ISO 27001
Bilgi Güvenliği Yönetim Sistemi
Uygulama

TÜBİTAK BİLGEM
Siber Güvenlik Enstitüsü

Sunum İçeriği

Bilgi Güvenliği Yönetim Sistemi: Özet

Bilgi Güvenliği Kavramları ve ISO 27001 Standardı

ISO 27002 (27001 Ek A) Güvenlik Önlemleri

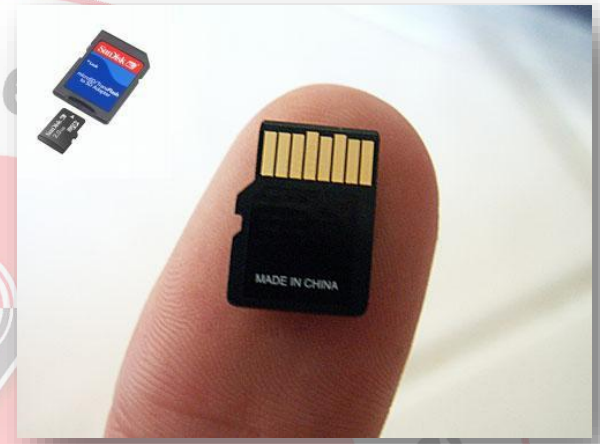
Denetim ve Sertifikasyon

Bilgi Güvenliği Yönetim Sistemi: Özet

Bilgi Güvenliği Gereksinimi

- ***Değerli bilgi varlıkları***
  - Ticari / Askeri açıdan gizli bilgi
  - Müşteri, tedarikçi ve personele ait bilgiler
  - Fikri mülkiyet
  - Kurumsal birikim
- ***Kanun ve sözleşmelerden kaynaklanan yükümlülükler***
- ***Bilgi sistemlerine bağımlılık***
  - Tüm bilgi sistemlerinde bulunabilen açıklar

Bilgi Güvenliğinin Artan Önemi



- ***Bilgisayar ve bilgisayar ağı sistemleri***
  - Bilgi, merkezi olarak toplanıyor ve işleniyor
  - Bilgiye erişim olanaklarının artması
- ***Kayıt ve depolama teknolojilerindeki gelişmeler***
  - Hafıza kartları, yazılabilir diskler, sayısal fotoğraf makineleri vb…
- ***Bilgi teknolojilerinin günlük hayata girmesi***

Bilgi Güvenliğini Tehdit Eden Unsurlar

- ***Dış***
  - Düşmanlar, rakipler ve diğer saldırganlar (“botnet” vb.)
  - Kötü niyetli yazılımlar (Virüs ve benzeri)
  - “Spam”: (Tüm elektronik postanın %80’i)
  - Bilgisayara sahip herhangi biri
- ***İç***
  - Personel hataları
  - Kasıtlı zarar verme

Bilgi Güvenliğinin Temelleri

- ***Bilgi güvenliğinin hedefi***, kuruma ait bilginin
  - Gizlilik
  - Bütünlük, ve
  - Erişilebilirliğini korumaktır.
- Bunların korunması için alınacak ***önlemler***
  - Erişim Kontrolü (Gizlilik ve Bütünlük için)
  - Yedekleme (Bütünlük ve Erişilebilirlik için)
  - Önlemlerin uygulanması için tüm yönetici ve kullanıcıların eğitilmesi gerekir.

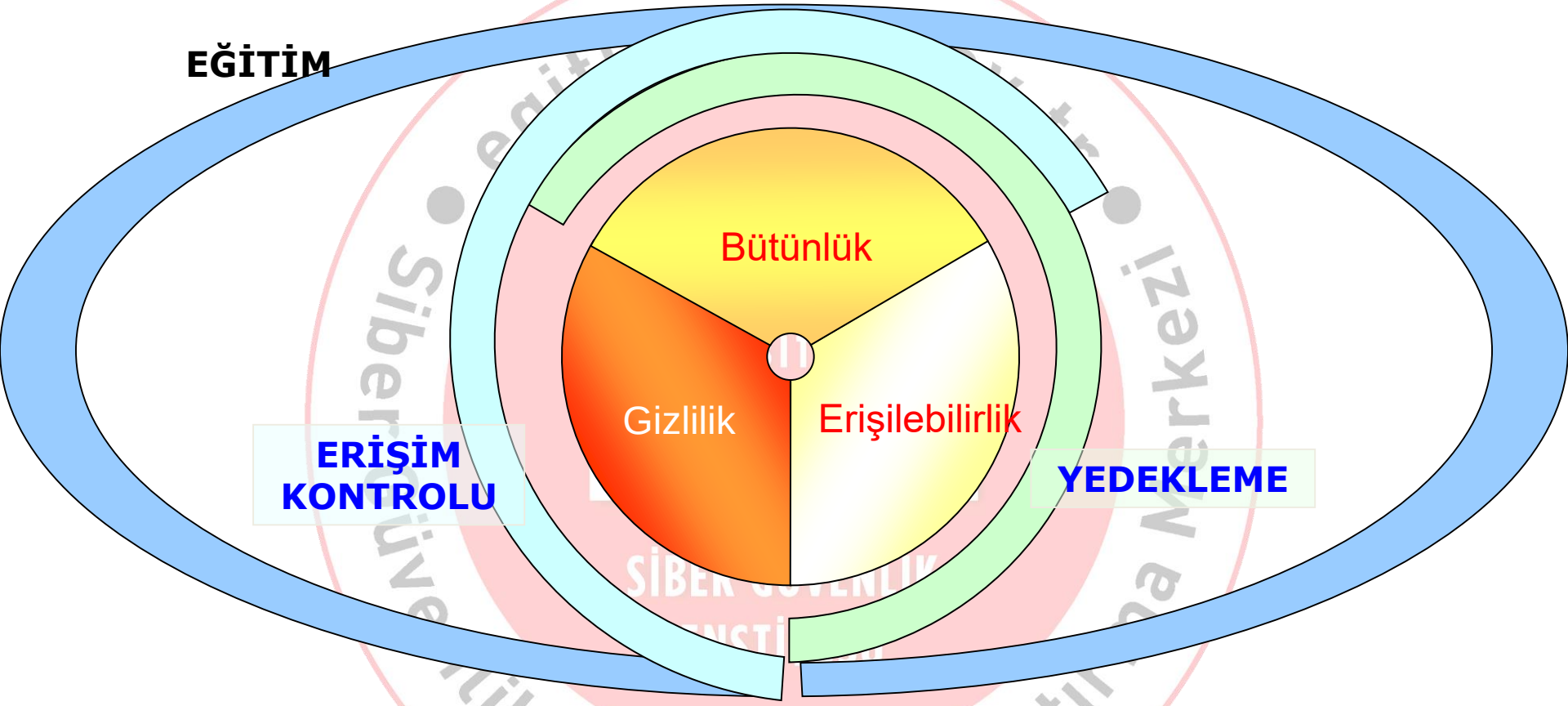
Başlıca Önlemler: Erişim Kontrolü ve Yedekleme

- Erişim Kontrolü
  - Önleyici tedbirdir.
  - Hasarın oluşmasını önlemeyi hedefler.
- Yedekleme,
  - Düzeltici tedbirdir.
  - Gizliliği koruyamaz.
  - Bütünlüğün veya erişilebilirliğin kaybedilmesi durumunda geri dönüş sağlar.

Bilginin Özellikleri ve Başlıca Önlemler

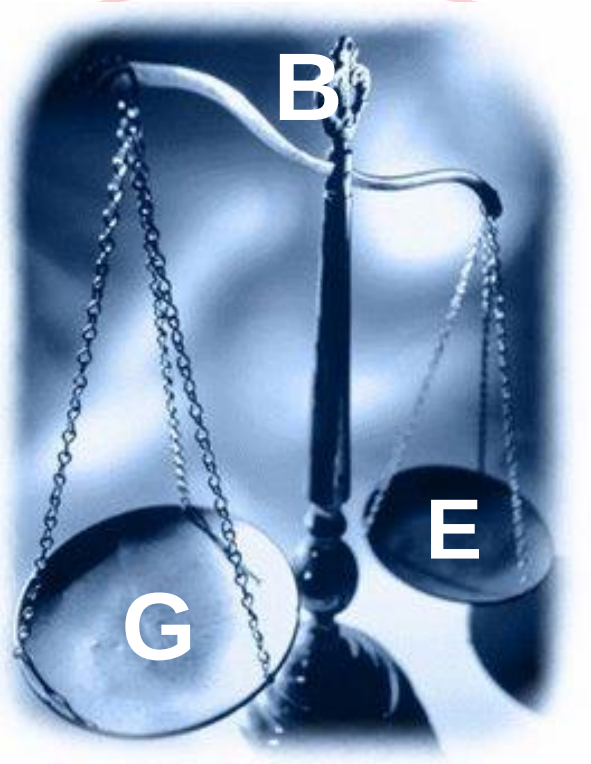
	Erişim Kontrolü	Yedekleme	Eğitim
Gizlilik	●	-	●
Bütünlük	●	●	●
Erişilebilirlik	-	●	●

Bilgi Güvenliğinin Temelleri



Bilgi Güvenliği

Bilgi Güvenliğinde Denge



Gizlilik x Erişilebilirlik dengesi:

Gizliliği korumak için alınan önlemler erişilebilirliği "bozar"

Bilgi Güvenliğinin Uygulanması

- Uygulama = İrade + Yöntem belirleme + Eğitim
- İrade kurumun stratejik kararları, yükümlülükleri ve kanunlarla oluşur.
  - Rol ve sorumlulukların belirlenmesi ile personele yansıtılır.
- Yöntem kurum yöneticileri ve teknik adamları tarafından belirlenir, *politika ve prosedürlerle* ifade edilir.
- Eğitim kurumun içinden veya dışından uzmanlar tarafından verilir.

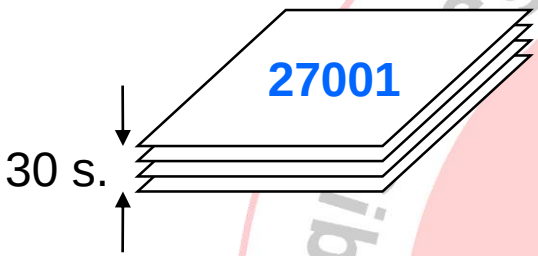
- Uygulama, kayıtlarla "kayıt altına" alınır.

Bilgi Güvenliğinde Yöntem

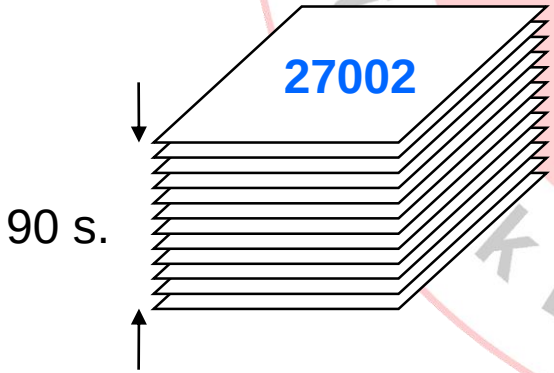
- Yöntem = Ne + Nasıl.
- Ne yapacağım?
  - Bilgi Güvenliği Politikası
  - 27001 BGYS döngüsü
  - Risk analizi, 27002 kontrolleri, iç tetkik vs...
- Nasıl yapacağım?
  - **Prosedürleri** belirleyip çalıştırarak
  - **Rol ve sorumlulukla**rın belirlenmesi ile
  - Tüm kurumun katılımı ile

Bilgi Güvenliği Standartları

International Organization for Standardization

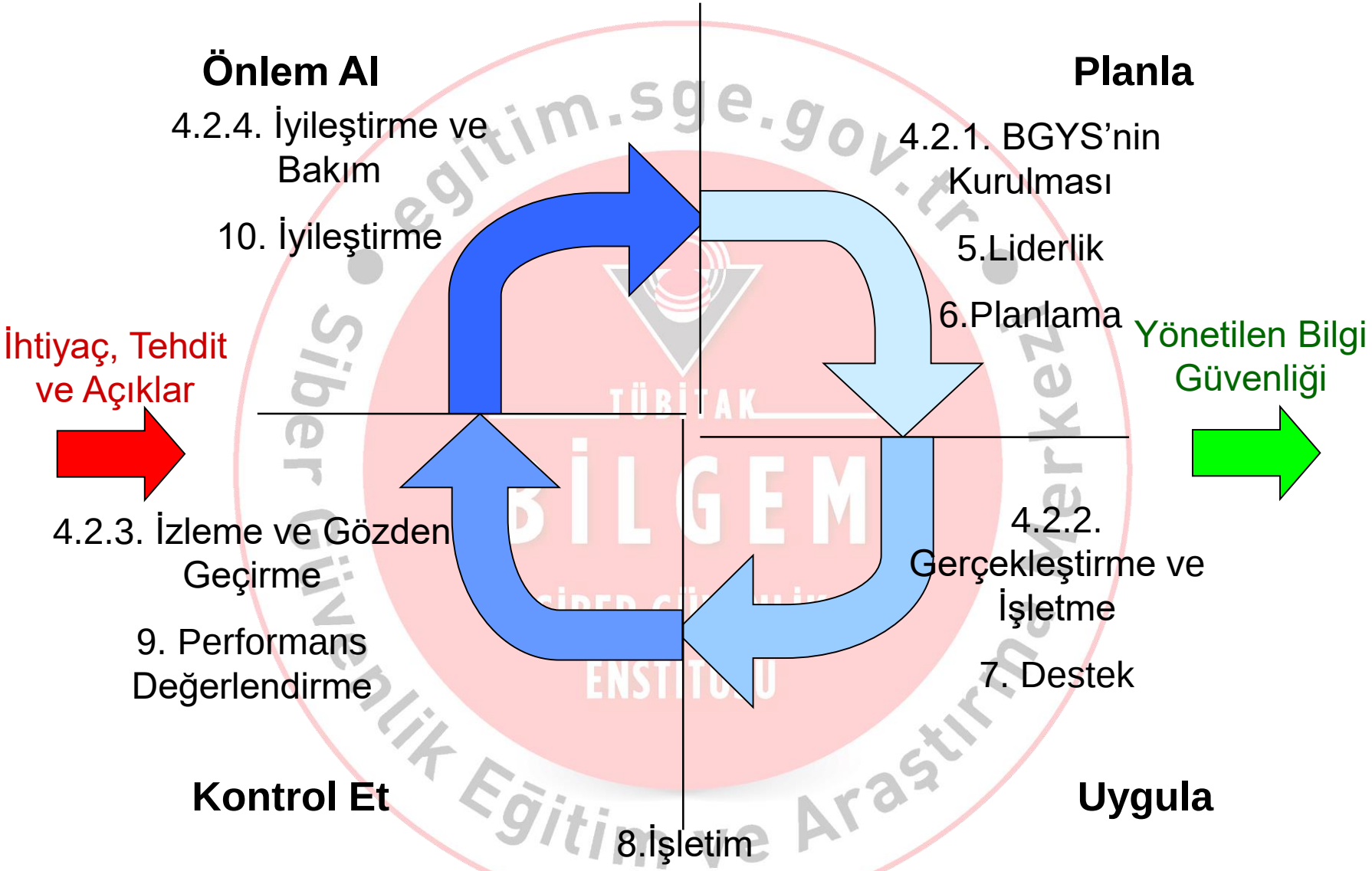


- ISO 27001: BGYS'nin kurulması ve yaşatılması için çalıştırılması gereken süreci tanımlar



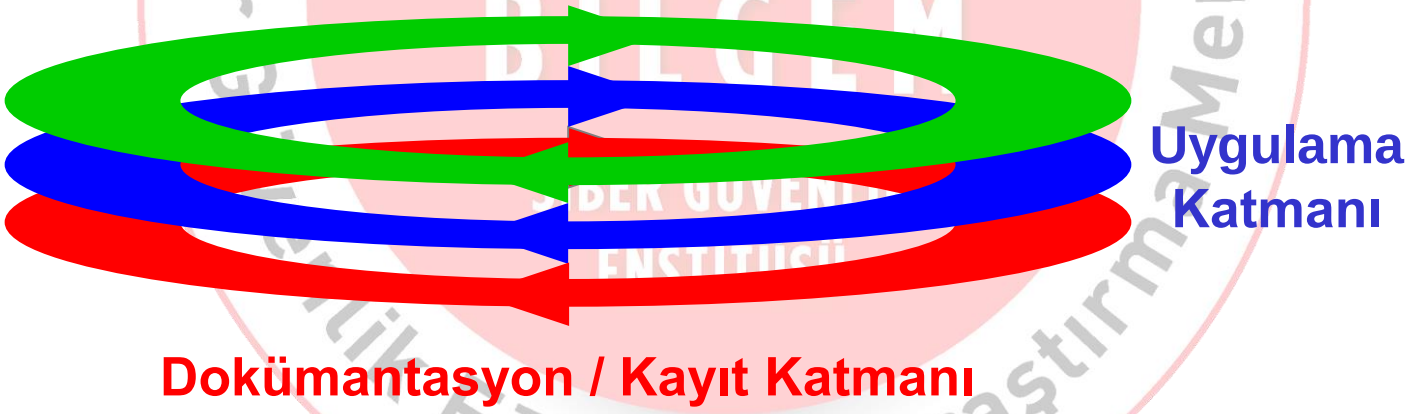
- ISO 27002: 14 temel başlık altında bir BGYS'de yer alabilecek güvenlik önlemlerini açıklar

ISO 27001:2005'e göre Bilgi Güvenliği Süreci



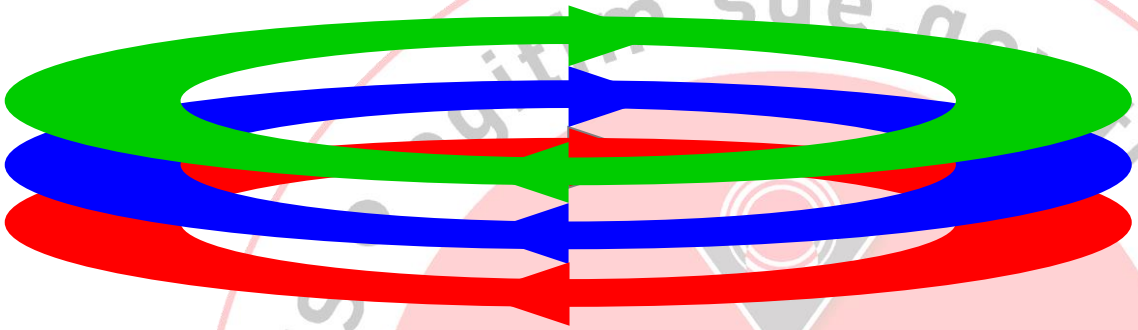
Bilgi Güvenliği Yönetim Sistemi (BGYS)

- Kurumsal bir iş sürecidir.
- Risklerin önlemlerle dengelenmesini hedefler.
- Yönetim, uygulama ve dokümantasyon/kayıt katmanlarından oluşur.



