

ZAYIFLIK ÖRNEKLERİ / EXAMPLES OF VULNERABILITIES
(ISO 27005:2011 EK-D)

Tehdit Türü / Type	Zayıflık Örnekleri / Examples of vulnerabilities	Tehdit Örnekleri / Examples of threats
Donanım / Hardware	Yetersiz Bakım / Depolama ortamının hatalı kurulumu / <i>Insufficient maintenance / faulty installation of storage media</i>	Bilgi Sistemi Sürdürülebilirliğinin ihlali / <i>Breach of information system maintainability</i>
	Periyodik Yedek planının olmayışı / <i>Lack of periodic replacement schemes</i>	Ekipman veya Medyanın İhması / <i>Destruction of equipment or media</i>
	Nem, Toz, Kirlenmeye duyarlılık / <i>Susceptibility to humidity, dust, soiling</i>	Toz, Korozyon, Donma / <i>Dust, corrosion, freezing</i>
	Elektromanyetik Radyasyona Duyarlılık / <i>Sensitivity to electromagnetic radiation</i>	Elektromanyetik Radyasyon / <i>Electromagnetic Radiation</i>
	Etkin Değişim kontrol yönetiminin olmayışı / <i>Lack of efficient configuration change control</i>	Kullanım hatası / <i>Error in Use</i>
	Gerilim değişikliklerine duyarlılık / <i>Susceptibility to voltage variations</i>	Elektrik Kesintisi / <i>Loss of Power supply</i>
	Sıcaklık değişimlerine duyarlılık / <i>Susceptibility to temperature variations</i>	Metorolojik Olaylar / <i>Meteorological phenomenon</i>
	Korumasız Depolama / <i>Unprotected storage</i>	Medya veya Dokümanların Çalınması / <i>Theft of media or documents</i>
	Lack of care at disposal	Medya veya Dokümanların Çalınması / <i>Theft of media or documents</i>
	Kontrolsüz Kopyalama / <i>Uncontrolled copying</i>	Medya veya Dokümanların Çalınması / <i>Theft of media or documents</i>
Yazılım / Software	Eksik yada yapılmamış Yazılım testleri / <i>No or insufficient software testing</i>	Yetki Suistimali / <i>Abuse of rights</i>
	Yazılımdaki bilindik kusurlar / <i>Well-known flaws in the software</i>	Yetki Suistimali / <i>Abuse of rights</i>
	No 'logout' when leaving the workstation	Yetki Suistimali / <i>Abuse of rights</i>
	Uygun silme işlemi gerçekleştirilmemiş depolama ortamının, envanterden kaldırılması ya da yeniden kullanımı / <i>Disposal or reuse of storage media without proper erasure</i>	Yetki Suistimali / <i>Abuse of rights</i>
	Denetim kayıtlarının eksikliği / <i>Lack of audit trail</i>	Yetki Suistimali / <i>Abuse of rights</i>
	Erişim haklarının yanlış tahsisi / <i>Wrong allocation of access rights</i>	Yetki Suistimali / <i>Abuse of rights</i>
	Yaygın dağıtım yazılım / <i>Widely-distributed software</i>	Datanın bozulması / <i>Corruption of data</i>
	Applying application programs to the wrong data in terms of time	Datanın bozulması / <i>Corruption of data</i>
	Karmaşık kullanıcı arayüzü / <i>Complicated user interface</i>	Kullanım hatası / <i>Error in Use</i>
	Dokümantasyon eksikliği / <i>Lack of documentation</i>	Kullanım hatası / <i>Error in Use</i>
	Yanlış parametre kurulumu / <i>Incorrect parameter Setup</i>	Kullanım hatası / <i>Error in Use</i>
	Yanlış Tarihler / <i>Incorrect Dates</i>	Kullanım hatası / <i>Error in Use</i>
	Kullanıcı kimlik doğrulaması gibi tanımlama ve kimlik doğrulama mekanizmasının eksikliği / <i>Lack of identification and authentication mechanisms like user authentication</i>	Yetkide zorlama / <i>Forging of rights</i>
	Korumasız şifre tabloları / <i>Unprotect password tables</i>	Yetkide zorlama / <i>Forging of rights</i>
