaç duyulan bir gereksinimin ikinci bölümde tanımlanmadığı durumlarda gereksinim formatına uygun olarak yeni bir bileşen tanımlanabilmektedir.
  4. Amaçların karşılanacağına dair gerekli garantinin sağlanması için Ortak Kriter standardının üçüncü bölümündeki Güvenlik Garanti Gereksinimleri kullanılır. İhtiyaç duyulan gereksinimleri Ortak Kriterler standardının üçüncü bölümündeki Garanti Gereksinimleri kataloğundan seçilmeli ve bir garanti paketi oluşturulmalıdır veya daha önceden belirlenmiş bir paketi (EAL paketleri) kullanılabilir, veya bu iki yaklaşımın bir birleşimi ST'de uygulanabilir.
  5. Tespit edilen Güvenlik Fonksiyonel Gereksinimlerin üründe hangi güvenlik fonksiyonları ile uygulandığı ve Güvenlik Garanti Gereksinimleri için hangi garanti tedbirlerinin alındığı da belirtilmelidir.
  6. Son bölümde ise seçilen fonksiyonel ve garanti gereksinimleri bileşenlerinin ürünün kullanılacağı ortamdaki tehditleri nasıl

karşıladığına dair ve güvenlik fonksiyonları ile garanti tedbirlerinin bu gereksinimleri nasıl karşıladığına dair gerekçeler belirtilmelidir..

Şekil 2.4. Güvenlik Hedefi Organizasyonu’de Güvenlik Hedefi dokümanının organizasyonu ve Şekil 2.5. Güvenlik Hedefi içeriği’de bu dokümanın içermesi gereken bölümler detaylı olarak gösterilmektedir.



Şekil 2.4. Güvenlik Hedefi Organizasyonu



Şekil 2.5. Güvenlik Hedefi içeriği [ISO 15408, 1999]

Bir ürünün Güvenlik Hedefinin değerlendirilmesi sırasında yukarıda belirtilen altı maddenin Güvenlik Hedefi'nde *bütün, anlaşılabilir ve tutarlı*<sup>6</sup> bir şekilde uygulandığı öncelikli olarak kontrol edilir. Bu kontrollerden sonra ürünün Güvenlik Hedefi, Ortak Kriterler Değerlendirme Metodolojisinde belirtilen değerlendirme eylemlerine tabi tutularak değerlendirilir. Güvenlik Hedefinin başarılı sayılabilmesi ve ürünün bu Güvenlik Hedefine uygun olarak değerlendirilebilmesi için bu bölümdeki bütün eylemlerden “Geçti” sonucu alması gerekmektedir.

<sup>6</sup> Ortak Kriterler standardı bütünlük, anlaşılabilirlik ve tutarlılık kavramını tanımlamaktadır.

### 2.3.2 EAL1 Değerlendirmesi

*Eğik Harfler:* Bir önceki seviyeye göre belirgin eklemeler veya değişiklikler.

Çizelge 2.1 EAL1 garanti gereksinimleri

|                                                                                                      |                  |
|------------------------------------------------------------------------------------------------------|------------------|
| <b>EAL 1 fonksiyonel olarak test edilmiş</b>                                                         |                  |
| <b><u>EAL1 düzeyindeki sınıflar, aileler, bileşenler ve elementler</u></b>                           |                  |
| <b>(A)</b>                                                                                           |                  |
| <b>ACM_CAP.1</b>                                                                                     |                  |
| ACM = Konfigürasyon Yönetimi   CAP = Yetenekler<br>1 = Versiyon numaraları                           |                  |
| <b>Bağımlılıklar:</b> Yok                                                                            |                  |
| <b>(B)</b>                                                                                           |                  |
| <b>ADO_IGS.1</b>                                                                                     |                  |
| ADO = Dağıtım ve İşletim   IGS = Kurulum ve başlatım<br>1 = Kurulum ve başlatım prosedürleri         |                  |
| <b>Bağımlılıklar</b>                                                                                 |                  |
| <b>(B.1) = (E)</b>                                                                                   | <b>AGD_ADM.1</b> |
| <b>(C)</b>                                                                                           |                  |
| <b>ADV_FSP.1</b>                                                                                     |                  |
| ADV = Geliştirme   FSP = Fonksiyonel spesifikasyon<br>1 = Biçimsel olmayan fonksiyonel spesifikasyon |                  |
| <b>Bağımlılıklar</b>                                                                                 |                  |
| <b>(C.1) = (D)</b>                                                                                   | <b>ADV_RCR.1</b> |
| <b>(D)</b>                                                                                           |                  |
| <b>ADV_RCR.1</b>                                                                                     |                  |
| ADV = Geliştirme   RCR = Temsilin karşılaştırılması<br>1 = Biçimsel olmayan karşılaştırma gösterimi  |                  |
| <b>Bağımlılıklar:</b> Yok                                                                            |                  |

|                                                                                |                  |
|--------------------------------------------------------------------------------|------------------|
| <b>(E)</b>                                                                     |                  |
| <b>AGD_ADM.1</b>                                                               |                  |
| AGD = Kılavuz Dokümanları   ADM = Yönetici kılavuzu<br>1 = Yönetici kılavuzu   |                  |
| <b>Bağımlılıklar</b>                                                           |                  |
| <b>(E.1) = (C)</b>                                                             | <b>ADV_FSP.1</b> |
| <b>(F)</b>                                                                     |                  |
| <b>AGD_USR.1</b>                                                               |                  |
| AGD = Kılavuz Dokümanları   USR = Kullanıcı kılavuzu<br>1 = Kullanıcı kılavuzu |                  |
| <b>Bağımlılıklar</b>                                                           |                  |
| <b>(F.1) = (C)</b>                                                             | <b>ADV_FSP.1</b> |
| <b>(G)</b>                                                                     |                  |
| <b>ATE_IND.1</b>                                                               |                  |
| ATE = Test   IND = Bağımsız testler<br>1 = Bağımsız testler – uygunluk         |                  |
| <b>Bağımlılıklar</b>                                                           |                  |
| <b>(G.1) = (C)</b>                                                             | <b>ADV_FSP.1</b> |
| <b>(G.2) = (E)</b>                                                             | <b>AGD_ADM.1</b> |
| <b>(G.3) = (F)</b>                                                             | <b>AGD_USR.1</b> |

EAL1 seviyesinde gerçekleştirilen değerlendirmelerde yukarıda belirtilen bileşenler ve bu bileşenlerin bağımlılıkları değerlendirilecek olan ürüne uygulanmalıdır. Bu bileşenlerin nasıl uygulanacağı ve gerçekleştirilmesi gereken bütün değerlendirici eylemleri Ortak Kriterler Değerlendirme Metodolojisinde belirtilmektedir. Ürünün EAL1 değerlendirmesinden başarılı sayılabilmesi için buradaki bütün değerlendirme eylemlerinden “geçti” alması gerekmektedir.

### 2.3.3 EAL2 Değerlendirmesi

*Eğik Harfler:* Bir önceki seviyeye göre belirgin eklemeler veya değişiklikler.

Çizelge 2.2 EAL2 garanti gereksinimleri

|                                                                                                      |                  |
|------------------------------------------------------------------------------------------------------|------------------|
| <b>EAL 2 yapısal olarak test edilmiş</b>                                                             |                  |
| <b><u>EAL2 düzeyindeki sınıflar, aileler, bileşenler ve elementler</u></b>                           |                  |
| <b>(A)</b>                                                                                           |                  |
| <b>ACM_CAP.2</b>                                                                                     |                  |
| ACM = Konfigürasyon Yönetimi   CAP = Yetenekler<br>2 = Konfigürasyon elemanları                      |                  |
| <b>Bağımlılıklar:</b> Yok                                                                            |                  |
| <b>(B)</b>                                                                                           |                  |
| <b>ADO_DEL.1</b>                                                                                     |                  |
| ADO = Dağıtım ve İşletim   DEL = Dağıtım<br>1 = Dağıtım prosedürleri                                 |                  |
| <b>Bağımlılıklar</b>                                                                                 |                  |
| <b>(B.1) = (G)</b>                                                                                   | <b>AGD_ADM.1</b> |
| <b>(C)</b>                                                                                           |                  |
| <b>ADO_IGS.1</b>                                                                                     |                  |
| ADO = Dağıtım ve İşletim   IGS = Kurulum ve başlatım<br>1 = Kurulum ve başlatım prosedürleri         |                  |
| <b>Bağımlılıklar</b>                                                                                 |                  |
| <b>(C.1) = (G)</b>                                                                                   | <b>AGD_ADM.1</b> |
| <b>(D)</b>                                                                                           |                  |
| <b>ADV_FSP.1</b>                                                                                     |                  |
| ADV = Geliştirme   FSP = Fonksiyonel spesifikasyon<br>1 = Biçimsel olmayan fonksiyonel spesifikasyon |                  |

|                                                                                                            |           |
|------------------------------------------------------------------------------------------------------------|-----------|
|                                                                                                            |           |
| <b>Bağımlılıklar</b>                                                                                       |           |
| (D.1) = (F)                                                                                                | ADV_RCR.1 |
| (E)                                                                                                        |           |
| <b>ADV_HLD.1</b>                                                                                           |           |
| ADV = Geliştirme   <b>HLD</b> = Üst düzey tasarım<br>1 = Üst düzey tasarımın açıklanması                   |           |
| <b>Bağımlılıklar</b>                                                                                       |           |
| (E.1) = (D)                                                                                                | ADV_FSP.1 |
| (E.2) =(F)                                                                                                 | ADV_RCR.1 |
| (F)                                                                                                        |           |
| <b>ADV_RCR.1</b>                                                                                           |           |
| ADV = Geliştirme   <b>RCR</b> = Temsilin karşılaştırılması<br>1 = Biçimsel olmayan karşılaştırma gösterimi |           |
| <b>Bağımlılıklar: Yok</b>                                                                                  |           |
| (G)                                                                                                        |           |
| <b>AGD_ADM.1</b>                                                                                           |           |
| AGD = Kılavuz Dokümanları   <b>ADM</b> = Yönetici kılavuzu<br>1 = Yönetici kılavuzu                        |           |
| <b>Bağımlılıklar</b>                                                                                       |           |
| (G.1) = (D)                                                                                                | ADV_FSP.1 |
| (H)                                                                                                        |           |
| <b>AGD_USR.1</b>                                                                                           |           |
| AGD = Kılavuz Dokümanları   <b>USR</b> = Kullanıcı kılavuzu<br>1 = Kullanıcı kılavuzu                      |           |
| <b>Bağımlılıklar</b>                                                                                       |           |
| (H.1) = (D)                                                                                                | ADV_FSP.1 |

|                                                                                                                                         |           |
|-----------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>(I)</b>                                                                                                                              |           |
| <b>ATE_COV.1</b>                                                                                                                        |           |
| ATE = Test   COV = Kapsam<br>1 = Kapsamın delili                                                                                        |           |
| <b>Bağımlılıklar</b>                                                                                                                    |           |
| (I.1) = (D)                                                                                                                             | ADV_FSP.1 |
| (I.1) = (J)                                                                                                                             | ATE_FUN.1 |
| <b>(J)</b>                                                                                                                              |           |
| <b>ATE_FUN.1</b>                                                                                                                        |           |
| ATE = Test   FUN = Fonksiyonel testler<br>1 = Fonksiyonel testler                                                                       |           |
| <b>Bağımlılıklar: Yok</b>                                                                                                               |           |
| <b>(K)</b>                                                                                                                              |           |
| <b>ATE_IND.2</b>                                                                                                                        |           |
| ATE = Test   IND = Bağımsız testler<br>2 = Bağımsız testler – örnek                                                                     |           |
| <b>Bağımlılıklar</b>                                                                                                                    |           |
| (K.1) = (D)                                                                                                                             | ADV_FSP.1 |
| (K.2) = (G)                                                                                                                             | AGD_ADM.1 |
| (K.3) = (H)                                                                                                                             | AGD_USR.1 |
| <b>(L)</b>                                                                                                                              |           |
| <b>AVA_SOF.1</b>                                                                                                                        |           |
| AVA = Açıklık Değerlendirmesi   SOF = TOE güvenlik fonksiyonlarının gücü<br>1 = TOE güvenlik fonksiyonlarının gücünün değerlendirilmesi |           |
| <b>Bağımlılıklar</b>                                                                                                                    |           |
| (L.1) = (D)                                                                                                                             | ADV_FSP.1 |
| (L.2) = (E)                                                                                                                             | ADV_HLD.1 |

|                                                                                          |           |
|------------------------------------------------------------------------------------------|-----------|
| (M)                                                                                      |           |
| <b>AVA_VLA.1</b>                                                                         |           |
| AVA = Açıklık Değerlendirmesi   VLA = Açıklık analizi<br>1 = Geliştirici açıklık analizi |           |
| <b>Bağımlılıklar</b>                                                                     |           |
| (M.1) = (D)                                                                              | ADV_FSP.1 |
| (M.2) = (E)                                                                              | ADV_HLD.1 |
| (M.3) = (G)                                                                              | AGD_ADM.1 |
| (M.4) = (H)                                                                              | AGD_USR.1 |

EAL2 seviyesinde gerçekleştirilen değerlendirmelerde yukarıda belirtilen bileşenler ve bu bileşenlerin bağımlılıkları değerlendirilecek olan ürüne uygulanmalıdır. Bu bileşenlerin nasıl uygulanacağı ve gerçekleştirilmesi gereken bütün değerlendirici eylemleri Ortak Kriterler Değerlendirme Metodolojisinde belirtilmektedir. Ürünün EAL2 değerlendirmesinden başarılı sayılabilmesi için buradaki bütün değerlendirme eylemlerinden “geçti” alması gerekmektedir.

### 2.3.4 EAL3 Değerlendirmesi

*Eğik Harfler:* Bir önceki seviyeye göre belirgin eklemeler veya değişiklikler.

Çizelge.2.3. EAL3 garanti gereksinimleri

|                                                                                 |           |
|---------------------------------------------------------------------------------|-----------|
| <b>EAL 3 Metodik olarak test ve kontrol edilmiş</b>                             |           |
| <b><u>EAL3 düzeyindeki sınıflar, aileler, bileşenler ve elementler</u></b>      |           |
| (A)                                                                             |           |
| <b>ACM_CAP.3</b>                                                                |           |
| ACM = Konfigürasyon Yönetimi   CAP = Yetenekler<br>3= Yetkilendirme kontrolleri |           |
| <b>Bağımlılıklar</b>                                                            |           |
| (A.1) = (N)                                                                     | ACM_SCP.1 |
| (A.2) = (O)                                                                     | ALC_DVS.1 |

|                                                                                                      |                  |
|------------------------------------------------------------------------------------------------------|------------------|
| <b>(B)</b>                                                                                           |                  |
| <b>ADO_DEL.1</b>                                                                                     |                  |
| ADO = Dağıtım ve İşletim   DEL = Dağıtım<br>1 = Dağıtım prosedürleri                                 |                  |
| <b>Bağımlılıklar</b>                                                                                 |                  |
| <b>(B.1) = (G)</b>                                                                                   | <b>AGD_ADM.1</b> |
| <b>(C)</b>                                                                                           |                  |
| <b>ADO_IGS.1</b>                                                                                     |                  |
| ADO = Dağıtım ve İşletim   IGS = Kurulum ve başlatım<br>1 = Kurulum ve başlatım prosedürleri         |                  |
| <b>Bağımlılıklar</b>                                                                                 |                  |
| <b>(C.1) = (G)</b>                                                                                   | <b>AGD_ADM.1</b> |
| <b>(D)</b>                                                                                           |                  |
| <b>ADV_FSP.1</b>                                                                                     |                  |
| ADV = Geliştirme   FSP = Fonksiyonel spesifikasyon<br>1 = Biçimsel olmayan fonksiyonel spesifikasyon |                  |
| <b>Bağımlılıklar</b>                                                                                 |                  |
| <b>(D.1) = (F)</b>                                                                                   | <b>ADV_RCR.1</b> |
| <b>(E)</b>                                                                                           |                  |
| <b>ADV_HLD.2</b>                                                                                     |                  |
| ADV = Geliştirme   HLD = Üst düzey tasarım<br>2 = Güvenliği sağlayan üst düzey tasarım               |                  |
| <b>Bağımlılıklar</b>                                                                                 |                  |
| <b>(E.1) = (D)</b>                                                                                   | <b>ADV_FSP.1</b> |
| <b>(E.2) = (F)</b>                                                                                   | <b>ADV_RCR.1</b> |
| <b>(F)</b>                                                                                           |                  |
| <b>ADV_RCR.1</b>                                                                                     |                  |
| ADV = Geliştirme   RCR = Temsilin karşılaştırılması                                                  |                  |

|                                                                                |           |
|--------------------------------------------------------------------------------|-----------|
| 1 = Biçimsel olmayan karşılaştırma gösterimi                                   |           |
| <b>Bağımlılıklar:</b> Yok                                                      |           |
| <b>(G)</b>                                                                     |           |
| <b>AGD_ADM.1</b>                                                               |           |
| AGD = Kılavuz Dokümanları   ADM = Yönetici kılavuzu<br>1 = Yönetici kılavuzu   |           |
| <b>Bağımlılıklar</b>                                                           |           |
| (G.1) = (D)                                                                    | ADV_FSP.1 |
| <b>(H)</b>                                                                     |           |
| <b>AGD_USR.1</b>                                                               |           |
| AGD = Kılavuz Dokümanları   USR = Kullanıcı kılavuzu<br>1 = Kullanıcı kılavuzu |           |
| <b>Bağımlılıklar</b>                                                           |           |
| (H.1) = (D)                                                                    | ADV_FSP.1 |
| <b>(I)</b>                                                                     |           |
| <b>ATE_COV.2</b>                                                               |           |
| ATE = Test   COV = Kapsam<br>2 = Kapsamın analizi                              |           |
| <b>Bağımlılıklar</b>                                                           |           |
| (I.1) = (D)                                                                    | ADV_FSP.1 |
| (I.1) = (J)                                                                    | ATE_FUN.1 |
| <b>(J)</b>                                                                     |           |
| <b>ATE_FUN.1</b>                                                               |           |
| ATE = Test   FUNC = Fonksiyonel testler<br>1 = Fonksiyonel testler             |           |
| <b>Bağımlılıklar:</b> Yok                                                      |           |
| <b>(K)</b>                                                                     |           |

|                                                                                                                                            |           |
|--------------------------------------------------------------------------------------------------------------------------------------------|-----------|
| <b>ATE_IND.2</b>                                                                                                                           |           |
| ATE = Test   IND = Bağımsız testler<br>2 = Bağımsız testler - örnek                                                                        |           |
| <b>Bağımlılıklar</b>                                                                                                                       |           |
| (K.1) = (D)                                                                                                                                | ADV_FSP.1 |
| (K.2) = (G)                                                                                                                                | AGD_ADM.1 |
| (K.3) = (H)                                                                                                                                | AGD_USR.1 |
| <b>(L)</b>                                                                                                                                 |           |
| <b>AVA_SOF.1</b>                                                                                                                           |           |
| AVA = Açıklık Değerlendirmesi   SOF = TOE güvenlik fonksiyonlarının<br>gücü<br>1 = TOE güvenlik fonksiyonlarının gücünün değerlendirilmesi |           |
| <b>Bağımlılıklar</b>                                                                                                                       |           |
| (L.1) = (D)                                                                                                                                | ADV_FSP.1 |
| (L.2) = (E)                                                                                                                                | ADV_HLD.1 |
| <b>(M)</b>                                                                                                                                 |           |
| <b>AVA_VLA.1</b>                                                                                                                           |           |
| AVA = Açıklık Değerlendirmesi   VLA = Açıklık analizi<br>1 = Geliştirici açıklık analizi                                                   |           |
| <b>Bağımlılıklar</b>                                                                                                                       |           |
| (M.1) = (D)                                                                                                                                | ADV_FSP.1 |
| (M.2) = (E)                                                                                                                                | ADV_HLD.1 |
| (M.3) = (G)                                                                                                                                | AGD_ADM.1 |
| (M.4) = (H)                                                                                                                                | AGD_USR.1 |
| <b>(N)</b>                                                                                                                                 |           |
| <b>ACM_SCP.1</b>                                                                                                                           |           |
| ACM = Konfigürasyon Yönetimi   SCP = KM kapsamı<br>1 = TOE KM kapsamı                                                                      |           |

|                                                                                                                   |           |
|-------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Bağımlılıklar</b>                                                                                              |           |
| (N.1) = (A)                                                                                                       | ACM_CAP.3 |
| <b>(O)</b>                                                                                                        |           |
| <b>ALC_DVS.1</b>                                                                                                  |           |
| <i>ALC = Yaşam Döngüsü Desteği   DVS = Geliştirme güvenliği</i><br><i>1 = Güvenlik tedbirlerinin belirlenmesi</i> |           |
| <b>Bağımlılıklar: Yok</b>                                                                                         |           |
| <b>(P)</b>                                                                                                        |           |
| <b>ATE_DPT.1</b>                                                                                                  |           |
| <i>ATE = Test   DPT = Derinlik</i><br><i>1 = Testler : Üst düzey tasarım</i>                                      |           |
| <b>Bağımlılıklar</b>                                                                                              |           |
| (P.1) = (E)                                                                                                       | ADV_HLD.1 |
| (P.2) = (J)                                                                                                       | ATE_FUN.1 |
| <b>(R)</b>                                                                                                        |           |
| <b>AVA_MSU.1</b>                                                                                                  |           |
| <i>AVA = Açıklık Değerlendirmesi   MSU = Kötüye kullanım</i><br><i>1 = Kılavuzun incelenmesi</i>                  |           |
| <b>Bağımlılıklar</b>                                                                                              |           |
| (R.1) = (C)                                                                                                       | ADO_IGS.1 |
| (R.2) = (D)                                                                                                       | ADV_FSP.1 |
| (R.3) = (G)                                                                                                       | AGD_ADM.1 |
| (R.4) = (H)                                                                                                       | AGD_USR.1 |

EAL3 seviyesinde gerçekleştirilen değerlendirmelerde yukarıda belirtilen bileşenler ve bu bileşenlerin bağımlılıkları değerlendirilecek olan ürüne uygulanmalıdır. Bu bileşenlerin nasıl uygulanacağı ve gerçekleştirilmesi gereken bütün değerlendirici eylemleri Ortak Kriterler Değerlendirme Metodolojisinde

belirtilmektedir. Ürünün EAL3 değerlendirmesinden başarılı sayılabilmesi için buradaki bütün değerlendirme eylemlerinden “geçti” alması gerekmektedir.

### 2.3.5 EAL4 Değerlendirmesi

*Eğik Harfler:* Bir önceki seviyeye göre belirgin eklemeler veya değişiklikler.

Çizelge.2.4. EAL4 garanti gereksinimleri

|                                                                                                                                                   |                  |
|---------------------------------------------------------------------------------------------------------------------------------------------------|------------------|
| <b>EAL 4 metodik olarak tasarlanmış, test edilmiş ve incelenmiş</b><br><b><u>EAL4 düzeyindeki sınıflar, aileler, bileşenler ve elementler</u></b> |                  |
| <b>(A)</b>                                                                                                                                        |                  |
| <b>ACM_CAP.4</b>                                                                                                                                  |                  |
| <b>ACM</b> = Konfigürasyon Yönetimi   <b>CAP</b> = Yetenekler<br><b>4</b> = Destek ve kabul oluşturma prosedürleri                                |                  |
| <b>Bağımlılıklar</b>                                                                                                                              |                  |
| <b>(A.1) = (N)</b>                                                                                                                                | <b>ACM_SCP.1</b> |
| <b>(A.2) = (O)</b>                                                                                                                                | <b>ALC_DVS.1</b> |
| <b>(B)</b>                                                                                                                                        |                  |
| <b>ADO_DEL.2</b>                                                                                                                                  |                  |
| <b>ADO</b> = Dağıtım ve İşletim   <b>DEL</b> = Dağıtım<br><b>2</b> = Değişikliklerin tespit edilmesi                                              |                  |
| <b>Bağımlılıklar</b>                                                                                                                              |                  |
| <b>(B.1) = (A)</b>                                                                                                                                | <b>ACM_CAP.3</b> |
| <b>(C)</b>                                                                                                                                        |                  |
| <b>ADO_IGS.1</b>                                                                                                                                  |                  |
| <b>ADO</b> = Dağıtım ve İşletim   <b>IGS</b> = Kurulum ve başlatım<br><b>1</b> = Kurulum ve başlatım prosedürleri                                 |                  |
| <b>Bağımlılıklar</b>                                                                                                                              |                  |

|                                                                                                     |           |
|-----------------------------------------------------------------------------------------------------|-----------|
| (C.1) = (G)                                                                                         | AGD_ADM.1 |
| (D)                                                                                                 | ADV_FSP.2 |
| ADV = Geliştirme   FSP = Fonksiyonel spesifikasyon<br>2 = Tam olarak tanımlanmış dış arayüzler      |           |
| Bağımlılıklar                                                                                       |           |
| (D.1) = (F)                                                                                         | ADV_RCR.1 |
| (E)                                                                                                 | ADV_HLD.2 |
| ADV = Geliştirme   HLD = Üst düzey tasarım<br>2 = Güvenliği sağlayan üst düzey tasarım              |           |
| Bağımlılıklar                                                                                       |           |
| (E.1) = (D)                                                                                         | ADV_FSP.1 |
| (E.2) = (F)                                                                                         | ADV_RCR.1 |
| (F)                                                                                                 | ADV_RCR.1 |
| ADV = Geliştirme   RCR = Temsilin karşılaştırılması<br>1 = Biçimsel olmayan karşılaştırma gösterimi |           |
| Bağımlılıklar: Yok                                                                                  |           |
| (G)                                                                                                 | AGD_ADM.1 |
| AGD = Kılavuz Dokümanları   ADM = Yönetici kılavuzu<br>1 = Yönetici kılavuzu                        |           |
| Bağımlılıklar                                                                                       |           |
| (G.1) = (D)                                                                                         | ADV_FSP.1 |
| (H)                                                                                                 | AGD_USR.1 |

|                                                                                                     |                  |
|-----------------------------------------------------------------------------------------------------|------------------|
| <b>AGD</b> = Kılavuz Dokümanları   <b>USR</b> = Kullanıcı kılavuzu<br><b>1</b> = Kullanıcı kılavuzu |                  |
| <b>Bağımlılıklar</b>                                                                                |                  |
| <b>(H.1) = (D)</b>                                                                                  | <b>ADV_FSP.1</b> |
| <b>(I)</b>                                                                                          |                  |
| <b>ATE_COV.2</b>                                                                                    |                  |
| <b>ATE</b> = Test   <b>COV</b> = Kapsam<br><b>2</b> = Kapsamın analizi                              |                  |
| <b>Bağımlılıklar</b>                                                                                |                  |
| <b>(I.1) = (D)</b>                                                                                  | <b>ADV_FSP.1</b> |
| <b>(I.1) = (J)</b>                                                                                  | <b>ATE_FUN.1</b> |
| <b>(J)</b>                                                                                          |                  |
| <b>ATE_FUN.1</b>                                                                                    |                  |
| <b>ATE</b> = Test   <b>FUN</b> = Fonksiyonel testler<br><b>1</b> = Fonksiyonel testler              |                  |
| <b>Bağımlılıklar: Yok</b>                                                                           |                  |
| <b>(K)</b>                                                                                          |                  |
| <b>ATE_IND.2</b>                                                                                    |                  |
| <b>ATE</b> = Test   <b>IND</b> = Bağımsız testler<br><b>2</b> = Bağımsız testler – örnek            |                  |
| <b>Bağımlılıklar</b>                                                                                |                  |
| <b>(K.1) = (D)</b>                                                                                  | <b>ADV_FSP.1</b> |
| <b>(K.2) = (G)</b>                                                                                  | <b>AGD_ADM.1</b> |
| <b>(K.3) = (H)</b>                                                                                  | <b>AGD_USR.1</b> |
| <b>(L)</b>                                                                                          |                  |
| <b>AVA_SOF.1</b>                                                                                    |                  |

**AVA** = Açıklık Değerlendirmesi | **SOF** = TOE güvenlik fonksiyonlarının gücü

**1** = TOE güvenlik fonksiyonlarının gücünün değerlendirilmesi

**Bağımlılıklar**

|                    |                  |
|--------------------|------------------|
| <b>(L.1) = (D)</b> | <b>ADV_FSP.1</b> |
| <b>(L.2) = (E)</b> | <b>ADV_HLD.1</b> |

**(M)**

**AVA\_VLA.2**

**AVA** = Açıklık Değerlendirmesi | **VLA** = Açıklık analizi

**2** = Bağımsız açıklık analizi

**Bağımlılıklar**

|                    |                  |
|--------------------|------------------|
| <b>(M.1) = (D)</b> | <b>ADV_FSP.1</b> |
| <b>(M.2) = (E)</b> | <b>ADV_HLD.2</b> |
| <b>(M.3) = (G)</b> | <b>AGD_ADM.1</b> |
| <b>(M.4) = (H)</b> | <b>AGD_USR.1</b> |
| <b>(M.5) = (S)</b> | <b>ADV_IMP.1</b> |
| <b>(M.6) = (T)</b> | <b>ADV_LLD.1</b> |