Görevler Ayrılığı

Yönetim: Yetkilendirme ve gözden geçirme işlevleri (Politika üretme)

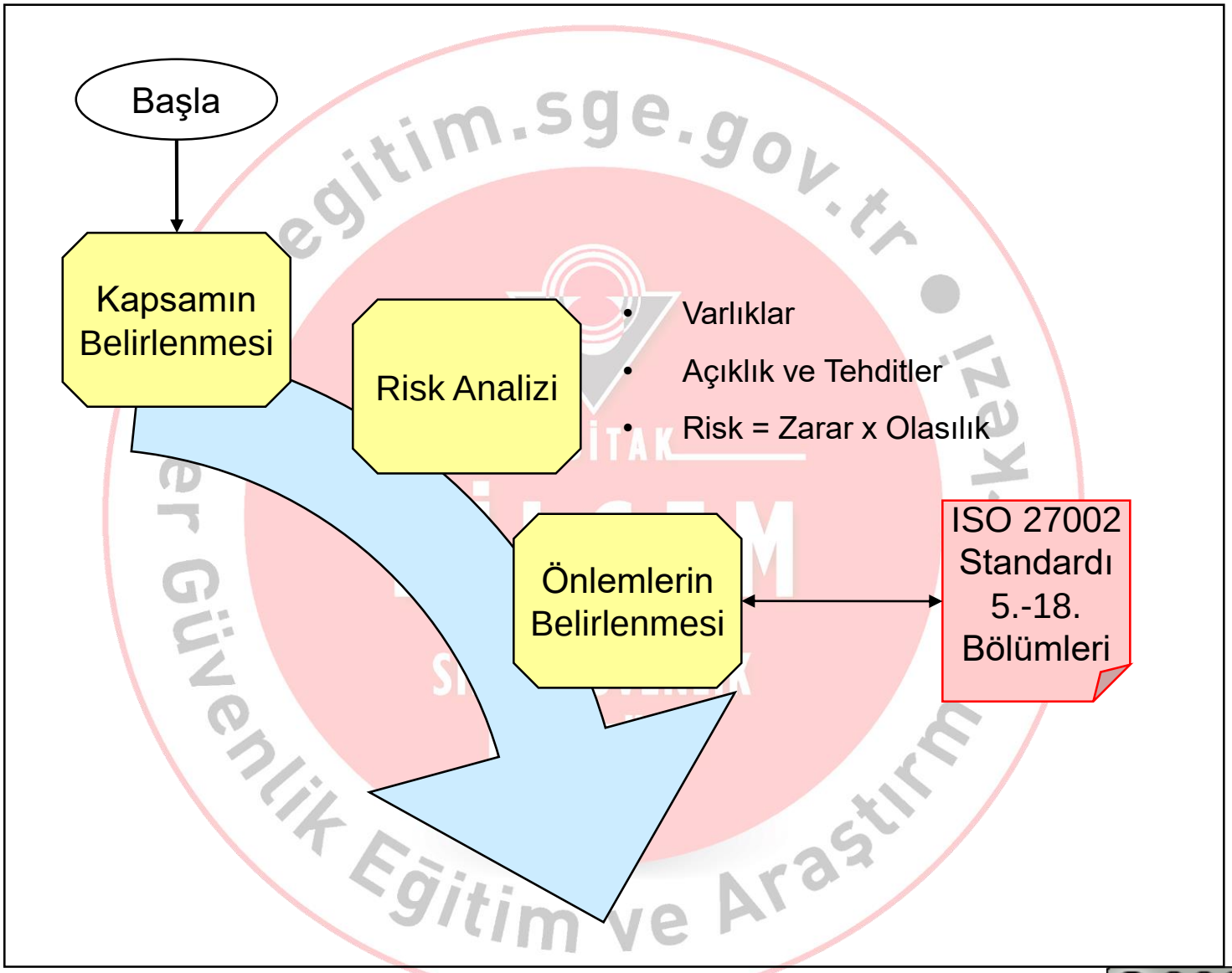


Yürütücü personel: BGYS işlerinin yapılması (Prosedür ve kayıtların üretilmesi)

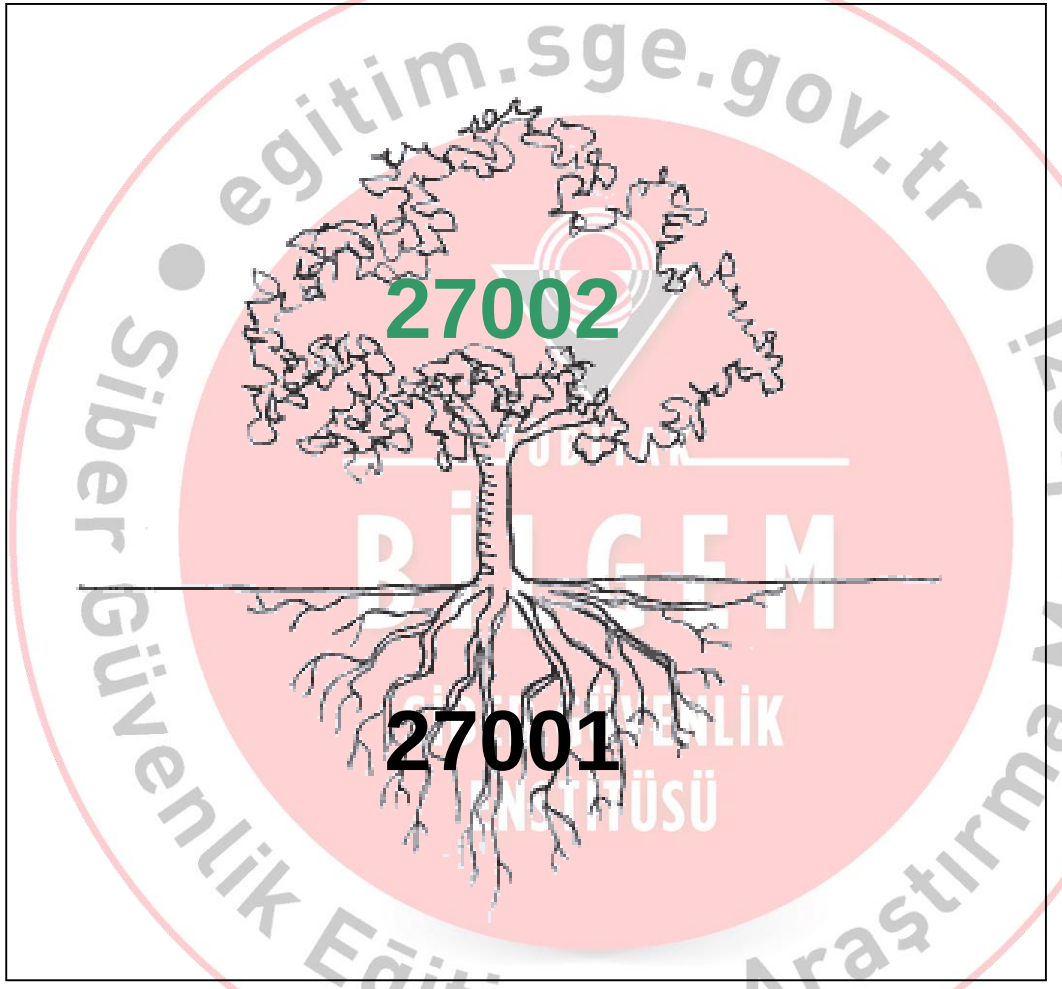
Tetkik / izleme (Doküman ve kayıtlar üstünden gerçekleştirilir)

- İşin yapılması ile yetkilendirilmesi birbirinden ayrılmalıdır. *(ISO 27002, 6.1.2 Görevler Ayrılığı)*
- Tetkikçiler kendi yaptıkları işi tetkik edemezler. *(ISO 27001, 9.2 İç Tetkik)*
- Yasama/Yürütme/Yargı => Yetkilendirme/Yürütme/Tetkik

Gereken Önlemlerin ISO 27002'den Seçilmesi



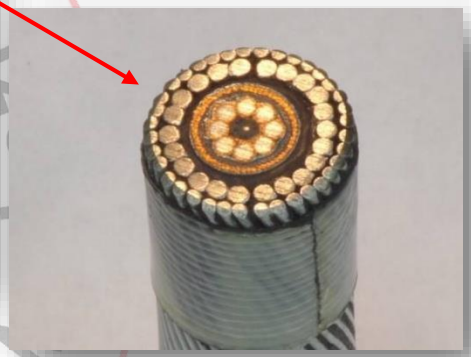
ISO 27001 ve 27002 Standartlarının İlişkisi



Güvenlik önlemleri

Yaşatma süreci

ISO 27001 ve 27002 Standartlarının İlişkisi



Kablonun seçilmesi, bağlanması ve kontrol edilmesi ISO 27001'e benzetilebilir

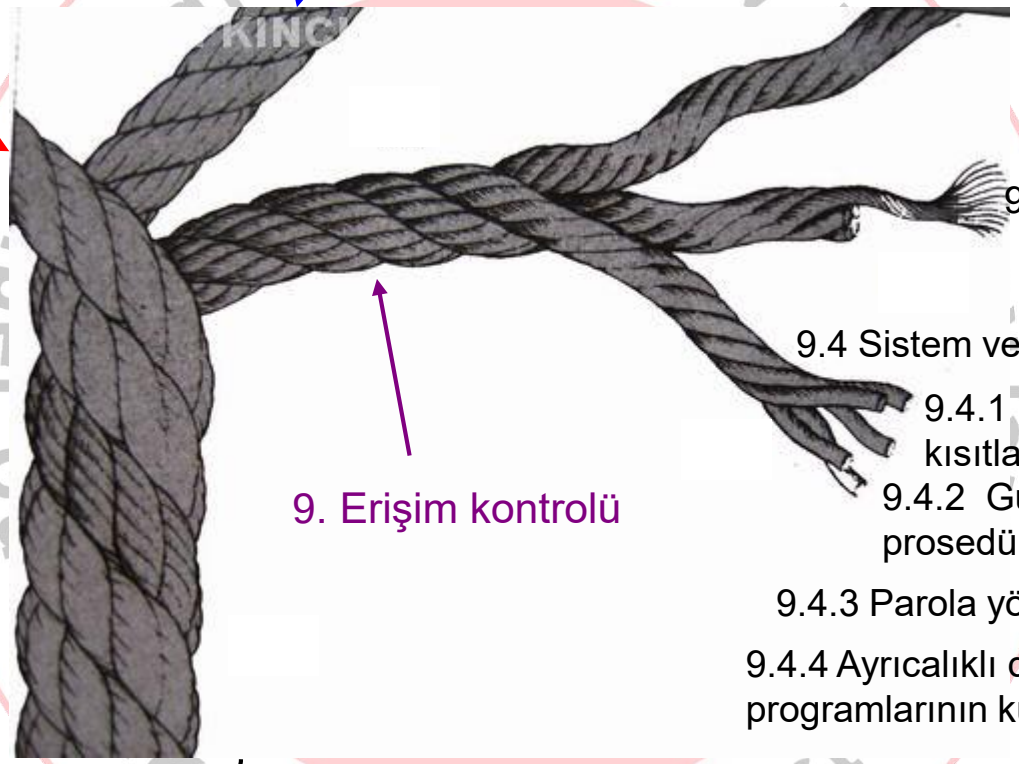
Bu örnekte gerekenden kalın kablo kullanılmış (27002 standardındaki önlemler körü körüne uygulanmış) durumda

Kablonun kendisi ve kabloyu oluşturan teller ISO 27002'den seçilen önlemlere benzetilebilir

ISO 27002 Önlemlerinin Hiyerarşik Yapısı

7. İnsan kaynakları güvenliği

6. Bilgi güvenliği organizasyonu



9.2 Kullanıcı erişim yönetimi

9.3 Kullanıcı sorumlulukları

9.4 Sistem ve uygulama erişim kontrolü

9.4.1 Bilgiye erişimin kısıtlanması

9.4.2 Güvenli oturum açma prosedürleri

9.4.3 Parola yönetim sistemi

9.4.4 Ayrıcalıklı destek programlarının kullanımı

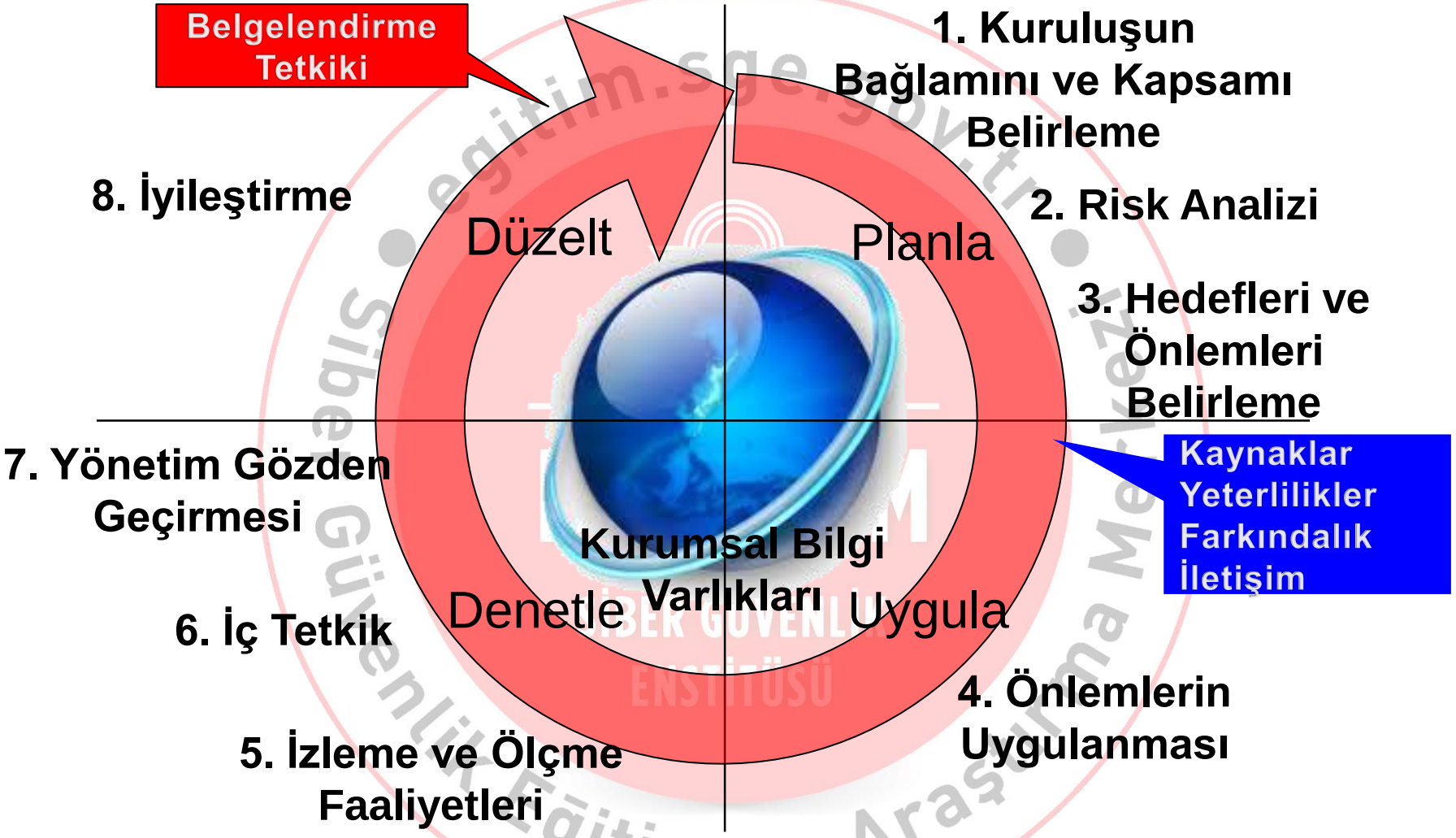
9. Erişim kontrolü

Tüm 27002 önlemleri:
14 grupta 114 önlem

ISO 27002: 14 Temel Başlık

1. Bilgi Güvenliği Politikaları
2. Bilgi Güvenliği Organizasyonu
3. İnsan Kaynakları Güvenliği
4. Varlık Yönetimi
5. Erişim Kontrolü
6. Kriptografi
7. Fiziksel ve Çevresel Güvenlik
8. İşletim Güvenliği
9. Haberleşme Güvenliği
10. Sistem Temini, Geliştirme ve Bakımı
11. Tedarikçi İlişkileri
12. Bilgi Güvenliği İhlal Olayı Yönetimi
13. İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları
14. Uyum

ISO 27001 BGYS Süreci, özet



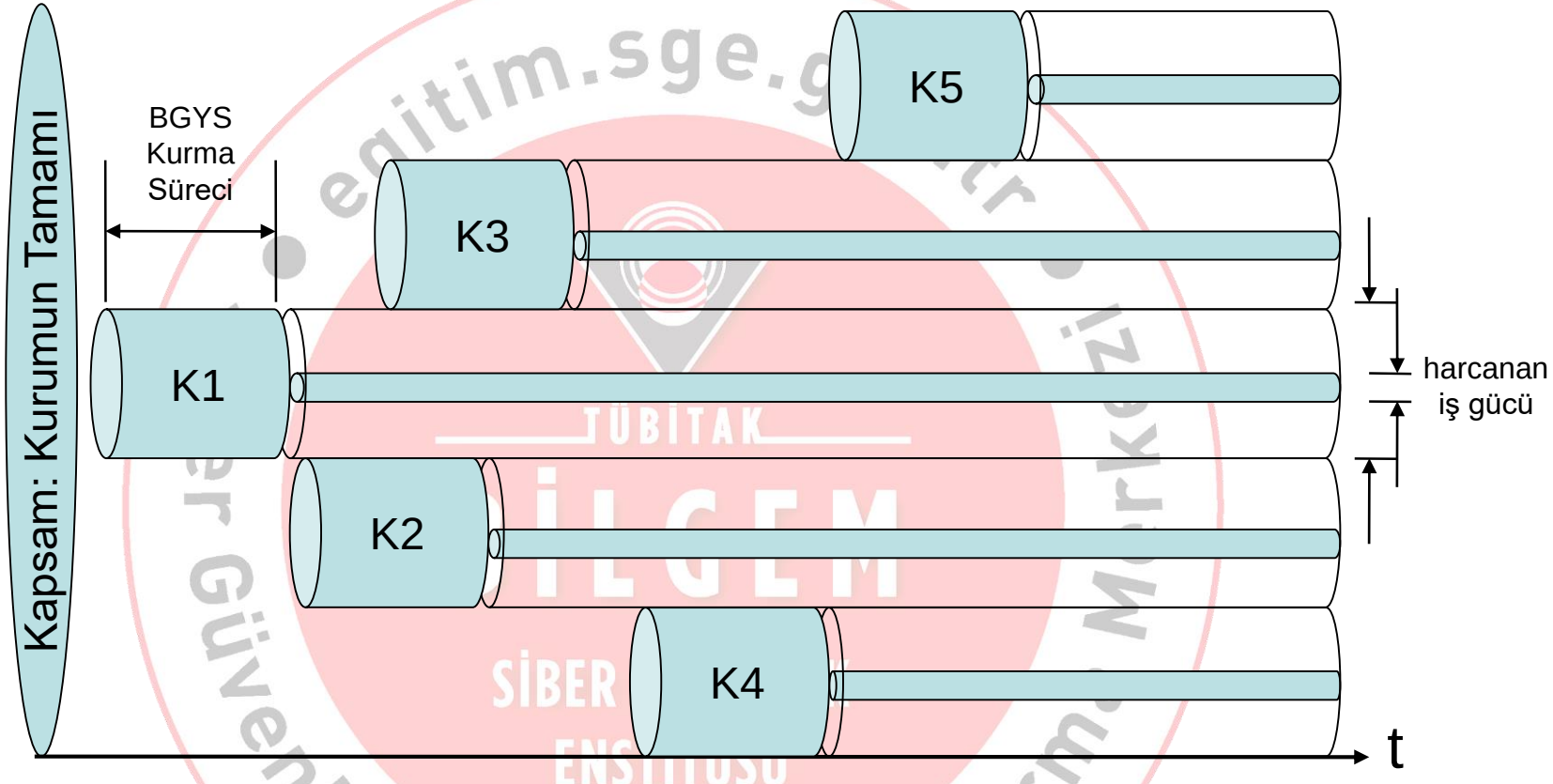
Sürecin Ana Hatları (1/2)

- İlgili tarafların, bilgi güvenliği gereksinimlerine göre kapsamın ve **kritik süreçler**in belirlenmesi
- Uygulanacak **risk metodolojisi**nin tanımlanması
- **Varlık envanteri**nin oluşturulması
- **Risk Analizi**nin gerçekleştirilmesi
  - Varlık envanteri üstünden,
  - Kavramsal güvenlik analizi (ISO 27002 kontrollerinin kurumdaki durumunun belirlenmesi)
  - Teknik güvenlik testlerinin yapılması

Sürecin Ana Hatları (2/2)

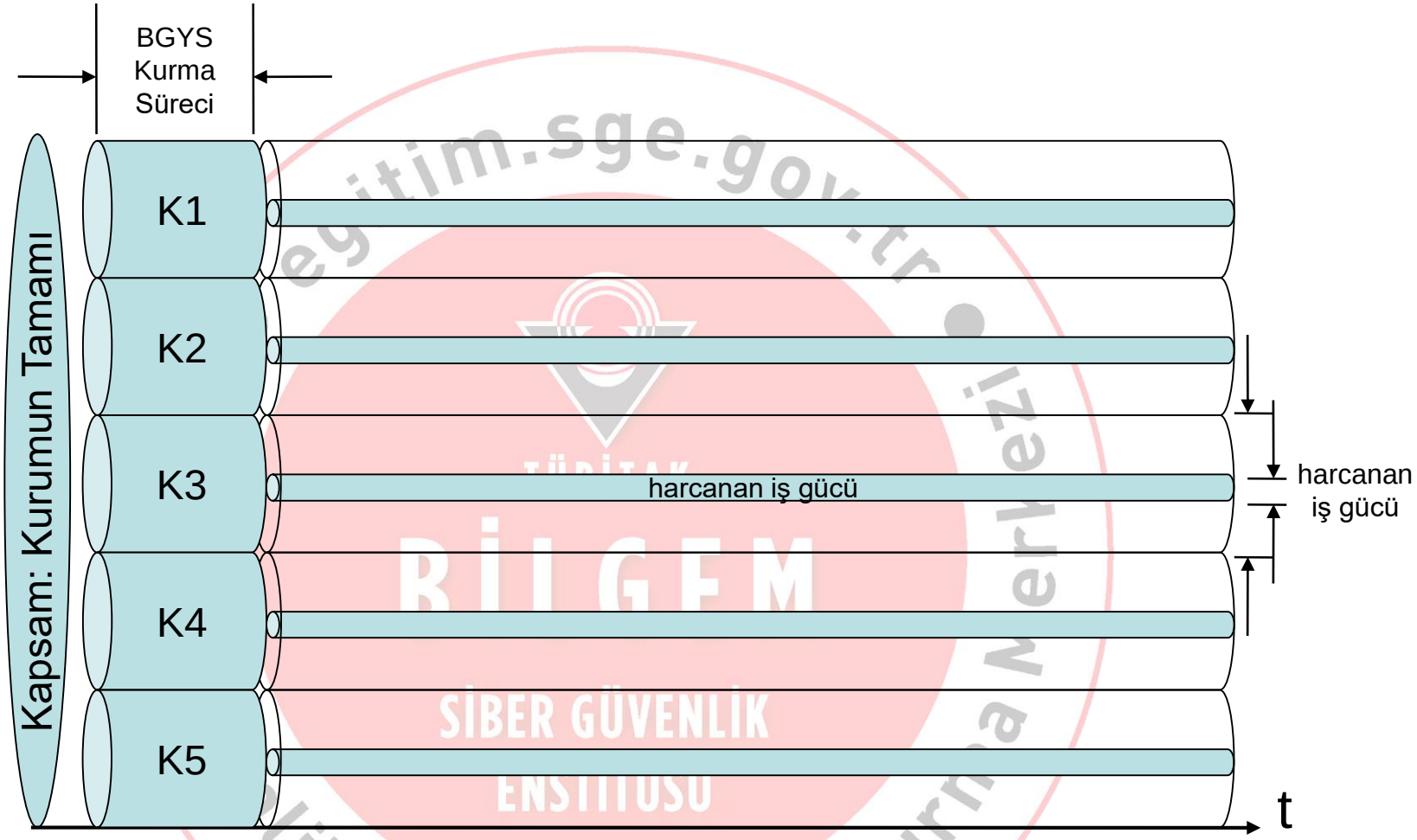
- **Risk işleme planı**nın oluşturulması ve risk sahipleri tarafından onaylanması
- Kaynakların sağlanması (Bütçe planlaması, personel yeterliliği, iletişim yöntemleri)
- Personele verilecek bilgi güvenliği bilinçlendirme **eğitimleri**
- BGYS **Dokümantasyonu**
- Risk işleme planının uygulanması (kritik olanlardan başlayarak)
- Performans İzleme ve Ölçme
- **İç Tetkik**
- Yönetimin gözden geçirmesi
- **Düzeltici faaliyetler**

BGYS Kurma Seçenekleri 1/2



- Dar kapsamlı “mini-projelerin” zamana yayılması.
- Konuya yabancı kurumlara tavsiye edilen bir yaklaşımdır.