	Zayıf şifre yönetimi / <i>Poor password management</i>	Yetkide zorlama / <i>Forging of rights</i>
	Gereksiz hizmetlerin etkin olması / <i>Unnecessary services enabled</i>	Bilginin Yasadışı İşlenmesi / <i>Illegal Processing of data</i>
	Olgunlaşmamış veya yeni yazılım / <i>Immature or new software</i>	Yazılım Arızası / <i>Software malfunction</i>
	Geliştiriciler için eksik veya Belirsiz olan özellikler / <i>Unclear or incomplete specifications for developers</i>	Yazılım Arızası / <i>Software malfunction</i>
	Etkin bir değişim kontrolünün olmayışı / <i>Lack of effective change control</i>	Yazılım Arızası / <i>Software malfunction</i>
	Kontrolsüz indilen ve kullanılan yazılım / <i>Uncontrolled downloading and use of software</i>	Yazılımla izinsiz değişiklik / <i>Tampering with software</i>
Yedek kopya eksikliği / <i>Lack of back-up copies</i>	Yazılımla izinsiz değişiklik / <i>Tampering with software</i>	
Bina, kapılar ve pencerelerde fiziksel korumanın eksikliği / <i>Lack of physical protection of the building, doors and windows</i>	Medya veya Dokümanların Çalınması / <i>Theft of media or documents</i>	
Yönetim raporlarını üretmeye başarısızlık / <i>Failure to produce management reports</i>	İzinsiz Ekipman Kullanımı / <i>Unauthorised use of equipment</i>	
Ağ / Network	Mesaj gönderim ve alımlarında kanıt (log) eksikliği / <i>Lack of proof of sending or receiving a message</i>	İşlemleri Engelleme / <i>Denial of actions</i>
	Korumasız iletişim hatları / <i>Unprotected communication lines</i>	Gizli Dinleme / <i>Eavesdropping</i>
	Korumasız hassas trafik / <i>Unprotected sensitive traffic</i>	Gizli Dinleme / <i>Eavesdropping</i>
	Zayıf ortak kablolama (Zayıf kablo bağlantıları) / <i>Poor joint cabling</i>	İletişim ekipmanları arızası / <i>Failure of telecommunication equipment</i>
	Tek noktada arıza / <i>Single point of failure</i>	İletişim ekipmanları arızası / <i>Failure of telecommunication equipment</i>
	Gönderici ve alıcının kimlik bilgisi ve kimlik doğrulamasının eksikliği / <i>Lack of identification and authentication sender and receiver</i>	Yetkide zorlama / <i>Forging of rights</i>
	Güvensiz ağ mimarisi / <i>Insecure network architecture</i>	Uzaktan Casusluk / <i>Remote spying</i>
	Şifrelerin açık transferi / <i>Transfer of passwords in clear</i>	Uzaktan Casusluk / <i>Remote spying</i>
	Yetersiz ağ yönetimi (yönlendirme esnekliği) / <i>Inadequate network management (resilience of routing)</i>	Saturation of the information system
	Korumasız kamu (ziyaretçi) ağ bağlantıları / <i>Unprotected public network connections</i>	İzinsiz Ekipman Kullanımı / <i>Unauthorised use of equipment</i>
Çalışanlar / Personnel	Personelin eksikliği / <i>Absence of personnel</i>	Breach of personnel availability
	Yetersiz istihdam prosedürleri / <i>Inadequate recruitment procedures</i>	Ekipman veya Medyanın İhması / <i>Destruction of equipment or media</i>
	Yetersiz güvenlik eğitimi / <i>Insufficient security training</i>	Kullanım hatası / <i>Error in Use</i>
	Yazılım ve donanımın yanlış kullanımı / <i>Incorrect use of software and hardware</i>	Kullanım hatası / <i>Error in Use</i>
	Güvenlik bilincinin eksikliği / <i>Lack of security awareness</i>	Kullanım hatası / <i>Error in Use</i>