**(N)**

**ACM\_SCP.2**

**ACM** = Konfigürasyon Yönetimi | **SCP** = KM kapsamı

**2** = KM Kapsamında problem takibi

**Bağımlılıklar**

|                    |                  |
|--------------------|------------------|
| <b>(N.1) = (A)</b> | <b>ACM_CAP.3</b> |
|--------------------|------------------|

**(O)**

**ALC\_DVS.1**

**ALC** = Yaşam Döngüsü Desteği | **DVS** = Geliştirme güvenliği

**1** = Güvenlik tedbirlerinin belirlenmesi

|                                                                                       |           |
|---------------------------------------------------------------------------------------|-----------|
| <b>Bağımlılıklar:</b> Yok                                                             |           |
| <b>(P)</b>                                                                            |           |
| <b>ATE_DPT.1</b>                                                                      |           |
| ATE = Test   DPT = Derinlik<br>1 = Testler : Üst düzey tasarım                        |           |
| <b>Bağımlılıklar</b>                                                                  |           |
| (P.1) = (E)                                                                           | ADV_HLD.1 |
| (P.2) = (J)                                                                           | ATE_FUN.1 |
| <b>(R)</b>                                                                            |           |
| <b>AVA_MSU.2</b>                                                                      |           |
| AVA = Açıklık Değerlendirmesi   MSU = Kötüye kullanım<br>2 = Analizlerin doğrulanması |           |
| <b>Bağımlılıklar</b>                                                                  |           |
| (R.1) = (C)                                                                           | ADO_IGS.1 |
| (R.2) = (D)                                                                           | ADV_FSP.1 |
| (R.3) = (G)                                                                           | AGD_ADM.1 |
| (R.4) = (H)                                                                           | AGD_USR.1 |
| <b>(S)</b>                                                                            |           |
| <b>ACM_AUT.1</b>                                                                      |           |
| ACM = Konfigürasyon Yönetimi   AUT = KM otomasyonu<br>1 = Kısmi KM otomasyonu         |           |
| <b>Bağımlılıklar</b>                                                                  |           |
| (S.1) = (A)                                                                           | ACM_CAP.3 |
| <b>(T)</b>                                                                            |           |
| <b>ADV_IMP.1</b>                                                                      |           |
| ADV = Geliştirme   IMP = Uygulamanın temsili<br>1 = TSF uygulamasının bir alt kümesi  |           |
| <b>Bağımlılıklar</b>                                                                  |           |

|                                                                                                                 |             |           |
|-----------------------------------------------------------------------------------------------------------------|-------------|-----------|
|                                                                                                                 | (T.1) = (U) | ADV_LLD.1 |
|                                                                                                                 | (T.2) = (F) | ADV_RCR.1 |
|                                                                                                                 | (T.3) = (Z) | ALC_TAT.1 |
| (U)                                                                                                             |             |           |
| ADV_LLD.1                                                                                                       |             |           |
| ADV = Geliştirme   LLD = Alt düzey tasarım<br>1 = Alt düzey tasarımın tanımlanması                              |             |           |
| Bağımlılıklar                                                                                                   |             |           |
|                                                                                                                 | (U.1) = (E) | ADV_HLD.2 |
|                                                                                                                 | (U.2) = (F) | ADV_RCR.1 |
| (V)                                                                                                             |             |           |
| ADV_SPM.1                                                                                                       |             |           |
| ADV = Geliştirme   SPM = Güvenlik politikası modellemesi<br>1 = Biçimsel olmayan TOE güvenlik politikası modeli |             |           |
| Bağımlılıklar                                                                                                   |             |           |
|                                                                                                                 | (V.1) = (D) | ADV_FSP.1 |
| (Y)                                                                                                             |             |           |
| ALC_LCD.1                                                                                                       |             |           |
| ALC = Yaşam Döngüsü Desteği   LCD= Yaşam döngüsü tanımı<br>1 = Geliştirici tarafından tanımlanan yaşam döngüsü  |             |           |
| Bağımlılıklar: Yok                                                                                              |             |           |
| (Z)                                                                                                             |             |           |
| ALC_TAT.1                                                                                                       |             |           |
| ALC = Yaşam Döngüsü Desteği   TAT = Araçlar ve teknikler<br>1 = İyi tanımlanmış geliştirme araçları             |             |           |
| Bağımlılıklar                                                                                                   |             |           |
|                                                                                                                 | (Z.1) = (D) | ADV_FSP.1 |

EAL4 seviyesinde gerçekleştirilen değerlendirmelerde yukarıda belirtilen bileşenler ve bu bileşenlerin bağımlılıkları değerlendirilecek olan ürüne uygulanmalıdır. Bu bileşenlerin nasıl uygulanacağı ve gerçekleştirilmesi gereken bütün değerlendirici eylemleri Ortak Kriterler Değerlendirme Metodolojisinde belirtilmektedir. Ürünün EAL4 değerlendirmesinden başarılı sayılabilmesi için buradaki bütün değerlendirme eylemlerinden “geçti” alması gerekmektedir.

## **2.4 ISO 17799 Bilgi Teknolojisi – Bilgi Güvenliği Yönetimi için Uygulama Prensipleri**

Organizasyonların bilgi varlıklarının bütünlük, gizlilik ve kullanılabilirlik amaçlarının sürekli olarak açıklıklardan kaynaklanan tehditlere karşı korunabilmesi için organizasyonda bir bilgi güvenliği yönetim sistemi kurulması ve bu sistemin ISO 17799’da belirtilen şartlara uygun olarak işletilmesi giderek yaygınlaşmaktadır. Bu standarda uygunluğun bir göstergesi olan BS 7799 sertifikası uluslararası alanda tanınmakta ve kabul görmektedir. [Höne, 2002]

ISO 17799 standardının uygulama adımları aşağıdaki gibidir:

1. Bilgi güvenliği politikasının tanımlanması; Oluşturulan güvenlik politikası ile bilgi güvenliği için yönetimin yönlendirilmesinin ve desteğinin amaçlanmaktadır. Yönetim organizasyon için geçerli olacak, ve bilgi güvenliğine ilişkin açık bir politikanın ortaya koyulduğu ve bu politikaya desteğini ve bağlılığını göstereceği bir güvenlik politikası hazırlamalı ve bütün çalışanları politika konusunda bilgilendirmeli ve gerekli eğitimleri vermelidir.
2. Bilgi güvenliği yönetim sisteminin kapsamının belirlenmesi ve bu sistemin kurulması; Bu sistem ile organizasyonda bilgi güvenliğinin yönetilmesi amaçlanmaktadır. Bilgi güvenliği gereksinimlerini uygulamak ve kontrollerini gerçekleştirmek bu yönetim sisteminin sorumluluğundadır. Ayrıca bu sistem oluşturulan güvenlik politikasının onaylanmasını, güvenlik rollerinin ve sorumluluklarının tanımlanmasını ve varlıkların sınıflandırılmasının detaylarını bu yönetim sistemi mekanizması tanımlamalıdır.

3. Risk deęerlendirmesinin gerekleřtirilmesi; Bilgi gvenlięi ynetim sisteminin belirledięi bilgi varlıklarına gerekleřtirilebilecek olan tehditlere karřı organizasyon ierisinde bir risk deęerlendirmesi gerekleřtirilmelidir. Risk deęerlendirmesi sonuları raporlanmalı ve incelenmelidir.
4. Risk ynetiminin gerekleřtirilmesi; Risk deęerlendirmesi sonuları dikkate alınarak hedeflenen garanti dzeyine ve organizasyonun risk ynetimi yaklařımlarına uygun olarak risk ynetimi gerekleřtirilmelidir.
5. Kontrol objelerinin seilmesi ve uygulanması; Gerekleřtirilen risk ynetiminin ardından riskin kabul edilebilir seviyeye indirilebilmesi iin ISO 17799’da tanımlanan kontrol objelerinden gerekli olanlar tespit edilmeli ve standardın nerdięi řekilde organizasyona uygun olarak uygulanmalıdır.
6. Uygunluk iddiası; ISO 17799’a uygunluk iin bilgi gvenlięi ynetimi gereksinimleri organizasyon iin uygulanmalıdır. Dikkat edilmesi gereken nokta bu iřlemin bir kerelik yapılmadıęı ve bir sre olduęudur. Yani belirlenen aralıklarda risk deęerlendirmesi tekrarlanmalı ve risk ynetimi tekrar gerekleřtirilmelidir. Sonulara uygun olarak organizasyonda uygulanan kontrol objeleri gncellenmelidir.

#### 2.4.1 ISO 17799 Kontrol Objeleri

ISO 17799 standardının tanımladıęı kontrol objeleri ve bu objelerin amaları ařaęıdaki gibidir. Organizasyonlar gerekleřtirdikleri risk ynetimi sonularına uygun olarak bu objelerden gereksinimleri olanları semeli ve uygulamalıdır;

1. **Gvenlik politikası;** Bilgi gvenlięinin saęlanması iin ynetimin ynlendirmesini ve desteęini saęlamak.
2. **Gvenlik organizasyonu;** Bilgi Gvenlięini organizasyon apında ynetmek, kurumda bilginin iřlendięi ve nc řahısların eriřebildikleri ortamların gvenlięini saęlamak ve kurumun bilgi sistemi dıř kaynaklarla idare ediliyorsa gerekli gvenlik nlemlerini saęlamak.
3. **Varlıkların sınıflandırılması;** Kurumun bilgilerini uygun seviyede korumak, ve kurum bilgilerinin yeterli ve uygun bir seviyede korunduęunu

garanti etmek.

4. **Personel güvenliği;** İnsan hataları, hırsızlık ve kötüye kullanımlardan kaynaklanacak riskleri en aza indirmek, kullanıcıları tehditler konusunda bilgilendirmek, ve bu tür kazalardan oluşacak etkileri en aza indirmek.
5. **Fiziksel güvenlik;** Kurum için değerli olan varlıklara yetkisiz erişimi engellemek, bu varlıkları olası hasarlardan korumak, ve bilgiyi çalınmalara ve değişikliklere karşı korumak.
6. **İletişim ve işlem güvenliği;** Bilgi işlem ve kayıt sistemlerinin doğru ve güvenli çalışmalarını sağlamak, sistem hata risklerini azaltmak, yazılımların ve bilginin bütünlüğünü korumak, iletişimin ve bilginin bütünlüğünü ve kullanılabilirliğini sağlamak, varlıkları hasarlara karşı korumak, iş eylemlerini kesintilere karşı korumak, kurumlar arası bilgi değişimlerini kayba, değiştirilmelere ve kötüye kullanıma karşı korumak.
7. **Erişim kontrolleri;** Bilgiye erişimi kontrol etmek, bilgi sistemlerine yetkisiz erişimleri engellemek, ağ servislerinin güvenliğini sağlamak, yetkisiz bilgisayar erişimlerini engellemek, ve yetkisiz aktiviteleri tespit etmek.
8. **Sistem geliştirilmesi ve bakımı;** İşlevsel sistemleri gerekli güvenlikle tasarlamak, uygulama sistemlerinde kullanıcı bilgilerini kayba, değiştirilmeye ve kötüye kullanıma karşı korumak, bilginin gizliliğini ve bütünlüğünü korumak ve doğrulamak, uygulama yazılımlarının ve donanımların güvenliğini sağlamak.
9. **İş devamlılık planı;** İş aktivitelerini kritik ve büyük hasarlı kazalardan sonrada devam ettirmek.
10. **Uygunluk;** Güvenlikle ilgili yasalara aykırı davranmamayı, ve sistemlerin güvenlik politikasına ve standartlara uygulugunu sağlamak.

## 2.5 COTS Ürünlerinin Değerlendirilmesi

Bu bölümde BT sisteminde bulunabilecek COTS ürünlerinin CC'ye uygun değerlendirilmesi için kullanılan bir yöntem olan V-RATE metodu gösterilmiştir.

COTS ürünleri piyasada yaygın olarak bulunan ve müşterilerin genel ihtiyacına yönelik hazırlanmış ticari ürünlerdir. Müşteri olarak bir COTS ürünü satın almak

istediğinizde ürün hakkında üreticinin iddia ettiği çok kısıtlı bilgilere ve bir kısım ürünler içinde bağımsız test kuruluşlarının yapmış olduğu testlere veya farklı ürünler hakkında karşılaştırmalara ulaşabilirsiniz, ve bu bilgilere ne kadar güvenebileceğiniz her zaman soru işaretidir. Bu ürünlerin tercih edilme sebebi genelde maliyetlerinin oldukça uygun olması ve üretici firmaların konu hakkındaki tecrübeleri ile verdikleri teknik destek ve bakımdır.

### 2.5.1 V-RATE Değerlendirme Modeli ile COTS Değerlendirmesi

BT sistemlerinin güvenliği söz konusu olduğunda sistemlerin dayanıklılığı kavramının incelenmesi gerekmektedir. Bir sistemin dayanıklılığının incelenmesi için de ilk olarak modern sistemlerin sınırları olmayan etki alanlarında (unbounded domains) nasıl çalıştıklarının anlaşılması gerekmektedir. Internet gibi sınırları olmayan etki alanları merkezi kontrolden yoksun, zamanında ve doğru bilgi sahibi olmadığınız ortamlardır. Aynı zamanda çağımızda tipik bir BT sistemi de sınırları olmayan etki alanlarına örnektir. Bu sistemlerde çalışan uygulama yazılımları bileşenlerinin güvenliği ve garantisi bu bakımdan son derece önemlidir.

Tam kontrolün olmadığı bir sistemde ve çalıştığı ortamda dayanıklılığı sağlayabilmek için iyi bir risk yönetimi yapmak gerekmektedir. Eğer sistem tamamen COTS bileşenlerinden oluşmaktaysa bu yazılımların özelliklerinden de gelen bir kontrol eksikliği yüzünden de sistemin dayanıklılığı çeşitli tehditler altındadır.

Normal bir sistem kullanıcısının eylemleri sonucu hatalar verebilecek sistem açıklıkları akıllı bir düşman kullanıcı tarafından kötüye kullanılabilir, örneğin hafıza taşması açıklıklarından faydalanma. Bu yüzden dayanıklılık aşağıdakilerden birinin de doğru olduğu bir yüksek garanti düzeyi gerektirmektedir:

- Bahsedilen açıklıklar sistemde bulunmamaktadır veya varsa kötüye kullanılamamaktadır.

- Eğer bahsedilen açıklık kötüye kullanılabiliriyorsa, bu kötüye kullanım sistemin görevini engellememeli veya göreve devam edilebilmesi için anında tanınabilmeli ve düzeltilebilmelidir.

Bu yüksek garanti gereksinimi yüzünden COTS ürünlerini kritik görevi olan sistemlerde kullanmak çok zor olmaktadır.

COTS bileşenleri kullanarak dayanıklı sistemler kurmak riskli bir yöntemdir çünkü sistemi kuran kişi kullanacağı bileşenlerin geliştirilmesi sırasında kullanılan yazılım mühendisliği metodları hakkında çok az bilgisi bulunmaktadır veya çoğu zaman bu metodlar hakkında bilgilere ulaşamamaktadır. COTS bileşenlerinin garanti düzeyinin belirlenebileceği bu metodlara ulaşamamanın dezavantajı satıcı-risk belirlemesi metodu kullanılarak dayanıklı sistemler kurmakla giderilebilmektedir. Bu değerlendirme ile geliştirme dokümanları hakkında çok fazla bilgi sahibi olunamayan COTS ürünlerinin garanti düzeylerinin tespit edilebilmesi için deliller elde edilebilecek ve yapılacak güvenlik testlerinde de başarılı olması halinde, bu COTS bileşenleri kritik görevi olan sistemlerde kullanılabilir. [Reifer, 2003]

Önerilen satıcı-risk belirlemesi aşağıda tanımlanacak olan satıcı-risk belirlemesi ve tehdit değerlendirmesi (V-RATE) yöntemini temel almaktadır.

#### 2.5.1.1 V-RATE Yöntemi [Lipson, 2002]

V-RATE yönteminin elemanları aşağıdakileri içermektedir:

Çizelge 2.5 V-RATE Yöntemi

##### 1. Satıcının Doğal Risk Elemanları

###### 1.1. Ürün Özelliklerinin Takibi

1.1.1. Açık olma – Tasarım ve mühendislik süreçlerinin takip derecesi

1.1.2. Bağımsız test kuruluşları

###### 1.2. Teknik Yeterlilik

1.2.1. Dayanıklılık kabiliyetinin olgunluğu

- 1.2.2. Satıcı değerlendirmelerinin/sertifikasyonlarının varlığı
- 1.2.3. Uygulamadaki standartlara ve devlet kanun/kurallarına bağlılığın kanıtları
- 1.2.4. Satıcının ürünlerindeki ve servislerindeki değişimin ve fazlalıkların gösterilmesi
- 1.2.5. Satıcının güvenlik ve dayanıklılık konularıyla verimli bir şekilde ilgilenen bir takımının varlığı

### **1.3. Performans Tarihçesi**

### **1.4. Uygunluk**

- 1.4.1. Güvenlik ve dayanıklılık konularına karşılıklar
- 1.4.2. Yeni özellik ve gelişme isteklerine karşılık
- 1.4.3. Bağımsız test laboratuvarları ve sertifikasyon kurumlarıyla ortak çalışma isteği

### **1.5. Güvenilirlik**

- 1.5.1. Kayıtlar / firma hakkında bilgiler
- 1.5.2. Personelin güvenilirliği konusunda deliller

### **1.6. İş yönetimi yeteneği**

- 1.6.1. Ekonomik izlenebilirlik
- 1.6.2. Satıcının mütahit firmalarla ilişkilerindeki risk yönetimi

### **1.7. Kontrollü gelişme**

- 1.7.1. Açıkça tanımlanmış gelişim hedefleri
- 1.7.2. Ürün entegrasyonu
- 1.7.3. Ürünlerin gelişiminin devamlı dayanıklılığı desteklemesi

## **2. Satıcı ile İlişkilerde Müşterilerin Risk Yönetimi Yetenekleri**

### **2.1. Risk hafifletici teknik faktörler**

- 2.1.1. Müşterinin ürünün güvenlik ve dayanıklılıkla ilgili kalite özelliklerini değerlendirmedeki yetenekleri
- 2.1.2. Müşterinin satıcının teknik yeterliliklerini değerlendirmedeki yetenekleri
- 2.1.3. Müşterinin satıcının sertifikalarının ve değerlendirme sonuçlarının farkında olması
- 2.1.4. Satıcının ürün ve servis entegrasyonundaki fazlalıkların ve değişimin gösterilmesi

2.1.5. Satıcının ürünü ile ilgili riskleri sınırlamak için mimari araç ve tekniklerin kullanılması

2.1.6. Müşterinin firma bünyesinde konusunda uzman bir grubun güvenlik ve dayanıklılık konusunda ürünü incelemesi

## **2.2. Teknik olmayan risk hafifletici faktörler**

2.2.1. Yasal

2.2.2. Ekonomik

2.2.3. Politik ve sosyal

## **2.3. Bağımsızlık / İç bağımlılıklar**

## **2.4. Müşterinin korunmasızlığı**

## **2.5. Görev düzenleme / satıcı yeterlilikleri**

## **2.6. Müşterinin pazarlık yetenekleri ve gücü**

### **2.5.1.2 Özel Satıcı-Risk Azaltma Teknikleri**

V-RATE metodu, COTS ürünlerinden kaynaklanacak risklerin belirlenebilmesi ve yüksek garanti sağlayacak ürünlerin seçilebilmesi için bir çatı oluşturmaktadır. Her ne kadar bir çok risk varsa ve yapılması gereken birçok iş varsa bile bu riskleri azaltmanın özel yöntemleri de vardır. Yukarıda belirtilen V-RATE yönteminin her bir elemanı için riskleri azaltmak üzere özel stratejiler geliştirilmelidir. Çizelge 2.6 V-RATE Risk Azaltma Yöntemi’da bu risk azaltma stratejilerine örnekler bulunmaktadır. [Lipson, 2002]

Çizelge 2.6 V-RATE Risk Azaltma Yöntemi

| <b>V-RATE Elemanları</b>       | <b>Örnekler</b>                                                                              |
|--------------------------------|----------------------------------------------------------------------------------------------|
| 1.1 Ürün Özelliklerinin Takibi | Satıcının müşteriye kaynak kodu göstermeye niyetli olup olmadığı incelenmelidir.             |
| 1.2 Teknik Yeterlilik          | Satıcı dayanıklılık ve güvenlik konularındaki kritik noktalarda yeterliliğini göstermelidir. |
| 1.3 Performans Tarihçesi       | Satıcının kayıtları, tecrübeleri, istatistikler ve hakkında çıkan haberler incelenmelidir.   |

|                                               |                                                                                                                                                            |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1.4 Uygunluk                                  | Satıcı güvenlik yamalarını zamanında erişilebilir hale getirebilmelidir.                                                                                   |
| 1.5 Güvenilirlik                              | Satıcı personelin güvenilirliğini belirli aralıklarla kontrol etmelidir.                                                                                   |
| 1.6 İş Yönetimi Yeteneği                      | Satıcının uzun vadeli ekonomik tabloları olumlu olmalıdır.                                                                                                 |
| 1.7 Kontrollü Gelişme                         | Satıcı ürünün gelişimi ile ilgili plan ve prosedürlerini müşteri ile paylaşmalıdır.                                                                        |
| 2.1 Risk Hafifletici Teknik Faktörler         | Müşteri, teknik bir risk değerlendirmesi yeteneğine sahip olmalıdır.                                                                                       |
| 2.2 Teknik Olmayan Risk Hafifletici Faktörler | Müşteri satıcı firmanın garanti, lisans anlaşması, performans ölçümleri, cezalar, düzenlemeler konularındaki yasal ve mali belgelerini inceleyebilmelidir. |
| 2.3 Bağımsızlık / İç bağımlılıklar            | Müşteri sistemi ile ilgili olan satıcı ürünlerini ve servislerini incelemeli, güvenliği tehdit eden iç bağımlılıkları araştırmalıdır.                      |
| 2.4 Müşterinin Korunmasızlığı                 | Müşteri sisteminin hangi bileşenlerinin satıcının yeterliliğine ve güvenilirliğine bağlı olduğunu araştırmalıdır.                                          |
| 2.5 Görev Düzenleme / Satıcı Yeterlilikleri   | Müşteri gereksinim duyduğu kalite özellikleri ile üründeki gerekli kalite özelliklerini karşılaştırmalıdır.                                                |
| 2.6 Müşterinin Pazarlık Yetenekleri ve Gücü   | Müşteri güvenlik problemlerini önceden öğrenebilmek ve zamanında çözümler uygulayabilmek için satıcı ile birlikte çalışmalıdır.                            |

V-RATE metodu kullanılarak bilgi sistemlerinde COTS ürünü tercih edilerek kullanılacak olan uygulama yazılımlarının garanti düzeyleri tespit edilir ve risk seviyesi azaltılabilir. Şimdi bu tablonun maddelerinden biri olan uygunluk elemanını örnek üzerinde biraz daha detaylı inceleyelim. Kullanılacak uygulama yazılımı

çeşidine göre bu metodun elemanlarının uygulamaları değişebilmektedir yani risk azaltma yöntemi ve gerekli güvenlik ihtiyaçları ürün çeşidine ve kullanıldığı sisteme göre değişiklik göstermektedir.

## **V-RATE Metodu Uygunluk Elemanı;**

### **1.4 Uygunluk**

#### *1.4.1 Güvenlik ve dayanıklılık konularına karşılıklar*

#### *1.4.2 Yeni özellik ve gelişme isteklerine karşılık*

#### *1.4.3 Bağımsız test laboratuvarları ve sertifikasyon kurumlarıyla ortak çalışma isteği*

Satıcı müşterinin güvenlik ve dayanıklılık ihtiyaçlarını karşılamaya istekli olduğunu aşağıdaki maddelere uygunlukla göstermelidir;

- Güvenlik yamalarını zamanında erişilebilir hale getirerek,
- Müşterinin kullanmayacağı özellikleri kapatması konusunda yardımcı olmak ve bu özelliklerden kaynaklanabilecek riskleri sıfıra indirmek. Bu sayede müşteri sadece ihtiyacı olan servisleri kullanabilir ve risk azaltılmış olur,
- Yazılımlara geriye alabilme mekanizmaları ekleyerek, örneğin bazı yazılımlarda otomatik olarak yedek alma ve hata durumlarında sistemi hatadan önceki haline getirebilme özellikleri bulunabilmektedir,
- Yazılımlara gerektiğinde sistemin güvenlik direncini arttıracak mekanizmaları ekleyerek, mesajları şifreleyerek veya şifre koruması desteği ile,
- Ürünün güvenlik özelliklerinin testlerini gerçekleştirerek,

Yukarıdaki örnekte olduğu gibi V-RATE metodu ürün veya sistem grubuna göre dallanarak genişleyebilmektedir. Fakat metodolojinin temel yapısı aynı kalmaktadır. Sistemde kullanılacak COTS ürünleri için bu metodolojinin uygulanması, özellikle kritik güvenli sistemler için, ürünün sağlayacağı garantinin tespit edilmesinde ve karşılaşılan risklerin azaltılmasında büyük rol oynayacaktır. Dikkat edilmesi gereken konu güvenliğin önemli olduğu BT ürünleri satın alınırken her ne kadar ürünün sağladığı garanti önemli olsa da ürünün güvenlik fonksiyonlarının da müşteri tarafından test edilmesi ve gerekli güvenlik

fonksiyonlarının her durumda düzgün olarak çalıştığının ispatlanması da gerekmektedir.

### 2.5.1.3 COTS Ürünlerinin Test Edilmesi

BT sistemlerinde kullanılacak olan uygulama yazılımlarının garanti seviyesi V-RATE metodolojisi ile belirlenip risk değeri minimumda olan ürünler tercih edildikten sonra yapılması gereken ürünün fonksiyonlarının test edilmesidir. Bu sayede uygulama yazılımının yapması gerekenleri yaptığı ve yapmaması gereken işlemlerin gerçekleştirilmesine ise izin vermediği ispatlanmıştır. [Reifer, 2003] Geleneksel yazılım geliştirme tekniklerinde yazılımların test edilmesi için kabul edilen iki farklı yöntem vardır. Bunlar beyaz ve siyah kutu testleridir. Fakat COTS ürünleri için bu iki yöntemin verimli bir şekilde uygulanıp uygulanmayacağı çok belirgin değildir, çünkü COTS ürünlerinin değerlendirilmesi için amaçlar ve erişilebilir dokümanlar oldukça farklıdır. Daha önce de belirtildiği gibi COTS ürünleri için değerlendirmelerde delil olarak kullanılabilecek dokümanlar çok kısıtlıdır.

COTS tabanlı sistemlerde testleri gerçekleştirebilmek için belli sayıda değişken bulunmaktadır. Genel olarak kaynak koda erişim yoktur veya olsa bile kod üzerinde değişiklik yapmak mümkün değildir. Ayrıca ürün geliştiricinin hazırlamış olduğu kullanıcı kılavuzu veya ürün özelliklerini anlatan broşürler değerlendirmelerde kaynak olarak kullanılabilecek yeterlilikte değildir. Örneğin, bu dokümanlar sistemin normal olmayan bir veri girişine vereceği tepkileri tanımlamamaktadırlar.

Bu değişkenler COTS ürünleri değerlendirilirken amaçları etkilemektedirler. Test stratejisi çoğunlukla sistemin aşırı zorlanma altındaki davranışlarının tespit edilmesine dayanmaktadır. Ayrıca satıcının üründe varolduğunu iddia ettiği fonksiyonların, bu fonksiyonların ürünün kullanılacağı ortamda da doğru çalıştığının ve sistemdeki diğer ürünlerle entegre edilebildiğinin test edilmesi ve onaylanması da gerekmektedir. Son olarak gerçekleştirilen testler sırasında üründe, varsa, istenmeyen fonksiyonlarında ortaya çıkartılması hedeflenmelidir.

### 2.5.1.3.1 Beyaz kutu testleri

Beyaz kutu testleri, testi gerçekleştiren kişinin yazılımın iç işlemlerini kaynak kodu seviyesinde incelemesine dayanmaktadır. Kabul edilen beyaz kutu test yöntemlerinden biri temel-yol testleridir. Bu yöntemde yapılan bir hamle kod modülünde her bağımsız yolu denemek için gerçekleştirilmektedir. Bağımsız yolları tespit etmenin birçok ilginç yöntem bulunmaktadır. Bu test yöntemi kaynak kodu seviyesinde olduğu için yazılım geliştirilirken uygulanabilmektedir. Bu test yöntemi sistem fonksiyonlarının doğruluğunun test edildiği doğrulama testleri ile uyuşmaktadır.