BGYS Kurma Seçenekleri 2/2



- BGYS'nin kurumun tamamında paralel çalışma ile kurulması
- Üst yönetim desteği, tecrübeli proje yönetimi ve odaklanma gerekli

Kritik Başarı Faktörleri

- **Yönetimin** hedef koyması, somut desteği ve bağlılığı
- Bilgi güvenliğinin **kalıcı bir iş süreci** olduğunun anlaşılması
- Güvenlik gereksinimlerinin anlaşılması
- Tutarlı bir **risk değerlendirmesi** ve risk yönetimi
- Kapsam dahilinde **eğitim** ve farkındalık
- Bilgi güvenliği performansının ölçülmesi

Bilgi Güvenliği Kavramları ve ISO27001 Standardı

Bilgi Nedir?

- **İşlenmiş veri**ye bilgi denir.
- Bilgi, kurumun kimliğidir.

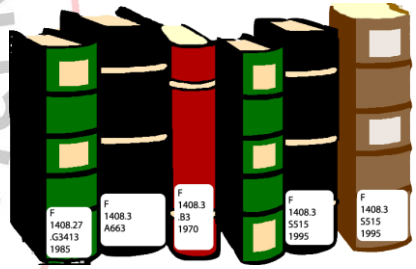
- Bilgi, diğer bütün kurum varlıkları gibi **organizasyon için değeri olan ve dikkatle korunması gereken bir varlıktır.**
- Bilgi somut bir varlık değildir.

Uygulama-1

- **5 adet kurumsal bilgi**yi yazınız.

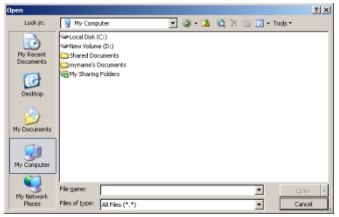
Bilgiyi Somutlaştıran Ögeler - 1

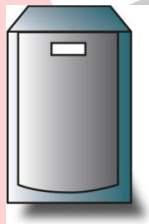
- Bilginin sahibi
- Bilginin tutulduğu ortam
  - Basılı doküman
  - Elektronik saklama ortamı
    - Sabit disk
    - Disk sistemi
    - Teyp ünitesi
    - Cd-rom
    - USB bellek
  - Elektronik erişim ortamı
    - Veritabanı kayıtları
    - Dosya, dosya sistemi
- Ortamın fiziksel yeri



Bilgiyi Somutlaştıran Ögeler - 2

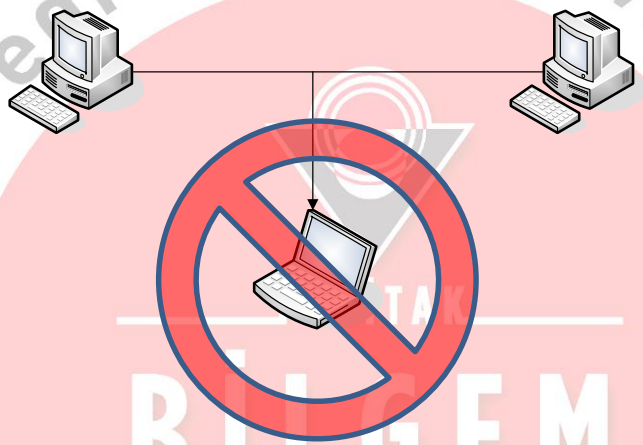
- Bilgiyi işleyen yazılımlar
- Bilgiyi işleyen donanımlar
  - Bilgisayarlar
  - Kablolu / kablosuz ağ cihazları
  - Yazıcı / tarayıcı vs…
- Bilgiye erişen taraflar
  - Kurum içinden (kişi/şube/daire)
  - Kurum dışından (kişi/kurum bağlısı/diğer kurum/vata
  - Erişim hakları: Değiştirme/silme/okuma
- Bilginin yedeklenme durumu





Gizlilik, Bütünlük ve Erişilebilirlik

- **Gizlilik**, bilginin yetkisiz kişi ve süreçlere açılmaması,



- **Bütünlük**, bilginin doğru ve eksiksiz olarak korunması,
- **Erişilebilirlik** ise yetkili kullanıcıların bilgiye istedikleri anda ulaşmalarının sağlanmasıdır.

Uygulama-2

- Uygulama-1'de yazmış olduğunuz 5 kurumsal bilginin **gizlilik, bütünlük, erişilebilirlik** özelliklerini belirtiniz (**var/yok** şeklinde).

Kurumsal Bilgi	Gizlilik	Bütünlük	Erişilebilirlik

Bilgi Güvenliği Nedir?

- Bilgi güvenliği, kurumsal bilginin
  - Gizliliğinin,
  - Bütünlüğünün ve
  - Erişilebilirliğinin sağlanmasıdır.

- Korunması gereken bilgi çeşitleri
  - Kurumsal bilgiler
  - Müşteri/Tedarikçilere ait bilgiler
  - İnternet üzerinden yayınlanan bilgiler
    - Kurum kullanıcılarına açık bilgi ve servisler
    - Halka açık bilgiler

Standartların Kısa Tanımları

- ISO/IEC 27001:2013> Bir Bilgi Güvenliği Yönetim Sisteminin kurulması, uygulanması, izlenmesi, sürdürülmesi ve geliştirilmesi için gerekli adımları ortaya koyan süreç yaklaşımını tanımlar.
  - ***Uyma zorunluluğu vardır ("shall" - zorunluluk)***

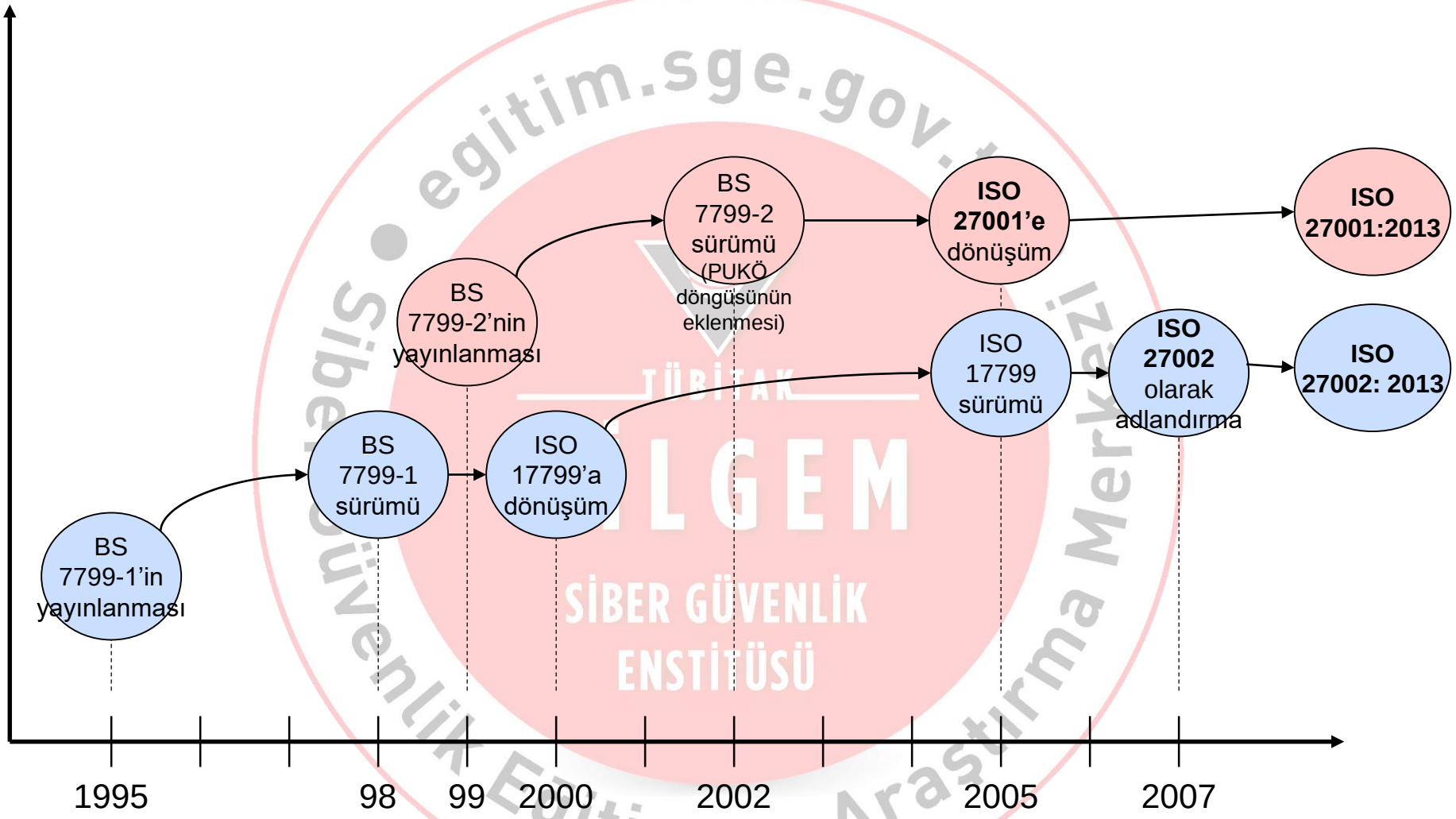
- ISO/IEC 27002:2013> Bir Bilgi Güvenliği Yönetim Sisteminde yer alabilecek güvenlik önlemlerine 14 temel başlık altında yer verir.
  - ***Uyma zorunluluğu yoktur ("should" – tavsiye)***

Standartların Tarihçesi

- ISO/IEC 27001:
  - BS 7799-2:1999: İlk BGYS kılavuzu, sertifikasyon
  - BS 7799-2:2002: BGYS kılavuzu için revizyon
  - ISO/IEC 27001:2005 (BS 7799-2:2005)
  - **ISO/IEC 27001:2013**

- ISO/IEC 27002:
  - BS 7799:1995: İlk yayımlanma (En iyi uygulamalar)
  - BS 7799:1999: Büyük ölçüde yenilendi (En iyi uygulamalar)
  - ISO/IEC 17799:2000: BS 7799:1999, çok az içerik değişikliği ile uluslararası standart olarak kabul edildi (En iyi uygulamalar)
  - ISO/IEC 17799:2005 (BS 7799-1:2005)
  - ISO/IEC 27002:2005
  - **ISO/IEC 27002:2013**

Standartların Tarihçesi



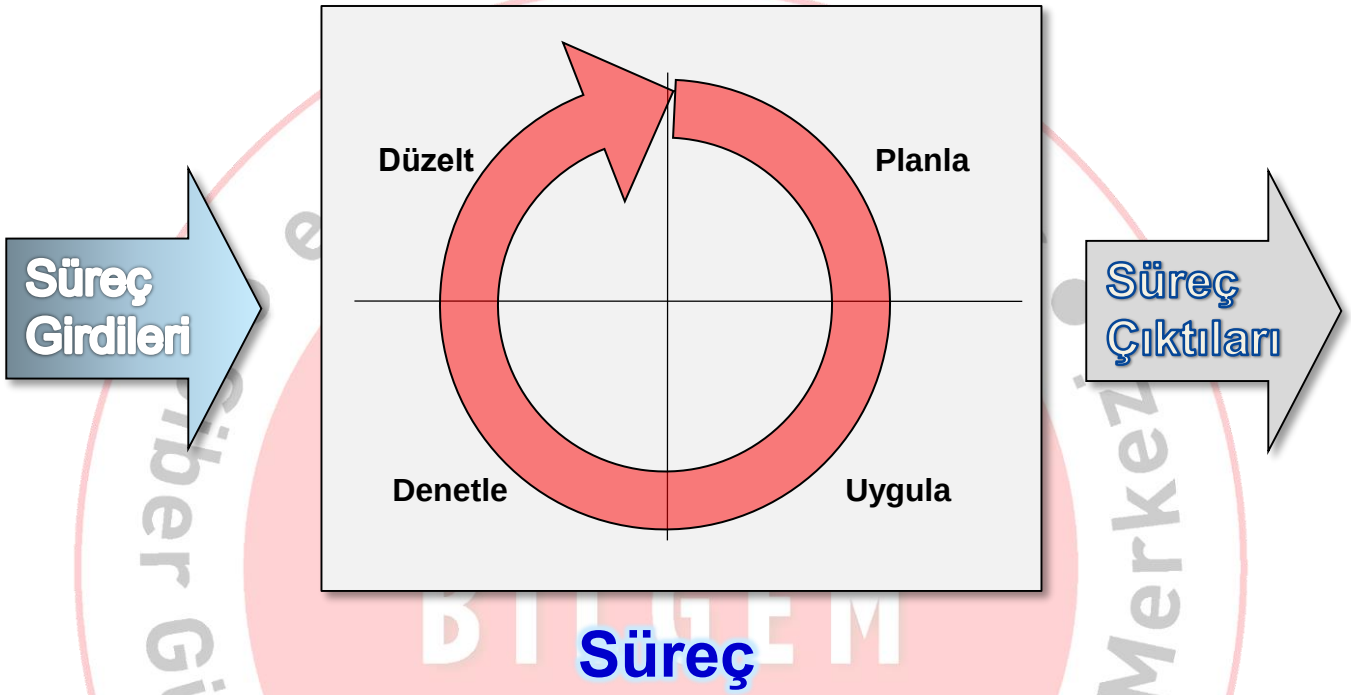
ISO 27001 – İçindekiler

1. Giriş
2. Kapsam
3. Atıf Yapılan Standartlar ve/veya Dokümanlar
4. Terimler ve Tarifler
5. Kuruluşun Bağlamı
6. Liderlik
7. Planlama
8. Destek
9. İşletim
10. Performans Değerlendirme
11. İyileştirme

Tartışma-1

Süreç nedir?

Süreç Nedir?



- Girdileri çıktılara dönüştüren, birbiri ile ilişkili ve etkileşimli faaliyetler dizisi.
  - Kurum tarafından tasarlanır ve yönetilir.
  - Kaynak kullanır.

ISO 9001 ve ISO 27001

- Süreç tabanlı sistemler (örnek):
  - ISO 9001 Kalite Yönetim Sistemi
    - *Müşteri memnuniyetini arttır!*
  - ISO 27001 Bilgi Güvenliği Yönetim Sistemi
    - *Bilgi güvenliği risklerini azalt!*
- Hedefler farklı, süreç ise benzerdir.

ISO 9001 ve 27001: Girdi ve Çıktılar

	ISO 9001 Kalite Yönetim Sistemi	ISO 27001 Bilgi Güvenliği Yönetim Sistemi
Süreç Girdileri	- Müşteri memnuniyeti ***<u>Müşteri</u>*** *tarafından objektif olarak değerlendirilir!*	- Kurumun bilgi güvenliği riskleri *Kurumun* ***<u>kendi çalışanları</u>*** *tarafından değerlendirilir!*
Süreç Çıktıları	- Artan müşteri memnuniyeti (kalitesi artmış ürün/servis)	- Kontrol altına alınmış riskler (gelişen güvenlik anlayışı ve iyileştirilmiş iş süreçleri)

PUKÖ Döngüsünün Standarttaki Yeri

4.Kuruluşun Bağlamı

5.Liderlik

6.Planlama (**Planla**)

7.Destek: Kaynaklar, Yeterlilik, Farkındalık, İletişim, Yazılı Bilgiler

8. İşletim (**Uygula**)

9. Performans Değerlendirme (**Kontrol et**)

10. İyileştirme (**Önlem al**)

Kuruluşun Bağlamı

Riski yönetirken dikkate alınması gereken iç ve dış hususları belirleyin*:

- Dış Hususlar
  - Kuruluşun içinde bulunduğu ortam (kültürel, politik, finansal, teknolojik ...)
  - Dış paydaşların ihtiyaç ve beklentileri
  - Yasa, mevzuat ve sözleşme gereksinimleri
- İç Hususlar
  - Yönetişim yapısı, kurum kültürü, kurumsal süreçler, organizasyon yapısı, kurumsal strateji ve hedefler
  - Bilgi sistemleri ve bilgi akışı

*ISO 31000:2009 Risk Yönetimi Madde 5.3

İlgili taraflar

a)Kuruluşun bilgi güvenliği yönetimi ile ilgili tarafları,

b)Bu ilgili tarafların bilgi güvenliği gereksinimlerini belirleyin

İlgili taraflar

İç Taraflar	Dış Taraflar
Çalışanlar	Devlet
Yükleniciler	Yasal merciler
İş ortakları	Düzenleyiciler
İşçi temsilcileri	Müşteriler
	Sigortacı
	Temel hizmet şirketleri (elektrik, su, yakıt, iletişim)
	Baskı grupları
	Ticari yapılar/Birlikler
	Rakipler
	İş ortakları
	Tedarikçiler / Yükleniciler

Yükümlülüklerinizi Belirleyin

Kanunlardan ve sözleşmelerden kaynaklanan yükümlülüklerinize göre

- BGYS kapsamını
- Varlık sınıflandırma/etiketleme esaslarını
- Varlık değeri/risk etki değeri ölçeklerini
- Kabul edilebilir risk değerini belirleyin

BGYS Kapsam Dokümanı

- Kuruluşun bağlamı
- BGYS kapsamı
  - **İş süreçleri**
  - Sözleşmeler, yasal gereksinimler
  - Bilgi, Yazılım, Donanım
- Sınırlar
  - İdari
  - Fiziksel
  - Bilişim teknolojileri boyutunda

Tartışma-2

Tartışarak BGYS kapsamında yer alması gereken **bir kurumsal süreci** belirleyelim.

Uygulama-3

- Seçtiğimiz kurumsal süreci tanımlayalım.

Liderlik

- Bilgi güvenliği politikası ve bilgi güvenliği amaçlarının oluşturulmasını temin etmek,
- Bilgi güvenliği süreçlerinin iş süreçlerine entegrasyonunu temin etmek
- Yeterli kaynak sağlamak
  - Personel, eğitim
  - Teçhizat, ofis vb…
  - Bilgi güvenliği yönetiminin önemini ve BGYS'nin şartlarına uyum sağlamanın önemini duyurmak,
- Bilgi güvenliği rol ve sorumluluklarını, yetkilerini atamak
- Bilgi güvenliği politikasına ve yasalara karşı uyumu sağlamak, sürekli iyileştirmeyi sağlamak

Liderlik

- Yönetim Desteğinin Somut Göstergeleri
  - BGYS toplantılarının bazılarına katılım veya temsilci gönderilmesi,
  - Bilgi güvenliği bilinçlendirme faaliyetlerine katılım,
  - Üst yönetim için hazırlanan raporların incelenmesi ve geri besleme verilmesi,
  - Kurum güvenlik politikalarının uygulatılması,
  - Önemli güvenlik uyarılarının yönetim aracılığıyla duyurulması.

Bilgi Güvenliği Politikası

- Bilgi güvenliği amaçları ve prensipleri
- İş, yasal ve düzenleyici gereksinimler
- BGYS şartlarının karşılanmasına dair taahhütü
- BGYS'nin sürekli iyileştirilmesi için taahhüt
- Yazılı olmalı, ilgili taraflara duyurulmalı

Politika nasıl yazılır?

- Kapsam
  - Hedef kitleyi veya konuyu tanımlar.

    "Bilgi bir varlıktır, kurumun mülkiyetindedir ve tüm çalışanlar bu varlığı korumakla yükümlüdür."
- Konu
  - Politikanın özellikle neyi **hedef**lediği **vurgulanmalı**,
  - Kısa ve **açık ifade** edilmelidir.

Politika nasıl yazılır?

- Sorumluluklar
  - **Sorumlulukları** tanımlayın
  - Şahıs isimleri değil **unvan kullanın**
  - Mümkün olduğunca edilgen fiil kullanmaktan kaçının:

"Bilgi işlem daire başkanı, BGYS'nin çalıştırılmasından sorumludur…"

Bilgi Güvenliği ve BGYS Rolleri

- Üst yönetim, bilgi güvenliğiyle ilgili rol ve sorumluluklar ve yetkilerin atanmasını sağlamalıdır.

  a) BGYS'nin ISO27001'e uygunluğunu sağlama

  b) BGYS'nin performasını üst yönetime raporlama sorumluluğu ve yetkisi atanmalıdır.

Riskin Genel Tanımı

- Kuruluşlar, hedeflerine ulaşıp ulaşamayacaklarını belirsiz hale getiren birtakım iç ve dış etkenlerle karşılaşırlar.

- Risk, bu belirsizliğin hedefler üzerinde oluşturabileceği etkidir.

Risk

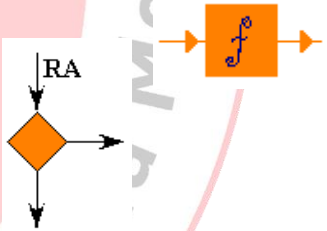
Varlık üzerindeki bir **açıklığın** bir **tehdit** tarafından kullanılmasına bağlı **zarar beklentisidir**.