	İzleme mekanizmalarının eksikliği / <i>Lack of monitoring Mechanisms</i>	Bilginin Yasadışı İşlenmesi / <i>Illegal Processing of data</i>
	Temizlik veya dış personelin denetimsiz çalışması / <i>Unsupervised work by outside or cleaning staff</i>	Medya veya Dokümanların Çalınması / <i>Theft of media or documents</i>
	Doğru mesajlaşma ve iletişim medyası kullanımı için politikaların olmayışı / <i>Lack of policies for the correct use of telecommunications media and messaging</i>	İzinsiz Ekipman Kullanımı / <i>Unauthorised use of equipment</i>
Yapı / Site	Fiziksel erişim kontrolünün binalar ve kapılarda yetersiz ve dikkatsiz kullanımı / <i>Inadequate or careless use of physical access control to buildings and rooms</i>	Ekipman veya Medyanın İhması / <i>Destruction of equipment or media</i>
	Lokasyonun sele duyarlı bir alanda olması / <i>Location in an area susceptible to flood</i>	Sel / Flood
	Kararsız Elektrik Şebekesi / <i>Unstable power grid</i>	Elektrik Kesintisi / <i>Loss of Power supply</i>

	Bina, Kapılar ve pencerelerin fiziksel koruma eksikliği / <i>Lack of physical protection of the building, doors and windows</i>	Ekipman çalınması / <i>Theft of equipment</i>
Organizasyon / Organization	Kullanıcı kayıt ve silme işlemleri için resmi bir prosedürün olmayışı / <i>Lack of formal procedure for user registration and de-registration</i>	Yetki Suistimali / <i>Abuse of rights</i>
	Erişim haklarının gözden geçirilmesi için resmi bir prosedürün olmayışı (denetim) / <i>Lack of formal process for access right review (supervision)</i>	Yetki Suistimali / <i>Abuse of rights</i>
	Müşteriler ve/veya üçüncü taraflarla yapılan sözleşmelerde (güvenlikle ilgili) hükümlerin eksikliği / <i>Lack or insufficient provisions (concerning security) in contracts with customers and/or third parties</i>	Yetki Suistimali / <i>Abuse of rights</i>
	Bilgi işleme tesislerinin izlenmesi ile ilgili prosedürlerinin olmayışı / <i>Lack of procedure of monitoring of information processing facilities</i>	Yetki Suistimali / <i>Abuse of rights</i>
	Düzenli denetimlerin eksikliği / <i>Lack of regular audits (supervision)</i>	Yetki Suistimali / <i>Abuse of rights</i>
	Risk tespiti ve değerlendirme prosedürlerinin olmayışı / <i>Lack of procedures of risk identification and assessment</i>	Yetki Suistimali / <i>Abuse of rights</i>
	Yönetici ve operatör loglarında hata kayıtlarının tutulmaması / <i>Lack of fault reports recorded in administrator and operator logs</i>	Yetki Suistimali / <i>Abuse of rights</i>
	Yetersiz servis bakım yanıtı / <i>Inadequate service maintenance response</i>	Bilgi Sistemi Sürdürülebilirliğinin ihlali / <i>Breach of information system maintainability</i>
	Yetersiz Hizmet Seviyesi Anlaşması / <i>Lack of insufficient Service Level Agreement</i>	Bilgi Sistemi Sürdürülebilirliğinin ihlali / <i>Breach of information system maintainability</i>
	Değişim Kontrol Prosedürünün eksikliği / <i>Lack of Change Control Procedure</i>	Bilgi Sistemi Sürdürülebilirliğinin ihlali / <i>Breach of information system maintainability</i>
	BGYS dokümantasyon kontrolü için resmi bir prosedürün olmayışı / <i>Lack of formal procedure for ISMS documentation Control</i>	Datanın bozulması / <i>Corruption of data</i>
	BGYS kayıtlarının denetimi için resmi bir prosedürün olmayışı / <i>Lack of formal procedure for ISMS record supervision</i>	Datanın bozulması / <i>Corruption of data</i>