### 2.5.1.3.2 Siyah kutu testleri

Siyah kutu testleri, testi gerçekleştiren kişinin bütün kod modüllerini yalnızca giriş ve çıkışlar olarak tanımlamasını, ve bu sırada girişlerin çıkışlara dönüşürken geçirdikleri değişimlerle ilgilenmemesini sağlayacak şekilde tasarlanmışlardır. Bu yöntem sayesinde kod modüllerinin içerideki çalışmalarının görülebilmesi gerekmediğinden kaynak koda ihtiyaç yoktur. Siyah kutu testlerine örnek bir metod sınır değeri testleridir. Sınır değeri testlerinde, test altındaki modüle, geçerli değerler, geçersiz değerler ve sınır değerleri sağlanarak modül test edilmektedir. Çıkışlar ise daha sonra ölçülmekte ve eğer beklenen çıkış aralığı içindeyseler kabul edilmektedirler. Siyah kutu testleri normalde sistem entegrasyonu sırasında veya modüllerin kodlaması bittikten sonra gerçekleştirilmektedir. Bu test çeşidi ayrıca kabul testleri sırasında görülmekte ve doğrulama testlerinin çıkış noktası olarak kabul edilmektedir.

COTS ürünleri, kaynak kodun erişilemez olmasından dolayı fiziksel testlere tabi tutulabilmektedir. Testlerden bazıları ürünün dokümanate edilmemiş özelliklerini ve/veya yazılımdaki hataları (bugs) tespit etmek için, bazıları ise ürün geliştiricinin yayınladığı ürün bilgisi ve spesifikasyonlarının doğruluğunu veya yanlışlığını ispatlamak için yapılmaktadır. Bu iki test şekli ürün onamanın özel bir durumudur. İlk testler ürün hakkındaki bilgilerin arttırılması için, ikinciler de ürün geliştirici firmanın ürün hakkındaki iddialarını doğrulamak için gerçekleştirilmektedir. Siyah kutu testleri ve beyaz kutu testleri gerçekleştiremeyecek bilgilere sahip olduğumuz

durumlarda tercih edilebilecek ideal yöntemdir.

#### **2.5.1.3.3 Test yöntemleri**

COTS ürünleri için tavsiye edilen yöntemlerden bir tanesi de senaryo tabanlı testler gerçekleştirmektir. Bu yöntemde ürün için geçerli olabilecek bir senaryo kütüphanesi oluşturulur. Burada dikkat edilmesi gereken oluşturulacak senaryoların sadece test edilecek ürün için değil, ürünün çalışacağı bütün sistemi kapsayacak işletim prosedürlerini içermesi olmalıdır. Daha sonra bu senaryolardan yola çıkarak yeterli derinlikte ve kapsamda test prosedürleri oluşturulmalıdır. Bu tür testlerin sonucunda test edilmekte olan ürünün çalıştığı sistemde düzgün çalıştığı onaylanmış olur.

Bir başka yöntemde hata enjeksiyon yöntemidir. Bu yöntem test edilecek ürünün iç işlemlerine erişimin mümkün olmadığı durumlarda kullanılabilir. Bu yöntemde test edilecek ürünün veri ve kontrol akışı girişlerine hatalı değerler yolladır ve sonuçları izlenir. Bu teknik test edilecek COTS ürünlerinin bilinmeyen ve beklenmeyen durumlarda vereceği tepkileri incelemek ve bu tepkileri kontrol edebilmek için çok faydalı olmaktadır.

#### **2.5.1.4 Test Yöntemlerinin Değerlendirilmesi**

Yukarıda anlatılan test teknikleri BT sistemlerinde kullanılacak COTS ürünlerinin fonksiyonelliklerini değerlendirmek amacıyla kullanılabilir. Kullanılacak ürünün sağlayacağı garantiden emin olunduktan sonra ürünün fonksiyonelliğinin de incelenmesi gerekmektedir. Bu incelemeyi yaparken kullanılabilecek en etkili yöntem beyaz kutu testleridir. Fakat COTS ürünleri için çoğu zaman beyaz kutu testlerini gerçekleştirmek mümkün olmamaktadır, çünkü beyaz kutu testleri için gereken birçok bilgi satın alınan COTS ürünleri ile birlikte gelmemekte ve üreticiler bu bilgileri şirket dışına hiçbir şekilde açmamaktadırlar. Kurulacak sistem için kullanılacak COTS ürünü hakkında beyaz kutu testi gerçekleştirebilecek kadar bilgi sahibi olduğunda (ürünün kaynak kodu) veya en azından ürünün beyaz kutu test sonuçları incelendiğinde, ürünün fonksiyonelliği hakkında çok daha kesin bilgilere ulaşılmış olur. Bir diğer yöntem olan siyah kutu

testleri ise ürün hakkında fazla bir bilgi sahibi olmadan da gerçekleştirilebilir. Kullanılacak COTS ürünleri sisteme entegre edilmeden önce bu testler yeterli ve bilgili personel tarafından mutlaka gerçekleştirilmelidir. Ayrıca 2.5.1.3 bölümünde anlatılan diğer iki test yöntemi de kesinlikle yeterli personel tarafından uygulanmalı ve sonuç raporları dikkatlice incelendikten sonra ürün sistemde kullanılmaya başlanmalıdır.

#### **2.5.1.5 V-RATE Metodu & Ortak Kriterler Standardı**

Ortak Kriterler, ISO 15408, BT ürün veya sistemlerinin sağladıkları fonksiyonellik ve garanti bakımından değerlendirilebilmeleri için müşterilere ve ürün geliştiricilere yardımcı olmaktadır. Ortak Kriterler iki adet dokümanın hazırlanmasını gerektirmektedir, güvenlik hedefi ve koruma profili dokümanları. Müşteriler koruma profillerini belli bir ürün çeşidi için (örneğin, güvenlik duvarları, işletim sistemleri, ve akıllı kartlar) güvenlik ihtiyaçlarını tanımlamakta kullanırlar ve yayınlırlar. Koruma profilleri spesifik bir uygulamadan bağımsız olarak geniş bir müşteri kitlesinin fonksiyonellik ve garanti ihtiyaçlarını tanımlamaktadır. Güvenlik hedefi ise belirli bir ürünün geliştiricisi tarafından hazırlanmış, ürünün desteklediği güvenlik fonksiyonlarını, geliştirme sırasında kullanılan süreçleri, ve hedeflenen koruma profiline uygunluğun nasıl sağlandığını açıklamaktadır. Ortak Kriterler standardı ise güvenlik hedefi dokümanının nasıl oluşturulması gerektiğini ve müşterinin hazırlamış olduğu koruma profiline uygun olarak nasıl değerlendirilmesi gerektiğini tanımlamaktadır. [Rottke, 2002]

Asıl amacı uluslararası kabul gören bilgi teknolojileri güvenlik değerlendirme standardı haline gelmek olan Ortak Kriterler COTS ürünlerinin güvenilirliğinin artırılması için V-RATE metodunu standarda dahil ederek önerebilir. V-RATE yöntemi ürün geliştiricinin ürünü ve süreçlerini incelemek için kriterler sunmaktadır ve bu sayede COTS ürününün belirli bir hedefe ulaşmasına yardımcı olabilir. V-RATE yöntemi teknolojiiden bağımsız olduğu için Ortak Kriterler'e göre çok daha soyuttur. Ortak Kriterler için yapılan eleştirilerden biri de standarda uygun olarak ürünleri değerlendirmenin çok fazla tekrarlanan gereksiz işler ortaya çıkarmasıdır. V-RATE modeli COTS ürünlerinin yalnızca siyah kutu testleri aracılığıyla kabul edilmesi ile Ortak Kriterler testlerinden geçmesi arasında bir köprü oluşturabilir.

[Lipson, 2002] Sistemde kullanılacak COTS ürünü seçilirken Ortak Kriterler sertifikası alan bir ürünün tercih edilmesi çok avantajlıdır. Fakat çoğu ürün grubu için şu anda bu mümkün olmamaktadır. Dolayısıyla ürünü satın alan müşteri birtakım testler ve değerlendirmeler gerçekleştirmelidir. Ürüne yalnızca fonksiyonel testler yapıldığında (siyah kutu testleri) ürünün iddia ettiği özellikleri sağladığı onaylanmış olur fakat güvenlik için bu yeterli değildir. Bu yüzden ürünün sağladığı garantinin de V-RATE yönteminin uygulanması ile belirlenmesi, risklerin tespit edilip azaltılması gerekmektedir.[Lipson, 2002] Ancak ikisi birlikte uygulandığında (V-RATE, fonksiyonellik testleri) Ortak Kriterler sertifikasına sahip olmayan bir uygulama yazılımı güvenliğin önemli olduğu sistemlerde kullanılabilir.

## 3 BİLGİ TEKNOLOJİLERİ SİSTEMLERİ GÜVENLİK GEREKSİNİMLERİ

### 3.1 Güvenlik Fonksiyonel Gereksinimleri

Güvenlik fonksiyonel gereksinimleri sınıflara ayrılmıştır. Sınıflar güvenlik gereksinimlerinin en genel gruplarıdır, ve bir sınıfın bütün üyeleri ortak bir konuda odaklanmışlardır. Ortak Kriterler'in ikinci bölümünde 11 tane fonksiyonel sınıf vardır. Bu sınıflar;

- FAU: Security audit (Güvenlik denetimi)
- FCO: Communication (İletişim)
- FCS: Cryptographic support (Kriptografi desteği)
- FDP: User data protection (Kullanıcı verilerinin korunması)
- FIA: Identification and authentication (Tanıma ve kimlik doğrulama)
- FMT: Security management (Güvenlik yönetimi)
- FPR: Privacy (Gizlilik)
- FPT: Protection of the TSF (TSF' nin korunması)
- FRU: Resource utilisation (Kaynak kullanımı)
- FTA: TOE access (TOE erişimi)
- FTP: Trusted path/channels (Güvenilir yollar/kanallar)

Bütün bu sınıflar çeşitli sayılarda aileler içermektedir. Ailelerin içindeki gereksinimler güvenlik amaçlarını paylaşmaktadır fakat bu gereksinimlerin yaptıkları vurgular farklıdır. Örneğin, güvenlik denetimi sınıfı denetlemenin farklı yönleriyle ilgilenen altı aile içermektedir. (veri üretimi denetimi, denetim analizi, denetim olaylarının saklanması)

Bütün aileler bir veya daha fazla bileşen içermektedir ve bu bileşenler arasında bir hiyerarşi olabilir veya olmayabilir. Örneğin, veri üretimi denetimi birbirleri arasında hiyerarşi olmayan iki bileşen içermektedir, bu bileşenlerden biri denetim kayıtlarının üretimi ile diğeri de kullanıcılar ile denetlenecek olayların eşleştirilmesi ile ilgilenmektedir.

### 3.2 Güvenlik Yönetim Gereksinimleri

Bu bölümde BT sistemlerinin tasarlanması ve Ortak Kriterler'e uygun olarak değerlendirilebilmesi için gerekli olan Güvenlik Yönetim Gereksinimleri tanımlanmıştır. Bu gereksinimler ISO 17799 standardının kontrol objelerin Ortak Kriterler standardının sınıf, aile ve bileşen yapısına çevrilerek gösterilmektedir. [BS 7799-2, 2002]

BT sistemlerinde gerçekleştirilen risk değerlendirmesi ve risk yönetimi sonuçlarına göre bu gereksinimlerden ihtiyaç duyulanlar seçilerek sistemin Güvenlik Hedefi dokümanı oluşturulmalıdır.

Çizelge 3.1 Güvenlik yönetim gereksinimleri [Tabuchi, 2002]

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>• Güvenlik Politikası (MSP)           <ul style="list-style-type: none"> <li>o Bilgi Güvenliği Politikası (MSP_ISP)               <ul style="list-style-type: none"> <li>▪ Bilgi Güvenliği Politikası Dokümanı (MSP_ISP.1)</li> <li>▪ İnceleme ve Değerlendirme (MSP_ISP.2)</li> </ul> </li> </ul> </li> <li>• Güvenlik Organizasyonu (MSO)           <ul style="list-style-type: none"> <li>o Bilgi Güvenliği Altyapısı (MSO_ISI)               <ul style="list-style-type: none"> <li>▪ Bilgi Güvenliği Forumunun Yönetimi (MSO_ISI.1)</li> <li>▪ Bilgi Güvenliği Koordinasyonu (MSO_ISI.2)</li> <li>▪ Bilgi Güvenliği Sorumluluklarının Paylaşımı (MSO_ISI.3)</li> <li>▪ Bilgi İşleme Merkezlerine Yetkilendirme Süreci (MSO_ISI.4)</li> <li>▪ Uzman Bilgi Güvenliği Tavsiyeleri (MSO_ISI.5)</li> <li>▪ Organizasyonlar Arasında Ortak Çalışma (MSO_ISI.6)</li> <li>▪ Bilgi Güvenliğinin Bağımsız İncelenmesi (MSO_ISI.7)</li> </ul> </li> <li>o Üçüncü Parti Erişimin Güvenliği (MSO_STA)               <ul style="list-style-type: none"> <li>▪ Üçüncü Parti Erişimden Kaynaklanan Risklerin Belirlenmesi (MSO_STA.1)</li> <li>▪ Üçüncü Parti Kontratların Güvenlik Gereksinimleri (MSO_STA.2)</li> </ul> </li> <li>o Dış Kaynak Kullanımı (MSO_OTS)               <ul style="list-style-type: none"> <li>▪ Dış Kaynak Kullanımı Kontratlarının Güvenlik</li> </ul> </li> </ul> </li> </ul> |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

### Gereksinimleri (MSO\_OT5.1)

- Varlık Sınıflandırma ve Kontrolü (MAC)
  - o Varlıklar için Hesap Verilebilirlik (MAC\_ACA)
    - Varlıkların Envanteri (MAC\_ACA.1)
  - o Bilgi Sınıflandırması (MAC\_IFC)
    - Sınıflandırma Kılavuzu (MAC\_IFC.1)
    - Bilgi Sınıflandırma ve Saklama (MAC\_IFC.2)
- Personel Güvenliği (MPS)
  - o İş Tanımlamada ve Kaynak Dağıtımında Güvenlik (MPS\_JDR)
    - Güvenliğin İş Sorumluluklarına Eklenmesi (MPS\_JDR.1)
    - Personel Takibi ve Politikalar (MPS\_JDR.2)
    - Gizlilik Anlaşması (MPS\_JDR.3)
    - İşe Alım Kural ve Koşulları (MPS\_JDR.4)
  - o Kullanıcı Eğitimi (MPS\_UTR)
    - Bilgi Güvenliği Eğitimi ve Alıştırmaları (MPS\_UTR.1)
  - o Güvenlik Olaylarının ve Hatalarının Cevaplanması (MPS\_SIM)
    - Güvenlik Olaylarının Raporlanması (MPS\_SIM.1)
    - Güvenlik Zayıflıklarının Raporlanması (MPS\_SIM.2)
    - Yazılım Hatalarının Raporlanması (MPS\_SIM.3)
    - Olaylardan Ders Çıkarılması (MPS\_SIM.4)
    - Disiplin Süreci (MPS\_SIM.5)
- Fiziksel Güvenlik ve Ortam Güvenliği (MPE)
  - o Güvenli Bölgeler (MPE\_SER)
    - Fiziksel Güvenlik Çevresi (MPE\_SER.1)
    - Fiziksel Giriş Kontrolleri (MPE\_SER.2)
    - Ofislerin, Odaların ve Yerleşkelerin Güvenliği (MPE\_SER.3)
    - Güvenli Bölgelerde Çalışmak (MPE\_SER.4)
    - İzole Dağıtım ve Yükleme Alanları (MPE\_SER.5)
  - o Teçhizat Güvenliği (MPE\_EQS)
    - Teçhizat Yeri ve Koruması (MPE\_EQS.1)
    - Güç Kaynakları (MPE\_EQS.2)
    - Kablolama Güvenliği (MPE\_EQS.3)
    - Teçhizat Bakımı (MPE\_EQS.4)

- Yerleşke Dışındaki Teçhizatın Güvenliği (MPE\_EQS.5)
- Teçhizatın Güvenli İmhası ve Tekrar Kullanımı (MPE\_EQS.6)
- o Genel Kontroller (MPE\_CTR)
  - Temiz Masa Üstü ve Temizlik Takip Politikası (MPE\_CTR.1)
  - Mülkiyetin Kaldırılması (MPE\_CTR.2)
- İletişim ve İşlemlerin Yönetimi (MCO)
  - o İşlemsel Prosedürler ve Sorumluluklar (MCO\_OPR)
    - Doküman Edilmiş İşlemsel Prosedürler (MCO\_OPR.1)
    - İşlemsel Değişiklik Kontrolü (MCO\_OPR.2)
    - Olay Yönetim Prosedürleri (MCO\_OPR.3)
    - Görevlerin Ayrılması (MCO\_OPR.4)
    - Geliştirme ve İşlemsel Yerleşkelerin Ayrılması (MCO\_OPR.5)
    - Dış Yerleşkelerin Yönetimi (MCO\_OPR.6)
  - o Sistem Planlama ve Kabul (MCO\_SPA)
    - Kapasite Planlama (MCO\_SPA.1)
    - Sistem Kabulü (MCO\_SPA.2)
  - o Kötü Niyetli Yazılımlara Karşı Korunma (MCO\_PMS)
    - Kötü Niyetli Yazılımlara Karşı Kontroller (MCO\_PMS.1)
  - o İdare (MCO\_HSP)
    - Bilgi Yedeklemesi (MCO\_HSP.1)
    - Operatör Logları (MCO\_HSP.2)
    - Hata Loglama (MCO\_HSP.3)
  - o Ağ Yönetimi (MCO\_NMG)
    - Ağ Kontrolleri (MCO\_NMG.1)
  - o Medyaların Kullanımı ve Güvenliği (MCO\_MHD)
    - Çıkarılabilir Bilgisayar Medyalarının Yönetimi (MCO\_MHD.1)
    - Medyaların İmhası (MCO\_MHD.2)
    - Bilgi Kullanımı Prosedürleri (MCO\_MHD.3)
    - Sistem Dokümantasyonunun Güvenliği (MCO\_MHD.4)

- o Bilginin ve Yazılımların Değişimi (MCO\_EIS)
  - Bilgi ve Yazılım Değişim Anlaşmaları (MCO\_EIS.1)
  - Geçişlerdeki Medyanın Güvenliği (MCO\_EIS.2)
  - Elektronik Ticaretin Güvenliği (MCO\_EIS.3)
  - Elektronik Postaların Güvenliği (MCO\_EIS.4)
  - Elektronik Ofis Sistemlerinin Güvenliği (MCO\_EIS.5)
  - Herkese Açık Sistemler (MCO\_EIS.6)
  - Bilgi Değişiminin Diğer Yöntemleri (MCO\_EIS.7)
- Erişim Kontrolü (MAC)
  - o Erişim Kontrolleri için İş Gereksinimleri (MAC\_BAC)
    - Erişim Kontrolü Politikaları (MAC\_BAC.1)
  - o Kullanıcı Erişim Yönetimi (MAC\_UAM)
    - Kullanıcı Kaydı (MAC\_UAM.1)
    - Ayrıcalıkların Yönetimi (MAC\_UAM.2)
    - Kullanıcı Şifre Yönetimi (MAC\_UAM.3)
    - Kullanıcı Erişim Haklarının İncelenmesi (MAC\_UAM.4)
  - o Kullanıcı Sorumlulukları (MAC\_URS)
    - Şifre Kullanımı (MAC\_URS.1)
    - Başboş Kullanıcı Teçhizatı (MAC\_URS.2)
  - o Ağ Erişim Kontrolleri (MAC\_NAC)
    - Ağ Servislerinin Kullanım Politikası (MAC\_NAC.1)
    - Zorunlu Yol (MAC\_NAC.2)
    - Dış Bağlantılar için Kullanıcı Doğrulanması (MAC\_NAC.3)
    - Düğüm Doğrulanması (MAC\_NAC.4)
    - Uzaktan Tanınmış Port Koruması (MAC\_NAC.5)
    - Ağların Ayrılması (MAC\_NAC.6)
    - Ağ Bağlantıları Kontrolü (MAC\_NAC.7)
    - Ağ Yönlendirme Kontrolleri (MAC\_NAC.8)
    - Ağ Servislerinin Güvenliği (MAC\_NAC.9)
  - o İşletim Sistemleri Erişim Kontrolleri (MAC\_OSA)
    - Otomatik Terminal Tanımlanması (MAC\_OSA.1)
    - Terminal Log-on Prosedürleri (MAC\_OSA.2)
    - Kullanıcı Tanımlama ve Doğrulama (MAC\_OSA.3)

- Şifre Yönetim Sistemi (MAC\_OSA.4)
- Sistem Özelliklerinin Kullanımı (MAC\_OSA.5)
- Koruyucu Kullanıcıların Zorlayıcı Alarmları (MAC\_OSA.6)
- Terminal Zamanının Dolması (MAC\_OSA.7)
- Bağlantı Süresinin Sınırlandırılması (MAC\_OSA.8)
- o Uygulama Erişim Kontrolü (MAC\_AAC)
  - Bilgi Erişim Sınırlamaları (MAC\_AAC.1)
  - Hassas Sistem İzolasyonu (MAC\_AAC.2)
- o Sistem Erişiminin ve Kullanımının İzlenmesi (MAC\_MAU)
  - Olay Logları (MAC\_MAU.1)
  - Sistem Kullanımının İzlenmesi (MAC\_MAU.2)
  - Saat Senkronizasyonu (MAC\_MAU.3)
- o Gezici Bilgisayarlar (MAC\_MCT)
  - Gezici Bilgisayarlar (MAC\_MCT.1)
  - Uzaktan Elektronik Ortam Çalışma (MAC\_MCT.2)
- Sistem Geliştirilmesi ve Bakımı (MDM)
  - o Sistemin Güvenlik Gereksinimleri (MDM\_RQS)
    - Güvenlik Gereksinimlerinin Analizi ve Spesifikasyonu (MDM\_RQS.1)
  - o Uygulama Sistemlerinin Güvenliği (MDM\_APS)
    - Girdilerin Onaylanması (MDM\_APS.1)
    - İç Süreçlerin Kontrolü (MDM\_APS.2)
    - Mesajların Doğrulanması (MDM\_APS.3)
    - Çıktıların Onaylanması (MDM\_APS.4)
  - o Kriptografik Kontroller (MDM\_CRP)
    - Kriptografik Kontrollerin Kullanım Politikası (MDM\_CRP.1)
    - Şifreleme (MDM\_CRP.2)
    - Dijital İmzalar (MDM\_CRP.3)
    - Kaynağın İnkarını Engelleyen Servisler (MDM\_CRP.4)
    - Anahtar Yönetimi (MDM\_CRP.5)
  - o Sistem Dosyalarının Güvenliği (MDM\_SFL)
    - İşlemsel Yazılımların Kontrolü (MDM\_SFL.1)
    - Sistem Test Verilerinin Korunması (MDM\_SFL.2)

- Program Kaynak Kütüphanelerine Erişim Kontrolü (MDM\_SFL.3)
- o Geliştirme ve Destek Süreçlerinde Güvenlik (MDM\_DSP)
  - Değişiklik Kontrol Prosedürleri (MDM\_DSP.1)
  - İşletim Sistemi Değişikliklerinin Teknik İncelemesi (MDM\_DSP.2)
  - Yazılım Paketlerinin Değiştirilmesinde Sınırlamalar (MDM\_DSP.3)
  - Saklı Kanallar ve Trojan Kodları (MDM\_DSP.4)
  - Yazılım Geliştirilmesinde Dış Kaynak Kullanımı (MDM\_DSP.5)
- İş Devamlılığı Yönetimi (MBC)
  - o İş Devamlılığı Yönetimi Konuları (MBC\_BCN)
    - İş Devamlılığı Yönetimi Süreci (MBC\_BCN.1)
    - İş Devamlılığı ve Etki Analizi (MBC\_BCN.2)
    - Devamlılık Planları Yazımı ve Uygulaması (MBC\_BCN.3)
    - İş Devamlılığı Planlama Çatısı (MBC\_BCN.4)
    - Test, Bakım ve İş Devamlılık Planlarının Yeniden Değerlendirilmesi (MBC\_BCN.5)
- Uyumluluk (MCP)
  - o Yasal Gereksinimlere Uyumluluk (MCP\_LRQ)
    - Uygulanabilir Yasaların Tespit Edilmesi (MCP\_LRQ.1)
    - Fikri Telif Hakları (MCP\_LRQ.2)
    - Organizasyon Kayıtlarının Korunması (MCP\_LRQ.3)
    - Kişisel Bilgilerin Gizliliği ve Veri Korunması (MCP\_LRQ.4)
    - Bilgi İşleme Yerlerinin Kötüye Kullanıma Karşı Korunması (MCP\_LRQ.5)
    - Kriptografik Kontrollerin Yönetmelikleri (MCP\_LRQ.6)
    - Kanıt Toplama (MCP\_LRQ.7)
  - o Güvenlik Politikasının Gözden Geçirilmesi ve Teknik Uyumluluk (MCP\_RPT)
    - Güvenlik Politikasına Uyumluluk (MCP\_RPT.1)
    - Teknik Uyumluluk Kontrolü (MCP\_RPT.2)

- o Sistem Denetimleri (MCP\_AUD)
  - Sistem Denetim Kontrolleri (MCP\_AUD.1)
  - Sistem Denetleme Araçlarının Korunması (MCP\_AUD.2)

**Çizelge 3.1 Güvenlik yönetim gereksinimleri**'de belirtilen Güvenlik Yönetim Gereksinimlerinin bileşen detayları Ortak Kriterler yapısına uygun olarak tanımlanmalıdır. Erişim kontrolü sınıfının kullanıcı kaydı bileşeni örnek olarak ele alınmıştır.

### 3.2.1 Örnek Güvenlik Yönetim Gereksinimleri

#### 3.2.1.1 Erişim Kontrolü Sınıfı

##### **Sınıf: Erişim Kontrolü (MAC)**

**Aile:** Kullanıcı Erişimi Yönetimi (MAC\_UAM)

**Amaç:** Bilgi sistemlerine yetkisiz erişimin engellenmesi.

**Bileşen:** Kullanıcı kaydı (MAC\_UAM.1)

Bağımlılık: Yok

Sistem entegrasyonunu gerçekleştiren ve işletenler için eylemler;

MAC\_UAM.1.1M Çok kullanıcıli sistemlere ve servislere erişimin sağlanması için kullanıcı kaydı gerçekleştirmek ve kullanıcı kayıtlarını silmek için biçimsel bir kayıt prosedürü hazırlanmalıdır.

MAC\_UAM.1.2M Çok kullanıcıli bir bilgi servisine erişim biçimsel bir [atama: kullanıcı kayıt süreci] ile gerçekleştirilmelidir.

MAC\_UAM.1.3M Kullanıcı kayıt sürecinde eşsiz kullanıcı ID'leri kullanılmalı ve kullanıcılar eylemlerinden sorumlu tutulabilmelidir. Grup ID'leri yalnızca [atama: grup çalışmaları durumları] hallerinde kullanılmalıdır.

MAC\_UAM.1.4M Kullanıcı kayıt süreci kullanıcının [atama: yetkili kişi]'den [atama: bilgi sistemlerini veya servislerini] kullanmak üzere onay alınmış olduğunu kontrol etmelidir.

MAC\_UAM.1.5M Kullanıcı kayıt süreci kullanıcının aldığı erişim hakkının [atama: iş amaçları] uygun olduğunu ve [atama: organizasyonel güvenlik politikaları] ile tutarlı olduğunu kontrol etmelidir.

MAC\_UAM.1.6M Kullanıcı kayıt süreci kullanıcılara erişim haklarının yazılı olarak teslim edilmesini içermelidir.

MAC\_UAM.1.7M Kullanıcı kayıt süreci kullanıcılara [atama: eylem listesi] sağlayarak erişim haklarını anlamasını garanti etmelidir.

MAC\_UAM.1.8M Kullanıcı kayıt süreci servis sağlayıcıların yetkilendirme işlemi tamamlayıncaya kadar kullanıcıya erişim vermemesini garanti etmelidir.

MAC\_UAM.1.9M Kullanıcı kayıt süreci servislerin kullanımı için kayıt olmuş tüm kullanıcıların resmi bir listesinin oluşturulmasını sağlamalıdır.

MAC\_UAM.1.10M Kullanıcı kayıt süreci kullanıcının [seçim: iş değiştirme, kurumdan ayrılma] durumlarında anında erişim haklarının kaldırılmasını sağlamalıdır.

MAC\_UAM.1.11M Kullanıcı kayıt süreci her [atama: periyodik süre]'de sistemi kontrol ederek kullanım dışı olan ID'leri ve hesapları silmelidir.

MAC\_UAM.1.12M Kullanıcı kayıt süreci kullanım dışı olan ID'lerin başka kullanıcılara verilmeyeceğini garanti etmelidir.

MAC\_UAM.1.13M Kullanıcı kayıt sürecinde erişim hakkı verilen kullanıcıların yetkileri dışında erişim sağlamaları durumunda alacakları cezaları belirtmelidir.