Risk = f (Varlık, Açıklık, Tehdit)

Risk Yönetimi

- Risk Yönetimi

  - Risklerin Belirlenmesi (Identification)
  - Risk Değerlendirme (Assessment)
    - Risk Analizi (Analysis)
    - Risk Derecelendirme (Evaluation)
  - Risk İşleme (Treatment)



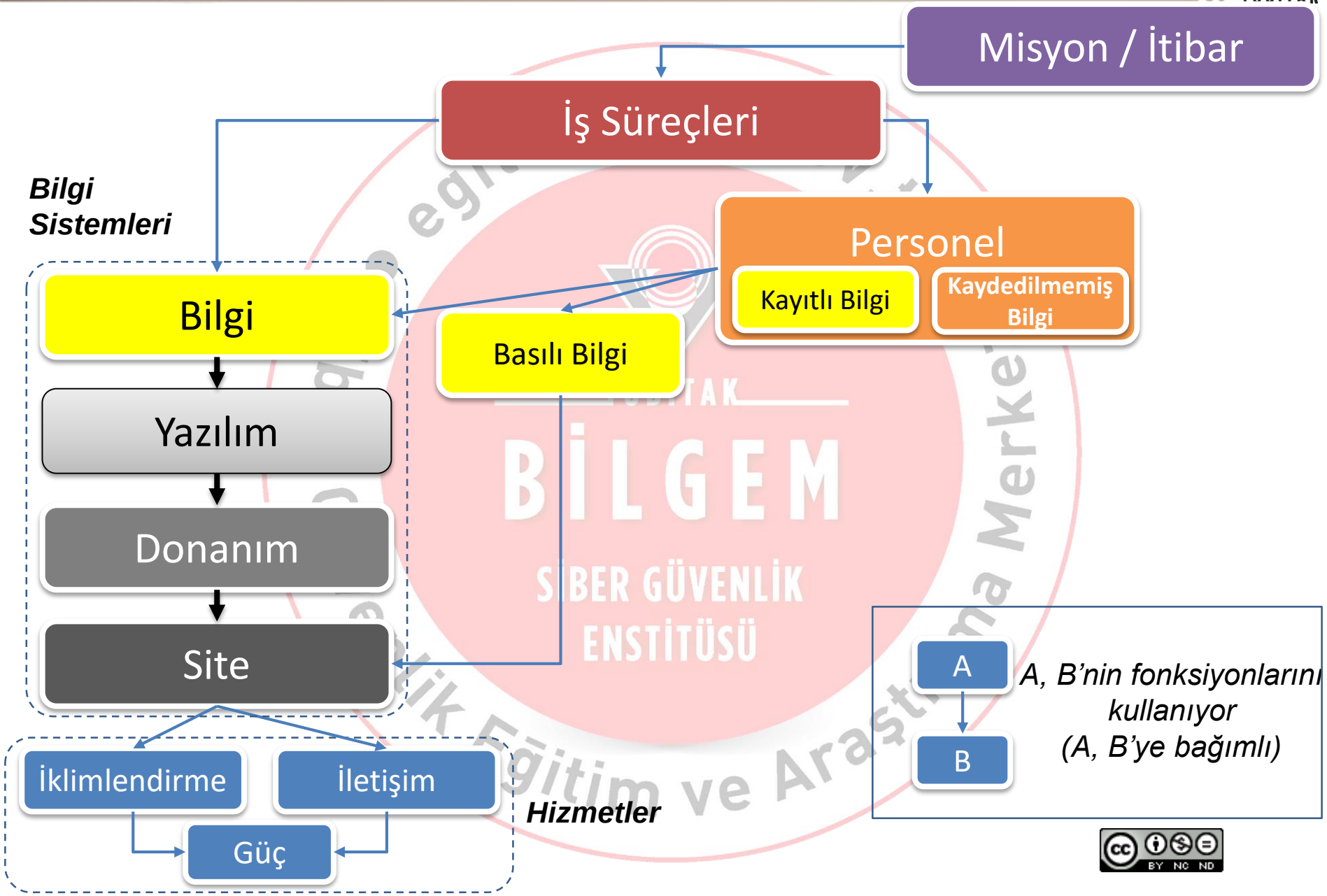
Risklerin Belirlenmesi

İş: Kapsamdaki bilgi ve ilgili varlıkların gizlilik, bütünlük ve erişilebilirliğini etkileyecek riskleri belirlemek

Örneğin:

- **Varlıkların ve** varlık **sahiplerinin** belirlenmesi
- Varlığa yönelik **tehditlerin** belirlenmesi
- Bu tehditlerin kullanabileceği **açıklıkların** belirlenmesi
- Tehdit ve açıklıkların varlığın gizlilik, bütünlük veya erişilebilirliğine **etkisinin belirlenmesi**

Varlıklar (ISO 27005, Annex B)



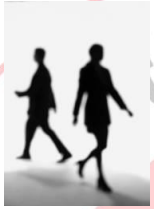
Varlık Sahipleri

- **Varlık sahibi** = Birey veya birim

  Varlığın üretilmesinden, geliştirilmesinden, bakımından, kullanımından ve güvenliğinden sorumludur.
  - Varlığın ***sınıflandırılması***
  - Erişim haklarının belirlenmesi ve ***gözden geçirilmesi***

  İş sürecine, bir uygulamaya veya veri setine sahip atanabilir.

Varlık Envanteri



Personel	Sahibi	Değeri	Konum
Bilgi (Elektronik/Basılı)	Sahibi	Değeri	Konum
Yazılım varlıkları	Sahibi	Değeri	Konum
Donanım Bilgisayar, Modem, vb.	Sahibi	Değeri	Konum
Hizmetler	Sahibi	Değeri	Konum

Uygulama-4

Uygulama-3'te seçilen kurumsal iş sürecinin;

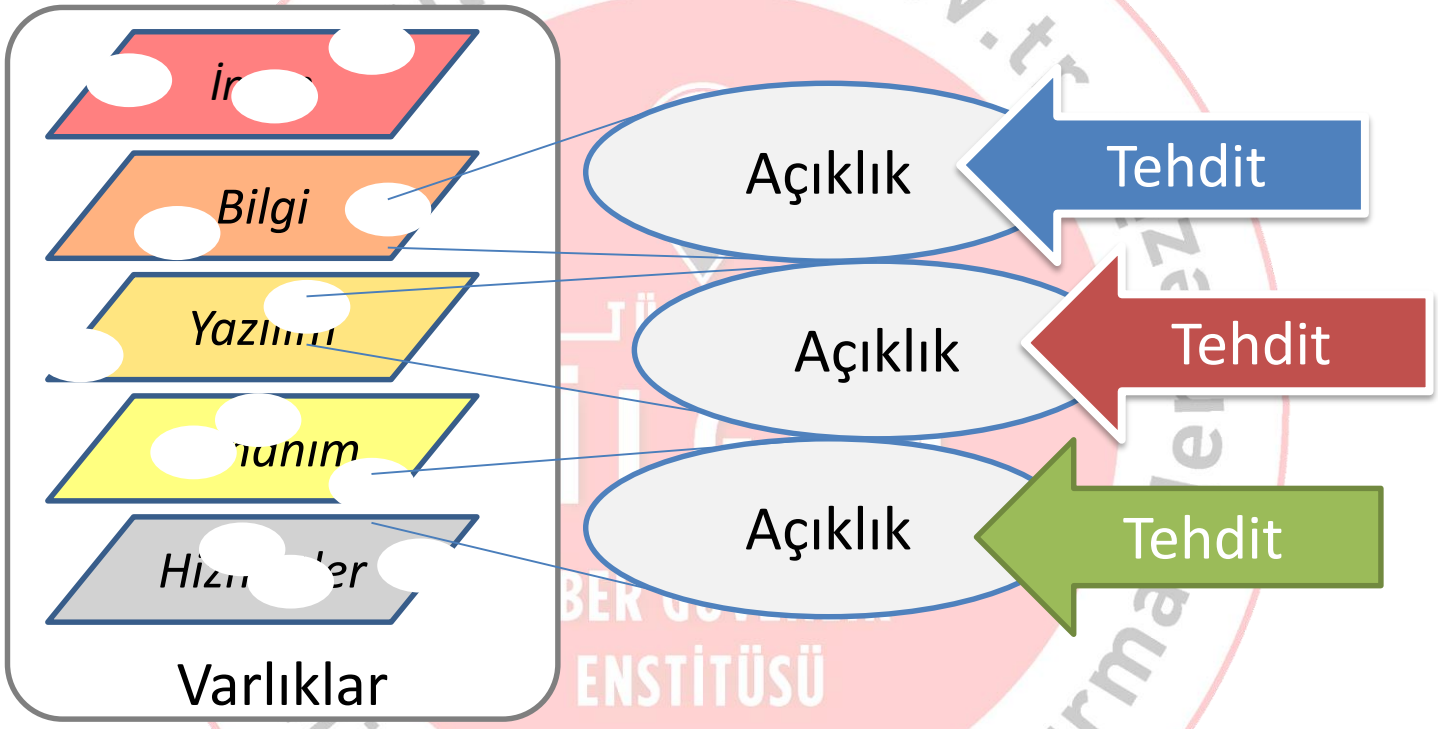
- Bilgi
- Yazılım
- Donanım, altyapı
- İnsan
- Alınan hizmet

varlıklarını ve varlık sahiplerini listeleyiniz.

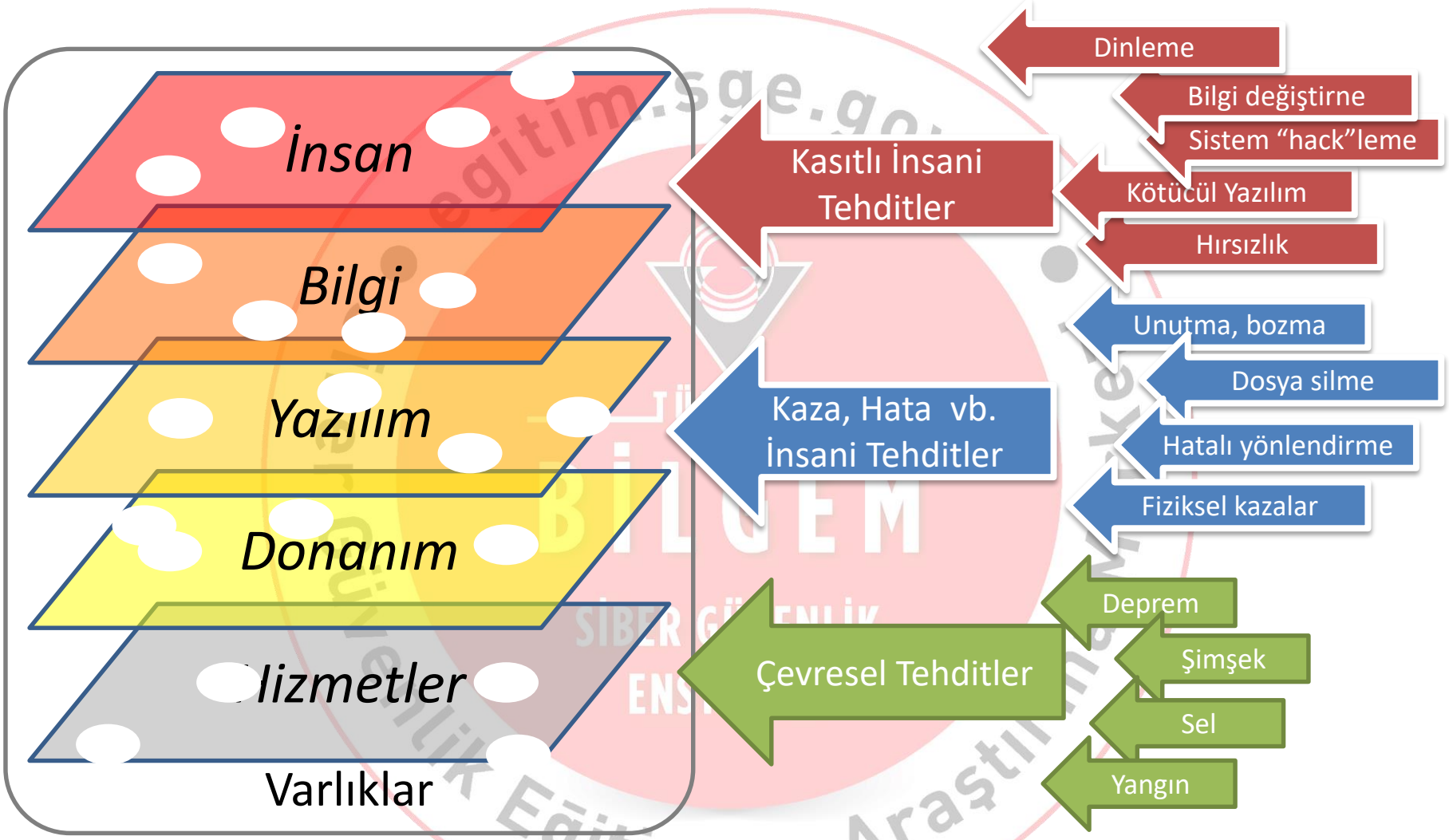
Açıklık – Tehdit – Karşı Önlem

- **Açıklık:** Varlıklarda bulunan kusurlardır.
- **Tehdit:** Varlıklardaki açıklıkları kullanarak zarar veren etkenlerdir.
- **Karşı Önlem:** Riski azaltmak amacıyla alınan tedbirler.
  - Varlığın değerini düşürücü
  - Açıklığın derecesini düşürücü
  - Tehdidin etkisini/olma ihtimalini düşürücü

Tehditler ve Açıklıklar



Tehditler*



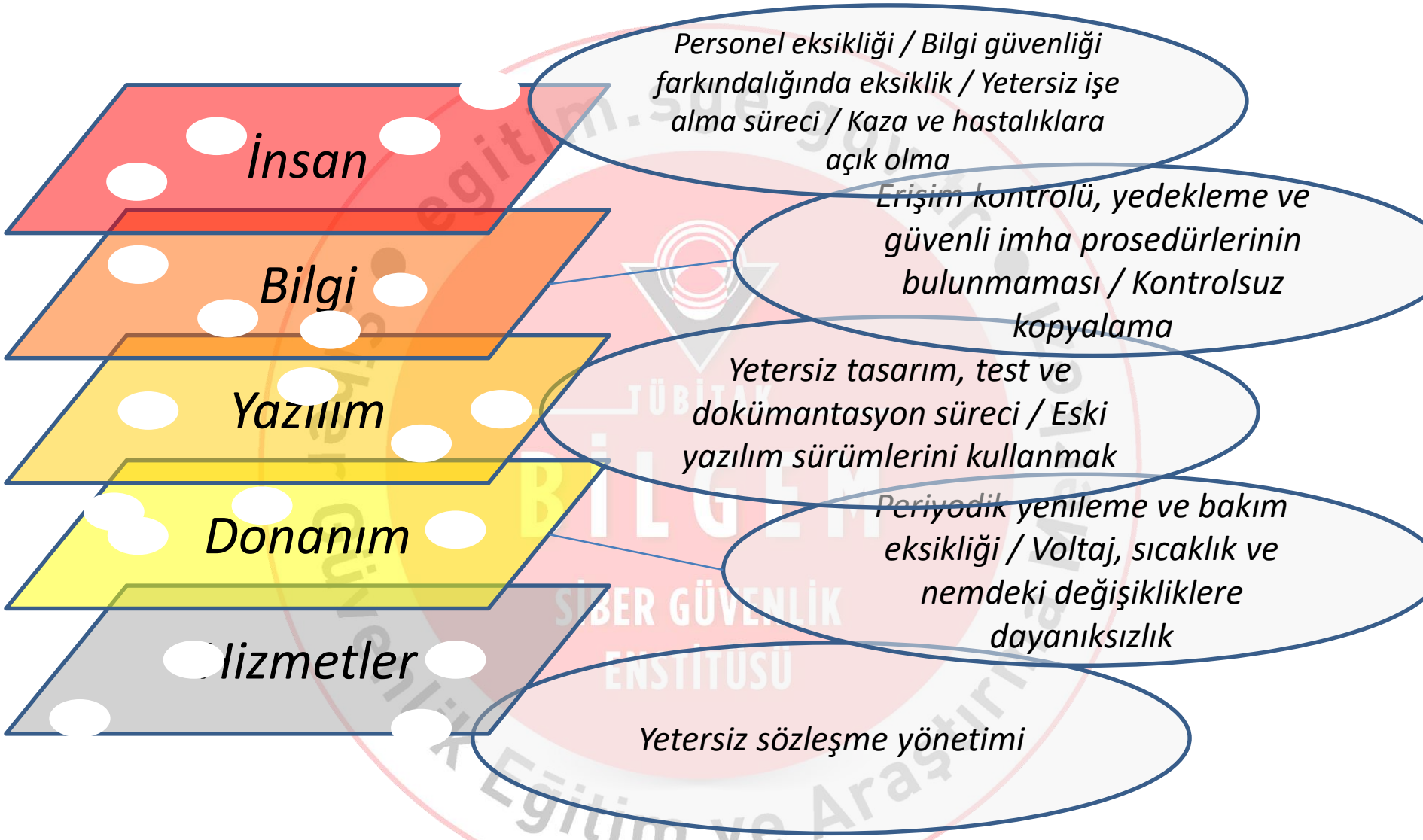
(*) ISO/IEC 13335-1:2004 - Concepts and models for information and communications technology security management – Threats.

Uygulama-5

- Tehdit Listesi dosyasını inceleyiniz.

- Uygulama-4 ’te listelenen bilgi varlıklarına yönelik *tehditleri* aynı dosyada ilgili varlığın karşısına kaydediniz.

Açıklıklar*



(*) ISO/IEC TR 13335-3 - Techniques for the Management of IT Security – Annex D - Common Vulnerabilities

Uygulama-6

- Açıklık Listesi dosyasını inceleyiniz.

- Uygulama-5'te belirlediğiniz tehditlerin kullanabileceği *açıklıkları* aynı dosyaya kaydediniz.

Uygulama-7

Uygulama-5'de belirlenen tehdit ve açıklıkların bilgi varlıklarının

- Gizlilik,
- Bütünlük ve
- Erişilebilirliğine

etkisini belirleyiniz.

Risklerin Analizi ve Derecelendirmesi

- Güvenlik ihlalinin oluşması sonucunda kurumun karşılaşacağı **zararın belirlenmesi**
- Güvenlik ihlalinin oluşma **olasılığın**ın **belirlenmesi**
- Riskin hesaplanması
- Riskin, önceden tanımlanmış olan risk ölçeğine göre değerlendirilmesi

Risk Derecelendirme

Pollice Verso (Thumbs Down) - Jean-Léon Gérôme

Tartışma-3

Zararın belirlenmesinde kullanılabilecek ölçek gözden geçirilir ve tartışmaya açılır.

Zarar Belirleme Ölçeği

Zararın Etki Derecesi		Zararın Açıklaması
4	Çok yüksek	•Kurumun itibarının kaybolması •Hayati tehlike / can kaybı •Çok yüksek düzeyde maddi kayıp
3	Yüksek	•Kurumun itibarının ciddi düzeyde zarara uğraması •Belirgin hayati tehlike / can kaybı olasılığı •Yüksek düzeyde maddi kayıp
2	Orta	•Kurumun itibarının orta düzeyde zarara uğraması •Orta düzeyde hayati tehlike •Orta düzeyde maddi kayıp
1	Düşük	•Kurumun itibarının hafif düzeyde zarara uğraması (durum kurtarılabilir) •Düşük düzeyde hayati tehlike •Düşük düzeyde maddi kayıp

Uygulama-8

Güvenlik ihlallerinin oluşması halinde kurumun karşılaşacağı **zararı belirleyiniz.**

Tartışma-4

Olasılığın belirlenmesinde kullanılabilecek ölçek gözden geçirilir ve tartışmaya açılır.

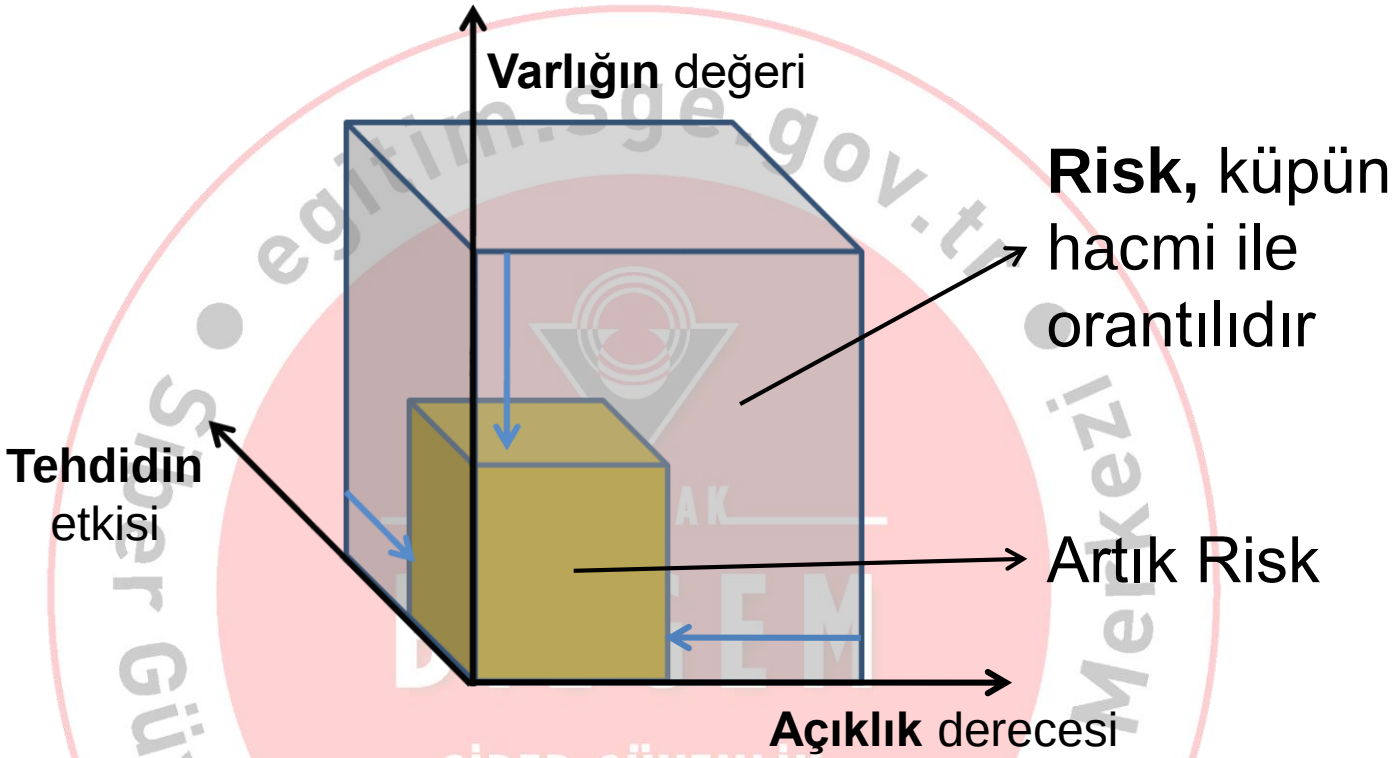
Tehdit Olasılığı Belirleme Ölçeği

Olasılık Değeri	Gerçekleşme sıklığı	Değer Adı
5	Günde en az bir defa	ÇY (Çok yüksek)
4	Haftada en az bir defa	Y (Yüksek)
3	Üç ayda bir defadan çok	O (Orta)
2	Yılda bir defadan çok	D (Düşük)
1	Yılda bir defadan az	ÇD (Çok düşük)

Uygulama-9

Güvenlik ihlallerinin oluşma **olasılıklarını belirleyiniz.**

Riskin Hesaplanması



Risk = F(Varlık, Açıklık, Tehdit)

Zarar x Olasılık

Uygulama-10

Risk değerlerini belirleyiniz.