	Kamuya açık bilgilerin erişimi için resmi bir sürecin olmayışı / <i>Lack of formal process for authorization of public available information</i>	Güvenilmeyen Kaynaklardan gelen veri / <i>Data from untrustworthy sources</i>
	Bilgi Güvenliği sorumluluklarının tahsisinde eksiklik / <i>Lack of proper allocation of information security responsibilities</i>	İşlemleri Engelleme / <i>Denial of actions</i>
	Süreklilik Planlarının eksikliği / <i>Lack of continuity plans</i>	Ekipman Hatası / <i>Equipment failure</i>
	E-Mail Kullanım politikasının olmayışı / <i>Lack of e-mail usage policy</i>	Kullanım hatası / <i>Error in Use</i>
	İşletim sistemlerine yazılım yüklenmesiyle ilgili prosedürlerin eksikliği / <i>Lack of procedures for introducing software into operational systems</i>	Kullanım hatası / <i>Error in Use</i>
	Yönetici ve operatör log kayıtlarındaki eksiklik / <i>Lack of records in administrator and operator logs</i>	Kullanım hatası / <i>Error in Use</i>
	Sınıflandırılmış bilginin kullanımıyla ilgili prosedürlerin eksikliği / <i>Lack of procedures for classified information handling</i>	Kullanım hatası / <i>Error in Use</i>
	İş tanımlarında bilgi güvenliği sorumluluklarının eksikliği / <i>Lack of information security responsibilities in job descriptions</i>	Kullanım hatası / <i>Error in Use</i>
	Çalışanlarla yapılan sözleşmelerde (bilgi güvenliği ile ilgili) hükümlerin Yetersiz/Eksik oluşu / <i>Lack of insufficient provisions (concerning information security) in contracts with employees</i>	Bilginin Yasadışı İşlenmesi / <i>Illegal Processing of data</i>
	Tanımlanmış disiplin süreçlerinde Bilgi güvenliği ihlal olaylarının yer almaması / <i>Lack of defined disciplinary process in case of information security incident</i>	Ekipman çalınması / <i>Theft of equipment</i>
	Mobil bilgisayar kullanımı üzerine resmi bir politikanın olmayışı / <i>Lack of formal policy on mobile computer usage</i>	Ekipman çalınması / <i>Theft of equipment</i>
	Saha dışındaki varlıkların kontrolünün eksikliği / <i>Lack of control of off-premise assets</i>	Ekipman çalınması / <i>Theft of equipment</i>
	Temiz masa temiz ekran politikasının yetersiz oluşu / <i>Lack of insufficient 'clear desk and clear screen' policy</i>	Medya veya Dokümanların Çalınması / <i>Theft of media or documents</i>
	Bilgi işleme olanaklarında yetkilendirme eksikliği / <i>Lack of information processing facilities authorization</i>	Medya veya Dokümanların Çalınması / <i>Theft of media or documents</i>
	Güvenlik ihlalleri için oluşturulan izleme mekanizmalarının eksikliği / <i>Lack of established monitoring mechanisms for security breaches</i>	Medya veya Dokümanların Çalınması / <i>Theft of media or documents</i>
	Düzenli yönetimin gözden geçirmesinin eksikliği / <i>Lack of regular management reviews</i>	İzinsiz Ekipman Kullanımı / <i>Unauthorised use of equipment</i>
	Güvenlik zayıflıklarının bildiri için prosedürlerin eksikliği / <i>Lack of procedures for reporting security weaknesses</i>	İzinsiz Ekipman Kullanımı / <i>Unauthorised use of equipment</i>
	Fikri Mülkiyet hakları ile uyum prosedürlerinin eksikliği / <i>Lack of procedures of provisions compliance with intellectual rights</i>	Sahte veya Kopyalanmış yazılım kullanımı / <i>Use of counterfeit or copied software</i>