Değerlendirme öğelerinin içeriği ve sunumu;

MAC\_UAM.1.1C Kullanıcı kayıt dokümantasyonu kayıt, kontrol ve kullanıcı kayıtlarının bakımı konusundaki tüm prosedürleri içermelidir.

Değerlendirici eylem öğeleri;

MAC\_UAM.1.1E Değerlendirici sağlanan bilginin bütün gereksinimleri karşıladığını onaylamalıdır.

### 3.2.1.2 Fiziksel Güvenlik ve Ortam Güvenliği Sınıfı

**Sınıf:** Fiziksel Güvenlik ve Ortam Güvenliği (MPE)

**Aile:** Güvenli Bölgeler (MPE\_SER)

**Amaç:** İş alanına ve bilgilerine yetkisiz erişim, hasar ve müdahalenin engellenmesi.

**Bileşen:** Fiziksel giriş kontrolleri (MPE\_SER.2)

Bağımlılık: Yok

Sistem entegrasyonunu gerçekleştiren ve işletenler için eylemler;

MPE\_SER.1.1M İş alanına ve bilgilerine fiziksel erişimin kontrollü olarak

sağlanabilmesi için fiziksel girişin kontrolü prosedürü hazırlanmalıdır.

MPE\_SER.1.2M İş alanına ve bilgilerine fiziksel erişim [atama: fiziksel girişin kontrolü süreci] ile gerçekleştirilmelidir.

MPE\_SER.1.3M Fiziksel giriş kontrolü prosedürüne göre [atama: güvenli alanlar]'da ziyaretçilere [seçim: eşlik edilmeli, üstleri aranmalı]'dır. Ziyaretçilerin giriş çıkış tarihleri ve saatleri kayıt edilmelidir.

MPE\_SER.1.4M Fiziksel giriş kontrolü prosedürüne göre ziyaretçilerin [atama: güvenli alanlar] [atama: yetili amaçlar] dahilinde erişimlerine izin verilmeli ve [atama: güvenlik gerekleri] ile [atama: acil durum yöntemleri] konularında bilgilendirilmelidir.

MPE\_SER.1.5M Fiziksel giriş kontrolü prosedürüne göre [atama: hassas bilgiler]'e ve [atama: bilgi işleme araçları]'na erişim denetlenmeli ve sadece [atama: yetkili kullanıcılar]la sınırlı olmalıdır. Kimlik doğrulama denetimleri [seçim: giriş kartı, parola] erişimleri yetkilendirmek için kullanılmalıdır.

MPE\_SER.1.6M Fiziksel giriş kontrolü prosedürüne göre [atama: personel listesi]'dekilerin görünür biçimde kimlik kartı taşımaları zorunlu tutulmalıdır.

MPE\_SER.1.7M Fiziksel giriş kontrolü prosedürüne göre güvenli alanlara erişim hakları [atama: periyodik süre] aralıklarla gözden geçirilmeli ve güncelleştirilmelidir. Değerlendirme öğelerinin içeriği ve sunumu;

MPE\_SER.1.1C Fiziksel giriş kontrolü dokümantasyonu tüm prosedürleri, güvenli bölgeleri ve giriş haklarını tanımlamalıdır.

Değerlendirici eylem öğeleri;

MPE\_SER.1.1E Değerlendirici sağlanan bilginin bütün gereksinimleri karşıladığını onaylamalıdır.

MPE\_SER.1.2E Değerlendirici fiziksel giriş kontrolü prosedürlerine uyulup uyulmadığını yerinde kontrol etmelidir.

### 3.3 Güvenlik Garanti Gereksinimleri

Güvenlik garanti gereksinimleri sınıflara ayrılmıştır. Sınıflar güvenlik gereksinimlerinin en genel gruplarıdır, ve bir sınıfın bütün üyeleri ortak bir konuda odaklanmışlardır. Ortak Kriterler'in üçüncü bölümünde 8 tane garanti sınıfı vardır. Bu sınıflar;

- ACM: Configuration management (Konfigürasyon yönetimi)
- ADO: Delivery and operation (Dağıtım ve işletim)
- ADV: Development (Geliştirme)
- AGD: Guidance documents (Kılavuz Dokümanları)
- ALC: Life cycle support (Hayat döngüsü desteği)
- ATE: Tests (Testler)
- AVA: Vulnerability Assessment (Açıklık değerlendirme)
- AMA: Maintenance of Assurance (Garantinin sürdürülmesi)

İki tane garanti sınıfı da Koruma Profilleri ve Güvenlik Hedefleri için garanti gereksinimlerini içermektedir.

Bütün bu sınıflar çeşitli sayılarda aileler içermektedir. Ailelerin içindeki gereksinimler güvenlik amaçlarını paylaşmaktadır fakat bu gereksinimlerin yaptıkları vurgular farklıdır. Örneğin, geliştirme sınıfı tasarım dokümantasyonunun farklı yönleriyle ilgilenen yedi farklı aile içermektedir. (fonksiyonel spesifikasyon, üst düzey tasarım ve temsilin karşılanması)

Bütün aileler bir veya daha fazla bileşen içermektedir, ve bu bileşenler arasında katı bir hiyerarşi vardır. Örneğin, fonksiyonel spesifikasyon ailesi birbirleri arasında hiyerarşi olan ve fonksiyonel spesifikasyonun bütünlüğü ve biçimselliği ile ilgilenen dört bileşen içermektedir. [ISO 15408, 1999]

Çizelge 3.2 Güvenlik garanti gereksinimleri

| Garanti Sınıfı                     | Garanti Ailesi              | Kısaltılmış Adı |
|------------------------------------|-----------------------------|-----------------|
| ACM Sınıfı: Konfigürasyon Yönetimi | KM otomasyon                | ACM_AUT         |
|                                    | KM yetenekleri              | ACM_CAP         |
|                                    | KM kapsamı                  | ACM_SCP         |
| ADO Sınıfı: Teslim ve çalışma      | Teslim                      | ADO_DEL         |
|                                    | Kurulum, üretim ve başlatma | ADO_IGS         |
| ADV Sınıfı: Geliştirme             | Fonksiyonel spesifikasyon   | ADV_FSP         |
|                                    | Üst düzeyde tasarım         | ADV_HLD         |
|                                    | Uygulama temsili            | ADV_IMP         |
|                                    | TSF iç öğeleri              | ADV_INT         |

|                                        |                                    |         |
|----------------------------------------|------------------------------------|---------|
|                                        | Alt düzey tasarım                  | ADV_LLD |
|                                        | Temsilin karşılanması              | ADV_RCR |
|                                        | Güvenlik politikası modellemesi    | ADV_SPM |
| AGD Sınıfı: Kılavuz<br>Dokümanlar      | Yönetici kılavuzu                  | AGD_ADM |
|                                        | Kullanıcı kılavuzu                 | AGD_USR |
| ALC Sınıfı: Yaşam<br>Döngüsü Desteği   | Geliştirme güvenliği               | ALC_DVS |
|                                        | Hata düzeltme                      | ALC_FLR |
|                                        | Kullanım ömrü tanımı               | ALC_LCD |
|                                        | Aletler ve teknikler               | ALC_TAT |
| ATE Sınıfı: Testler                    | Kapsam                             | ATE_COV |
|                                        | Derinlik                           | ATE_DPT |
|                                        | Fonksiyonel testler                | ATE_FUN |
|                                        | Bağımsız testler                   | ATE_IND |
| AVA Sınıfı: Açıklık<br>değerlendirmesi | Gizli kanal analizi                | AVA_CCA |
|                                        | Kötüye kullanım                    | AVA_MSU |
|                                        | TOE güvenlik fonksiyonlarının gücü | AVA_SOF |
|                                        | Zayıflık analizi                   | AVA_VLA |

## 4 BİLGİ TEKNOLOJİLERİ SİSTEMLERİ GÜVENLİK DEĞERLENDİRMESİ

Çalışmanın giriş bölümünde belirtildiği gibi BT sistemlerinin güvenlik değerlendirilmesinden geçebilmesi için Ortak Kriterler standardı kullanılabilir fakat standardın sistem değerlendirmeleri konusunda birtakım eksiklikleri vardır. [Apted, 2002] İlk olarak sistemler gerçek ortamlarında kullanılmaktadır ve sistemi kullanan insan kaynağı güvenlik açısından dikkat edilmesi gereken bir konudur. Oysa standardın bu konuda herhangi bir yorumu yoktur. Aksine Ortak Kriterler standardının ilk bölümünde açıkca standardın insan unsurlu ve fiziksel güvenlik tehditleri ile ilgilenmediği belirtilmektedir. [ISO 15408, 1999] Bu sebeple bu çalışmada ISO 17799 standardından kontrol objeleri alınarak Ortak Kriterler standardının sınıf yapısına uyarlanması ve sistem değerlendirmelerinde yönetim gereksinimleri olarak kullanılması önerilmiştir. Sistem değerlendirmelerinde karşılaşılan bir diğer zorluk ise sistemdeki COTS ürünlerinin değerlendirme delillerinin oluşturulması ve bu ürünlerin test edilmesidir. [Tabuchi,2002] Bu çalışmada COTS ürünleri için V-RATE değerlendirme metodolojisinin kullanılması önerilmiştir. [Lipson, 2002] Son olarak Ortak Kriterler standardının ürünler için önermiş olduğu güvenlik garanti paketleri sistemler için yetersiz kalmaktadır.[Tabuchi, 2002] Bu çalışmada dört farklı güvenlik seviyesindeki sistemler için garanti paketleri oluşturulmuştur. Önerilecek garanti paketlerinin ürünler için hazırlanmış olan EAL seviyelerinden en temel farkı daha ayrıntılı açıklık değerlendirmeleri ve sistemde garantinin devamının sağlanması konularında olmaktadır.

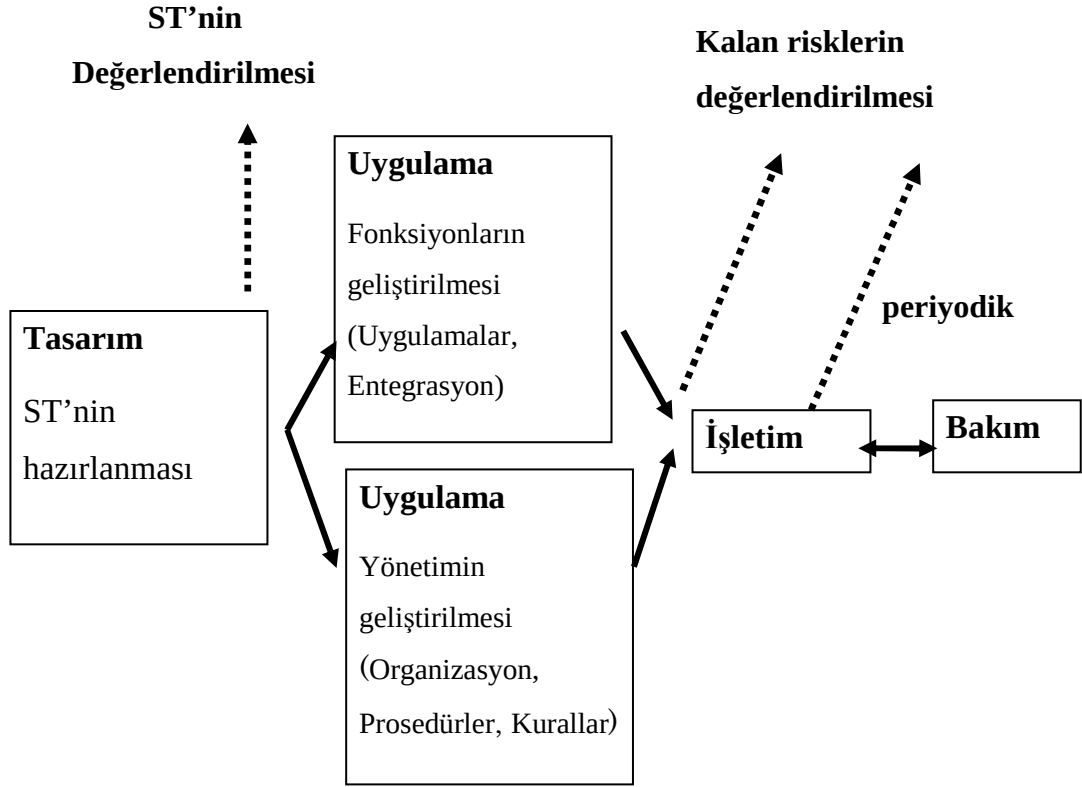
Bu çalışmada BT sistemlerinin Ortak Kriterler'e uygun olarak değerlendirilebilmesi için standartta varolan eksiklikler kapatılarak yeni bir yöntem önerilmiştir. Bu yöntem ile değerlendirmeden geçecek BT sistemi için değerlendirme süreci tanımlanmıştır. Bu süreçte ilk olarak sistemde risk değerlendirmesi ve risk yönetimi uygulanmalıdır. Gerçekleştirilen risk yönetimi sonuçlarına göre sistemin varlıkları için kabullenmeler, tehditler ve güvenlik politikaları çıkarılmalıdır. Oluşturulan bu güvenlik ortamı için güvenlik amaçları belirlendikten sonra güvenlik amaçlarını karşılamak için fonksiyonel,garanti ve yönetim gereksinimleri tespit

edilmeli ve bütün güvenlik amaçları bu yolla karşılanmalıdır. Önerilen yöntemin Ortak Kriterler standardından en büyük farkı bu noktada sistemler için ihtiyaç duyulan güvenlik amaçlarının yönetim gereksinimleri ile karşılanmasıdır. Sistemin garanti gereksinimleri oluşturulurken de sistemin taşıdığı bilgi sınıfına uygun olarak bu yöntemde önerilmiş olan garanti paketleri seçilmelidir. Sistemde kullanılan COTS ürünlerinin de değerlendirme delillerinin oluşturulmasında V-RATE yöntemi kullanılmalıdır. Sistemin güvenlik amaçlarını karşılayan bütün gereksinimler belirlendikten sonra bu gereksinimleri karşılayacak karşı tedbirler sistem için uygulanmalı ve risk değerlendirmesi tekrar edilmelidir. Sağlanan güvenliğin ve garantinin sürdürülmesi için garantinin devamı (AMA) sınıfı gereksinimlerinin denetimleri düzenli olarak gerçekleştirilmelidir.

Bu bölümde önerilen değerlendirme süreci incelenmiş, Güvenlik Hedefi dokümanının hazırlanması için gerekenler belirtilmiş ve sistemler için garanti paketleri oluşturulmuştur. Sistemin gerçekleşmesi ve değerlendirme bölüm 5'te örnek bir uygulama ile incelenmiştir.

## 4.1 Değerlendirme Süreci

Bir organizasyonun bilgi teknolojileri sistemlerinin değerlendirme süreci Güvenlik Hedefi'nin (ST) hazırlanması ile başlanmalıdır. Sistemler için ST'nin içeriği bölüm 4.3' de incelenmiştir. ST hazırlandıktan sonra bütünlük, tutarlılık ve anlaşılabilirlik gibi özellikleri göz önüne alınarak değerlendirilmeli ve daha sonra ST'de belirtilen kabullenmelere, tehditlere ve politikalara uygun olarak fonksiyonlar gerçekleştirilmelidir. Sistemi işler hale gelmeden önce ST'de tespit edilen yönetim gereksinimlerine karşı alınmış olan tedbirlerde sistemde uygulanmalı ve daha sonra BT sistemi işletilmeye başlanmalıdır. İşletim başladıktan sonra periyodik risk değerlendirmesi süreci de başlamalı ve bu değerlendirme sonuçlarına uygun olarak sistem bakıma alınmalıdır. Tasarım, uygulama, işletim ve bakım aşamalarından oluşan bir BT sistemi üretilmiş değerlendirme delilleri ile birlikte iddia ettiği garanti düzeyine ve Ortak Kriterler'e uygun olarak değerlendirilebilir. Taşınan bilginin güvenlik sınıfına uygun olarak önerilen garanti paketleri bölüm 4.2'de ele alınmıştır.



Şekil 4.1 Bilgi Teknolojileri sistem değerlendirilmesi süreci

## 4.2 Sistemler için Değerlendirme Garanti Düzeyleri

### 4.2.1 Tasnif Dışı Bilgi Ağ Sistemleri

Tasnif dışı bilgi hassas, özel veya gizli olarak sınıflandırılmamış organizasyon bilgisidir. Bu bilgiler halka açıktır ve organizasyon dışından ulaşılmasında bir sakıncanın olmadığı bilgilerdir. Bu tür bilgilerin yetkisiz kişilerin eline geçmesinin organizasyona ciddi bir etkisi yoktur. Bu tür bilgilerin taşındığı ağlarda güvenlik ön planda değildir ve ağların fonksiyonel özelliklerini sağlaması yeterli olmaktadır.

Tasnif dışı bilgi ağ sistemlerinin güvenlik düzeylerinin değerlendirilebilmesi için gereken değerlendirme delillerinin hazırlanması için sistemin entegrasyonunu sağlayan firmanın desteği yeterli olmaktadır.

Tasnif dışı bilgilerin taşındığı ağların güvenlik garanti gereksinimleri **Çizelge 4.1 Tasnif dışı bilgi ağ sistemleri**'deki gibi olmalıdır.

Çizelge 4.1 Tasnif dışı bilgi ağ sistemleri

| Garanti sınıfı                              | Garanti bileşenleri                                |
|---------------------------------------------|----------------------------------------------------|
| ACM Sınıfı: Konfigürasyon yönetimi          | ACM_CAP.2 Konfigürasyon öğeleri                    |
| ADO Sınıfı: Teslim ve çalıştırma            | ADO_IGS.1 Kurulum, üretim ve başlatma prosedürleri |
| ADV Sınıfı: Geliştirme                      | ADV_FSP.1 Biçimsel olmayan fonksiyonel belirtim    |
|                                             | ADV_RCR.1 Biçimsel olmayan karşılık gelme gösterme |
| AGD Sınıfı: Kılavuz belgeler                | AGD_ADM.1 Yönetici kılavuzu                        |
|                                             | AGD_USR.1 Kullanıcı kılavuzu                       |
| ALC Sınıfı: Yaşam döngüsü desteği           | ALC_FLR.1 Temel hataları düzeltme                  |
| ATE Sınıfı: Testler                         | ATE_IND.1 Bağımsız test – uygunluk                 |
| AMA Sınıfı: Garantinin devamının sağlanması | AMA_AMP.1 Garantinin sürdürülmesi planı            |
|                                             | AMA_CAT.1 TOE bileşen sınıflandırma raporu         |

#### 4.2.2 Hassas Bilgi Ağ Sistemleri

Normal bir bilgidен daha yüksek bir sınıflandırmaya gereksinimi olan bilgilere hassas bilgi denilmektedir. Bu tür bilgiler gizliliğin kaybına, ve bütünlüğünün yetkisiz bir şekilde değiştirilmesine karşı korunmalıdır. Hassas bilgilerin taşındığı ağlarda aynı zamanda tasnif dışı bilgilerde bulundurulabilir.

Hassas bilgi ağ sistemlerinin güvenlik düzeylerinin değerlendirilebilmesi için gereken değerlendirme delillerinin hazırlanması için sistemin entegrasyonunu sağlayan firmanın desteği yeterli olmaktadır.

Hassas bilgilerin taşındığı ağların güvenlik garanti gereksinimleri Çizelge 4.2 Hassas bilgi ağ sistemleri’deki gibi olmalıdır.

Çizelge 4.2 Hassas bilgi ağ sistemleri

| Garanti sınıfı                              | Garanti bileşenleri                                                                |
|---------------------------------------------|------------------------------------------------------------------------------------|
| ACM Sınıfı: Konfigürasyon yönetimi          | ACM_CAP.2 Konfigürasyon öğeleri                                                    |
| ADO Sınıfı: Teslim ve çalışma               | ADO_DEL.1 Teslim prosedürleri (varsa)                                              |
|                                             | ADO_IGS.1 Kurulum, üretim ve başlatma prosedürleri                                 |
| ADV Sınıfı: Geliştirme                      | ADV_FSP.1 Biçimsel olmayan fonksiyonel spesifikasyon, dış arayüzlerin tanımlanması |
|                                             | ADV_HLD.1 Tanımlayıcı üst düzeyde tasarım, sistemin mimarisi                       |
|                                             | ADV_RCR.1 Biçimsel olmayan karşılık gelmenin gösterilmesi                          |
| AGD Sınıfı: Kılavuz belgeler                | AGD_ADM.1 Yönetici kılavuzu                                                        |
|                                             | AGD_USR.1 Kullanıcı kılavuzu                                                       |
| ALC Sınıfı: Yaşam Döngüsü Desteği           | ALC_FLR.1 Temel hataları düzeltme                                                  |
| ATE Sınıfı: Testler                         | ATE_COV.1 Kapsam kanıtı                                                            |
|                                             | ATE_FUN.1 Fonksiyonel test                                                         |
|                                             | ATE_IND.2 Bağımsız test – örnek                                                    |
| AVA Sınıfı: Açıklık değerlendirmesi         | AVA_SOF.1 TOE güvenlik fonksiyonu gücü değerlendirmesi                             |
|                                             | AVA_VLA.2 Düşük atak potansiyeline karşı bağımsız açıklık analizi                  |
| AMA Sınıfı: Garantinin devamının sağlanması | AMA_AMP.1 Garantinin sürdürülmesi planı                                            |
|                                             | AMA_CAT.1 TOE bileşen sınıflandırma raporu                                         |

### 4.2.3 Özel Bilgi Ağ Sistemleri

Kişisel önemi olan ve yalnızca organizasyonun kullanımına açık olan bilgilere özel bilgi denilmektedir. Bu tür bilgilerin açığa çıkması ve yetkisi olmayan kişilerin eline geçmesi şirketi ve çalışanlarını kötü bir şekilde etkileyecektir. Organizasyondaki ücretlendirme seviyeleri, çalışanların performans değerlendirmeleri veya sağlık bilgileri özel bilgilere örnektir. Özel bilgilerin taşındığı ağlarda aynı zamanda hassas ve tasnif dışı bilgilerde bulundurulabilir.

Özel bilgi ağ sistemlerinin güvenlik düzeylerinin değerlendirilebilmesi için gereken değerlendirme delillerinin hazırlanması için sistemin entegrasyonunu sağlayan firmanın desteğinin yanı sıra sistemi geliştirenlerin de desteği gerekmektedir. Sistemde kullanılan COTS ürünleri için V-RATE yöntemi kullanılarak değerlendirme delilleri oluşturulurken özel olarak hazırlanmış yazılım ve donanımlar için geliştiricinin hazırladığı dokümanlar ve entegrasyon dokümanları değerlendirme delili olarak kullanılmaktadır.

Özel bilgilerin taşındığı ağların güvenlik garanti gereksinimleri **Çizelge 4.3 Özel bilgi ağ sistemleri**'deki gibi olmalıdır.

Çizelge 4.3 Özel bilgi ağ sistemleri

| Garanti sınıfı                     | Garanti bileşenleri                                            |
|------------------------------------|----------------------------------------------------------------|
| ACM Sınıfı: Konfigürasyon yönetimi | ACM_CAP.3 Yetkilendirme kontrolleri                            |
|                                    | ACM_SCP.1 TOE KM kapsamı                                       |
| ADO Sınıfı: Teslim ve çalışma      | ADO_DEL.1 Teslim prosedürleri (varsa)                          |
|                                    | ADO_IGS.1 Kurulum, üretim ve başlatma prosedürleri             |
| ADV Sınıfı: Geliştirme             | ADV_FSP.1 Biçimsel olmayan fonksiyonel belirtim                |
|                                    | ADV_HLD.2 Güvenliği uygulayan üst düzeyde tasarım              |
|                                    | ADV_IMP.1 TSF uygulamasının alt kümesi                         |
|                                    | ADV_SPM.1 Biçimsel olmayan TOE güvenlik politikası modellemesi |
|                                    | ADV_RCR.1 Biçimsel olmayan karşılık gelmenin gösterilmesi      |
| AGD Sınıfı: Kılavuz belgeler       | AGD_ADM.1 Yönetici kılavuzu                                    |
|                                    | AGD_USR.1 Kullanıcı kılavuzu                                   |
| ALC Sınıfı: Yaşam döngüsü desteği  | ALC_DVS.1 Güvenlik önlemlerinin belirtilmesi                   |
|                                    | ALC_FLR.2 Hata bildirme prosedürleri                           |
| ATE Sınıfı: Testler                | ATE_COV.2 Kapsamın incelenmesi                                 |
|                                    | ATE_DPT.1 Test: üst düzeyde tasarım                            |
|                                    | ATE_FUN.1 Fonksiyonel test                                     |

|                                             |                                                                            |
|---------------------------------------------|----------------------------------------------------------------------------|
|                                             | ATE_IND.2 Bağımsız test – örnek                                            |
| AVA Sınıfı: Açıklık değerlendirilmesi       | AVA_MSU.1 Kötüye kullanımın incelenmesi                                    |
|                                             | AVA_SOF.1 TOE güvenlik fonksiyonu gücü değerlendirilmesi                   |
|                                             | AVA_VLA.3 Orta derecede atak potansiyeline karşı açıklık değerlendirilmesi |
| AMA Sınıfı: Garantinin devamının sağlanması | AMA_AMP.1 Garantinin sürdürülmesi planı                                    |
|                                             | AMA_CAT.1 TOE bileşen sınıflandırma raporu                                 |

#### 4.2.4 Gizli Bilgi Ağ Sistemleri

Çok hassas ve sadece organizasyon içi kullanım amacıyla sınıflandırılmış bilgilere gizli bilgi adı verilir. Bu bilgilerin açığa çıkması ve yetkisiz kişilerin eline geçmesi organizasyona ciddi ve olumsuz etkilerde bulunur. Yeni geliştirilen ürünler hakkındaki bilgiler, ticari sırlar ve ortaklarla yapılan pazarlıklar gizli bilgilere örnektir. Gizli bilgilerin taşındığı ağlarda aynı zamanda özel, hassas ve tasnif dışı bilgilerde bulundurulabilir.

Gizli bilgi ağ sistemlerinin güvenlik düzeylerinin değerlendirilebilmesi için gereken değerlendirme delillerinin hazırlanması için sistemin entegrasyonunu sağlayan firmanın desteğinin yanı sıra sistemi geliştirenlerin de desteği gerekmektedir. Sistemde kullanılan COTS ürünleri için V-RATE yöntemi kullanılarak değerlendirme delilleri oluşturulurken özel olarak hazırlanmış yazılım ve donanımlar için geliştiricinin hazırladığı dokümanlar ve entegrasyon dokümanları değerlendirme delili olarak kullanılmaktadır. Ayrıca bu güvenlik seviyesindeki bir sistemin bütün bileşenlerinin de ayrı ayrı Ortak Kriterler'e uygun olarak değerlendirilmesi gerekmektedir.

Gizli bilgilerin taşındığı ağların güvenlik garanti gereksinimleri **Çizelge 4.4 Gizli bilgi ağ sistemleri**'deki gibi olmalıdır.