Terminoloji

Kabul edilebilir risk:

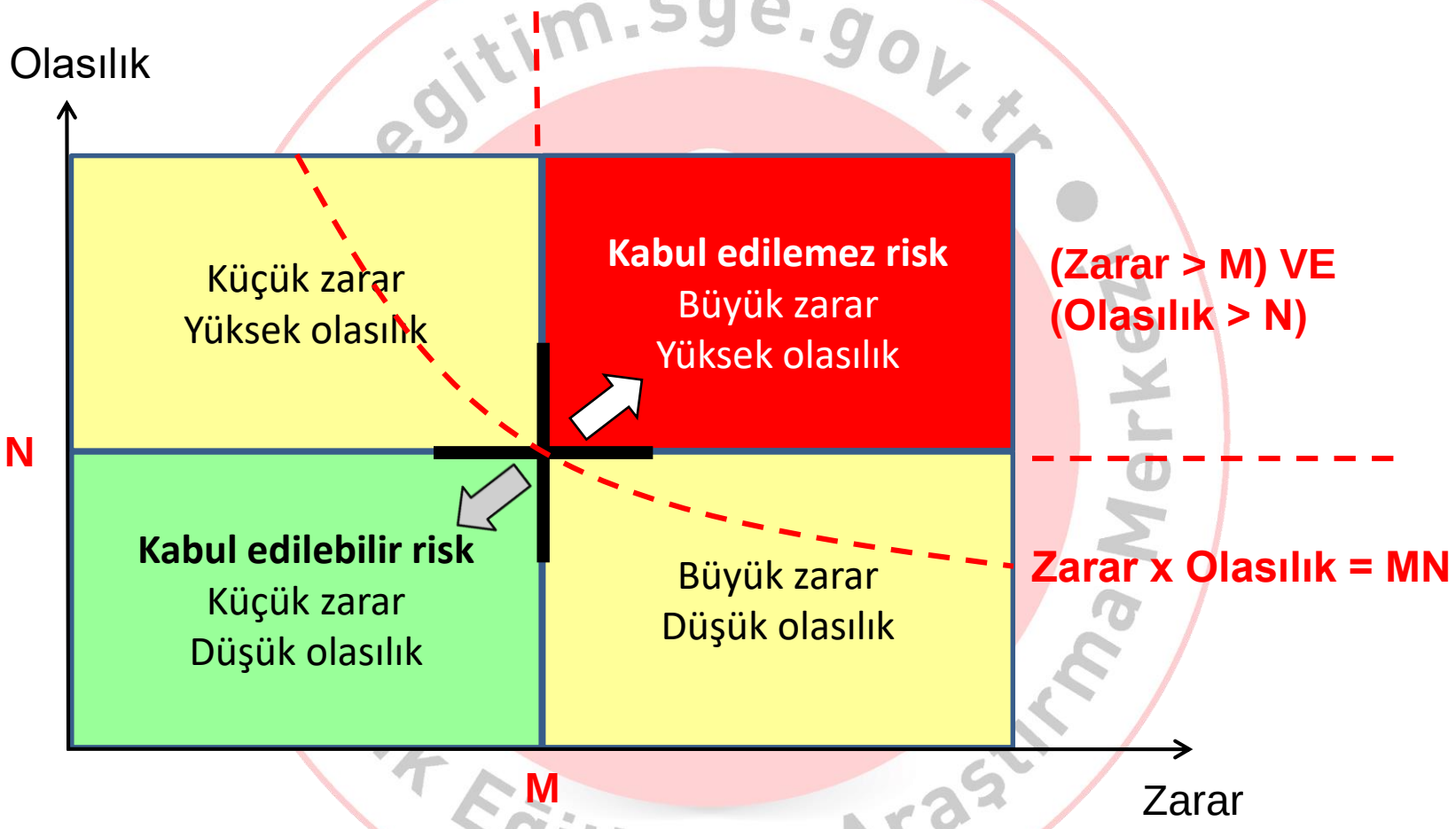
Belli bir sistem veya varlık için kurumun güvenlik ihtiyaçları çerçevesinde kabul edebileceği risk derecesi.

Risk Derecelendirme Kriterleri

- **Kabul edilebilir risk** seviyesi belirlenirken
  - Yasal gereksinimler
  - Müşteri ve kontrat gereksinimleri
  - Güvenlik ihtiyaçları
  - Bütçe / Maliyet
  - Uygulama kolaylığı

  göz önünde bulundurulur.

Risk Derecelendirme



Tartışma-5

- Risk değerleri gözden geçirilerek kabul edilebilir risk seviyesinin ne olabileceği tartışılır.

Risk İşleme Seçeneklerinin Tanımlanması ve Derecelendirilmesi

- Risk işleme seçenekleri
  - Uygun kontrollerin uygulanması
  - Risk kabulü
  - Riskten kaçınma
  - Riski transfer etme

Risk Değerlendirme

- Risk analizi ve risk derecelendirme süreçlerinin bütünü ...
- Risk değerlendirmesi sonucunda:
  - Kabul edilebilir risk seviyesi belirlenir
  - Hangi risk için ne yapılacağı belirlenir
    - Risk işleme
    - Diğer seçenekler
  - Riskler kritiklik sırasına göre sıralanır
  - Azaltılacak risk kalemlerinin öncelikleri belirlenir

Kontrollerin Seçimi

- Risk kabul etme kriterleri dikkate alınır.

- Kontroller 27001 Ek-A'da…
- Mevcut kontroller gözden geçirilir
- İlave kontroller uygulanabilir

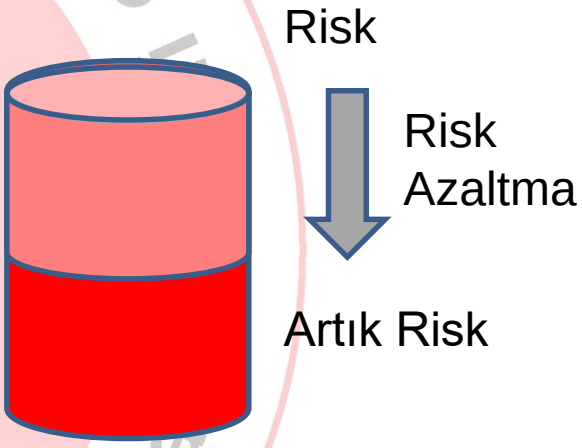
Kontrollerin Seçilmesi

- Aşağıdakileri sağlayacak kontroller uygulayın:
  - Risk ortaya çıkarsa olası etkilerinin azaltılması *(Kriptolama ve yedekleme…)*
  - Riske yol açan tehdidin açıklığı kullanma olasılığının azaltılması *(Erişim kontrolü önlemlerinin hayata uygulanması…)*
  - İstenmeyen durumların tespit edilmesi, bu olaylara tepki ve kurtarma

    (Yedekten geri dönme prosedürleri…)

Artık Risk

- Risk işleme sonrasında kalan risk
- Artık riski değerlendirin (Kabul edilebilir / edilemez…)
  - Daha fazla kontrol uygulayın
  - Kabul etmek zorunda kalınabilir
- **Risk sahibinin onayı gerekir.**



Uygulanabilirlik Bildirgesi

Kontrollerin amaçlarını ve BGYS kapsamında **kuruluşta uygulanan kontrolleri** tanımlayan yazılı bildirgedir.

- İçeriği:
  - Seçilen kontroller, seçilme nedenleri ve ilgili dokümanlar
  - Seçilmeyen kontrollerin gerekçeleri

Uygulanabilirlik Bildirgesi

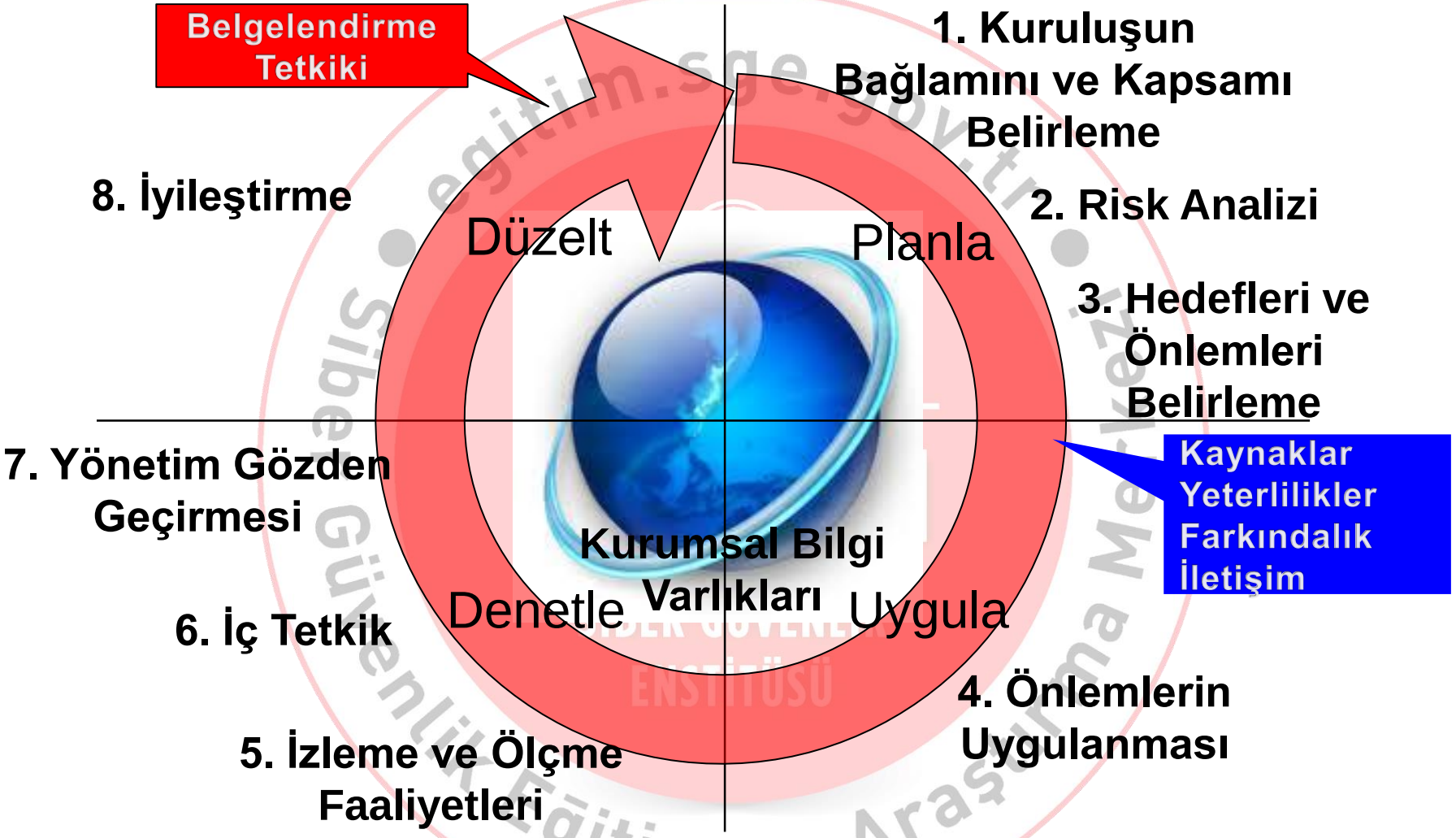
Bir kontrol neden uygulanmadı:

- Riskli olabilir
- O andaki bütçe yetersiz
- Çevresel şartlar
- Teknolojik kısıtlar
- Kurum kültürü
- Süre…
- Uygulanamaz (N/A)
- Diğer

Tartışma-6

Örnek Uygulanabilirlik Bildirgesi'ni inceleyip tartışalım.

ISO 27001 BGYS Süreci, özet



Risk İşleme Planı

Tanımlanan risklerin kabul edilebilir seviyeye getirilmesi için,

- Her bir risk ile ilgili olarak:
- **Hangi** faaliyeti **kimin** yapacağını tanımlayan

detaylı bir programdır.

Risk İşleme Planı

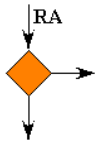
- Her risk için:
  - Uygulanacak kontrol(ler) / yapılacak iş
  - Sorumluluklar
  - Uygulama planı (zaman kısıtları / öncelik / kritiklik)
  - Açıklama
    - Gerekli kaynaklar (finansman, vb.)
    - Eğitim planlaması
- Yaşayan bir dokümandır (yeni riskler, yeni kontroller, sorumluluklar, vb…)

Risk İşleme Planı

Bilgi Varlığı/Açıklık	Tehdit	Risk	Faaliyet	Sorumlu	Tarih
Kurumun WEB Sitesi	Servis dışı bırakma saldırıları	**WEB sitesinin servis veremez duruma düşmesi** - maddi kayıp	İnternet Servis Sağlayıcı ile görüşme ve hizmet satın alımı	***Bilgi İşlem + Satın Alma***	2 Ay
USB belleklere ilişkin politika ve eğitim eksiği / taşıma kolaylığı	İnsani zayıflıklar	**Belleklerin kurum dışında kaybolması** - kurumsal bilginin açığa çıkması	Politika , prosedür + eğitim	***Bilgi Güvenliği Şubesi***	1 Ay
Sunucu sabit diskleri / sınırlı dayanıklılık	Sistem odası sıcaklığında ve nem düzeyinde dalgalanmalar	**Sabit disk arızası -** kurumsal bilginin kaybedilmesi	Klima sisteminin güçlendirilmesi	***Bilgi İşlem + Satın Alma***	Gelecek bütçe yılı
Güvenlik duvarı kural listesi	Sistem yöneticilerinin iş yoğunluğu / prosedürsüz çalışması	**Personel hatası -** sunucuların Internet'ten saldırıya açık hala gelmesi.	1.İlave personel alımı 2. Prosedür hazırlanması	***1.Kurum yöneticisi*** ***2.Bilgi İşlem***	6 Ay

Risk Yönetimi Özeti

Risk Değerlendirme

	Risk Analizi	• Risk (ham risk değeri) • Varlık, açıklık, tehdit • Risk modeli • Hesaplama • Matematik (örn: olasılık hesabı) • Nitel, Nicel yöntemler • Yazılımlar • Risk=F (Varlık, Açıklık, Tehdit)
	Risk Derecelendirme	• Riskleri sıralandırma • Kabul edilebilir risk seviyesi • Karar verme – Risk işleme – Diğer risk kontrolleri
	Risk İşleme	• Para • Hizmet - mal alımı • Karşı önlem • Artık risk
	Risk Yönetimi 	• Üst yönetim desteği • Süreç • Süreklilik • Girdiler – Çıktılar (Risk - yönetilebilir risk içeren süreçler)

6.2 Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama

- Kuruluş, uygun işlevler ve seviyelerde bilgi güvenliği amaçlarını tesis etmelidir.
- Kuruluş bilgi güvenliği amaçları ile ilgili yazılı bilgileri muhafaza etmelidir.

Uygulama - 11

ISO 27001 Standardına göre:

- Belirlenen bilgi güvenliği amaçları neyi sağlamalı?
- Bilgi güvenliği amaçlarına ulaşmayı planlarken neleri belirlemeli?

Örnek bir amaç için yöntem ve hedef belirlenir.

Uygulama - 11

Amaç	Kuruluşta bilgi güvenliği bilincini arttırmak
Yöntem	Periyodik bilgi güvenliği farkındalık eğitimleri düzenlemek
Hedef	
Kaynaklar	
Sorumlular	
Tamamlanma Tarihi	
Sonuç Değerlendirme	

6.2 Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama

Amaç	Kuruluşta bilgi güvenliği bilincini arttırmak
Yöntem	Periyodik bilgi güvenliği farkındalık eğitimleri düzenlemek
Hedef	Çalışanların %90'ının periyodik bilgi güvenliği farkındalık eğitimleri alması
Kaynaklar	Eğitmen, eğitim içeriği, organizasyon
Sorumlular	BGYS Sorumlusu, İK Birim Müdürü
Tamamlanma Tarihi	Her yıl Haziran ve Aralık ayları, oryantasyon süreci
Sonuç Değerlendirme	Her yıl Ocak ayında, katılım listeleri üzerinden katılım yüzdesinin hesaplanması

Uygulama-11

Amaç	İş süreçlerinin elektrik kesintilerinden etkilenmemesi
Yöntem	Elektrik kesintisi anında UPS'in yükü üzerine alması, periyodik test yapılması
Hedef	
Kaynaklar	
Sorumlular	
Tamamlanma Tarihi	
Sonuç Değerlendirme	

6.2 Bilgi güvenliği amaçları ve bu amaçları başarmak için planlama

Amaç	İş süreçlerinin elektrik kesintilerinden etkilenmemesi
Yöntem	Elektrik kesintisi anında UPS'in yükü üzerine alması, periyodik test yapılması
Hedef	%100
Kaynaklar	Sistem odasının ve binanın kesintisiz güç kaynakları
Sorumlular	İdari İşler Birim Müdürü
Tamamlanma Tarihi	Her ayın 1. gününde test edilmesi
Sonuç Değerlendirme	Haziran ve Aralık aylarında bilgi güvenliği olayları kayıtlarından oranın (alma sayısı/ kesinti sayısı) hesaplanması, yapılan yıllık test sayısı

7. Destek

BGYS'yi uygulamak ve işletmek için neler gerekir?

- Bütçe
- Yeterlilikler
- Farkındalık
- İletişim

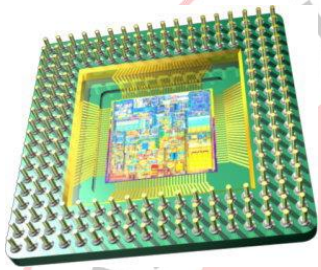
Dokümantasyon

Politika	Ne yapacağım?
Prosedür	Nasıl yapacağım?
Kayıt **(= Delil)**	Ne yapıldı / Ne oldu?

- Belirlenen güvenlik önlemleri **politika ve prosedürlere** dönüştürülür. (Gözden geçirme ve geliştirmeye açıktır)

- **Kayıtlar** aracılığı ile önlemlerin çalışması izlenir. (Kayıtlar <u>değiştirilemez</u>).

Politika ile Yazılım arasındaki farklar

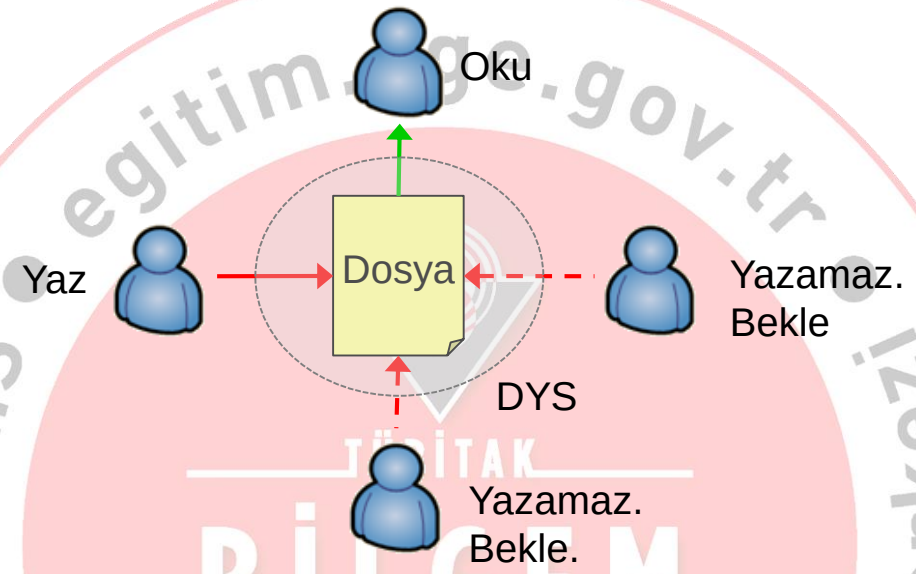


Yazılım	Politika / prosedür
CPU'da çalışır.	İnsanlar tarafından uygulanır.
(+) CPU'nun yazılımı beğenmemesi tanımlı değildir. Mutlaka çalıştırır.	(-) İnsanlar tarafından benimsenmesi gerekir. Yoksa rafta kalır.
(-) CPU yazılımdaki hatayı bulamaz / düzeltemez.	(+) Personel politika veya prosedürdeki hatayı belirleyebilir / düzeltebilir.