Çizelge 4.4 Gizli bilgi ağ sistemleri

| <b>Garanti sınıfı</b>                       | <b>Garanti bileşenleri</b>                                        |
|---------------------------------------------|-------------------------------------------------------------------|
| ACM Sınıfı: Konfigürasyon yönetimi          | ACM_AUT.1 Kısmi KM otomasyonu                                     |
|                                             | ACM_CAP.4 Üretim desteği ve kabul prosedürleri                    |
|                                             | ACM_SCP.2 Sorun izleme KM kapsamı                                 |
| ADO Sınıfı: Teslim ve çalışma               | ADO_DEL.2 Değişmenin tespiti (varsa)                              |
|                                             | ADO_IGS.1 Kurulum, üretim ve başlatma prosedürleri                |
| ADV Sınıfı: Geliştirme                      | ADV_FSP.2 Bütünüyle tanımlanmış dış arayüzler                     |
|                                             | ADV_HLD.2 Güvenliği uygulayan üst düzeyde tasarım                 |
|                                             | ADV_IMP.2 TSF uygulanması                                         |
|                                             | ADV_LLD.1 Tanımlayıcı alt düzeyde tasarım                         |
|                                             | ADV_RCR.1 Biçimsel olmayan karşılık gelmenin gösterilmesi         |
|                                             | ADV_SPM.1 Biçimsel olmayan TOE güvenlik politikası modeli         |
| AGD Sınıfı: Kılavuz Belgeler                | AGD_ADM.1 Yönetici kılavuzu                                       |
|                                             | AGD_USR.1 Kullanıcı kılavuzu                                      |
| ALC Sınıfı: Yaşam döngüsü desteği           | ALC_DVS.1 Güvenlik önlemlerinin belirlenmesi                      |
|                                             | ALC_LCD.1 Geliştirici tarafından tanımlanan kullanım ömrü modeli  |
|                                             | ALC_TAT.1 İyi tanımlanmış geliştirme aletleri                     |
|                                             | ALC_FLR.3 Sistemli hata düzeltme                                  |
| ATE Sınıfı: Testler                         | ATE_COV.2 Kapsamın incelenmesi                                    |
|                                             | ATE_DPT.1 Test: üst düzeyde tasarım                               |
|                                             | ATE_FUN.1 Fonksiyonel test                                        |
|                                             | ATE_IND.2 Bağımsız test - örnek                                   |
| AVA Sınıfı: Açıklık değerlendirmesi         | AVA_MSU.2 İncelemenin geçerliliğinin doğrulanması                 |
|                                             | AVA_SOF.1 TOE güvenlik fonksiyon gücü değerlendirmesi             |
|                                             | AVA_VLA.4 Yüksek atak potansiyeline karşı açıklık değerlendirmesi |
| AMA Sınıfı: Garantinin devamının sağlanması | AMA_AMP.1 Garantinin sürdürülmesi planı                           |
|                                             | AMA_CAT.1 TOE bileşen sınıflandırma raporu                        |

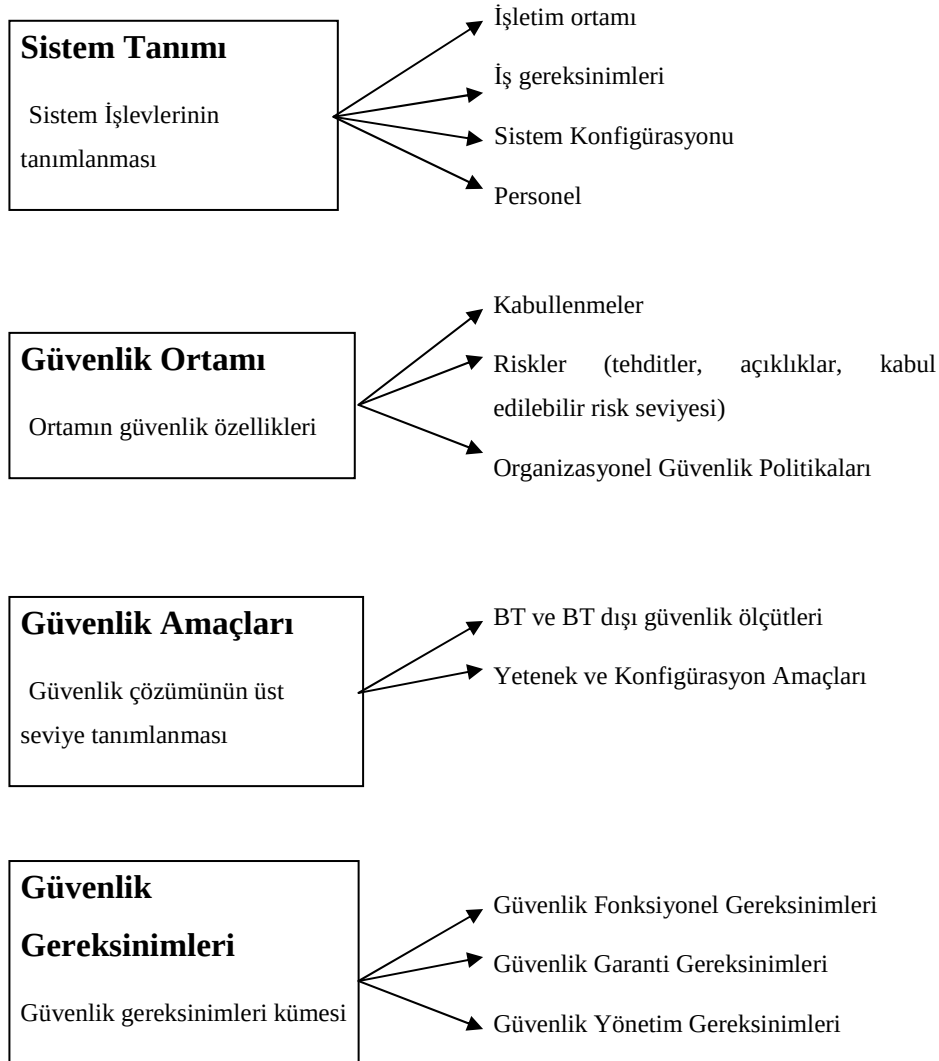
|  |                                                           |
|--|-----------------------------------------------------------|
|  | AMA_EVD.1 Garantinin devamının kanıtlanması               |
|  | AMA_SIA.1 Güvenlik etkisi incelemesinin örneklendirilmesi |

### 4.3 Güvenlik Hedefi'nin Hazırlanması

BT Sistemi değerlendirme sürecinin ilk ve en önemli adımı sistemin Güvenlik Hedefi'nin oluşturulmasıdır. Bölüm 2.3.1 incelenen ürünler için ST dokümanının içeriğinden farklı olarak sistemlerin Güvenlik Hedefi'nin hazırlanması çok daha karmaşık bir süreçtir. Bu sürecin adımları sırasıyla aşağıdaki gibi olmalı ve sistem ST'si ortaya çıkartılmalıdır.

1. **Sistem Tanımı;** Sistem ST'lerinde tanım kısmı temel olarak işletim ortamı, iş gereksinimleri, sistem konfigürasyonu ve personel konularında detaylı bir tanım içermelidir. Dikkat edilmesi gereken nokta sistemi oluşturan bütün BT bileşenlerinin bütün olarak düşünülmesi ve **Şekil 1.2. Değerlendirme hedefi (TOE)**de gösterildiği gibi Sis-TOE'nin tanımının yapılmasıdır. Tek tek bütün bileşenlerin değil Sis-TOE'nin fiziksel ve mantıksal sınırları çizilmelidir.
2. **Güvenlik Ortamı;** Sistemin güvenlik ortamı tanımlanırken ürün ST'sinde olduğu gibi ortama ve TOE'nin koruduğu varlıklara olası tehditler, ortam için yapılan kabullenmeler ve organizasyonel güvenlik politikaları tespit edilmelidir. Bunların yanı sıra sistemin açıklıkları ve kabul edilebilir risk seviyeleri de bu bölümde tespit edilmeli ve ST'de belirtilmelidir.
3. **Güvenlik Amaçları;** Sistemin güvenlik amaçları güvenlik ortamında belirtilen açıklıklar, tehditler, kabullenmeler, politikalar ve kabul edilebilir risk seviyelerine karşı alınacak tedbirleri içermelidir. BT ve BT dışı güvenlik amaçlarının yanı sıra sistem için kapasite ve kontrol amaçlarında ST'nin bu kısmında belirtilmelidir.
4. **Güvenlik Gereksinimleri;** Tespit edilen güvenlik amaçlarının karşılanabilmesi ve tedbirlerin uygulanabilmesi için gerekli güvenlik gereksinimleri bu bölümde belirtilmelidir. Fonksiyonel gereksinimler bölüm 3.1'de belirtilen Ortak Kriterler standardından alınmış olan

Güvenlik Fonksiyonel Gereksinimlerinden ihtiyaca göre alınmalıdır. Bu katalogdaki gereksinimler dışında ihtiyacın olduğu durumda standarda belirtilen bileşen oluşturma yöntemlerine uygun olarak yeni fonksiyonel bileşenler tanımlanabilir. Garanti gereksinimleri ise sistemin güvenliğini sağladığı varlıkların sınıflarına göre önerilen güvenlik paketlerinin içerisinden alınmalıdır. Bu güvenlik paketlerine ek olarak Ortak Kriterler standardının Güvenlik Garanti Gereksinimleri bölümünden garanti bileşenleri sistem için seçilebilir. Sistemlerin ürünlerden en önemli farklarından biri olan yönetim gereksinimleri ise bölüm 3.2’ de tanımlanmış güvenlik yönetim gereksinimleri arasından organizasyonun bilgi güvenliği yönetim sisteminin gerçekleştirmiş olduğu risk değerlendirmesi sonuçlarına uygun olarak seçilmelidir.



Şekil 4.2 Güvenlik Hedefi'nin hazırlanması

## 5 SİSTEMİN GERÇEKLENMESİ VE TESTLER

Güvenlik Hedefi hazırlanmış ve değerlendirilmiş bir sistemin gerçekleşmesi iki bölümde incelenebilir. Bunlardan ilki güvenlik fonksiyonel gereksinimlerine uygun olarak güvenlik fonksiyonlarının geliştirilmesidir. Gerekli güvenlik fonksiyonlarını sağlayan BT ürünlerinin ve uygulamalarının COTS ürünlerden veya özel olarak hazırlanmış yazılım veya donanımlardan seçilerek sisteme entegrasyonu sağlanmalıdır. Sistemin sağlayacağı garanti düzeyine uygun olarak (bölüm 4.2) gerçekleştirilecek entegrasyonda değerlendirme için gerekli garanti delilleri de hazırlanmalıdır. Güvenlik fonksiyonları gerçekleştirildiğinde ve sisteme entegrasyonu sağlanarak garanti delilleri de ortaya çıkartıldığında ikinci bölüme yani yönetim sisteminin geliştirilmesine geçilebilir. Bölüm 2.4’de incelenen ISO 17799 standardına uygun olarak bir bilgi güvenliği yönetim sistemi organizasyonda kurulmalı ve gerçekleştirilecek risk değerlendirmesi ve risk yönetiminin ardından seçilen, ve ST’de listelenen kontrol objeleri sistemde uygulanmalıdır. Bu uygulamalar güvenlik politikasını, seçilen kontrol objeleri için prosedürleri ve kuralları içermeli ve her bir yönetim gereksiniminin sistemde çalıştırılmasını sağlamalıdır.

Sistemin gerçekleşmesinin ardından işletimine geçilmelidir. Bu aşamada denetim logları ve kayıtları, işletim riskleri, güvenlik tedbirleri sürekli olarak incelenmeli ve güvenlik fonksiyonlarının işletimi denetlenmelidir. Ayrıca riskler, güvenlik olayları, ve sistemin güvenli durumunun periyodik olarak gözden geçirilmesi ile sistemin geliştirilmesine yazılı yönetim prosedürlerine uygun olarak devam edilmelidir.

### 5.1 Değerlendirme Metodolojisinin Uygulanması

Güvenlik Hedefi’ne ve iddia ettiği garanti düzeyine uygun olarak tasarlanan ve gerçekleşen bir sistemin değerlendirilmesi için Ortak Kriterler Değerlendirme Metodolojisi kullanılmalıdır. Bölüm 4.2’de önerilen garanti paketlerini sağlayan bir sisteme uygulanacak değerlendirme eylemleri metodolojide yer almaktadır. Ayrıca yönetim gereksinimlerinin karşılandığı tedbirlerin değerlendirilmesi için de BS 7799

standartının ikinci bölümü kılavuz olarak kullanılmalı ve Ortak Kriterler'e uygun değerlendirici eylemleri haline getirilerek sisteme uygulanmalıdır.

## 5.2 Garantinin Devamının Sağlanması

BT Sistemlerinin değerlendirilmesinde en önemli noktalardan biri de değerlendirmeden başarı ile geçmiş bir sistemin sağladığı garantinin devamının kontrol edilmesidir. Çünkü organizasyonların kullanmakta oldukları ağ sistemleri hemen hemen her gün geliştirilmekte, yeni yamalar yüklenmekte ve uygulama programları güncellenmektedir. Bu sebeple sistemin değerlendirilmesi kadar garantinin devamının da sağlanması önem taşımaktadır. Garantinin devamının sağlanması için ulusal bir yapının kurulması gerekmektedir. Almanya'da ZKA'nın<sup>7</sup> gerçekleştirdiği gibi BT sistemlerinin garantisinin devamının kontrolünü sağlayacak bir kuruma gerekmektedir. [von Faber, 1999] Çünkü sistemler her geçen gün yenilendiği ve geliştirildiği gibi açıklıklar ve tehditlerde gelişmekte ve etkileri artmaktadır. Kurulacak olan bu yapı sertifikalandırılmış sistemlerde garantinin devamının sağlandığının denetimlerini gerçekleştirmelidir. Bunun yanı sıra değerlendirmeleri gerçekleştirecek olan laboratuarlara sızma testleri ve bağımsız testler konusunda teknik öngörülerde bulunarak bu testlerin içeriklerinin sürekli olarak güncel tutulmasını sağlamalıdır.

Özet olarak garantinin devamının sağlanması için ZKA modeli incelenerek sistemler için uygulanmalıdır. BT sistemlerinin garanti paketleri içerisinde zorunlu olarak belirtilmiş olan AMA sınıfı ailelerinin denetiminin periyodik olarak gerçekleştirilmesiyle garantinin devamı BT sistemleri için sağlanmalıdır.

## 5.3 Örnek Bir Sistemin Değerlendirilmesi

Bu bölümde BT sistemleri için önerilen değerlendirme yöntemi örnek bir sistem üzerinde uygulanmıştır. Bu uygulamada ilk olarak A şirketinin BT sisteminin (TOE) bölüm 4'te önerilen metodoloji uygulanmadan önceki hali tanımlanmıştır.

---

<sup>7</sup> Almanya'da Akıllı Kart sistemleri için böyle bir yapı bulunmaktadır. Zentraler Kreditausschuss (ZKA) akıllı kart sistemleri için akreditasyon kurumudur.

Sistemin BT bileşenleri ile varlıkları ve varolan prosedürleri belirtilmiştir. Ardından önerilen yöntem kullanılarak BT sisteminin değerlendirilmesi gerçekleştirilmiş ve sonuç incelenmiş, eksiklikleri listelenmiştir.

### 5.3.1 Ağ Topolojisi [Karabacak, 2002]

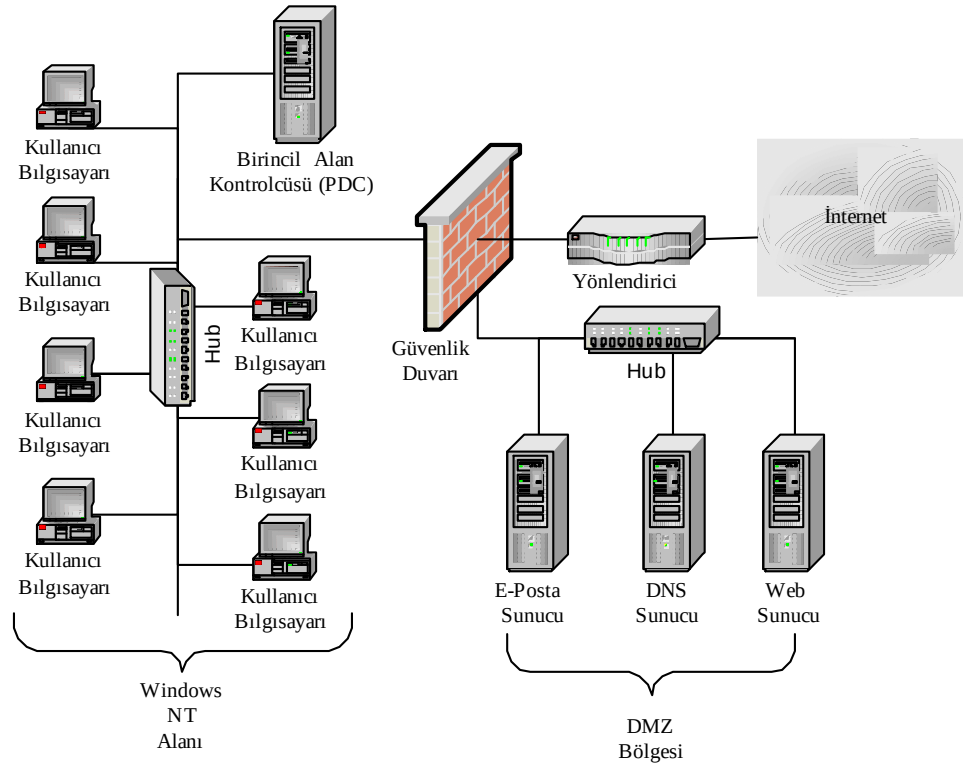
A şirketi **Şekil 5.1 A şirketi ağ** 'de gösterildiği gibi küçük bir kurum ağına sahiptir. Kurum internete bağlıdır ve kurumun ağ üzerinde taşıdığı en yüksek bilginin güvenlik sınıfı “özel”dir.

Kurum ağının güvenlik duvarının arkasında bulunan tam korumalı kısmında, 7 kullanıcı bilgisayarı, bu kullanıcı bilgisayarlarını yöneten bir adet birincil alan kontrolcüsü ve bu bilgi sistemlerini birbirine bağlayan bir adet hub cihazı bulunmaktadır.

Kurumda, üç adet arayüzü bulunan bir adet güvenlik duvarı kullanılmaktadır. Bu arayüzlerden biri, önceki paragrafta bahsedilen iç ağa bağlı bulunmakta, diğer ikisi ise, DMZ olarak adlandırılan yarı korumalı bölge ile yönlendiriciye bağlı durumda bulunmaktadır.

DMZ ağında, kurumun üç adet sunucu bilgisayarı bulunmaktadır. E-posta sunucu, kullanıcılara kurum içinden ya da dışından e-posta hizmeti vermektedir. DNS sunucu, FQDN ve IP adresi eşleşmesi yapmaktadır. Web sunucu ise standart WWW hizmeti veren bilgi sistemidir. Bu üç sunucu, dış dünyaya (İnternet) hizmet verdiklerinden dolayı DMZ bölgesinde bulunması gerekmektedir. Güvenlik duvarında, bu üç sunucuya özel erişim kontrol listeleri vardır. Bu üç sunucu ve güvenlik duvarının DMZ arayüzü bir hub ile birbirine bağlı durumdadır.

Yönlendirici, güvenlik duvarının ön kısmında bulunan ve kurumun İnternet arayüzünde bulunan ağ cihazıdır. Yönlendiricinin iç arayüzü ile güvenlik duvarının dış arayüzü birbirine bağlı durumdadır. Yönlendirici dış arayüzü ise İnternet ağına bağlıdır.



Şekil 5.1 A şirketi ağ topolojisi

### 5.3.2 Kurumun Varlıkları ve Güvenlik Politikaları

Kurumun varlıkları yazılım, donanım, veri, prosedürler, ve insan olarak sınıflandırılmıştır.

#### 5.3.2.1 BT Varlıkları

1. Yazılım: Kullanıcı bilgisayarlarında, sunucu bilgisayarlarda, güvenlik duvarında ve yönlendiricide çalışan yazılımlardır. Yazılımları üç ana başlık altında inceleyebiliriz. Bunlar, işletim sistemleri, uygulamalar ve protokollerdir.

a. İşletim sistemleri:

| Tipi                       | Adet | Kurulum                         |
|----------------------------|------|---------------------------------|
| Windows NT Workstation 4.0 | 7    | Tüm kullanıcı bilgisayarlarında |

|                       |   |                                                                                    |
|-----------------------|---|------------------------------------------------------------------------------------|
| Windows NT Server 4.0 | 5 | Birincil alan kontrolcüsü, güvenlik duvarı, e-posta sunucu, DNS sunucu, web sunucu |
| Cisco IOS 12.0        | 1 | Yönlendirici                                                                       |

b. Uygulamalar:

| Tipi                            | Özellikler                      |
|---------------------------------|---------------------------------|
| Microsoft Office 97             | Tüm kullanıcı bilgisayarlarında |
| Internet Explorer 4.0           | Tüm kullanıcı bilgisayarlarında |
| Internet Information Server 4.0 | Web sunucuda                    |
| Microsoft Exchange 5.5          | E-posta sunucuda                |
| DNS servisi                     | DNS sunucuda                    |
| Checkpoint Firewall –1          | Güvenlik duvarında              |

Sunucu bilgisayarlarda ve güvenlik duvarında Microsoft Office ve Internet Explorer kurulu değildir.

Sunucu bilgisayarda koşan uygulama ve servislerin açıklıkları takip edilmektedir. (Microsoft Security Bulletin)

c. Protokoller:

| Tipi   | Kullanıldığı yer                                                              |
|--------|-------------------------------------------------------------------------------|
| TCP/IP | Kullanıcı bilgisayarlarının ve sunucu bilgisayarların İnternet ile iletişimde |
| SMB    | Windows NT alanındaki bilgisayarlar kendi aralarında haberleşirken            |

DMZ bölgesinde SMB protokolü kullanılmamaktadır. Bu bölgedeki tüm sunucularda bu protokol kapatılmıştır. Güvenlik duvarında da SMB protokolü kapatılmıştır.

Güvenlik duvarı SMB trafiğine izin vermemektedir.

- Donanım: Üzerlerinde işletim sistemleri ve yazılımların koştuğu bilgi sistemleridir. Donanım üç ana başlık altında incelenmiştir. Bunlar, sunucu donanımları, istemci donanımları ile iletişim cihazları ve kablolardır.

## a. Sunucular:

| Tipi                      | Adet | Donanım özellikleri        |
|---------------------------|------|----------------------------|
| E-Posta sunucusu          | 1    | PII 800, 128 Mbyte hafıza  |
| DNS sunucusu              | 1    | PIII 600, 128 Mbyte hafıza |
| Web sunucusu              | 1    | PIII 600, 128 Mbyte hafıza |
| Birincil alan kontrolcüsü | 1    | PIII 600, 128 Mbyte hafıza |

## b. İstemciler:

| Tipi                     | Adet | Donanım özellikleri      |
|--------------------------|------|--------------------------|
| Kullanıcı bilgisayarları | 7    | PII 500, 64 Mbyte hafıza |

## c. İletişim cihazları ve kablolar:

| Tipi                           | Adet | Donanım Özellikleri            |
|--------------------------------|------|--------------------------------|
| Yönlendirici                   | 1    | Cisco 2600                     |
| Güvenlik duvarı                | 1    | PIII 600,128 Mbyte hafıza      |
| Hub                            | 2    | 10 portlu 10 Mb/s standart hub |
| UTP (bakır) iletişim kabloları | -    | Kategori 5                     |

Güvenlik duvarının BIOS şifresi vardır.

3. Veri: Bilgi sistemleri üzerinde bulunan bilgilerdir. Veri üç ana başlık altında incelenmiştir. Bunlar, kurum, kullanıcı ve ağ verileridir.

## a. Kurum verisi:

| Tipi                      | Yeri                          |
|---------------------------|-------------------------------|
| Erişim kontrol listeleri  | Güvenlik duvarı, yönlendirici |
| Genel kurum bilgileri     | Web sunucu                    |
| Genel kullanıcı bilgileri | Birincil alan kontrolcüsü     |

## b. Kullanıcı verisi:

| Tipi                  | Yeri                     |
|-----------------------|--------------------------|
| Kullanıcı dosyaları   | Kullanıcı bilgisayarları |
| Kullanıcı e-postaları | E-posta sunucu           |

## c. Ağ verisi: Kablolardaki ağ trafiği.

### 5.3.2.2 BT Dışı Varlıklar

1. Politikalar ve prosedürler: Yazılı olan kurum içi kullanım standartlarıdır. Prosedürlerin durumları ISO 17799 standardına uygunluklarına göre değerlendirilmiştir. Standarda uygunlukları 0 ve 3 arasında değerlerle ifade edilmektedir. Değerlerin karşılıkları

Çizelge 5.1 BT Dışı varlıkların değer çizelgesi

| Değer | Karşılık    |
|-------|-------------|
| 0     | Uygun Değil |
| 1     | Yetersiz    |
| 2     | Eksik       |
| 3     | Uygun       |

| Adı                               | ISO 17799 Standardına Uygunluk |
|-----------------------------------|--------------------------------|
| Bilgi güvenliği politikası        | 1                              |
| Bilgi sınıflandırılması prosedürü | 3                              |
| İnternet kullanım politikası      | 1                              |
| Sistem işletimi prosedürü         | 1                              |
| Erişim kontrolü prosedürü         | 2                              |
| Fiziksel güvenlik                 | 1                              |
| Veri yedekleme                    | 2                              |
| Virüs önleme ve tespit            | 2                              |

2. İnsan: Kurum çalışanlarıdır. Normal kullanıcılar, sistem yöneticileri ve geçici personel olmak üzere üç ana başlık altında incelenmiştir.
  - a. Normal kullanıcılar: 8 adet
  - b. Sistem yöneticileri: 1 adet
  - c. Geçici personel: Yok

### 5.3.3 Değerlendirme Yönteminin Uygulanması

#### 5.3.3.1 Risk Değerlendirmesi ve Risk Yönetimi [Karabacak, 2002]

##### 5.3.3.1.1 Açıklıklar ve Tehditler

Risk analizinin gerçekleştirilebilmesi için ilk önce BT sisteminin açıklıkları tespit edilmelidir. A şirketinin varlıklarının açıklıkları aşağıda sıralanmıştır.

##### 1. Yazılım açıklıkları

| Açıklık                                                                                                    | Açıklığın bulunduğu varlık(lar)                                                              |
|------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------|
| İşletim sistemleri varsayılan ayarlardadır. Üzerlerinde herhangi bir güvenlik sıkılaştırması yapılmamıştır | Tüm kullanıcı bilgisayarları, birincil alan kontrolcüsü, DMZ’de bulunan sunucu bilgisayarlar |
| Erişim kontrol yazılımı yoktur                                                                             | Tüm kullanıcı bilgisayarları                                                                 |
| FTP servisi açıktır                                                                                        | Web sunucu                                                                                   |
| İçerik güvenliği yazılımının olmaması                                                                      | E-posta sunucu ve güvenlik duvarı                                                            |
| Saldırı tespit sisteminin olmaması                                                                         | -                                                                                            |
| Anti-virüs yazılımı kullanılmaması                                                                         | Kullanıcı bilgisayarları                                                                     |

##### 2. Donanım açıklıkları

| Açıklık                      | Açıklığın bulunduğu varlık(lar)                                                            |
|------------------------------|--------------------------------------------------------------------------------------------|
| BIOS şifresi yoktur          | DMZ bölgesindeki sunucu bilgisayarlar, birincil alan kontrolcüsü, kullanıcı bilgisayarları |
| Özel bir sistem odası yoktur | DMZ bölgesindeki sunucu bilgisayarlar, güvenlik duvarı, yönlendirici, hub cihazları        |
| Düşük donanım özellikleri    | E-posta sunucu, Hub                                                                        |
| İç ağda hub kullanılması     | Hub                                                                                        |
| Özel kablo yolları yoktur    | Kablolar                                                                                   |

##### 3. Veri açıklıkları

| Açıklık | Açıklığın bulunduğu varlık(lar) |
|---------|---------------------------------|
|---------|---------------------------------|

|                                             |                                                                   |
|---------------------------------------------|-------------------------------------------------------------------|
| Yedekleme yok                               | Birincil alan kontrolcüsü, web sunucu, DNS sunucu, e-posta sunucu |
| Dosya şifreleme yazılımı kullanılmamaktadır | Kullanıcı bilgisayarları                                          |

#### 4. Politika ve prosedür açıklıkları

| Açıklık         | Açıklığın bulunduğu varlık(lar)   |
|-----------------|-----------------------------------|
| Uygulanamaması  | Bilgi güvenliği politikası        |
| -               | Bilgi sınıflandırılması prosedürü |
| Çok eski olması | İnternet kullanım politikası      |
| Uygulanmaması   | Sistem işletimi prosedürü         |
| Eksik olması    | Erişim kontrolü prosedürü         |
| Eksik olması    | Fiziksel güvenlik                 |
| Eksik olması    | Veri yedekleme                    |
| Çok eski olması | Virüs önleme ve tespit            |

#### 5. İnsan açıklıkları

| Açıklık                                    | Açıklığın bulunduğu varlık(lar)     |
|--------------------------------------------|-------------------------------------|
| Eğitimleri yoktur                          | Normal kullanıcı, sistem yöneticisi |
| İki personelin aynı bilgisayarı kullanması | Normal kullanıcı                    |
| İş yükü fazlalığı                          | Sistem yöneticisi                   |

Açıklıkların belirlendiği A şirketinde bu açıklıklara gerçekleştirilebilecek tehditler aşağıda sıralanmıştır.

#### 1. Yazılımlardaki açıklıklardan doğan tehditler

| Tehdit                                                        | Kullandığı açıklık                                                     | Etkilenen varlık(lar)                                                                                                                                |
|---------------------------------------------------------------|------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kasıtlı ya da kasıtsız yapılan illegal kullanıcı aktiviteleri | Erişim kontrol yazılımı yoktur.<br>Varsayılan işletim sistemi ayarları | Kullanıcı bilgisayarları, kullanıcı bilgisayarlarının işletim sistemleri, kullanıcı bilgisayarlarındaki yazılımlar, bilgisayarlarda bulunan veriler, |

|                                                                     |                                                                        |                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------------|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                     |                                                                        | birincil alan kontrolcüsündeki veriler                                                                                                                                                                                                                                                                      |
| Kullanıcıların ihtiyacından çok erişime sahip olması                | Erişim kontrol yazılımının olmaması                                    | Kullanıcı bilgisayarları, kullanıcı bilgisayarlarının işletim sistemleri, kullanıcı bilgisayarlarındaki yazılımlar, bilgisayarlarda bulunan veriler                                                                                                                                                         |
| İnternet'ten yapılan hacker saldırıları                             | Varsayılan işletim sistemi ayarları<br>FTP servisinin açık olması      | Kurumun prestiji. Web sunucu, DNS sunucu, e-posta sunucu, bu sunucuların işletim sistemleri, bu sunucularda çalışan servisler ve uygulamalar depolanan veriler, yönlendirici güvenlik duvarı, yönlendiricinin ve güvenlik duvarının işletim sistemi, yönlendiricide ve güvenlik duvarında depolanan veriler |
| Virüsler                                                            | İçerik güvenliği yazılımının olmaması, anti-virüs yazılımının olmaması | Kurumun prestiji. Kullanıcı ve kurum verileri, e-posta sunucunun işletim sistemi ve üzerinde koşan yazılım, kullanıcı bilgisayarlarının ve birincil alan kontrolcüsünü işletim sistemleri ve üzerlerinde koşan yazılımlar. Kurum çalışanları, kurumun sistem yöneticisi                                     |
| İnternet'ten yapılan hacker saldırılarından erken haberdar olamamak | Saldırı tespit sisteminin olmaması                                     | Kurumun prestiji. DMZ ağındaki bilgisayarlar (özellikle web sunucu), işletim sistemleri, üzerlerinde koşan yazılımlar ve servisler. Daha az olarak kullanıcı bilgisayarları ve birincil alan kontrolcüsü, işletim sistemleri ve yazılımları                                                                 |

## 2. Donanımlardaki açıklıklardan doğan tehditler

| <b>Tehdit</b>                                                      | <b>Kullandığı açıklık</b>                               | <b>Etkilenen varlık(lar)</b>                                                                                                                                  |
|--------------------------------------------------------------------|---------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Toz, nem güneş ışığı gibi çevresel faktörler                       | Özel bir sistem odasının olmaması                       | DMZ bölgesindeki sunucu bilgisayarlar, güvenlik duvarı, yönlendirici, hub cihazları, kurum çalışanları                                                        |
| Bilgisayarlara yetkisiz erişim                                     | BIOS şifresinin olmaması, özel sistem odasının olmaması | DMZ bölgesindeki sunucu bilgisayarlar, birincil alan kontrolcüsü, bazı kullanıcı bilgisayarları, kurum çalışanları                                            |
| Sistemlerin çok yavaş çalışması, hata vererek çalışmasının durması | Düşük donanım özellikleri                               | E-posta sunucu, Hub, kurum çalışanları                                                                                                                        |
| Dinleme ( <b>sniffing</b> ) yapılması                              | İç ağda hub kullanılması                                | Kullanıcı verileri, kurum çalışanları, iç ağdaki kullanıcı bilgisayarları ve birincil alan kontrolcüsü, işletim sistemleri ve üzerlerinde koşturan yazılımlar |
| Sistemin sürekliliğinin kaybolması                                 | Özel kablo yolları yoktur                               | Kurum çalışanları                                                                                                                                             |

## 3. Verideki açıklıklardan doğan tehditler

| <b>Tehdit</b>                                                                             | <b>Kullandığı açıklık</b>                   | <b>Etkilenen varlık(lar)</b>                                                         |
|-------------------------------------------------------------------------------------------|---------------------------------------------|--------------------------------------------------------------------------------------|
| Sistem hatalarından ya da elektrik kesintisi gibi çevre etkilerinden dolayı verinin kaybı | Yedeklemenin olmaması                       | Birincil alan kontrolcüsü, web sunucu, DNS sunucu, e-posta sunucu, kurum çalışanları |
| Kullanıcı verilerinin başkaları tarafından okunması                                       | Dosya şifreleme yazılımı kullanılmamaktadır | Kullanıcı verisi, kurum çalışanları                                                  |

## 4. Politika ve prosedürlerdeki açıklıklardan doğan tehditler

| <b>Tehdit</b>                                                          | <b>Kullandığı açıklık</b> | <b>Etkilenen varlık(lar)</b> |
|------------------------------------------------------------------------|---------------------------|------------------------------|
| Sistemde bilgi güvenliği için bir politikanın olmaması                 | Uygulanamaması            | Şirket varlıkları            |
| İnternet kullanım politikasında yazılmamış olan kullanıcı aktiviteleri | Çok eski olması           | Kullanıcı bilgisayarları     |
| Güvenlik olaylarının takip edilmemesi, tepki verilememesi              | Uygulanmaması             | Şirket varlıkları            |
| Yetkisiz erişimler                                                     | Eksik olması              | Şirket varlıkları            |
| Fiziksel güvenlik ihlalleri                                            | Eksik olması              | Şirket varlıkları            |
| Yedekleme yapılamaması                                                 | Eksik olması              | Şirket varlıkları            |
| Virüs tanımlarının güncel olmaması                                     | Çok eski olması           | Şirket varlıkları            |

## 5. İnsanlardaki açıklıklardan doğan tehditler

| <b>Tehdit</b>                                             | <b>Kullandığı açıklık</b>                                      | <b>Etkilenen varlık(lar)</b>                                                                                                                                                                |
|-----------------------------------------------------------|----------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Kasıtsız yapılan zarar verici kullanıcı aktiviteleri      | Normal kullanıcıların eğitimsiz olması                         | Kullanıcı bilgisayarları, kullanıcı bilgisayarlarının işletim sistemleri, kullanıcı bilgisayarlarındaki yazılımlar, bilgisayarlarda bulunan veriler, birincil alan kontrolcüsündeki veriler |
| Sistemde olabilecek bir arızanın uzun süre giderilememesi | Sistem yöneticisinin yeterli derecede eğitimi olmaması, sistem | Kurumun işlerliği                                                                                                                                                                           |

|                                                           |                                           |                                                                                                                                         |
|-----------------------------------------------------------|-------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
|                                                           | yöneticisindeki fazla iş yükü             |                                                                                                                                         |
| İllegal kullanıcı aktivitesinin sorumlusunun bulunamaması | İki personelin aynı bilgisayar kullanması | Kullanıcı bilgisayarı, kullanıcı bilgisayarının işletim sistemleri, kullanıcı bilgisayarındaki yazılımlar, bilgisayarda bulunan veriler |

#### 5.3.3.1.2 Güvenlik Önlemleri

Kurumda varolan tek güvenlik önlemi güvenlik duvarıdır. Güvenlik duvarı, kurumun iç ağında bulunan kullanıcı bilgisayarlarını ve DMZ bölgesindeki sunucuları İnternet’ten gelebilecek saldırılardan korumaktadır. Güvenlik duvarı üzerinde, kurum politikalarını yansıtacak şekilde yazılmış kurallar bulunmaktadır. Sistem yöneticisi, güvenlik duvarının gerekli güncellemelerini yapmaktadır. Güvenlik kayıtlarına bakmaktadır.

#### 5.3.3.1.3 Varlık Puanlaması

Varlık puanlaması çizelge **Çizelge 5.2 Varlık puanlaması değer çizelgesi**’ye uygun olarak gerçekleştirilmiştir.

Çizelge 5.2 Varlık puanlaması değer çizelgesi

|                            |                                                                                                                                                                               |
|----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Önemsiz (0)</b>         | Varlığın zarar görmesi bilgi sistemini hiç etkilemez.<br>Zarar görmesi, kurumun ismini etkilemez.                                                                             |
| <b>Çok önemli değil(1)</b> | Varlığın zarar görmesi bilgi sistemini çok az etkiler.<br>Bilgi sistemi işlemeye devam eder.<br>Zarar görmesi, kurumun ismini etkilemez.                                      |
| <b>Orta (2)</b>            | Varlığın zarar görmesi bilgi sistemini etkiler. Bilgi sistemi işlemeye devam eder ancak varlığın yerine konması gereklidir.<br>Zarar görmesi kurumun ismini kötü yönde çok az |

|                             |                                                                                                                                                                                                                                                 |
|-----------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                             | etkileyebilir.                                                                                                                                                                                                                                  |
| <b>Önemli (3)</b>           | Varlığın zarar görmesi bilgi sistemini oldukça etkiler.<br>Bilgi sistemi yarı yarıya kullanılabilir. Varlığın yerine konması gerekir.<br>Zarar görmesi, kurumun ismini kötü yönde etkiler.                                                      |
| <b>Çok Önemli (4)</b>       | Varlığın bilgi sisteminin işleminde önemli rolü vardır.<br>Varlığın zarar görmesi bilgi sisteminin işlerliğini büyük ölçüde etkiler. Bilgi sisteminin çok az kısmı kullanılabilir.<br>Zarar görmesi, kurumun ismini kötü yönde oldukça etkiler. |
| <b>Son Derece Önemli(5)</b> | Varlığın bilgi sisteminin işleminde için gereklidir.<br>Varlığın zarar görmesi, bilgi sistemini doğrudan etkiler.<br>Bilgi sistemi kullanılamaz.<br>Zarar görmesi, kurumun ismini çok kötü yönde etkiler.                                       |

| <b>Varlık</b>                   | <b>Puan</b> |
|---------------------------------|-------------|
| <b>Yazılım</b>                  |             |
| <b>İşletim Sistemleri</b>       |             |
| Windows NT Workstation 4.0      | 3           |
| Windows NT Server 4.0           | 3-4-5       |
| Cisco IOS 12.0                  | 4           |
| <b>Uygulamalar</b>              |             |
| Microsoft Office 97             | 1           |
| İnternet Explorer 4.0           | 1           |
| Internet Information Server 4.0 | 5           |
| Microsoft Exchange 5.5          | 4           |
| DNS servisi                     | 4           |
| Checkpoint Firewall –1          | 5           |
| <b>Protokoller</b>              |             |

|                                                      |     |
|------------------------------------------------------|-----|
| TCP/IP                                               | 1   |
| SMB                                                  | 1   |
| <b>Donanım</b>                                       |     |
| <b>Sunucular</b>                                     |     |
| E-Posta sunucusu                                     | 4   |
| DNS sunucusu                                         | 4   |
| Web sunucusu                                         | 5   |
| Birincil alan kontrolcüsü                            | 3   |
| <b>İstemciler</b>                                    |     |
| Kullanıcı bilgisayarları                             | 3   |
| <b>İletişim cihazları ve kablolar</b>                |     |
| Yönlendirici                                         | 4   |
| Güvenlik duvarı                                      | 5   |
| Hub                                                  | 1   |
| UTP (bakır) iletişim kabloları                       | 1   |
| <b>Veri</b>                                          |     |
| <b>Kurum verisi</b>                                  |     |
| Erişim kontrol listeleri                             | 4-5 |
| Genel kurum bilgileri-Web sunucu                     | 5   |
| Genel kullanıcı bilgileri- Birincil alan kontrolcüsü | 3   |
| <b>Kullanıcı verisi</b>                              |     |
| Kullanıcı dosyaları                                  | 3   |
| Kullanıcı e-postaları                                | 3   |
| <b>Ağ verisi</b>                                     |     |
| Kablolardaki ağ trafiği.                             | 3   |
| <b>Politikalar ve prosedürler</b>                    |     |
| Bilgi güvenliği politikası                           | 5   |
| Bilgi sınıflandırılması prosedürü                    | 3   |
| İnternet kullanım politikası                         | 2   |
| Sistem işletimi prosedürü                            | 4   |
| Erişim kontrolü prosedürü                            | 4   |
| Fiziksel güvenlik                                    | 4   |
| Veri yedekleme                                       | 5   |

|                          |   |
|--------------------------|---|
| Virüs önleme ve tespit   | 4 |
| <b>İnsan</b>             |   |
| 8 adet normal kullanıcı  | 4 |
| 1 adet sistem yöneticisi | 5 |

#### 5.3.3.1.4 Tehdidin Gerçekleşme İhtimali

Varlıkların puanları tespit edildikten sonra varlıklara olabilecek tehditlerin olma ihtimalleri hesaplanmalıdır. Bu hesaplamada **Çizelge 5.3**'de gösterilen tehdit değer çizelgesindeki puanlar kullanılmıştır.

Çizelge 5.3 Tehdit değer çizelgesi

|                              |                                                       |
|------------------------------|-------------------------------------------------------|
| <b>İhmal Edilebilir (0)</b>  | Olması imkan dahilinde değil                          |
| <b>Çok Düşük (1)</b>         | Beş senelik bir sürede iki ya da üç defa              |
| <b>Düşük (2)</b>             | Senede ya da daha kısa bir sürede bir kere olabilir   |
| <b>Orta (3)</b>              | Altı ayda ya da daha kısa bir sürede bir kez olabilir |
| <b>Yüksek (4)</b>            | Ayda ya da daha kısa bir sürede bir kez olabilir      |
| <b>Çok Yüksek (5)</b>        | Ayda ya da daha kısa bir sürede bir çok kez olabilir  |
| <b>Son derece Yüksek (6)</b> | Günde birçok kere olabilir                            |

| <b>Tehdit</b>                                                       | <b>Olma İhtimali</b> |
|---------------------------------------------------------------------|----------------------|
| Kasıtlı ya da kasıtsız yapılan illegal kullanıcı aktiviteleri       | 4                    |
| Kullanıcıların ihtiyacından çok erişime sahip olması                | 5                    |
| İnternet'ten yapılan hacker saldırıları                             | 3                    |
| Virüsler                                                            | 5                    |
| İnternet'ten yapılan hacker saldırılarından erken haberdar olamamak | 3                    |
| Toz, nem güneş ışığı gibi çevresel faktörler                        | 5                    |
| Bilgisayarlar yetkisiz erişim                                       | 1                    |
| Sistemlerin çok yavaş çalışması, hata vererek                       | 4                    |

|                                                                                           |   |
|-------------------------------------------------------------------------------------------|---|
| çalışmasının durması                                                                      |   |
| Dinleme ( <b>sniffing</b> ) yapılması                                                     | 2 |
| Sistemin sürekliliğinin kaybolması                                                        | 2 |
| Sistem hatalarından ya da elektrik kesintisi gibi çevre etkilerinden dolayı verinin kaybı | 2 |
| Kullanıcı verilerinin başkaları tarafından okunması                                       | 2 |
| Sistemde bilgi güvenliği için bir politikanın olmaması                                    | 3 |
| İnternet kullanım politikasında yazılmamış olan kullanıcı aktiviteleri                    | 2 |
| Güvenlik olaylarının takip edilmemesi, tepki verilememesi                                 | 4 |
| Yetkisiz erişimler                                                                        | 3 |
| Fiziksel güvenlik ihlalleri                                                               | 3 |
| Yedekleme yapılamaması                                                                    | 3 |
| Virüs tanımlarının güncel olmaması                                                        | 3 |
| Sistemde olabilecek bir arızanın uzun süre giderilememesi                                 | 3 |
| İllegal kullanıcı aktivitesinin sorumlusunun bulunamaması                                 | 3 |

#### 5.3.3.1.5 Tehdidin Mutlak Etkisi

Tehditlerin mutlak etkisinin belirlenmesi gerekmektedir. Etki değerlerinin hesaplanmasında **Çizelge 5.4**'te verilen değerler kullanılmıştır.

Çizelge 5.4 Tehditlerin mutlak etkilerinin değer çizelgesi

|                    |                                                                                                                       |
|--------------------|-----------------------------------------------------------------------------------------------------------------------|
| <b>Önemsiz (0)</b> | Tehditin varlık üzerinde hiç etkisi yoktur.                                                                           |
| <b>Küçük (1)</b>   | Tehditin varlık üzerinde küçük etkisi olur. Varlıkları tamir etmeye ya da yeniden konfigüre etmeye gerek yoktur.      |
| <b>Önemli (2)</b>  | Tehditin etkisi küçük olmasına ve birkaç kişi ya da kuruluş tarafından söylenmesine rağmen, tehditin somut bir zararı |

|                         |                                                                                                                                                                                               |
|-------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                         | olabilir. Hasarın giderilmesi ve önlem alınması için bir takım harcamalar olabilir.                                                                                                           |
| <b>Zarar verici (3)</b> | Varlığın ya da sistemin sahiplerine ve yöneticilerine kötü ün kazandırabilir ve/veya kaynakta önemli zararlar olur. Hasarın giderilmesi ve önlem alınması için önemli harcamalar gerekebilir. |
| <b>Ciddi (4)</b>        | Varlığa büyük ölçüde zarar verir ve/veya birçok kişi ve kurumun kendisi zarardan etkilenebilir. Zarar gören sistemde büyük ölçüde yeniden yapılandırma gerekmektedir.                         |
| <b>Çok Ciddi (5)</b>    | Varlığın süresiz olarak işlem yapamamasına ve tamamıyla zarar görmesine yol açar. Sistem tamamen baştan dizayn edilmesini ve yapılandırmasını gerektirir.                                     |

| <b>Tehdit</b>                                                                             | <b>Mutlak Etki Değeri</b> |
|-------------------------------------------------------------------------------------------|---------------------------|
| Kasıtlı ya da kasıtsız yapılan illegal kullanıcı aktiviteleri                             | 4                         |
| Kullanıcıların ihtiyacından çok erişime sahip olması                                      | 3                         |
| İnternet'ten yapılan hacker saldırıları                                                   | 5                         |
| Virüsler                                                                                  | 5                         |
| İnternet'ten yapılan hacker saldırılarından erken haberdar olamamak                       | 4                         |
| Toz, nem güneş ışığı gibi çevresel faktörler                                              | 2                         |
| Bilgisayarlara yetkisiz erişim                                                            | 4                         |
| Sistemlerin çok yavaş çalışması, hata vererek çalışmasının durması                        | 4                         |
| Dinleme ( <b>sniffing</b> ) yapılması                                                     | 5                         |
| Sistemin sürekliliğinin kaybolması                                                        | 4                         |
| Sistem hatalarından ya da elektrik kesintisi gibi çevre etkilerinden dolayı verinin kaybı | 4                         |
| Kullanıcı verilerinin başkaları tarafından okunması                                       | 4                         |

|                                                                        |   |
|------------------------------------------------------------------------|---|
| Sistemde bilgi güvenliği için bir politikanın olmaması                 | 4 |
| İnternet kullanım politikasında yazılmamış olan kullanıcı aktiviteleri | 3 |
| Güvenlik olaylarının takip edilmemesi, tepki verilememesi              | 4 |
| Yetkisiz erişimler                                                     | 4 |
| Fiziksel güvenlik ihlalleri                                            | 3 |
| Yedekleme yapılamaması                                                 | 4 |
| Virüs tanımlarının güncel olmaması                                     | 4 |
| Sistemde olabilecek bir arızanın uzun süre giderilememesi              | 3 |
| İllegal kullanıcı aktivitesinin sorumlusunun bulunamaması              | 3 |

### 5.3.3.1.6 Risk Hesaplanması

Tehditler ve tehditlerin mutlak etkileri tespit edildikten sonra risk hesaplanması gerçekleştirilmelidir. Bu hesaplamalarda **Çizelge 5.5**'deki değerler kullanılmıştır.

Çizelge 5.5 Risk hesaplaması değer çizelgesi

| Tehditin olma olasılığı * Tehditin Mutlak Etkisi | Önemsiz (0) | Küçük (1) | Önemli (2) | Zarar Verici (3) | Ciddi (4)   | Çok Ciddi (5) |
|--------------------------------------------------|-------------|-----------|------------|------------------|-------------|---------------|
| İhmal Edilebilir (0)                             | Yok (0)     | Yok (0)   | Yok (0)    | Yok (0)          | Yok (0)     | Yok (0)       |
| Çok Düşük (1)                                    | Yok (0)     | Düşük (1) | Düşük (2)  | Düşük (3)        | Orta (4)    | Orta (5)      |
| Düşük (2)                                        | Yok (0)     | Düşük (2) | Orta (4)   | Orta (6)         | Yüksek (8)  | Yüksek (10)   |
| Orta (3)                                         | Yok (0)     | Düşük (2) | Orta (6)   | Yüksek (8)       | Yüksek (10) | Kritik (15)   |

|                              |         |          |             |             |                 |                 |
|------------------------------|---------|----------|-------------|-------------|-----------------|-----------------|
|                              |         | (3)      |             | (9)         | (12)            | (15)            |
| <b>Yüksek (4)</b>            | Yok (0) | Orta (4) | Yüksek (8)  | Yüksek (12) | Kritik (16)     | Çok Yüksek (20) |
| <b>Çok Yüksek (5)</b>        | Yok (0) | Orta (5) | Yüksek (10) | Kritik (15) | Çok Yüksek (20) | Çok Yüksek (25) |
| <b>Son Derece Yüksek (6)</b> | Yok (0) | Orta (6) | Yüksek (12) | Kritik (18) | Çok Yüksek (24) | Çok Yüksek (30) |

| Tehdit                                                               | Tehditin Olma İhtimali | Tehditin Mutlak Etkisi | Mutlak Risk | Etkilediği varlık (lar)ın puanı | Gerçek risk değeri (Taban Risk) |
|----------------------------------------------------------------------|------------------------|------------------------|-------------|---------------------------------|---------------------------------|
| Kasıtlı ya da kasıtsız yapılan illegal kullanıcı aktiviteleri        | 4                      | 4                      | 16          | 3                               | 48                              |
| Kullanıcıların ihtiyacından çok erişime sahip olması                 | 5                      | 3                      | 15          | 3                               | 45                              |
| İnternet'ten yapılan hacker saldırıları                              | 3                      | 5                      | 15          | 5                               | 75                              |
| Virüsler                                                             | 5                      | 5                      | 25          | 4                               | 100                             |
| İnternet'ten yapılan hacker saldırılarından erken haberdar olamamak  | 3                      | 4                      | 12          | 5                               | 60                              |
| Toz, nem güneş ışığı gibi çevresel faktörler                         | 5                      | 2                      | 10          | 5                               | 50                              |
| Bilgisayarlara yetkisiz erişim                                       | 1                      | 4                      | 4           | 5                               | 20                              |
| Sistemlerin çok yavaş çalışması, hata vererek çalışmasının durması   | 4                      | 4                      | 16          | 4                               | 64                              |
| Dinleme ( <b>sniffing</b> ) yapılması                                | 2                      | 5                      | 10          | 3                               | 30                              |
| Sistemin sürekliliğinin kaybolması                                   | 2                      | 4                      | 8           | 4                               | 32                              |
| Sistem hatalarından ya da elektrik kesintisi gibi çevre etkilerinden | 2                      | 4                      | 8           | 5                               | 40                              |

|                                                                        |   |   |    |   |    |
|------------------------------------------------------------------------|---|---|----|---|----|
| dolayı verinin kaybı                                                   |   |   |    |   |    |
| Kullanıcı verilerinin başkaları tarafından okunması                    | 2 | 4 | 8  | 4 | 32 |
| Sistemde bilgi güvenliği için bir politikanın olmaması                 | 3 | 4 | 12 | 5 | 60 |
| İnternet kullanım politikasında yazılmamış olan kullanıcı aktiviteleri | 2 | 3 | 6  | 3 | 18 |
| Güvenlik olaylarının takip edilmemesi, tepki verilememesi              | 4 | 4 | 16 | 4 | 64 |
| Yetkisiz erişimler                                                     | 3 | 4 | 12 | 4 | 48 |
| Fiziksel güvenlik ihlalleri                                            | 3 | 3 | 9  | 4 | 36 |
| Yedekleme yapılamaması                                                 | 3 | 4 | 12 | 5 | 60 |
| Virüs tanımlarının güncel olmaması                                     | 3 | 4 | 12 | 4 | 48 |
| Sistemde olabilecek bir arızanın uzun süre giderilememesi              | 3 | 3 | 9  | 4 | 36 |
| İllegal kullanıcı aktivitesinin sorumlusunun bulunamaması              | 3 | 3 | 9  | 3 | 27 |

### 5.3.3.1.7 Risk Yönetimi

Risk değerleri belirlendikten sonra karşı önlemler alınarak risk yönetimi yapılmalıdır. İlk olarak risk puanlarına göre tehditlerin önem sırası belirlenmelidir.

| Tehdit                                                              | Gerçek risk değeri<br>(Taban Risk) | İstenen<br>(taşına-bilir) risk | Karşı önlem alınma<br>önceliği |
|---------------------------------------------------------------------|------------------------------------|--------------------------------|--------------------------------|
| Virüsler                                                            | 100                                | 50                             | 50                             |
| Sistemde bilgi güvenliği için bir politikanın olmaması              | 60                                 | 20                             | 40                             |
| İnternet'ten yapılan hacker saldırıları                             | 75                                 | 40                             | 35                             |
| Güvenlik olaylarının takip edilmemesi, tepki verilememesi           | 64                                 | 30                             | 34                             |
| Sistemlerin çok yavaş çalışması, hata vererek çalışmasının durması  | 64                                 | 30                             | 34                             |
| İnternet'ten yapılan hacker saldırılarından erken haberdar olamamak | 60                                 | 30                             | 30                             |

|                                                                                           |    |    |    |
|-------------------------------------------------------------------------------------------|----|----|----|
| Yetkisiz erişimler                                                                        | 48 | 20 | 28 |
| Yedekleme yapılamaması                                                                    | 60 | 35 | 25 |
| Kasıtlı ya da kasıtsız yapılan illegal kullanıcı aktiviteleri                             | 48 | 25 | 23 |
| Kullanıcı verilerinin başkaları tarafından okunması                                       | 32 | 15 | 17 |
| Fiziksel güvenlik ihlalleri                                                               | 36 | 20 | 16 |
| Dinleme ( <b>sniffing</b> ) yapılması                                                     | 30 | 15 | 15 |
| Virüs tanımlarının güncel olmaması                                                        | 48 | 35 | 13 |
| Sistemin sürekliliğinin kaybolması                                                        | 32 | 20 | 12 |
| Sistemde olabilecek bir arızanın uzun süre giderilememesi                                 | 36 | 25 | 11 |
| Bilgisayarlara yetkisiz erişim                                                            | 20 | 9  | 11 |
| Kullanıcıların ihtiyacından çok erişime sahip olması                                      | 45 | 35 | 10 |
| İllegal kullanıcı aktivitesinin sorumlusunun bulunamaması                                 | 27 | 20 | 7  |
| Sistem hatalarından ya da elektrik kesintisi gibi çevre etkilerinden dolayı verinin kaybı | 40 | 35 | 5  |
| Toz, nem güneş ışığı gibi çevresel faktörler                                              | 50 | 45 | 5  |
| İnternet kullanım politikasında yazılmamış olan kullanıcı aktiviteleri                    | 18 | 15 | 3  |

### 5.3.3.2 Sistemin Güvenlik Hedefinin Oluşturulması

#### 5.3.3.2.1 Kabullenmeler, Tehditler, Riskler ve Güvenlik Politikaları

A şirketinin BT ve BT dışı ortamı için kabullenmeler aşağıda sıralanmıştır.

##### 1. Güvenlik Kabullenmeleri TOE için

|                                  |                                                                                                                   |
|----------------------------------|-------------------------------------------------------------------------------------------------------------------|
| A.COTS                           | TOE’de yakın dönemli gerçekleştirilebilir, ticari hazır bilgi teknolojisiyle bulunur                              |
| A.KÖTÜ NİYETLİ İÇERİDEN BİR KİŞİ | TOE'nin yetkilendirilmiş hakların kötüye kullanımıyla oluşan riskleri yeterince azaltabilmesi beklenmemektedir.   |
| A.GELİŞMİŞ BİR SALDIRI           | TOE'nin gelişmiş saldırı yöntemlerinin uygulanmasından kaynaklanan riskleri yeterince azaltması beklenmemektedir. |

## 2. Güvenlik Kabullenmeleri Personel için

|                       |                                                                                                                                                             |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A. YÖNETİM            | TOE'nin güvenlik özellikleri sürekli bir şekilde başarılı olarak idare edilmektedir.                                                                        |
| A. KULLANICI İHTİYACI | Kimliği doğrulanan kullanıcılar güvenli BT ortamı ihtiyacını kabul etmektedir.                                                                              |
| A. KULLANICI GÜVENİ   | Kimliği doğrulanan kullanıcılara kendi takdirlerindeki eylemleri güvenlik politikalarına uygun olarak gerçekleştirmeleri bakımından genel olarak güvenilir. |

A şirketinin BT sistemi (TOE) için tehditler aşağıda sıralanmıştır.