İyi Politika / Prosedür

- *Çok uzun olmamalı ("İnsan okuyacak ☺")*
- *Talep ettikleri makul olmalı*
- *Tutarlı olmalı (bir işi bir yerde tanımla!)*
- *Orta derecede detaya girmeli*
  - *Çok detaylı olduğu zaman boşluklar oluşur.*
  - *Az detaylı olduğu zaman işe yaramaz.*
- *Okunaklı / biçim olarak çekici olmalı*

Doküman Yönetim Sistemi



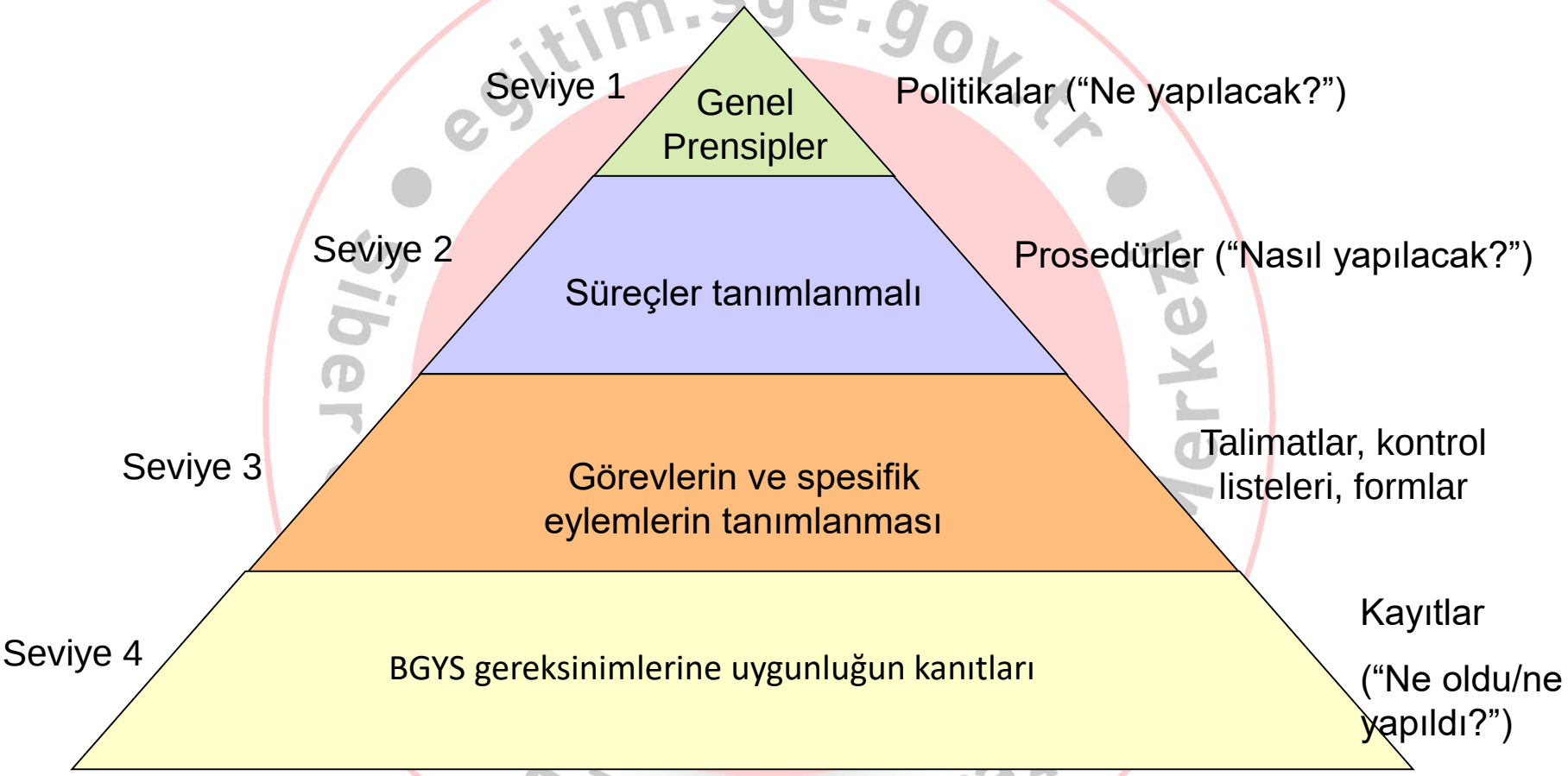
- Çok yazarlı dosyalara sıralı erişim yapılması
- Dosyaların yerinin belli olması (Dosyalar kişisel bilgisayarlara dağılıp gitmesin)
- Revizyon kontrolü ve eski revizyonlara erişim
- Erişim kontrolü ve yedekleme

BGYS Dokümanları

- BGYS Kapsamı
- Bilgi güvenliği politikası
- Bilgi güvenliği hedefleri
- Risk değerlendirme metodu
- Risk değerlendirme sonuçları
- Risk işleme planı
- Uygulanabilirlik bildirgesi
- Bilgi güvenliği amaçları
- Performans izleme ve ölçme tanımları

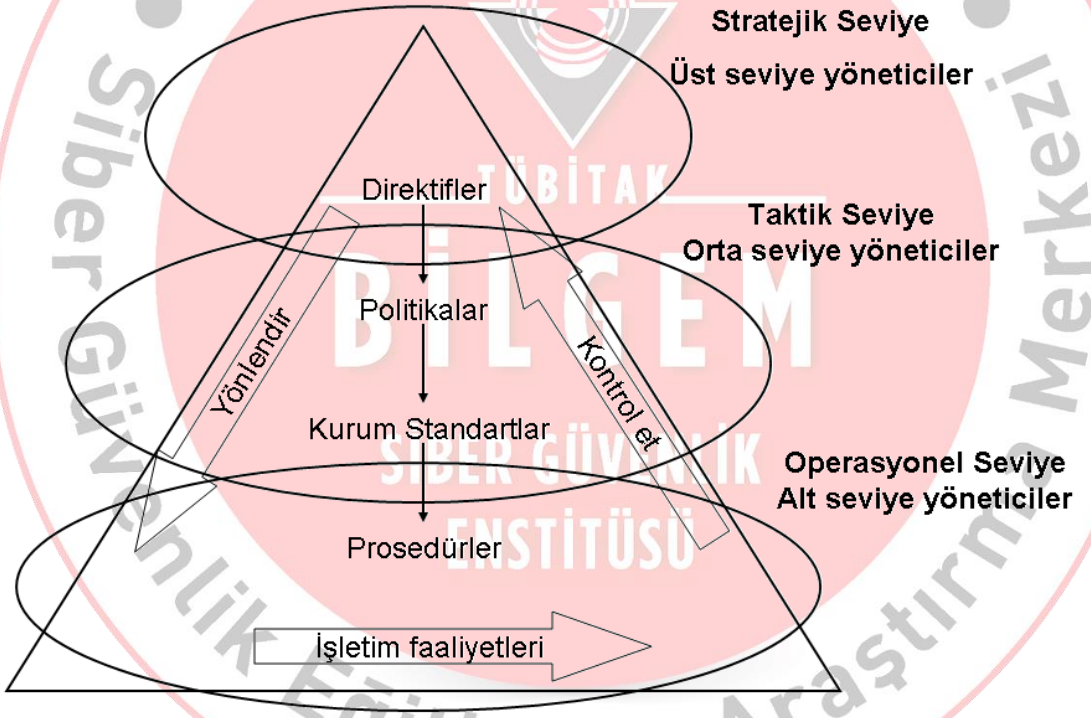
+ Prosedürler
+ Kayıtlar

BGYS Dokümantasyonu



Seviye 1 - Politikalar

- Bilgi güvenliği için yönetim mekanizmalarının harekete geçirilmesi ve gerekli desteğin sağlanması.
- Yönetim politikayı belirler ve politikaya destek sağlar



Seviye 2 - Prosedürler

- Prosedürler
  - Uygulanan kontrollerin gerektirdiği prosedürler
    - Güvenlik süreçleri ile ilgili kim, ne, ne zaman ve nerede sorularının cevapları tanımlanmalı
- Örnek prosedürler;
  - Düzeltici/önleyici faaliyet prosedürü
  - Yedekleme prosedürü
  - Sistem işletme prosedürleri
  - Risk değerlendirme prosedürü
  - Risk işleme prosedürü

Seviye 3

- İş talimatları, kontrol listeleri ve formlar
  - Spesifik talimatların veya eylemlerin detaylarının açıklamaları ve nasıl uygulanacakları listelenmeli
  - Ayrıntılı iş talimatları, formlar, akış diyagramları, servis standartları ve sistem kullanım kılavuzları bu seviyede bulunur

Seviye 4 - Kayıtlar

- Kayıtlar
  - **Yasalardan ve sözleşmelerden** kaynaklanan kayıt yükümlülükleri
  - **Kurumsal** bilgi güvenliği **politikaları**nın uygulandığını gösteren kayıtlar
  - Kayıtlar **denetimlere girdi** oluşturacaktır
  - BGYS ile ilgili tüm güvenlik olaylarına dair kayıt tutulur
  - Hukuk/kurum içi disiplin süreçlerinin devreye girdiği durumlarda, **Kayıt = Delil**

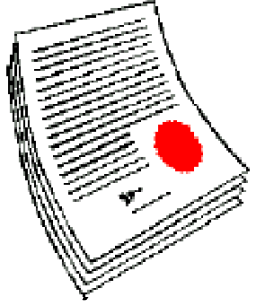
Seviye 4 - Kayıtlar

- **Örnekler:**
  - *Ziyaretçi defteri*
  - *Erişim yetkilendirme formları*
  - *İşletim sistemi güvenlik kayıtları*
  - *Güvenlik duvarı logları*
  - *Kritik bilgiye erişim logları*
  - *Diğer veritabanı erişim logları*
  - *Sistem yöneticilerinin yaptığı işlemlerin logları*

7.5 Yazılı Bilgiler

a) Bu standardın gerektirdiği yazılı bilgiler
b) Kuruluş tarafından bilgi güvenliği yönetim sisteminin etkinliği için gerekli olduğu belirlenen yazılı bilgiler

7.5 Yazılı Bilgiler



- Dokümanların kontrolü için bir prosedür bulunmal prosedürdeki yönetim eylemleri:
  - Yayınlanmadan önce dokümanları uygunluk açısından onaylama
  - Gerektiğinde dokümanları gözden geçirme, güncelleme ve tekrar onaylama
  - Doküman sürüm değişikliklerinin ve güncel sürümün tanınmasını sağlama
  - İlgili dokümanların en son sürümlerinin kullanım noktalarında kullanılabilir olmasını sağlama
  - Yürürlükte olmayan dokümanların istenmeden kullanımını engelleme

7.5 Yazılı Bilgiler

- Kayıt alma mekanizmaları kurulmalı ve sürdürülmeli:
  - Kanıt: BGYS'nin etkin çalıştığına ilişkin
- Kayıtlar korunmalı ve yönetilmeli
- Yasal ve düzenleyici hükümleri dikkate almalı
- Yazılı bilgilerin:
  - Tanınması (identification)
  - Depolanması (storage)
  - Korunması (protection)
  - Bulup getirilmesi (retrieval)
  - Muhafaza zamanı (retention time)
  - Düzenleme zamanları (disposition of records)

  için yöntem belirlenmeli ve dokümante edilmelidir.

8. İşletim

- Risk işleme planı
- Bilgi güvenliği amaçları
- Belirli aralıklarda veya önemli değişiklik olduğunda risk değerlendirme

9. Bilgi Güvenliği Performansını Değerlendirme

- **BGYS'nin ve kontrollerin etkinliğini** izleme, ölçme, analiz etme ve **değerlendirme** (9.1)
- BGYS **iç denetimler**inin planlanan aralıklarla yapılması (9.2)
- BGYS'nin **yönetim tarafından gözden geçirilmesi** (9.3)

İzleme, ölçme, analiz ve değerlendirme

- Örnek metrikler:
  - **Yama yüzdesi** = (yüklenmiş yamalar / (yüklenmiş yama + eksik yama)) * 100
  - Kritik bilginin şifrelenmesinde kullanılan **anahtar uzunluğu**
  - **Yedeklenme yüzdesi** = (yedeklenmiş veri (GByte) / tüm veri (GByte)) * 100
  - Bilgi güvenliği teknik **eğitiminin süresi**
  - Bilgi güvenliği farkındalık **eğitimine katılan personel sayısı**
  - **Eğitimlerin periyodu**
- Kontroller aracılığı ile işlenmesi beklenen ***risklerin izlenmesi ve sayılması.***

9.2 BGYS İç Denetimleri

- Kurum içinden veya dışından bir ekip tarafından **kurum adına** gerçekleştirilir.
  - Denetlenen unsurlar:
    - Süreçler, prosedürler, güvenlik önlemleri,
  - Denetim içeriği:
    - Yasal düzenlemelere uyum
    - Bilgi güvenliği gereksinimlerine uyum
    - BGYS'nin etkinliği ve sürekliliği
    - Beklentileri karşılaması
  - Denetim programı:
    - Bir önceki denetim sonuçları →Denetlenecek alanların önemi
    - Denetim kriterleri , denetim yöntemleri

9.2 BGYS İç Denetimleri

- Nesnellik ve tarafsızlık
  - *İç denetçiler kurum içinden ise **kendi çalışmalarını denetleyemezler.***
- İç denetim prosedürü:
  - Denetim planlaması
  - Denetim gerçekleştirilmesi
  - Sonuçların raporlanması
  - Kayıtların tutulması
- Denetlenen alandan sorumlu yönetim:
  - Uygunsuzlukları gidermek için önlemlerin alınması

9.3 Yönetimin Gözden Geçirmesi

- **Kuruluşun yönetimi,**
  - **Planlı aralıklarla BGYS'yi gözden geçirir.**
  - Amaç, BGYS'nin uygunluğunu, doğruluğunu ve etkinliğini sağlamaktır.
  - Bilgi güvenliği politikası ve bilgi güvenliği hedefleri de gözden geçirilir.
  - Gözden geçirme çıktıları kayıt altına alınmalıdır.

9.3 Gözden Geçirme Girdisi

- Bir önceki yönetim gözden geçirmesi sonucunda gerçekleşmesi gereken eylemlerin takibi
- BGYS'yi ilgilendiren iç ve dış konulardaki değişiklikler
- Bilgi güvenliği performansı:
  - *Düzeltici faaliyetlerin durumu*
  - *İç tetkik raporu*
  - *İzleme ve ölçme sonuçları*
  - *Bilgi güvenliği amaçları*
- İlgili bölümlerden gelen geri bildirimler
- Risk değerlendirme sonuçları ve risk işleme planı
- Sürekli iyileştirme için fırsatlar

Örnek Gözden Geçirme Çıktısı

- Risk işleme planının güncellenmesi
- Bilgi güvenliği ve BGYS'yi etkileyen değişiklerle ilgili prosedürlerin güncellenmesi
- Gereken kaynakların ayrılması
- Kontrol etkinliğini ölçme metotlarındaki değişiklikler

10. İyileştirme

- Uygunsuzluk ve Düzeltici Faaliyet (10.1)
  - Uygunsuzluğa tepki verilmesi
  - Tekrarın önlenmesi – kök sebebin bulunması
  - İyileştirmenin etkinliğinin gözden geçirilmesi

- Sürekli İyileştirme (10.2)
  - Uygunluk
  - Yeterlilik
  - Etkinlik

10.1 Uygunsuzluk ve Düzeltici Faaliyetler

- BGYS de ortaya çıkan problemlerin yeniden yaşanmaması için **“kök sebebin” ortadan kaldırılması.**
  - **Aynı hatayı tekrarlamayın.** Hataya neden olan açığı bulup ortadan kaldırın.
  - *Yazılımda bulunan hatayı değil sürecin hataya neden olan eksiklerini giderin (dokümantasyon, test, vb.)*
- Prosedür uyarınca gerçekleştirilir.
  - DF’nin açılması, izlenmesi ve kapatılması?
  - DF’lere ilişkin kayıt “bitiş tarihi”, “sorumlu”, “durum” vb..

Uygulama-12

Aşağıdaki durum için düzeltici faaliyet belirlenir.

“ Bilgi güvenliği hedeflerinde, personelin yıllık farkındalık eğitimlerine katılımında hedeflenen oran %90 iken, katılım %65 oranında olmuştur.”

Düzeltici faaliyet örneği

Konu	Farkındalık eğitimlerine katılım
Durum ve Bulgu	Personelin yıllık farkındalık eğitimlerine katılımında hedeflenen oran %90 iken, %65 oranında olmuştur.
Kök Sebepler	
Önerilen Çözüm	
Yapılan Çalışma	
Çalışmayı Yapan	

Düzeltici faaliyet örneği

Konu	Farkındalık eğitimlerine katılım
Durum ve Bulgu	Personelin yıllık farkındalık eğitimlerine katılımında hedeflenen oran %90 iken, %65 oranında olmuştur.
Kök Sebepler	1. Bilgi güvenliği eğitimlerinin kurum için önemi anlaşılamıştır. 2. Eğitim tarihleri haziran ayında kullanılan yıllık izinlere denk gelmiştir. 3. Eğitim duyurusunun geç yapıldığına dair geri bildirim alınmıştır, personel planlı işlerini aksatmamak adına katılamamıştır.
Önerilen Çözüm	1. Sn. Genel Müdür'ün eğitimlere katılması 2. Eğitimlerin Haziran yerine Mayıs ayında düzenlenmesi 3. Eğitim duyurularının eğitimden en az 15 gün önce yapılması
Yapılan Çalışma	Tarihler Sn. Genel Müdür ile koordine edilerek, eğitimlerin 15 Mayıs'ta yapılması, 30 Mart tarihinde duyurulması planlanmıştır. Yıllık eğitim programı güncellenmiştir.
Çalışmayı Yapan	BGYS Sorumlusu, İK Eğitim Sorumlusu

Özet

Bilgi Güvenliği Yönetim Sistemi

- Sadece kurulum ve uygulama değildir
- İşletilmesi, izlenmesi, gözden geçirilmesi, geliştirilmesi gerekir
- Kurumda yeni yapılanmalar gerektirir
  - Bilgi güvenliği koordinasyon ekibi
  - Rol ve sorumluluklar
  - Güvenlik bilinçlendirme faaliyetleri
- Dokümantasyon ihtiyaçları:
  - Politikalar
  - Standartlar
  - Kılavuzlar
  - Prosedürler
  - Kayıtlar

Başvuru Dokümanları

- Ulusal Bilgi Güvenliği Kapısı BGYS kılavuzları: (http://www.bilgiguvenligi.gov.tr)
  - Bilgi Güvenliği Yönetim Sistemi Kurulum Kılavuzu
  - BGYS Kapsamı Belirleme Kılavuzu
  - BGYS Risk Yönetim Süreci Kılavuzu
  - Bilgi Güvenliği Politikası Oluşturma Kılavuzu
  - Erişim Kontrol Politikası Oluşturma Kılavuzu
  - Bilgi Güvenliği Bilinçlendirme Süreci Oluşturma Kılavuzu
  - Veri Yedekleme Kılavuzu
  - ISO IEC 27001 Denetim Listesi
  - Varlık Envanteri Oluşturma Kılavuzu
  - Bilgi Sistemleri Kabul Edilebilir Kullanım Politikası Oluşturma Kılavuzu

ISO 27002 (27001 Ek.A) Güvenlik Önlemleri

ISO/IEC 27002:2013 > Standardın Yapısı

1. KONTROL ALANI - #

1.1 Güvenlik Kategorisi – 1

Güvenlik kategorisi için tanım ve kontrol hedefi tanımı

1.1.1 Kontrol - 1

- Tanım
- Uygulama Kılavuzu
- Varsa diğer bilgiler

1.1.1 Kontrol - 2

- Tanım
- Uygulama Kılavuzu
- Varsa diğer bilgiler

1.2 Güvenlik Kategorisi – 2

Güvenlik kategorisi için tanım kontrol hedefi tanımı

1.2.1 Kontrol - 1

- Tanım
- Uygulama Kılavuzu
- Varsa diğer bilgiler

Yasal Gereksinimler

- Uygulanabilir yasa ve sözleşme gereksinimlerini tanımlama (18.1.1)
- Fikri mülkiyet hakları(18.1.2)
- Organizasyonun kayıtlarının korunması (18.1.3)
- Verinin korunması ve kişisel bilgilerin gizliliği (18.1.4)
- Kriptografik kontrollerin düzenlenmesi (18.1.5)