TOE için tehditler;

|                        |                                                                                                                                                                                                                                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| T.ERİŞİM-TOE           | İzin verilen bir kullanıcı, kullanıcı hatası, sistem hatası ya da gelişmiş olmayan, teknik bir saldırı yoluyla, TOE'ye ya da TOE tarafından doğrudan kontrol edilen bir kaynağa ya da bilgiye izin verilmeyen, kötü niyetli olmayan bir erişim elde edebilir. |
| T.DENETİM-GİZLİLİK-TOE | TOE'nin kontrolü altındaki denetim izlerinde, güvenlik olaylarının kayıtları yetkilendirilmemiş kişilere ya da işlemlere açıklanabilir.                                                                                                                       |
| T.DENETİM-BOZUK-TOE    | TOE'nin kontrolü altındaki denetim izlerinde, güvenlik olaylarının kayıtları yetkilendirilmemiş değiştirmeye ya da silinmeye maruz kalabilir.                                                                                                                 |
| T.KİLİTLENME-TOE       | TOE'nin güvenli durumu bir sistem kilitlenmesi durumunda tehlikeye düşebilir.                                                                                                                                                                                 |
| T.HİZMET REDDİ-TOE     | TOE, gelişmiş olmayan, hizmet reddi saldırısına maruz bırakılabilir.                                                                                                                                                                                          |
| T.GİRİŞ-TOE            | İzin verilen bir kullanıcı dışındaki bir kişi, gelişmiş olmayan, teknik bir saldırı yoluyla                                                                                                                                                                   |

|                       |                                                                                                                                                                                                                                                                 |
|-----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                       | TOE kontrolündeki işlem kaynaklarına ya da bilgiye yetkilendirilmemiş, kötü niyetli erişim elde edebilir.                                                                                                                                                       |
| T.GÖZLEM-TOE          | TOE'nin çalışmasında BT güvenliğini tehlikeye düşüren olaylar oluşur ama TOE, spesifikasyonu, tasarımı ya da uygulamasındaki hatalar nedeniyle bilgili bir kullanıcının ya da güvenlik yöneticisinin sistemin hala güvenli olduğunu düşünmesine neden olabilir. |
| T.KAYIT-OLAY-TOE      | TOE tarafından kontrol edilen güvenlikle ilgili olaylar kaydedilmeyebilir.                                                                                                                                                                                      |
| T.KAYNAKLAR           | Paylaşılan, iç TOE kaynakları sistem hatası ya da kötü niyetli olmayan kullanıcı eylemleri nedeniyle tüketilebilir.                                                                                                                                             |
| T.BOZUK               | TOE'nin güvenlik durumu, gelecekteki güvenli olmayan durumlara olanak tanımak için düşük dereceli bir saldırı sonucunda kasıtlı olarak bozulabilir.                                                                                                             |
| T.ERİŞİM-KÖTÜ NİYETLİ | Yetkilendirilmiş bir kullanıcı kötü niyetli amaçlar için yetkilendirilmemiş erişim elde edebilir.                                                                                                                                                               |
| T.YÖNETİM-HATA        | Sistemin güvenliği sistemin güvenlik özelliklerinin yönetimindeki hatalar ya da eksiklikler nedeniyle azalabilir ya da aşılabilir.                                                                                                                              |
| T.KURULUM             | Sistem, güvenliği riske atacak bir şekilde sunulabilir ya da kurulabilir.                                                                                                                                                                                       |
| T.İŞLETME             | Sistemin uygun olmayan bir şekilde işletilmesi nedeniyle güvenlik hataları oluşabilir; örneğin yetkilendirilmiş hakların kötüye kullanımı.                                                                                                                      |
| T.SİSTEM-BOZUK        | Sistemin güvenlik durumu, başka bir tehdit                                                                                                                                                                                                                      |

|                       |                                                                                                |
|-----------------------|------------------------------------------------------------------------------------------------|
|                       | nedeniyle kasıtlı olarak bozularak gelecekteki güvenli olmayan durumlara zemin hazırlanabilir. |
| T.VİRÜS               | İnternet yoluyla kullanıcılar virüslü dosyaları TOE ortamına bulaştırabilir.                   |
| T.DİNLEME             | Yetkisi olan veya olmayan kullanıcılar diğer kullanıcıların iletişimini dinleyebilir.          |
| T.SÜREKLİLİK          | TOE'nin hizmet verememesi durumu geç müdahale edilmesi durumunda uzayabilir.                   |
| T.KÖTÜ ORTAM ŞARTLARI | Toz, nem vb. ortam şartlarından dolayı TOE bileşenleri zarar görebilir.                        |

A şirketinin BT sistemi (TOE) için güvenlik politikaları aşağıda sıralanmıştır.

|                  |                                                                                                                                                                                                     |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| P. SORUMLULUK    | Kullanıcılar güvenlikle ilgili eylemleri nedeniyle sorumlu tutulmalıdır.                                                                                                                            |
| P. UYUM          | Kuruluşun BT sistemlerinin uygulaması ve kullanımı bütün ilgili yasalara, düzenlemelere ve kuruluşun imzaladığı sözleşmelere uygun olmalıdır.                                                       |
| P. GEREKEN ÖZEN  | Kuruluşun BT sistemleri, kuruluşa yönelik risklere karşı GEREKEN ÖZEN ve dikkat gösterecek şekilde uygulanmalı ve çalıştırılmalıdır.                                                                |
| P. BİLİNEN       | İzin verilen çok iyi tanımlanmış işlemler dışında, TOE erişimi izni için TOE kullanıcılarının kimliğinin belirlenmesi ve onaylanması gerekmektedir.                                                 |
| P. FİZİKSEL      | Güvenlik hedeflerine ulaşılmasını sağlamak için fiziksel olarak korunması gereken TOE'nin işlem kaynakları, izinsiz, fiziksel erişimi ortadan kaldıran kontrollü erişim bölgelerinde yer alacaktır. |
| P. HAYATTA KALMA | BT sistemi, ortamıyla birlikte güvenli                                                                                                                                                              |

|                   |                                                                                                                                                                                                                                                                                                                                          |
|-------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                   | olmayan durumlara karşı esnek olmalı ve güvenli olmayan durumlara direnmeli ve/veya güvenli olmayan durumu belirlemek için yollar sağlamalı ve bu tür durumlardan tekrar güvenli durumlara dönebilmelidir.                                                                                                                               |
| P. EĞİTİM         | Sistemi kullanmasına izin verilen kimliği doğrulanmış kullanıcılar aşağıdakileri yapmalarına olanak tanıyacak şekilde eğitilmelidir: (1) kendi takdirlerinde olan işlerde kurumsal güvenlik politikalarını etkili bir şekilde uygulama (2) bu politikaları uygulamak için kullanılan isteğe bağlı olmayan kontrol ihtiyacını destekleme. |
| P.BİLGİ GÜVENLİĞİ | Kurum bilgi güvenliği politikasına uygun olarak işletilmelidir.                                                                                                                                                                                                                                                                          |
| P. KULLANIM       | Kuruluşun BT kaynakları sadece yetkilendirilmiş amaçlarla kullanılmalıdır.                                                                                                                                                                                                                                                               |

A şirketinin BT sisteminin riskleri 5.3.3.1.7 bölümünde gösterilmiştir.

#### 5.3.3.2.2 TOE için Güvenlik Amaçları

|                                                                                                                                                                                                     |                                                               |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------|
| <b>O.ERİŞİM-TOE:</b> TOE, yetkilendirildikleri TOE kaynakları ve eylemleri için herkese açık erişim ve izin verilen kullanıcılara erişim sağlamalıdır.                                              | T.ERİŞİM                                                      |
| <b>O.SORUMLULUK-TOE:</b> TOE, kendi kontrolü ya da bilgisindeki eylemler için bütün TOE kullanıcılarının güvenlikle ilgili eylemleri için sonradan sorumlu tutulabilmesini sağlaması gerekmektedir. | P.SORUMLULUK<br>T.DENETİM-BOZUK-TOE<br>T.DENETİM-GİZLİLİK-TOE |
| <b>O.YETKİLENDİRME-TOE:</b> TOE'nin, kullanıcı ve sistem işlem erişim haklarını kontrolü altındaki ayrı işlem kaynakları ve veri öğelerine atayabilme ve                                            | T.ERİŞİM                                                      |

|                                                                                                                                                                                                                                                  |                                       |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| yönetebilme yeteneği sağlaması ve kuruluşun erişim kontrolüyle ilgili güvenlik politikasını desteklemesi gerekmektedir.                                                                                                                          |                                       |
| <b>O.KULLANILABİLİR-TOE:</b> TOE'nin kendisini gelişmemiş, hizmet reddi saldırılarına karşı koruması gerekmektedir.                                                                                                                              | P.HAYATTA KALMA<br>T.HİZMET REDDİ-TOE |
| <b>O.DEVRE DIŞI BIRAKMA-TOE:</b> TOE, yetkilendirilmiş yazılım ya da kullanıcıların kazara ya da kötü niyetli olmayan bir şekilde TOE güvenlik politikası uygulamasını devre dışı bırakmasını önlemelidir.                                       | T.ERİŞİM-TOE                          |
| <b>O.BELİRLEME-TOE:</b> TOE'nin, TOE'ye özgü güvenli olmayan durumların belirlenmesine olanak tanınması gerekmektedir. Burada hedef düşük dereceli saldırılar için yüksek etkinliktir.                                                           | P.HAYATTA KALMA<br>T.BOZUK            |
| <b>O.GİRİŞ-TOE:</b> TOE, erişim iznine sahip olmayan kişiler tarafından gelişmiş olmayan teknik yöntemler kullanılarak TOE'ye mantıksal girişi önlemesi gerekmektedir.                                                                           | P.KULLANIM<br>T.GİRİŞ-TOE             |
| <b>O.BİLİNEN-TOE:</b> TOE'nin kendi kontrolü altındaki bütün eylemler için, izin verilen iyi tanımlanmış bir dizi eylem dışında, bütün kullanıcıların erişim hakkı vermeden önce tanınması ve kimliğinin doğrulanmasını sağlaması gerekmektedir. | P.BİLİNEN                             |
| <b>O.GÖZLEM-TOE:</b> TOE'nin kendi güvenlik durumunun yönetici ya da kullanıcıya yanlış gösterilmemesini sağlaması gerekmektedir.                                                                                                                | T.GÖZLEM-TOE                          |
| <b>O.GERİ DÖNDÜRME-TOE:</b> TOE'nin bir sistem sorunu, hizmet kesintisi ya da güvenli olmayan bir durumun belirlenmesinin ardından güvenli bir duruma geri dönülmesini sağlaması gerekmektedir.                                                  | P.HAYATTA KALMA<br>T.KİLİTLENME-TOE   |
| <b>O.KAYNAKLAR:</b> TOE, paylaşılan kaynakların tüketilmesine neden olan kullanıcı ya da sistem hatalarından kendisini korumalıdır.                                                                                                              | P.HAYATTA KALMA<br>T.KAYNAKLAR        |

|                                                                                                                                                                                                                                                                                                                                                                                                               |                                                     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------|
| <b>O.BELİRLEME-SİSTEM:</b> TOE, güvenli olmayan durumların belirlenmesine olanak tanımalıdır. Amaç, düşük dereceli saldırılar için yüksek etkinliktir.                                                                                                                                                                                                                                                        | P.HAYATTA KALMA<br>T.SİSTEM-BOZUK                   |
| <b>O.ERİŞİM-KÖTÜ NİYETLİ:</b> TOE kontrolleri bu amaca ulaşılmasına yardım edecektir ama yeterli olmayacaktır. İzin verilen kullanıcılar tarafından kötü niyetli eylemlerin yeterince ortadan kaldırılması (azaltılması) için ek, ortamla ilgili kontroller gerekmektedir.                                                                                                                                    | T.ERİŞİM-KÖTÜ NİYETLİ                               |
| <b>O.YÖNETİM:</b> Sistemden sorumlu olanlar (TOE tarafından sağlanan mekanizmalarla birlikte) sistemin, BT güvenliği sürdürülecek şekilde yönetilmesini ve idare edilmesini sağlamalıdır.                                                                                                                                                                                                                     | T.YÖNETİM-HATA                                      |
| <b>O.ESKİ DURUMA DÖNDÜRME-SİSTEM:</b> Sistem, bir sistem sorunu, hizmet kesintisi ya da güvenli olmayan bir durumun belirlenmesinin ardından güvenli bir duruma geri dönülmesine olanak tanımalıdır. Bu da biraz önleme ve daha çok da belirleme ve tepki göstermeyle gerçekleştirilecektir ve belirli sorunlar için yüksek etkinlik sağlanacaktır. Genel sorunlarda, düşük etkinlikle gerçekleştirilecektir. | P.HAYATTA KALMA<br>T.KİLİTLENME-TOE<br>T.SÜREKLİLİK |
| <b>O.ÇALIŞTIRMA:</b> Sistemden sorumlu olanlar (TOE tarafından sağlanan mekanizmalarla birlikte) sistemin BT güvenliğini sürdüren bir şekilde teslim edilmesi, kurulması ve çalıştırılmasını sağlamalıdır.                                                                                                                                                                                                    | T.KURULUM<br>T.İŞLETME<br>P.EĞİTİM                  |
| <b>O.KAYIT:</b> TOE tarafından kontrol edilen BT ortamında güvenlikle ilgili konular kayıt edilecektir.                                                                                                                                                                                                                                                                                                       | T.KAYIT-OLAY-TOE                                    |
| <b>O.VİRÜS KORUMA:</b> TOE dışarıdan gelebilecek virüslere karşı koruma sağlamalıdır.                                                                                                                                                                                                                                                                                                                         | T.VİRÜS                                             |
| <b>O.DİNLENEME:</b> TOE içerisinde kullanıcıların diğer kullanıcıların bilgilerini takip etmesi ve dinlemesi engellenecektir.                                                                                                                                                                                                                                                                                 | T.DİNLEME                                           |
| <b>O.GÜVENLİK POLİTİKASI:</b> TOE hazırlanmış olan                                                                                                                                                                                                                                                                                                                                                            | P.BİLGİ GÜVENLİĞİ                                   |

|                                                                                                                                                                                                                                                                                                                         |                          |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------|
| güvenlik politikasına uygun olarak işletilecektir.                                                                                                                                                                                                                                                                      |                          |
| <b>O.TEMİZ ORTAM:</b> TOE kaynaklarının düzgün ve devamlı bir şekilde çalışabileceği bir ortamda tutulacaktır.                                                                                                                                                                                                          | T.KÖTÜ ORTAM<br>ŞARTLARI |
| <b>O.FİZİKSEL:</b> TOE'den sorumlu olanların TOE'nin güvenlik politikası açısından önemli bölümlerinin BT güvenliğini tehlikeye düşürebilecek fiziksel saldırıdan korunmasını sağlaması gerekmektedir.                                                                                                                  | P.FİZİKSEL               |
| <b>O.UYUM:</b> TOE ortamı, TOE tarafından uygulanan kontrollerle birlikte ilgili yasalar, düzenlemeler ve sözleşmeyle getirilen koşullara tam olarak uymalıdır. Bu da bazı teknik kontrollerle gerçekleştirilecektir ama bu hedefi yüksek etkinlikle gerçekleştirmek için teknik olmayan kontrollere önem verilecektir. | P.UYUM                   |
| <b>O.UYGUN-DİKKAT:</b> TOE ortamı, TOE'nin kendisiyle birlikte, kuruluştaki BT ile ilgili risklere gereken özenin ve dikkatin gösterildiğini açık bir şekilde sergileyecek şekilde uygulanmalı ve çalıştırılmalıdır.                                                                                                    | P.GEREKEN-ÖZEN           |

### 5.3.3.2.3 TOE Güvenlik Gereksinimleri

TOE'nin güvenlik fonksiyonel gereksinimleri;

| Fonksiyonel Gereksinim | Açıklaması                | Karşıladığı Güvenlik Amacı                                                                                                                            |
|------------------------|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------|
| FAU_GEN.1              | Denetim verileri Üretimi  | <b>O.SORUMLULUK-TOE</b><br><b>O.GERİ DÖNDÜRME-TOE</b><br><b>O.BELİRLEME-TOE</b><br><b>O.BELİRLEME-SİSTEM</b><br><b>O.ÇALIŞTIRMA</b><br><b>O.KAYIT</b> |
| FAU_GEN.2              | Kullanıcı Kimliği Üretimi | <b>O.SORUMLULUK-TOE</b>                                                                                                                               |

|           |                                                 |                                                                                                                                                      |
|-----------|-------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| FAU_SAR.1 | Denetim Gözden Geçirmesi                        | FAU_SAR.2<br>FAU_SAR.3<br>için gerekli bağımlılık                                                                                                    |
| FAU_SAR.2 | Sınırlı Denetim Gözden Geçirmesi                | <b>O.GERİ DÖNDÜRME-TOE</b>                                                                                                                           |
| FAU_SAR.3 | Seçilebilir Denetim Gözden Geçirmesi            | <b>O.SORUMLULUK-TOE</b><br><b>O.GERİ DÖNDÜRME-TOE</b><br><b>O.BELİRLEME-TOE</b><br><b>O.BELİRLEME-SİSTEM</b><br><b>O.ÇALIŞTIRMA</b><br><b>O.UYUM</b> |
| FAU_SEL.1 | Seçici Denetim                                  | <b>O.BELİRLEME-TOE</b><br><b>O.BELİRLEME-SİSTEM</b><br><b>O.ÇALIŞTIRMA</b><br><b>O.UYUM</b>                                                          |
| FAU_STG.1 | Korunmuş denetim izinin saklanması              | <b>O.BELİRLEME-TOE</b><br><b>O.BELİRLEME-SİSTEM</b><br><b>O.UYUM</b><br><b>O.SORUMLULUK-TOE</b>                                                      |
| FAU_STG.3 | Olası Denetim Verisi Kaybı durumunda Eylem      | <b>O.SORUMLULUK-TOE</b>                                                                                                                              |
| FDP_ACC.1 | Alt Küme Erişim Kontrolü                        | <b>O.ERİŞİM-TOE</b><br><b>O.ERİŞİM-KÖTÜ NİYETLİ</b><br><b>O.GİRİŞ-TOE</b><br><b>O.UYUM</b><br><b>O.KULLANILABİLİR-TOE</b><br><b>O.KAYNAKLAR</b>      |
| FDP_ACF.1 | Güvenlik Özniteliklerine Dayalı Erişim Kontrolü | <b>O.ERİŞİM-TOE</b><br><b>O.ERİŞİM-KÖTÜ NİYETLİ</b><br><b>O.GİRİŞ-TOE</b><br><b>O.UYUM</b><br><b>O.KULLANILABİLİR-TOE</b><br><b>O.KAYNAKLAR</b>      |

|           |                                                                   |                                                                                                                                                |
|-----------|-------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|
| FDP_ETC.1 | Kullanıcı verilerinin güvenlik öznitelikleri olmadan gönderilmesi | <b>O.GİRİŞ-TOE</b><br><b>O.KULLANILABİLİR-TOE</b>                                                                                              |
| FIA_AFL.1 | Kimlik Doğrulama Başarısızlığının İdaresi                         | <b>O.BELİRLEME-TOE</b><br><b>O.BELİRLEME-SİSTEM</b><br><b>O.GİRİŞ-TOE</b><br><b>O.DEVRE DIŞI-TOE</b><br><b>O.GEREKEN ÖZEN</b><br><b>O.UYUM</b> |
| FIA_ATD.1 | Kullanıcı Özniteliği Tanımı                                       | <b>O.YETKİLENDİRME-TOE</b>                                                                                                                     |
| FIA_SOS.1 | Sırların Doğrulanması                                             | <b>O.UYUM</b>                                                                                                                                  |
| FIA_UAU.1 | Kimlik doğrulamanın zamanlaması                                   | <b>O.BİLİNEN-TOE</b>                                                                                                                           |
| FIA_USB.1 | Kullanıcı-Özne Bağlaması                                          | <b>O.ERİŞİM-TOE</b><br><b>O.ERİŞİM-KÖTÜ NİYETLİ</b>                                                                                            |
| FMT_MSA.1 | Güvenlik özniteliklerinin yönetimi                                | <b>O.YETKİLENDİRME-TOE</b>                                                                                                                     |
| FMT_MSA.3 | Statik öznitelik başlatma                                         | <b>O.YETKİLENDİRME-TOE</b>                                                                                                                     |
| FMT_SAE.1 | Zaman Sınırlı Yetkilendirme                                       | <b>O.ERİŞİM-TOE</b><br><b>O.ERİŞİM-KÖTÜ NİYETLİ</b><br><b>O.GİRİŞ-TOE</b><br><b>O.YETKİLENDİRME-TOE</b>                                        |
| FPT_FLS.1 | Güvenlik durumun korunduğu sorun                                  | <b>O.GERİ DÖNDÜRME-TOE</b>                                                                                                                     |
| FPT_RCV.2 | Hatadan Sonra Geri Dönüş                                          | <b>O.GERİ DÖNDÜRME-TOE</b>                                                                                                                     |
| FRU_RSA.1 | Maksimum kota                                                     | <b>O.KAYNAKLAR</b>                                                                                                                             |
| FTA_LSA.1 | Seçilebilir özniteliklerinin kapsamında sınırlama                 | <b>O.ERİŞİM-TOE</b><br><b>O.ERİŞİM-KÖTÜ NİYETLİ</b><br><b>O.GİRİŞ-TOE</b>                                                                      |
| FTA_MCS.1 | Çoklu eşzamanlı oturumlarda temel kısıtlama                       | <b>O.ERİŞİM-TOE</b><br><b>O.ERİŞİM-KÖTÜ NİYETLİ</b><br><b>O.GİRİŞ-TOE</b>                                                                      |

|           |                                   |                                                                           |
|-----------|-----------------------------------|---------------------------------------------------------------------------|
| FTA_SSL.2 | Kullanıcının başlattığı kilitleme | <b>O.ÇALIŞTIRMA</b>                                                       |
| FTA_TAH.1 | TOE erişim tarihi                 | <b>O.GÖZLEM-TOE</b><br><b>O.GİRİŞ-TOE</b><br><b>O.UYUM</b>                |
| FTA_TSE.1 | TOE oturumu kurulması             | <b>O.ERİŞİM-TOE</b><br><b>O.ERİŞİM-KÖTÜ NİYETLİ</b><br><b>O.GİRİŞ-TOE</b> |

TOE'nin güvenlik garanti gereksinimleri;

TOE'nin taşıdığı en yüksek varlık sınıfı özel olduğu için aşağıdaki garanti gereksinimleri paketini içermelidir.

|                                    |                                                                |
|------------------------------------|----------------------------------------------------------------|
| ACM Sınıfı: Konfigürasyon yönetimi | ACM_CAP.3 Yetkilendirme kontrolleri                            |
|                                    | ACM_SCP.1 TOE KM kapsamı                                       |
| ADO Sınıfı: Teslim ve çalıştırma   | ADO_DEL.1 Teslim prosedürleri (varsa)                          |
|                                    | ADO_IGS.1 Kurulum, üretim ve başlatma prosedürleri             |
| ADV Sınıfı: Geliştirme             | ADV_FSP.1 Biçimsel olmayan fonksiyonel belirtim                |
|                                    | ADV_HLD.2 Güvenliği uygulayan üst düzeyde tasarım              |
|                                    | ADV_IMP.1 TSF uygulamasının alt kümesi                         |
|                                    | ADV_SPM.1 Biçimsel olmayan TOE güvenlik politikası modellemesi |
|                                    | ADV_RCR.1 Biçimsel olmayan karşılık gelmenin gösterilmesi      |
| AGD Sınıfı: Kılavuz belgeler       | AGD_ADM Yönetici kılavuzu                                      |
|                                    | AGD_USR Kullanıcı kılavuzu                                     |
| ALC Sınıfı: Yaşam döngüsü desteği  | ALC_DVS.1 Güvenlik önlemlerinin belirtilmesi                   |
|                                    | ALC_FLR.2 Hata bildirme prosedürleri                           |
| ATE Sınıfı: Testler                | ATE_COV.2 Kapsamın incelenmesi                                 |
|                                    | ATE_DPT.1 Test: üst düzeyde tasarım                            |
|                                    | ATE_FUN.1 Fonksiyonel test                                     |
|                                    | ATE_IND.2 Bağımsız test – örnek                                |
| AVA Sınıfı: Açıklık                | AVA_MSU.1 Kötüye kullanımın incelenmesi                        |

|                                            |                                                                            |
|--------------------------------------------|----------------------------------------------------------------------------|
| değerlendirmesi                            | AVA_SOF.1 TOE güvenlik fonksiyonu gücü değerlendirilmesi                   |
|                                            | AVA_VLA.3 Orta derecede atak potansiyeline karşı açıklık değerlendirilmesi |
| AMA Sınıf: Garantinin devamının sağlanması | AMA_AMP.1 Garantinin sürdürülmesi planı                                    |
|                                            | AMA_CAT.1 TOE bileşen sınıflandırma raporu                                 |

TOE'nin güvenlik yönetim gereksinimleri;

Yönetim gereksinimleri belirlenirken bölüm 5.3.3.1.7 risk yönetimi sonuçları dikkate alınmalıdır. Bu sonuçlara göre belirlenen yönetim gereksinimleri aşağıda sıralanmıştır.

| Yönetim Gereksinimi | Açıklaması                                                | Karşıladığı Güvenlik Amacı               |
|---------------------|-----------------------------------------------------------|------------------------------------------|
| MSP_ISP.1           | Bilgi Güvenliği Politikası Dokümanı                       | <b>O.GÜVENLİK POLİTİKASI</b>             |
| MSP_ISP.2           | İnceleme ve Değerlendirme                                 | <b>O.GÜVENLİK POLİTİKASI</b>             |
| MSO_ISI.1           | Bilgi Güvenliği Forumunun Yönetimi                        | <b>O.GÜVENLİK POLİTİKASI</b>             |
| MSO_ISI.2           | Bilgi Güvenliği Koordinasyonu                             | <b>O.YÖNETİM</b>                         |
| MSO_ISI.3           | Bilgi Güvenliği Sorumluluklarının Paylaşımı               | <b>O.GÜVENLİK POLİTİKASI</b>             |
| MSO_STA.1           | Üçüncü Parti Erişimden Kaynaklanan Risklerin Belirlenmesi | <b>O.ERİŞİM-TOE</b>                      |
| MAC_IFC.1           | Sınıflandırma Kılavuzu                                    | Bilgi sınıflandırılması prosedürü hazır. |
| MAC_IFC.2           | Bilgi Sınıflandırma ve Saklama                            | Bilgi sınıflandırılması prosedürü hazır. |
| MPS_JDR.1           | Güvenliğin İş                                             | <b>O.SORUMLULUK-</b>                     |

|           |                                              |                                                 |
|-----------|----------------------------------------------|-------------------------------------------------|
|           | Sorumluluklarına<br>Eklenmesi                | <b>TOE</b>                                      |
| MPS_JDR.2 | Personel Takibi ve<br>Politikalar            | <b>O.SORUMLULUK-<br/>TOE</b>                    |
| MPS_JDR.3 | Gizlilik Anlaşması                           | <b>O.SORUMLULUK-<br/>TOE</b>                    |
| MPS_UTR.1 | Bilgi Güvenliği Eğitimi ve<br>Alıştırmaları  | <b>O.ÇALIŞTIRMA</b>                             |
| MPS_SIM.1 | Güvenlik Olaylarının<br>Raporlanması         | <b>O.BELİRLEME-<br/>SİSTEM<br/>O.GÖZLEM-TOE</b> |
| MPS_SIM.5 | Disiplin Süreci                              | <b>O.SORUMLULUK-<br/>TOE</b>                    |
| MPE_SER.1 | Fiziksel Güvenlik Çevresi                    | <b>O.FİZİKSEL</b>                               |
| MPE_SER.2 | Fiziksel Giriş Kontrolleri                   | <b>O.FİZİKSEL</b>                               |
| MPE_EQS.2 | Güç Kaynakları                               | <b>O.FİZİKSEL<br/>O.TEMİZ ORTAM</b>             |
| MPE_EQS.3 | Kablolama Güvenliği                          | <b>O.FİZİKSEL</b>                               |
| MCO_PMS.1 | Kötü Niyetli Yazılımlara<br>Karşı Kontroller | <b>O.VİRÜS KORUMA</b>                           |
| MCO_HSP.1 | Bilgi Yedeklemesi                            | <b>O.ESKİ DURUMA<br/>DÖNDÜRME-TOE</b>           |
| MCO_HSP.2 | Operatör Logları                             | <b>O.YÖNETİM</b>                                |
| MCO_EIS.4 | Elektronik Postaların<br>Güvenliği           | <b>O.DİNLEMEME</b>                              |
| MCO_EIS.6 | Herkese Açık Sistemler                       | <b>O.DEVRE DIŞI<br/>BIRAKMA-TOE</b>             |
| MAC_BAC.1 | Erişim Kontrolü<br>Politikaları              | <b>O.ERİŞİM-TOE</b>                             |
| MAC_UAM.1 | Kullanıcı Kaydı                              | <b>O.ERİŞİM-TOE</b>                             |
| MAC_UAM.2 | Ayrıcalıkların Yönetimi                      | <b>O.ERİŞİM-TOE</b>                             |
| MAC_UAM.3 | Kullanıcı Şifre Yönetimi                     | <b>O.ERİŞİM-TOE</b>                             |
| MAC_UAM.4 | Kullanıcı Erişim                             | <b>O.ERİŞİM-TOE</b>                             |

|           |                                                      |                               |
|-----------|------------------------------------------------------|-------------------------------|
|           | Haklarının İncelenmesi                               |                               |
| MAC_MAU.1 | Olay Logları                                         | <b>O.GÖZLEM-TOE</b>           |
| MAC_MAU.2 | Sistem Kullanımının İzlenmesi                        | <b>O.GÖZLEM-TOE</b>           |
| MDM_RQS.1 | Güvenlik Gereksinimlerinin Analizi ve Spesifikasyonu | <b>O.UYGUN DİKKAT</b>         |
| MDM_CRP.3 | Dijital İmzalar                                      | <b>O.DİNLEMEME</b>            |
| MDM_CRP.4 | Kaynağın İnkarnı Engelleyen Servisler                | <b>O.DİNLEMEME</b>            |
| MBC_BCN.1 | İş Devamlılığı Yönetimi Süreci                       | <b>O.ESKİ DURUMA DÖNDÜRME</b> |
| MCP_LRQ.1 | Uygulanabilir Yasaların Tespit Edilmesi              | <b>O.UYUM</b>                 |
| MCP_LRQ.3 | Organizasyon Kayıtlarının Korunması                  | <b>O.UYUM</b>                 |
| MCP_LRQ.4 | Kişisel Bilgilerin Gizliliği ve Veri Korunması       | <b>O.UYUM</b>                 |
| MCP_RPT.1 | Güvenlik Politikasına Uyumluluk                      | <b>O.BİLGİ GÜVENLİĞİ</b>      |

#### 5.3.3.2.4 Gereksinimlere Karşı Tedbirler

##### Güvenlik Fonksiyonları;

Tespit edilen güvenlik fonksiyonlarının sağlanması için ilk olarak sistemde kurulu olan Windows NT 4.0 Server'ın ayarları sıkılaştırılmalı ve son yamaları yapılmalıdır. Bunun dışında erişim kontrolü kullanılacak yazılımlarla sağlanmalı ve sisteme saldırı tespit sistemi kurulmalıdır. Virüs tehditleri için anti virüs yazılımı ve içerik güvenliği yazılımları kullanılmalıdır. Ayrıca yedekleme sistemi kurulmalı ve periyodik olarak sistemin yedeği alınarak hata anında geri getirme sağlanmalıdır. Hattın içeriden dinlenmesi tehdidine karşı hublar switchlerle değiştirilmelidir. İşletim sisteminin ürettiği denetim kayıtları kullanılmalıdır.[Ramachandran, 2002]

Gereken yazılım ve donanımlar mümkünse Ortak Kriterler sertifikalı ürünlerden seçilmelidir. Eğer alınacak COTS ürünleri sertifikalı değilse bölüm 2.5’de incelenen V-RATE değerlendirme metodu ürünlere uygulanmalıdır.