1. Bilgi Güvenliği Politikaları (ISO 27002, 5.x)

5.1.1 Bilgi güvenliği politikaları

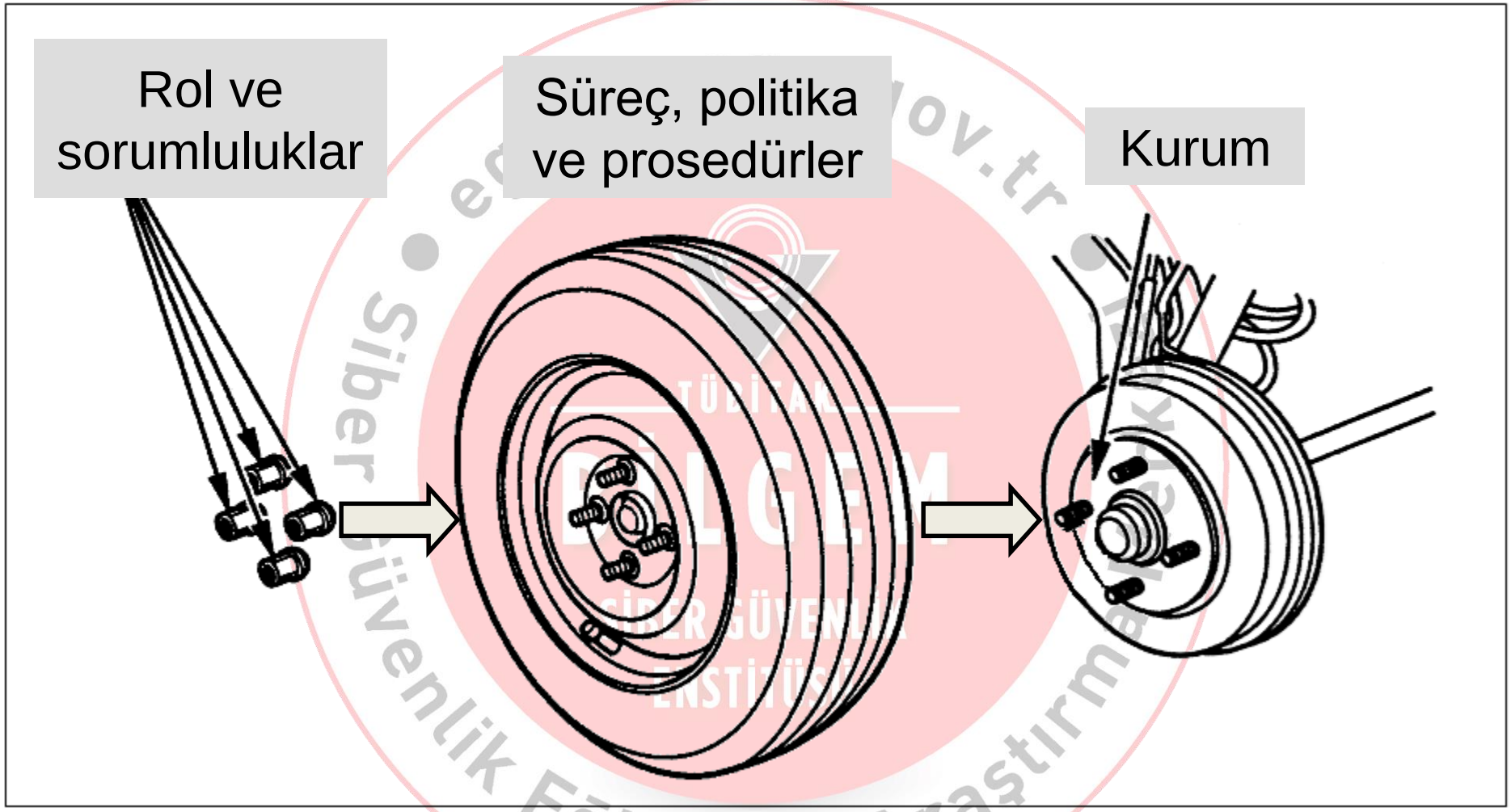
1. Bilgi Güvenliği Politikaları (ISO 27002, 5.x)

- Bir bilgi güvenliği politikası oluşturulmalı ve bu politika **kurum yönetiminin desteğini yansıtmalıdır**.
- Bilgi güvenliği politikası periyodik olarak gözden geçirilmeli ve **kurum çalışanları tarafından özümsenmelidir.**

2. Bilgi Güvenliği Organizasyonu (ISO 27002, 6.x)

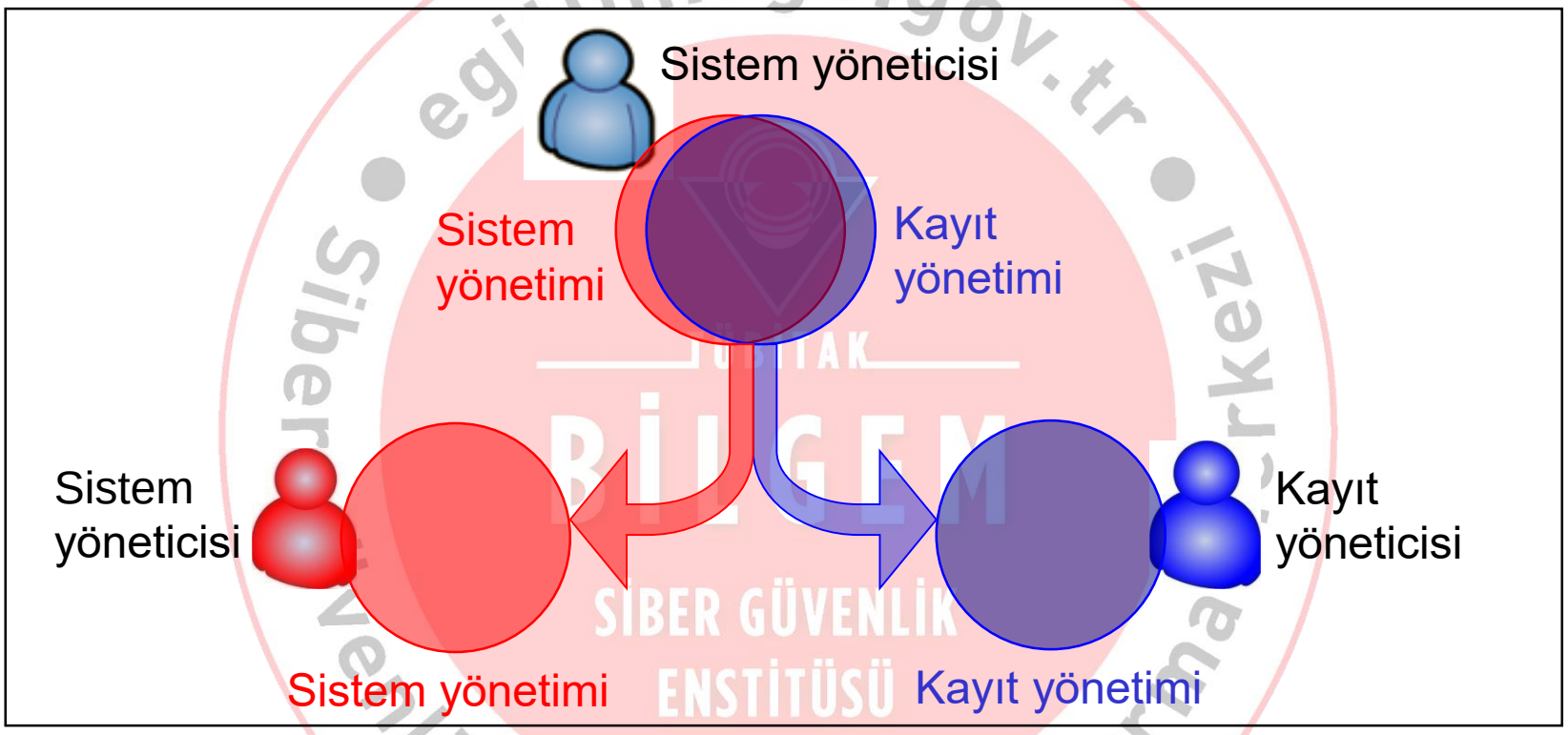
- Bilgi güvenliği ile ilgili aktiviteler kurum içerisinde **koordine edilmelidir,**
- Çelişen görev ve sorumluluklar ayrılmalıdır,
- Otoriteler ve **teknik çalışma grupları ile sürekli iletişim** halinde olunmalıdır,
- Proje yönetiminde, proje çeşidine bakılmaksızın bilgi güvenliği ele alınmalıdır.

2. Bilgi Güvenliği Organizasyonu (ISO 27002, 6.x)

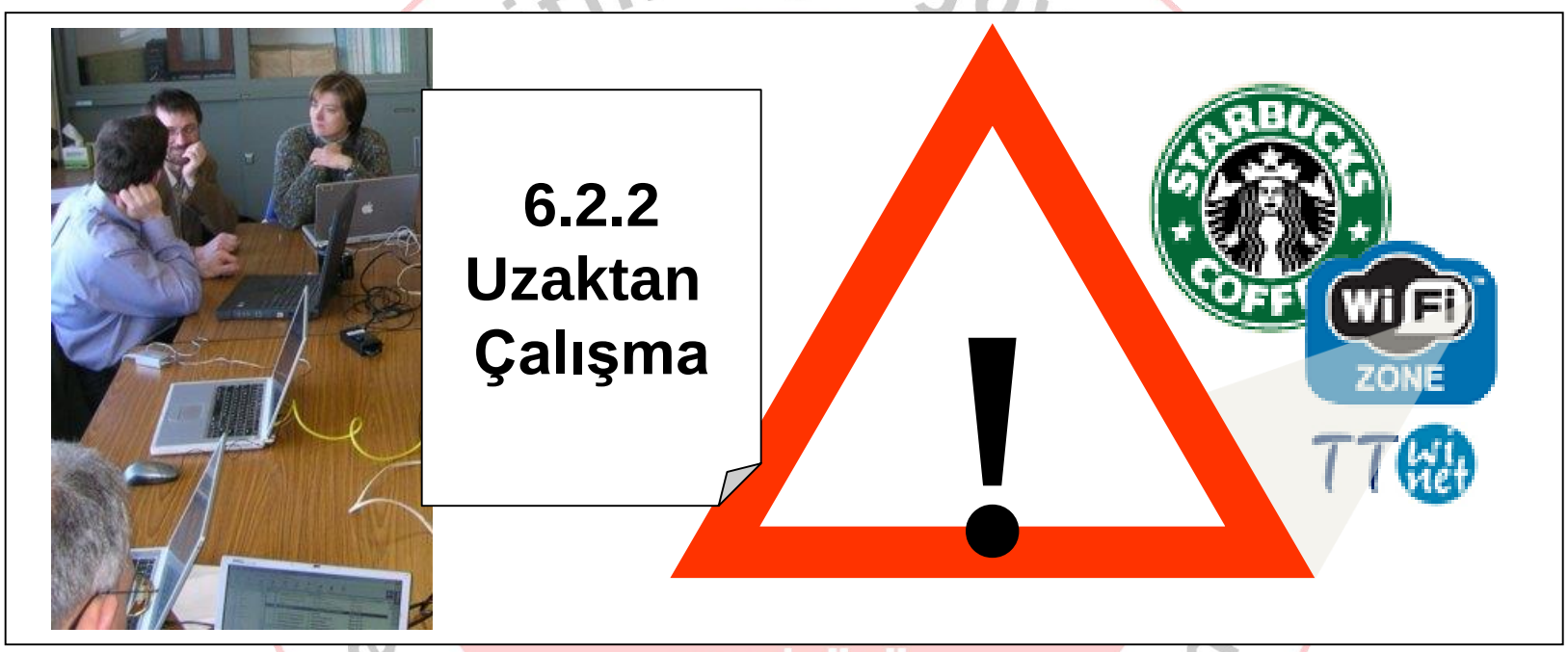


6.1.1 Bilgi güvenliği sorumluluklarının atanması

A.6.1.2 Görevler Ayrılığı

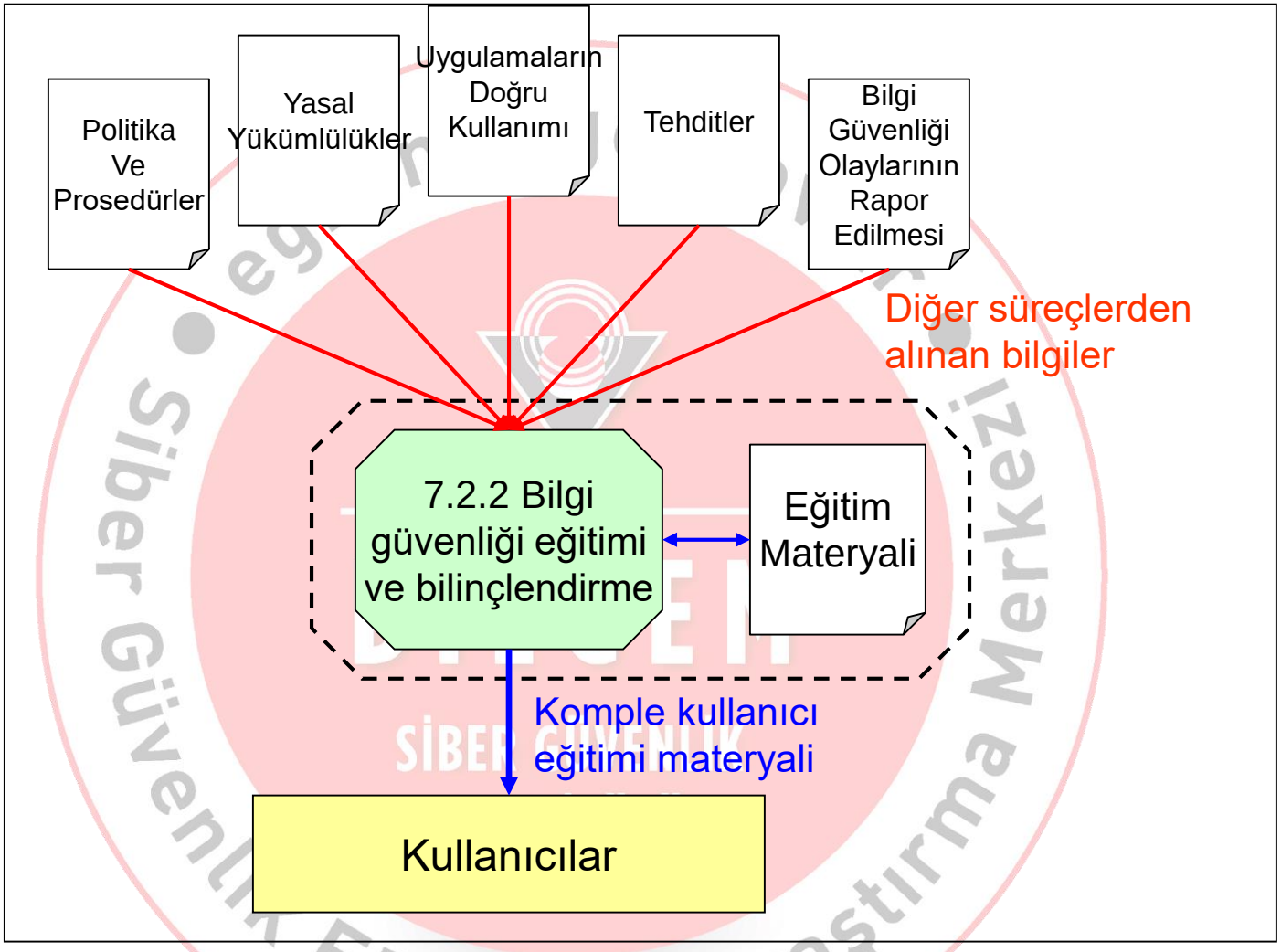


2. Bilgi Güvenliği Organizasyonu (ISO 27002, 6.x)



A.6.2 Mobil Cihazlar ve Uzaktan Çalışma

3. İnsan Kaynakları Güvenliği (ISO 27002, 7.x)



7.2.2 Bilgi güvenliği eğitimi ve bilinçlendirme

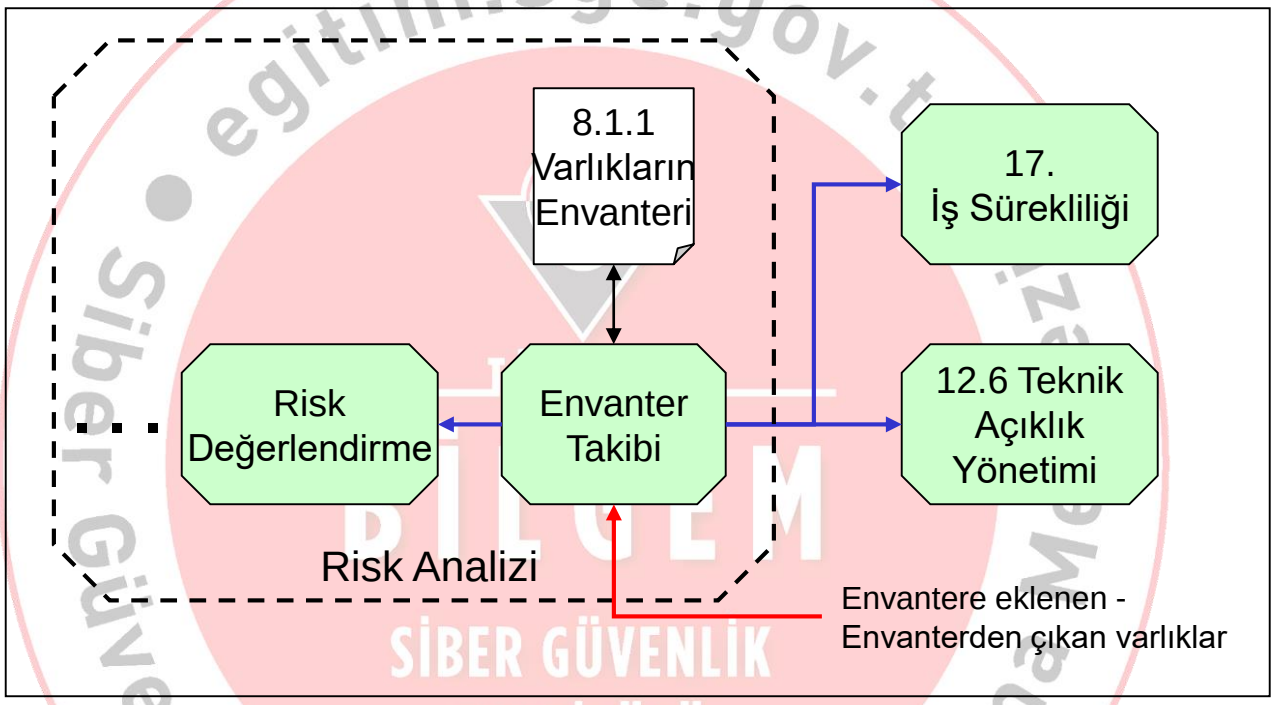
3. İnsan Kaynakları Güvenliği (ISO 27002, 7.x)

- İşe başlama öncesi, istihdam ve işten ayrılması aşamalarında **personelin sağlaması gereken güvenlik kıstasları**
- Güvenlik taraması yapılmalıdır.
- Güvenlik ile ilgili sorumluluklar, gizlilik anlaşmaları ve çalışma kontratlarının bir parçası olmalıdır.
- Bütün çalışanların güvenlik bilinci **bilgi güvenliği eğitim faaliyetleri** ile artırılmalıdır.
- Güvenlik ilkelerini çiğneyen personel için resmi bir **disiplin süreci** işlemelidir.
- İstihdamın sonlanması ve değiştirilmesi ile ilgili kurallar tanımlanmalı ve uygulanmalıdır.

4. Varlık Yönetimi (ISO 27002, 8.x)

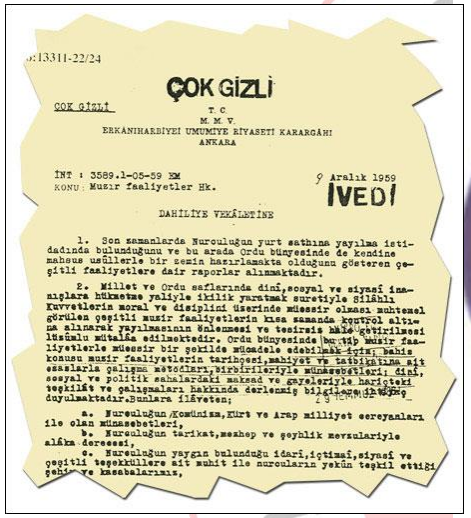
- İnsanlar *(personel, müşteriler, tedarikçiler..)*
- Bilgi *(kağıt ve elektronik ortamdaki)*
- Yazılım varlıkları
- Fiziksel varlıklar *(bilgisayar ve iletişim donanımı, altyapı varlıkları)*
- Hizmetler *(bilişim, ısıtma, havalandırma..)*
- Kurum imajı ve itibarı

4. Varlık Yönetimi (ISO 27002, 8.x)



8.1.1 Varlık envanteri (ve diğer süreçler için girdi olarak rolü)

4. Varlık Yönetimi (ISO 27002, 8.x)



ÇOK GİZLİ

T.C.
M.M.V.
ERKANIHARBİYEİ UMUMİYE RİYASETİ KARARGÂHI
ANKARA

İNT : 3589.1-05-59 KM
KONU : Muzir faaliyetler Hk.

9 Aralık 1959
İVEDİ

DAHİLİYE VEKÂLETİNE

1. Son zamanlarda Nurculuğun yurt sathına yayılma istidadında bulunduğunu ve bu arada Ordu bünyesinde de kendine mahsus usûllerle bir zemin hazırlamakta olduğunu gösteren çeşitli faaliyetlere dair raporlar alınmaktadır.