### **Garanti gereksinimleri;**

Özel sistemlerin içermesi gereken garanti gereksinimleri A şirketinin BT sistemi için sağlanmalı ve değerlendirme için hazır hale getirilmelidir. Bu gereksinimlerin karşılanması için;

1. Konfigürasyon Yönetimi; Sistem bileşenlerinin konfigürasyon yönetimi gerçekleştirilmelidir.
2. Teslim ve Çalıştırma; Satın alınan ürünlerin teslim alınması ve çalıştırılması için varsa prosedürler elde edilmeli ve satın alımların bu prosedürlere uygun gerçekleştirilmesi sağlanmalıdır.
3. Geliştirme; Sistemin geliştirme dokümanları hazırlanmalıdır.
4. Kılavuz Belgeler; Sistem için kullanıcı ve yönetici kılavuzu hazırlanmalıdır.
5. Yaşam Döngüsü Desteği; Sistemin yaşam döngüsü tanımlanmalıdır.
6. Testler; Sistemin güvenlik gereksinimlerini karşılayıp karşılamadığı tespit edilmelidir.
7. Açıklık Değerlendirmesi; Sisteme bilinen açıklıklara karşı ataklar düzenlenmeli ve açıklık analizi gerçekleştirilmelidir.
8. Garantinin Devamının Sağlanması; Sistemin sağladığı garantinin devamının nasıl sağlanacağı konusunda bir plan ortaya koyulmalıdır.

### **Yönetim gereksinimleri;**

Risk yönetimi sonucu tespit edilen yönetim gereksinimlerinin karşılanması için aşağıdaki adımlar ISO 17799’a uygun olarak gerçekleştirilmelidir.

1. Bilgi güvenliği politikası düzeltilmeli ve ISO 17799’a tam uygun hale getirilmelidir.
2. Bilgi güvenliği yönetim sistemi oluşturulmalıdır.

3. Bilgi sınıflandırma kılavuzu oluşturulmalıdır.
4. Üçüncü parti erişimlerden kaynaklanan risklerin tespit edilmesi konusunda bir prosedür oluşturulmalıdır.
5. Çalışanlar bilgi güvenliği konusunda eğitilmelidir.
6. Çalışanlar işe alınırken gizlilik anlaşması imzalamalı ve aykırı davranışları durumunda gerçekleştirilecek disiplin süreci konusunda bilgilendirilmelidir.
7. Fiziksel güvenlik kontrolü prosedürleri oluşturulmalıdır.
8. Kablolama güvenliğine dikkat edilmeli, güç kaynakları kontrol edilmeli ve sistem kaynakları bir sistem odasında toplanmalıdır.
9. Kötü niyetli virüs, Trojan benzeri yazılımlar konusunda çalışanlar bilgilendirilmeli ve kontroller yapılmalıdır.
10. Sistem işletimi prosedürü çıkartılmalıdır.
11. Sistemin yedeklenmesi için prosedürler yazılmalı ve periyodik yedekleme sağlanmalıdır.
12. Erişim kontrolü prosedürleri oluşturulmalıdır.
13. Sistem yöneticileri olay loglarını kontrol etmeli ve raporlamalıdır.
14. İş devamlılığı yönetim süreci oluşturulmalıdır.
15. Uyulması gereken yasal zorunluluklar tespit edilmeli ve bu yasalara uygunluk gerçekleştirilmelidir.

### 5.3.4 Uygulamanın Sonuçları

Örnek olarak verilen A şirketinin BT sistemine önerilen sistem değerlendirme metodolojisinin uygulanması ile sistem sertifikalandırılmaya hazır hale getirilmiş ve eksikleri kapatılmıştır. İlk olarak risk değerlendirmesi gerçekleştirilmiş ve sistemin varlıkları, bu varlıklara gerçekleştirilebilecek tehditler ortaya çıkartılmıştır. Risk değerlendirmesi sonucunda risk yönetimi gerçekleştirilmiş ve sistemin güvenlik amaçları ortaya çıkartılmıştır. Bu güvenlik amaçları metodolojide de önerildi gibi güvenlik gereksinimleri ile karşılanmıştır. Güvenlik gereksinimleri ilk olarak güvenlik gereksinimleri için çıkartılmış ve sisteme eklenmesi gereken güvenlik fonksiyonları tespit edilmiştir. Ayrıca sistemin taşımakta olduğu bilgi sınıfına göre sağlaması gereken garanti paketleri belirtilmiş ve bu paketlerin sistemde nasıl

karşılanacağı belirtilmiştir. Son olarak sistemin başlangıçta varolan fakat eksik veya yetersiz olan yönetim gereksinimleri güncellenmiş, güvenlik amaçlarına uygun olarak yeni yönetim gereksinimleri oluşturulmuştur. Bu yönetim gereksinimleri ISO 17799'a uygun olarak karşılanması halinde karşılık geldikleri güvenlik amaçlarını karşılayacaklardır.

A şirketi için önerilen fonksiyonel, garanti ve güvenlik gereksinimleri sistemde uygulandığında ve risk değerlendirmesi tekrarlandığında **Çizelge 5.6**'daki değerler ortaya çıkmıştır.

Çizelge 5.6 Metodoloji uygulandıktan sonra gerçekleştirilen risk değerlendirmesi

| Tehdit                                                               | Tehditin Olma İhtimali | Tehditin Mutlak Etkisi | Mutlak Risk | Etkilediği varlık (lar)ın puanı | Gerçek risk değeri (Taban Risk) |
|----------------------------------------------------------------------|------------------------|------------------------|-------------|---------------------------------|---------------------------------|
| Kasıtlı ya da kasıtsız yapılan illegal kullanıcı aktiviteleri        | 2                      | 4                      | 8           | 3                               | 24                              |
| Kullanıcıların ihtiyacından çok erişime sahip olması                 | 1                      | 3                      | 3           | 3                               | 9                               |
| İnternet'ten yapılan hacker saldırıları                              | 1                      | 5                      | 5           | 5                               | 25                              |
| Virüsler                                                             | 2                      | 5                      | 10          | 4                               | 40                              |
| İnternet'ten yapılan hacker saldırılarından erken haberdar olamamak  | 1                      | 4                      | 4           | 5                               | 20                              |
| Toz, nem güneş ışığı gibi çevresel faktörler                         | 1                      | 2                      | 2           | 5                               | 10                              |
| Bilgisayarlara yetkisiz erişim                                       | 1                      | 4                      | 4           | 5                               | 20                              |
| Sistemlerin çok yavaş çalışması, hata vererek çalışmasının durması   | 2                      | 4                      | 8           | 4                               | 32                              |
| Dinleme ( <b>sniffing</b> ) yapılması                                | 1                      | 5                      | 5           | 3                               | 15                              |
| Sistemin sürekliliğinin kaybolması                                   | 1                      | 4                      | 4           | 4                               | 16                              |
| Sistem hatalarından ya da elektrik kesintisi gibi çevre etkilerinden | 1                      | 4                      | 4           | 5                               | 20                              |

|                                                                        |   |   |   |   |    |
|------------------------------------------------------------------------|---|---|---|---|----|
| dolayı verinin kaybı                                                   |   |   |   |   |    |
| Kullanıcı verilerinin başkaları tarafından okunması                    | 1 | 4 | 4 | 4 | 16 |
| Sistemde bilgi güvenliği için bir politikanın olmaması                 | 1 | 4 | 4 | 5 | 20 |
| İnternet kullanım politikasında yazılmamış olan kullanıcı aktiviteleri | 1 | 3 | 3 | 3 | 9  |
| Güvenlik olaylarının takip edilmemesi, tepki verilememesi              | 1 | 4 | 4 | 4 | 16 |
| Yetkisiz erişimler                                                     | 1 | 4 | 4 | 4 | 16 |
| Fiziksel güvenlik ihlalleri                                            | 1 | 3 | 3 | 4 | 12 |
| Yedekleme yapılamaması                                                 | 1 | 4 | 4 | 5 | 20 |
| Virüs tanımlarının güncel olmaması                                     | 1 | 4 | 4 | 4 | 16 |
| Sistemde olabilecek bir arızanın uzun süre giderilememesi              | 2 | 3 | 6 | 4 | 24 |
| İllegal kullanıcı aktivitesinin sorumlusunun bulunamaması              | 1 | 3 | 3 | 3 | 9  |

**Çizelge 5.6 Metodoloji uygulandıktan sonra gerçekleştirilen risk değerlendirmesi** incelendiğinde varlıklar için yeni tespit edilen risk değerlerinin kabul edilen risk değerlerine eşit veya altında olacağı görülmüştür.

### 5.3.5 Koruma Profili Kullanımı

Uygulama sonuçları Ortak Kriterler ve ISO 17799 standartlarının bir organizasyonun ağ yapısında ve bu yapının işletiminde kullanılması ile riskin büyük ölçüde azaltıldığını göstermektedir. Fakat bu standartların uygulanmasının zaman ve para olarak maliyetinin yüksek olması özellikle küçük ölçekli organizasyonlarda kullanımını zorlaştırmaktadır. Bu organizasyonlar için Ortak Kriterler’de tanımlanan Koruma Profillerinin kullanılması faydalı olacaktır. Standartta göre Koruma Profili müşteriler veya belli bir ürün/sistem çeşidinde bir standardı ortaya koymak isteyenler, yazarlar ve PP aracılığıyla almak istedikleri ürünün güvenlik özelliklerini

ve güvenlik garanti düzeyini belirlerler. Yapı olarak Güvenlik Hedefi'ne çok benzemekte olan Koruma Profilleri'nin en önemli farkı ürün/sistem uygulamasından bağımsız olarak tehditlerin, kabullenmelerin tanımlanması ve yalnızca bunlara göre gereksinimlerin tespit edilmesini içermektedir. [ISO 15408, 1999]

Ağ sistemleri için belirli bir uygulamadan bağımsız olarak hazırlanacak Koruma Profillerini şirketlerin kendi ağlarına uygun ürün ve tedbirlerle uygulaması değerlendirme ve hazırlık sürecini hızlandıracak ve maliyetleri düşürecektir. [Kekicheff, 2000]

## 6 SONUÇLAR VE ÖNERİLER

Organizasyonların kullandıkları bilgi sistemleri korumakta olan varlıkların değerleri sürekli olarak artmaktadır. Bunun yanı sıra bu sistemlere gerçekleştirilen saldırıların sayıları da artmakta ve saldırılarda kullanılan tekniklerde gelişmektedir. Organizasyonlar kullandıkları BT sistemlerinin sağladığı garantinin bağımsız kuruluşlar tarafından nitelik olarak ölçülmesine ve varolan risklerin azaltılmasına ihtiyaç duymaktadırlar.

Ortak Kriterler standardı BT ürünlerinin güvenlik değerlendirmesinde kullanılmakta ve üreticilerin iddialarının doğrulanarak müşteriye ihtiyacı olan garantiyi sağlamaktadır. Fakat Ortak Kriterler BT sistemlerinin değerlendirilmesinde yetersiz kalmaktadır. Çünkü sistem değerlendirmelerinde standardın tanımladığı fonksiyonel güvenlik gereksinimleri ve garanti güvenlik gereksinimlerinin yanı sıra sistemlerin kullanım ortamlarında yönetimden kaynaklanan açıklıklara karşı yönetim güvenlik gereksinimleri de tanımlanmalıdır. Ayrıca standardın BT ürünleri için hazırlamış olduğu garanti seviyesi paketleri de sistemler için yetersiz kalmakta sistemlerin taşıdıkları varlıkların güvenlik sınıflarına uygun olarak yeni tanımlanmış garanti paketlerine ihtiyacı ortaya çıkmaktadır. Bu ihtiyaçların yanı sıra sistemlerin güvenlik değerlendirmeleri sırasında BT ürünlerinden farklı olarak COTS ürünlerinin değerlendirilmesinde çeşitli zorluklar yaşanmakta ve sistemlerin sağladığı garantinin sürekli değişen koşullarda devamının denetlenmesi gerekmektedir.

Bu çalışmada ilk olarak sistem değerlendirmelerinde ihtiyaç duyulan yönetim gereksinimleri ISO 17799 standardından alınan kontrol objeleri ile tanımlanmış ve bu yönetim gereksinimleri kullanılarak BT sistemlerinin Güvenlik Hedef'lerinin nasıl hazırlanacağı tanımlanmıştır. Ayrıca sistemler taşıdıkları varlıkların sınıflarına göre sağlamaları gereken garanti gereksinimleri için paketler önerilmiş ve bu paketlerin sistemlerin değerlendirilmeleri sırasında nasıl sisteme uygulanacağı tanımlanmıştır. Sistem değerlendirme süreci tanımlanmış ve sistemin hazırlanan güvenlik hedefine ve Ortak Kriterler standardına uygun olarak nasıl gerçekleştirileceği incelenmiştir.

Standarda uygun olarak tasarlanmış ve gerçekleşmiş, güvenlik hedefi ve diğer değerlendirme delilleri hazırlanmış sistemlerin değerlendirmesinde ise Ortak Kriterler Değerlendirme Metodolojisinin kullanılması önerilmiştir. Ayrıca sistemdeki COTS ürünlerinin değerlendirme delillerinin oluşturulması için V-RATE yönteminin kullanılması ve test metodları önerilmiştir. Sistemde yönetim gereksinimlerine karşı uygulanmış olan tedbirlerin değerlendirilmesinde ise ISO 17799 standardında tanımlanmış kontrol objelerinin Ortak Kriterler standardındaki gibi sınıf, aile ve bileşen yapısında tanımlanarak değerlendirici eylemlerinin ortaya çıkarılması gerektiği belirtilmiştir.

Değerlendirmelerin ardından BT sisteminin sağladığı garantinin sürekli değişen ortamda devamının garanti edilmesi için bir akreditasyon yapısının kurulması ve sistemlerin garanti paketleri içerisinde bulunan AMA sınıfı bileşenlerinin denetimini sağlamaları önerilmiştir. Bu yapı için Almanya’da akıllı kart sistemleri için aynı görevi gerçekleştirmekte olan ZKA model olarak önerilmiştir.

Bu çalışmada BT sistemlerinin değerlendirilmesi için Ortak Kriterler standardı kullanılmış fakat standardın sistem değerlendirmeleri için yetersiz olduğu konularda çözümler önerilmiştir. Bu çalışmada önerilen yöntemin sistemlere uygulanması ve bağımsız bir kuruluş tarafından bu sistemin değerlendirilmesi ile değerlendirilen BT sisteminin güvenliğinin garantisi doğrulanmıştır.

Önerilen metodoloji örnek bir BT sistemi üzerinde uygulanmıştır. Uygulama sonucunda organizasyonun BT sistemindeki eksikler tespit edilmiş ve Güvenlik Hedefi tutarlı ve anlaşılabilir bir şekilde oluşturulmuştur. Güvenlik Hedefi’nde belirlenen güvenlik gereksinimlerini karşılayacak amaçların sağlanması için oluşturulacak karşı tedbirler çıkartılmış ve sistem Ortak Kriterler standardı sertifikasyonuna hazır hale getirilmiştir.

Bu çalışmada tam olarak gerçekleştirilmemiş olan ISO 17799 standardı kontrol objelerinin Ortak Kriterler’deki sınıf, aile ve bileşen yapısına çevrilmesi ve bu bileşenlerin değerlendirilmesi için gereken bütün değerlendirici eylemlerinin tanımlanması ileride gerçekleştirilmesi gereken konulardan biridir. Ayrıca sistemler

için önerilmiş bu yöntemin dört farklı sistem için uygulanması gerekmekte ve bu yöntemin zaman ve maliyet analizlerinin gerçekleştirilmesi gerekmektedir. Çünkü varolan yapısıyla Ortak Kriterler Değerlendirme Metodolojisi ürün değerlendirmelerinde dört ay ıla 12 ay arasında zaman almakta ve yüksek maliyetlerde sonuçlanabilmektedir. Ürün değerlendirmelerine birde sistemler için önerilmiş olan çözümler eklendiğinde zaman ve maliyet çok yükselecektir. Değerlendirmelerin verimli olabilmesi için bu konunun analizi gerçekleştirilmelidir.

## KAYNAKLAR

- A.J Apted, M. Carthigaser, C. Lowe, 2002, “Common Problems with Common Criteria”, 3.International Common Criteria Conference, Canada
- B. Karabacak, 2003, “Bilgi Güvenliği Risk Analizi Yöntemi”, Gebze Yüksek Teknoloji Enstitüsü Yüksek Lisans Tezi
- B. Karabacak, 2002, “Bilgi ve İletişim Teknolojilerinde Risk Analizi ve Yönetimi”, Gebze Yüksek Teknoloji Enstitüsü Seminer Çalışması
- B. Schneier, 2000, “Secret and Lies”, Wiley Computer Publishing
- Common Evaluation Methodology v2.1, August 1999
- D.J. Reifer, B.W. Boehm, Gangadharan M., 2003, “Estimating Cost of Security for COTS Software”, Springer-Verlag Berlin Heidelberg pp. 178-186
- Dr. R. Ross, 2002, “Building More Secure Systems for the Critical Infrastructure”, 3.International Common Criteria Conference, Canada
- D. Trcek, 2003, “An integral framework for information security management systems”, Computers&Security vol. 22 no.4 pp. 337-360
- E. von Faber, 1999, “Security Evaluation Schemas for the Public and Private Market with a Focus on Smart Card Systems”, Springer-Verlag Berlin Heidelberg pp.187-203
- H. F. Lipson, N.R. Mead, A.P. Moore, 2002, “Can We Ever Build Survivable Systems From COTS Components”, Springer-Verlag Berlin Heidelberg, CAISE 2 pp. 216-229
- H. Tabuchi, 2002, “Guideline for System Evaluation”, 3.International Common Criteria Conference, Canada
- Information security management systems – Specfication with guidance for use, BS 7799-2, 2002
- Information Technology – Code of Practice for information security management, ISO 17799, November 2002
- Information Technology – Security Techniques- Security Evaluation Criteria for IT Security, ISO 15408, Part 1,2 and 3, v .1, August 1999
- J. Cugini, 1995, “The Common Criteria: On the road to international harmonization”, Computer Standards & Interfaces vol. 17 pp. 315-320
- J. Ramachandran, 2002, “Designing Security Architecture Solutions”, Wiley

Computer Publishing

K. Buzzard, 2003, “ “Adequate” Security – What exactly do you mean?”, Computer Law&Security Report vol. 19 no. 5 pp. 406-410

K. G. Olthoff, 2000, “Thoughts and Questions on Common Criteria Evaluations”, 23rd National Information Systems Security Conference

K. Höne, J. H. P. Eloff, 2002, “Information Security Policy – What do international information security standards say?”, Elsevier Science, pp. 402-409

K. Vedder, 1998, “International Standardisation of IT Security”, Springer-Verlag Berlin Heidelberg pp. 353-365

M. Donaldson, 2002, “Evaluation of IT Security Products and Systems”, 3.International Common Criteria Conference, Canada

M. Kekicheff, F. Kashef, and D. Brewer, 2000, “The Open Platform Protection Profile taking the Common Criteria to the outer limits”, 23rd National Information Systems Security Conference

M. M. Eloff, S.H. von Solms, 2000, “Information Security Management: An Approach to Combine Process Certification and Product Evaluation”, Computer&Security 19 pp. 698-709

S. Kondakçı, 2003, “National E-Business Trust Infrastructure Evaluation Scheme”, Netsekuritas

T. Rottke, D. Hatebur, M. Heisel, M. Heiner, 2002, “A Problem Oriented Approach to Common Criteria Certification”, Springer-Verlag Berlin Heidelberg, SAFECOMP pp. 334-246

W. List, 1997, “The Common Criteria – Good, Bad or Indifferent?”, Information Security Technical Report, 1997, Vol. 2 No.1 pp. 19-23

W. Shi, Y. Sun, 2001, “An Investigation of CC’s Contribution to Confidence in Security”, IEEE pp. 333-338

## ÖZGEÇMİŞ

Mehmet Çakır, 16 Şubat 1981 tarihinde Samsun’da doğdu. İlk, orta ve lise eğitimini Samsun’da tamamladı. Bilkent Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği bölümünden 2001 senesinde mezun oldu. 2001 senesi ağustos ayından itibaren TÜBİTAK Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü’nde araştırmacı olarak görev yapmaktadır.

## EKLER

### Ek-1: Tanımlar

**Varlıklar** – Bir TOE'nin karşı önlemleri tarafından korunacak bilgi ya da kaynaklar.

**Garanti** – Bir ürünün güvenlik hedeflerine ulaştığına dair güven veren nedenler.

**Saldırı potansiyeli** – Bir saldırı olması durumunda, saldırının, saldırganın becerisi, kaynakları, ve amacı göz önüne alınarak hesaplanan başarı potansiyeli.

**Kimlik doğrulama verisi** – Bir kullanıcının iddia ettiği kimliği doğrulamak için kullanılan bilgi.

**Sınıf** – Aynı konuda yoğunlaşmış ailelerden oluşan grup.

**Bileşen** – Bir PP, ST ya da paket içinde yer alabilecek en küçük seçilebilir öğeler kümesi.

**Bağımlılık** – Gereksinimler arasında, diğer gereksinimlerin hedeflerine ulaşabilmesi için bağımlı olunan gerekliliğin normal bir şekilde yerine getirilmesinin gerektiği bir ilişki.

**Öge** – Bölünemeyen bir güvenlik gereksinimi.

**Değerlendirme** – Bir PP, ST ya da TOE'nin tanımlanmış kriterlere göre değerlendirilmesi.

**Değerlendirme Garanti Düzeyi (EAL)** – Ortak Kriterler'in önceden tanımlanmış garanti ölçeğinde bir noktayı temsil eden 3. bölümdeki garanti öğelerinden oluşan bir paket.

**Değerlendirme Makamı** – Bir değerlendirme programı yoluyla Ortak Kriterler'i belli bir topluluk için uygulayan ve böylece standartları belirleyen ve o topluluktaki grupların gerçekleştirdiği değerlendirmelerin kalitesini kontrol eden grup.

**Aile** – Güvenlik hedeflerini paylaşan ama vurgu ya da duyarlılık bakımından farklı olabilen bir grup öge.

**Biçimsel** – Yerleşik matematiksel kavramlara dayalı olarak tanımlanmış anlamlarla sınırlı bir sözdizimine sahip bir dilde ifade edilen.

**Kimlik** – Yetkilendirilmiş bir kullanıcıyı benzersiz bir şekilde ayırt eden bir gösterim (örneğin bir dizgi) ki bu, o kullanıcının tam ya da kısaltılmış adı ya da takma adı olabilir.

**Biçimsel Olmayan** – Doğal dilde ifade edilen.

**Kurumsal Güvenlik Politikaları** – Bir Kuruluş Tarafından Kendi Çalışmalarında Uygulanan bir ya da daha fazla güvenlik kuralı, yordamı, uygulaması ya da yönergesi.

**Paket** – Belirlenmiş bir dizi güvenlik hedefine ulaşmak için bir araya getirilmiş yeniden kullanılabilir fonksiyonel bileşimler ya da garanti bileşenleri (örneğin bir EAL).

**Ürün** – Birçok sistemde kullanılmak ya da sistemin içine yerleştirilmek üzere tasarlanmış bir fonksiyonellik sunan bir BT yazılımı, bellenimi ve/veya donanımı paketi.

**Koruma Profili (PP)** – Belli müşteri ihtiyaçlarını karşılayan bir TOE kategorisi için uygulamadan bağımsız bir dizi güvenlik gerekliliği.

**Rol** – Kullanıcı ile TOE arasında izin verilen etkileşimleri oluşturan önceden belirlenmiş kurallar.

**Güvenlik Fonksiyonu (SF)** – TSP'nin yakından bağlantılı bir kurallar alt kümesini uygulamak için güvenilmesi gereken TOE'nin bir bölümü ya da bölümleri.

**Güvenlik Fonksiyonu Politikası (SFP)** - SF tarafından uygulanan güvenlik politikası.

**Güvenlik Amacı** – Belirlenmiş tehditlere karşı koymak ve/veya belirlenmiş örgüt güvenlik politikaları ve varsayımlarını uygulamak için bir amaç beyanı.

**Güvenlik Hedefi (ST)** – Belirlenmiş bir TOE'nin değerlendirilmesinde temel alınacak bir dizi güvenlik gereği ve özelliği.

**Yarı Biçimsel** – Ölçülü sözdizimine sahip bir dilde tanımlanmış anlamlarla ifade edilen.

**Fonksiyon Gücü (SOF)** – Beklenen güvenlik davranışını, temelinde yatan güvenlik mekanizmalarına doğrudan saldırarak alt etmek için gereken en az çabayı ifade eden bir TOE güvenlik fonksiyonunun niteliği.

**SOF-Temel** – İnceleme sonucunda, fonksiyonun, düşük saldırı potansiyeline sahip saldırganlar tarafından TOE güvenliğinde şansa oluşturulan ihlallere karşı yeterli koruma sağladığını gösterdiği bir TOE gücü düzeyi.

**SOF-Orta** – İnceleme sonucunda, fonksiyonun, ortalama saldırı potansiyeline sahip saldırganlar tarafından TOE güvenliğinde doğrudan ve kasıtlı ihlallere karşı yeterli koruma sağladığını gösterdiği bir TOE gücü düzeyi.

**SOF-Yüksek** – İnceleme sonucunda, fonksiyonun, yüksek saldırı potansiyeline

sahip saldırganlar tarafından TOE güvenliğinde planlı ve organize ihlallere karşı yeterli koruma sağladığını gösterdiği bir TOE gücü düzeyi.

**Özne** – TSC içinde işlemlerin gerçekleştirilmesine neden olan bir varlık.

**Sistem (Dizge)** – Belli bir amaca ve çalışma ortamına sahip özel bir BT kurulumu.

**Değerlendirme Hedefi (TOE)** – Bir değerlendirmeye konu olan bir BT ürünü ya da sistemi ve bununla ilgili yönetici ve kullanıcı kılavuzu belgeleri.

**TOE Güvenlik Fonksiyonları (TSF)** – TSP'nin doğru bir şekilde uygulanmasında güvenilmesi gereken TOE'nin bütün donanım, yazılım ve belleniminden oluşan bir küme.

**TOE Güvenlik Fonksiyonları Arayüzü (TSFI)** – TSF'nin aracılık ettiği ya da TSF'den bilgi edinildiği, TOE kaynaklarına erişimi sağlayan etkileşimli (insan-makine arayüzü) ya da programlı (uygulama programlama arayüzü) bir dizi arayüz.

**TOE Güvenlik Politikası (TSP)** – Bir TOE'nin kapsamı içinde varlıkların yönetilmesini, korunmasını ve dağıtılmasını düzenleyen kurallar.

**TOE Güvenlik Politikası Modeli** – TOE tarafından uygulanacak güvenlik politikasının yapısal bir temsili.

**Kullanıcı** – TOE'nin dışında olan ve TOE ile etkileşime giren herhangi bir varlık (insan kullanıcı ya da dış BT varlığı).