2. Millet ve Ordu saflarında dinî,sosyal ve siyasî inanışlara hükmetme yoluyle ihtilâl yaratmak suretiyle Silâhlı Kuvvetlerin moral ve disiplini üzerinde müessir olması muhtemel görülen çeşitli muzir faaliyetlerin kısa zamanda kontrol altına alınarak yayılmasının önlenmesi ve tesirsiz hâle getirilmesi lâzımlı mütalâa edilmektedir. Ordu bünyesinde bu tip muzir faaliyetlerle müessir bir şekilde mücadele edebilmek için, bahis konusu muzir faaliyetlerin tarihçesi,mahiyet ve tabiatına ait esaslarla gelişme safhaları,kirletirleriyle münasebetleri; dinî, sosyal ve politik sahalardaki maksad ve gayeleriyle hariçteki teşkilât ve çalışmaları hakkında derlenmiş bilgilere ihtiyaç duyulmaktadır.Bunlara ilâveten;

a. Nurculuğun Komünizm,Kürt ve Arap milliyet cereyanları ile olan münasebetleri,

b. Nurculuğun tarikat,mezhep ve şeyhlik mevzularıyle alâkası derecesi,

c. Nurculuğun yaygın bulunduğu idarî,içtimaî,siyasî ve çeşitli teşekküllere ait muhit ile nurcuların yekûn teşkil ettiği şehir ve kasabalarımız,

8.2.1 – 8.2.2 Bilginin sınıflandırılması ve etiketlenmesi

4. Varlık Yönetimi (ISO 27002, 8.x)

- **Varlık envanteri** oluşturulmalı, envanterdeki varlıkların korunması için **sahipleri** belirlenmelidir.
- Varlıkların **kullanımı** belirlenmiş **kurallara göre** yapılmalıdır.
- **Bilgiler sınıflandırılmalı ve etiketlenmelidir.**

Ortam İşleme (ISO 27002, 8.3)

Risk
(Kaybetme, çaldırma ve yetkisiz erişim…)

Taşınabilir Saklama Ortamları

Dizüstü Bilgisayarlar

SADECE DOSYA TAŞIMAK İÇİN KULLANIN!

SAKLANAN BİLGİYİ ASGARİ DÜZEYE İNDİRİN

Masaüstü Bilgisayarlar

Taşınabilir Saklama Ortamları

Dizüstü Bilgisayarlar

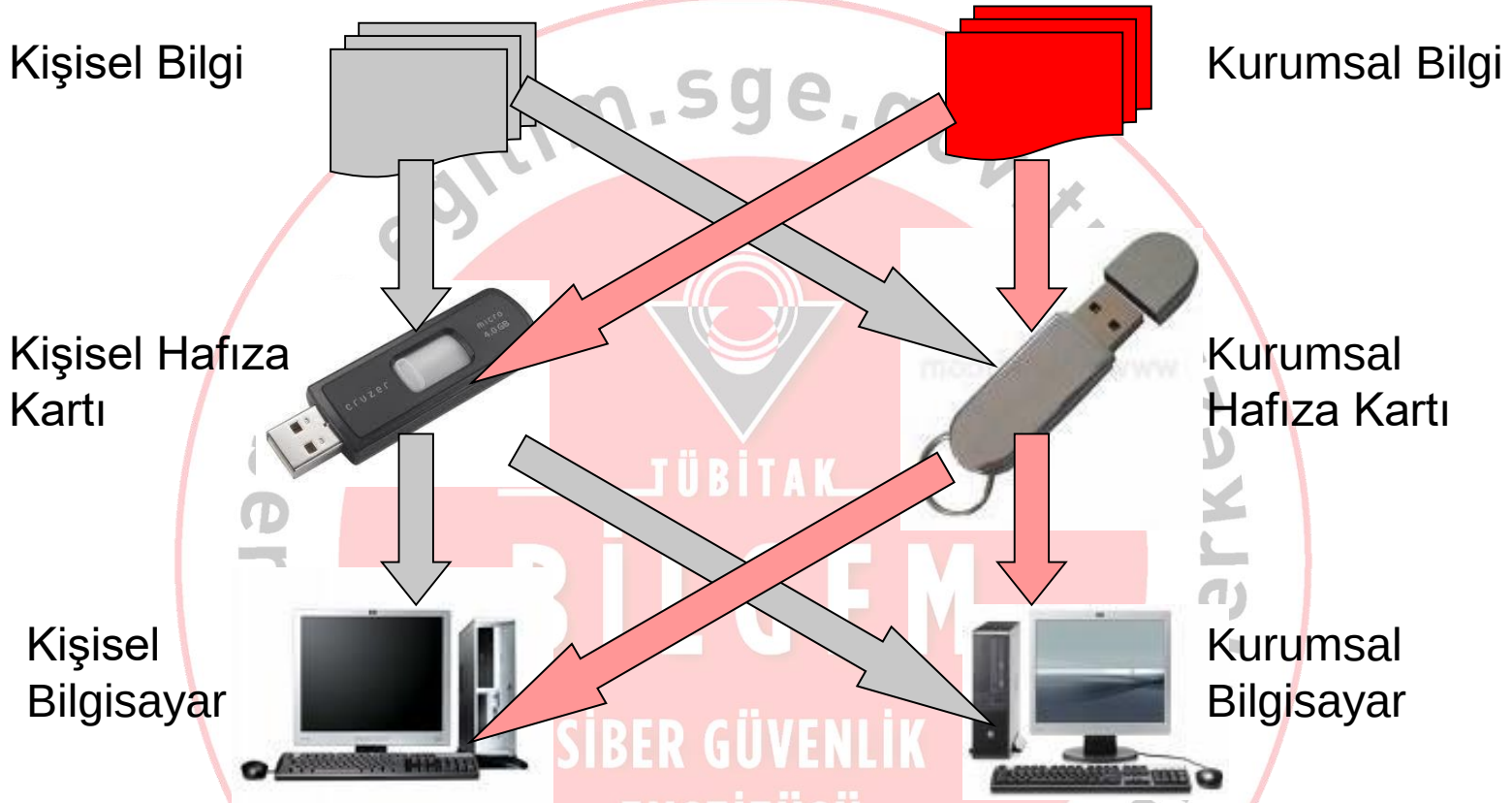
Dosya Sunucu vb. Yerlerdeki Dizinler

Taşınabilirlik

Ortam İşleme (ISO 27002, 8.3)

- Bilgi ortamına ihtiyaç kalmadığında, bilgi ortamı belirlenmiş yöntemlerle güvenli bir şekilde yokedilmelidir.
- Bilgi bulunduran ortamlar taşınırken, yetkisiz erişim, kötüye kullanım ve bozulmaya karşı korunmalıdır.

Taşınabilir Ortam Yönetimi (ISO 27002, 8.3.1)



8.3.1 Taşınabilir saklama ortamlarının yönetilmesi

- **Kişisel bilgiler** ve **iş ile ilgili bilgiler** aynı hafıza kartında saklanmamalıdır.
- **Kurumsal hafıza kartları yabancı/kişisel bilgisayarlara** takılmamalıdır.

5. Erişim Kontrolü (ISO 27002, 9.x)

	Dizinler					Tesisler		
Kullanıcı ↓	A Projesi Dizinleri	B Projesi Dizinleri	C Projesi Dizinleri	Aktif Dizin	Kayıtlar Dizini	Ar-Ge	Sistem Merkezi	İdari Merkez
A Projesi Yöneticisi	VAR	YOK	YOK	YOK	YOK	VAR	YOK	VAR
B Projesi Yöneticisi	YOK	VAR	YOK	YOK	YOK	VAR	YOK	VAR
C Projesi Yöneticisi	YOK	YOK	VAR	YOK	YOK	VAR	YOK	VAR
Projeler Direktörü	VAR	VAR	VAR	YOK	YOK	VAR	YOK	VAR
Sistem Yöneticisi	YOK	YOK	YOK	VAR	YOK	YOK	VAR	VAR
Kayıt Yöneticisi	YOK	YOK	YOK	YOK	VAR	YOK	VAR	VAR

9.1.1 Erişim politikası tablosu

Uygulama-13

- İş sürecimizdeki bilgi, yazılım, donanım varlıklarını ve bunlara erişmesi gereken kurum çalışanlarını göz önünde bulundurun

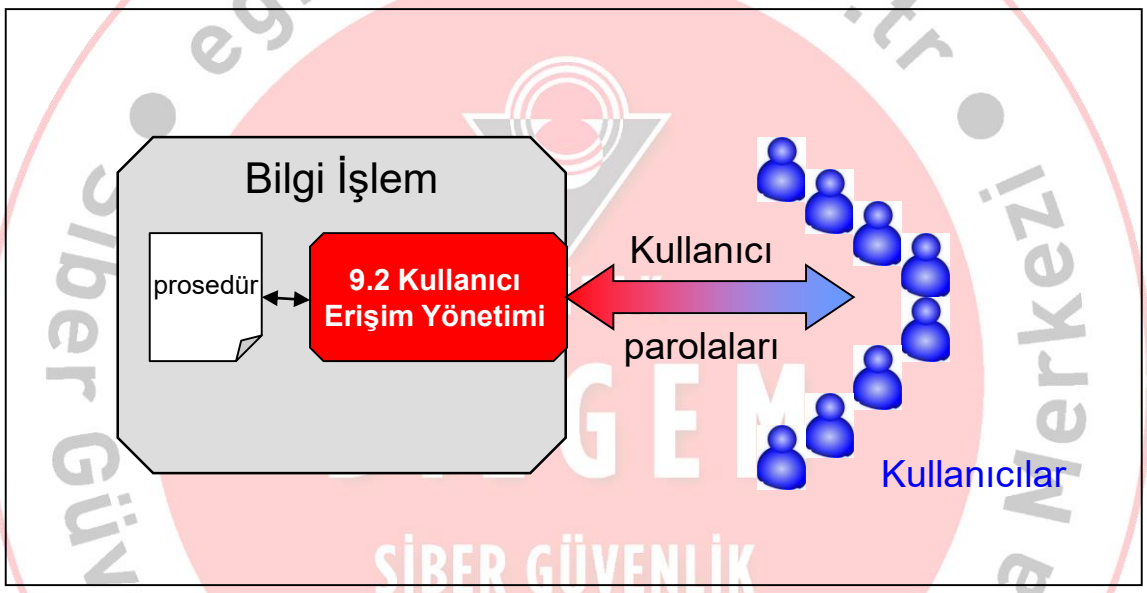
- **Kullanıcı gruplarını** belirleyin ve Erişim Kontrol Tablosu.xlsx dosyasına kaydedin.

Uygulama-14

- Erişim Kontrol Tablosu.xlsx dosyasının sütunlarına iş sürecinizin bilgi, yazılım ve donanım varlıklarını kopyalayın.

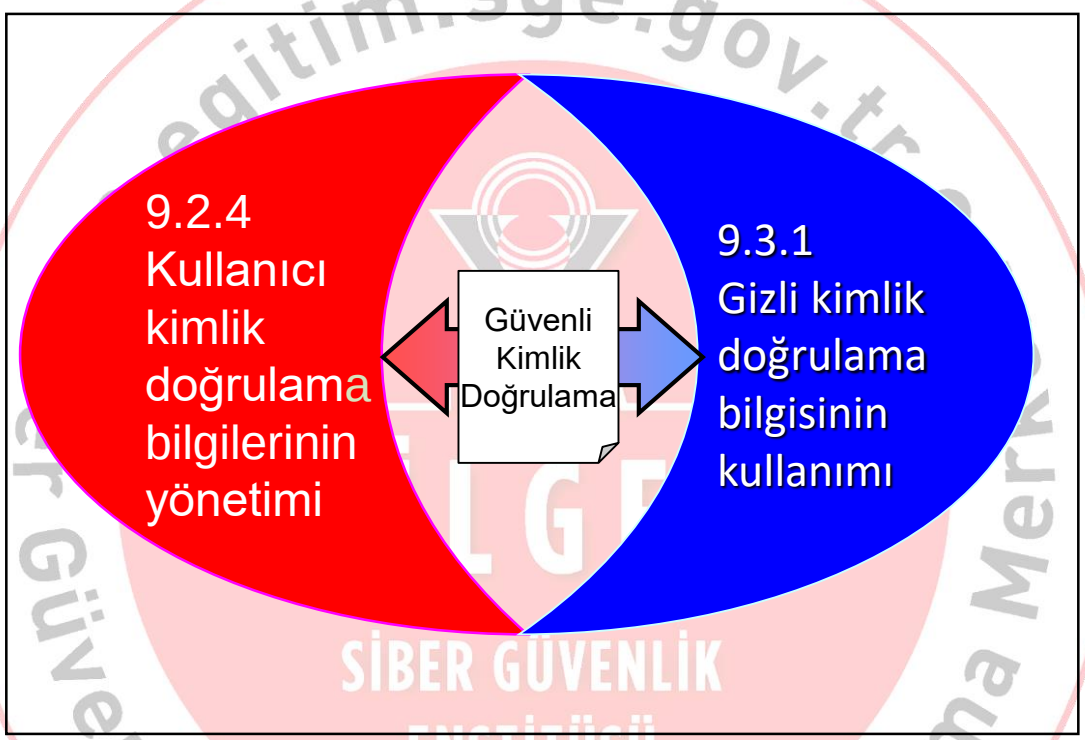
- Bilgi, yazılım ve donanım varlıkları ve kullanıcı grupları için **erişim haklarını** (“var/yok” şeklinde) belirleyin.

5. Erişim Kontrolü (ISO 27002, 9.x)



9.2 Kullanıcı erişim yönetimi

5. Erişim Kontrolü (ISO 27002, 9.x)



Uygulama-15

Parola karmaşıklığının ölçülmesi

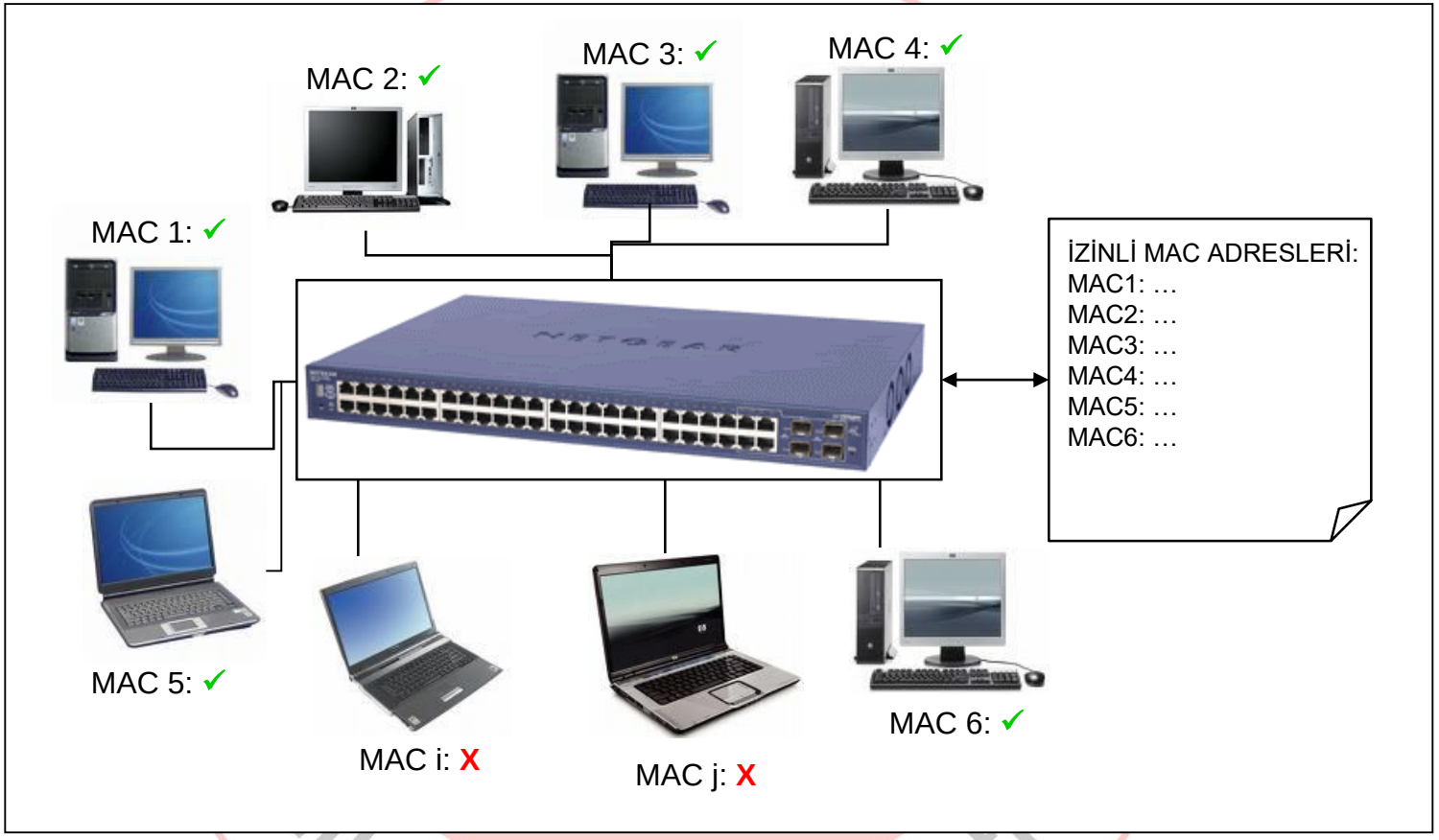
- **Hodri meydan ☺ :**

http://www.bilgimikoruyorum.org.tr/?b223_yaparak_ogrenelim

- Güçlü parola oluşturma önerileri:

http://www.bilgimikoruyorum.org.tr/?b222_guclu_parola_olusturma

5. Erişim Kontrolü (ISO 27002, 9.x)



Örnek: MAC adres kilitlemesi

5. Erişim Kontrolü (ISO 27002, 9.x)

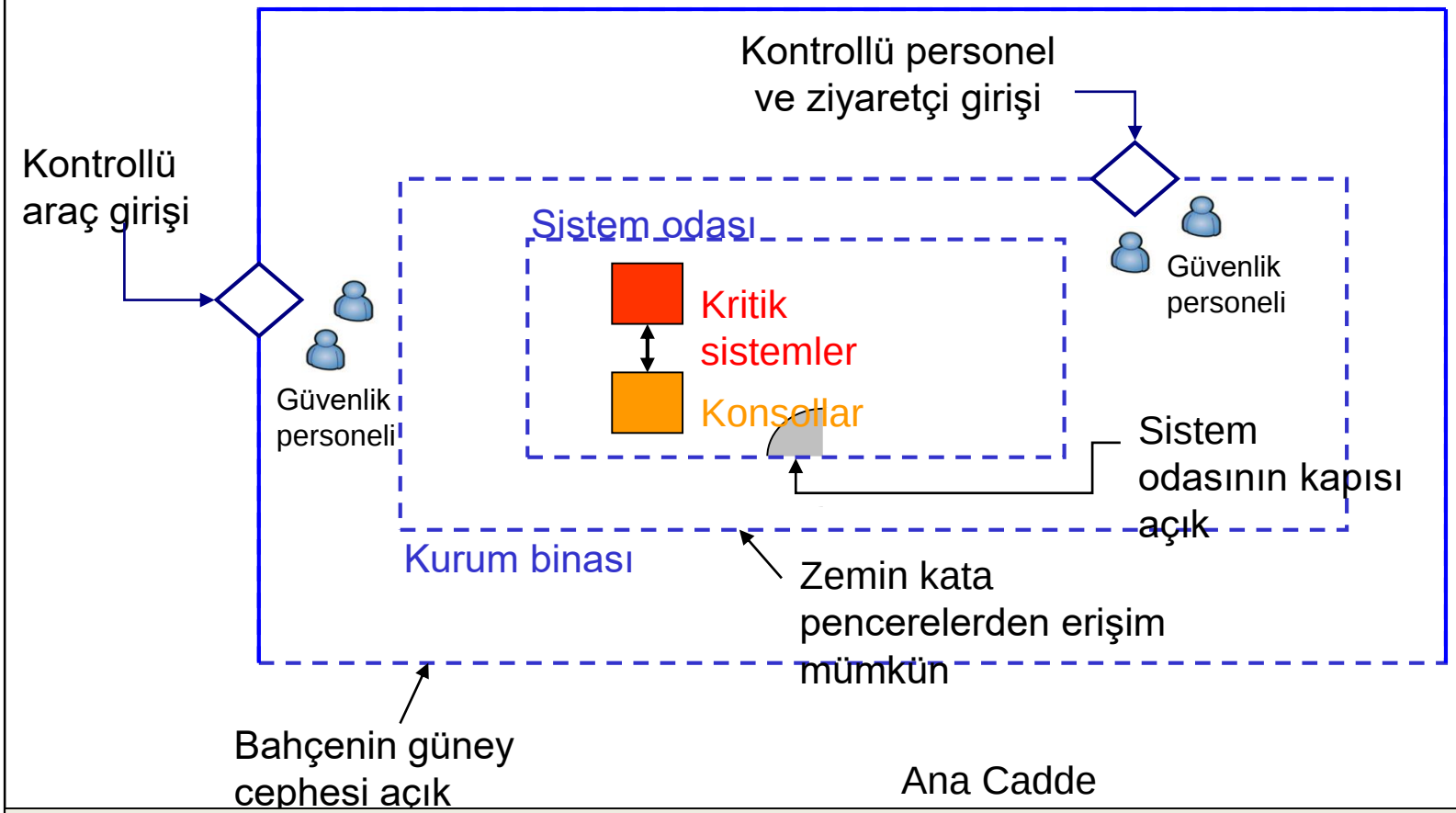
- Yazılı bir erişim denetimi politikası oluşturulmalıdır.
- Parola kullanımı, korunması, sahipsiz ekipmanların korunması, gibi **kullanıcı sorumlulukları** açıkça tanımlanmalıdır.
- **Kullanıcı erişim yönetimi**
  - (kayıt, ayrıcalık yönetimi, şifre yönetimi, kullanıcı haklarının gözden geçirilmesi v.b.) resmi süreç uyarınca yönetilmelidir.
- **Sistem erişim ve kullanımı,**
  - Güvenli giriş prosedürleri, kullanıcı tanıma ve kimlik doğrulaması, parola yönetimi, sistem araçlarının kullanımı ve oturum süre aşımı unsurları göz önüne alınarak kontrol edilmelidir.
- Ağ hizmetleri, işletim sistemleri ve uygulamalar uygun şekilde korunmalıdır.

6. Kriptografi (ISO 27002, 10.x)

- Kriptografik kontrollerin kullanımına ilişkin politika
  - Risk değerlendirme sonucu kontrolün çeşidi, amacı ve ilgili iş süreci belirlenir
- Kriptografik anahtar politikası ve uygulanması

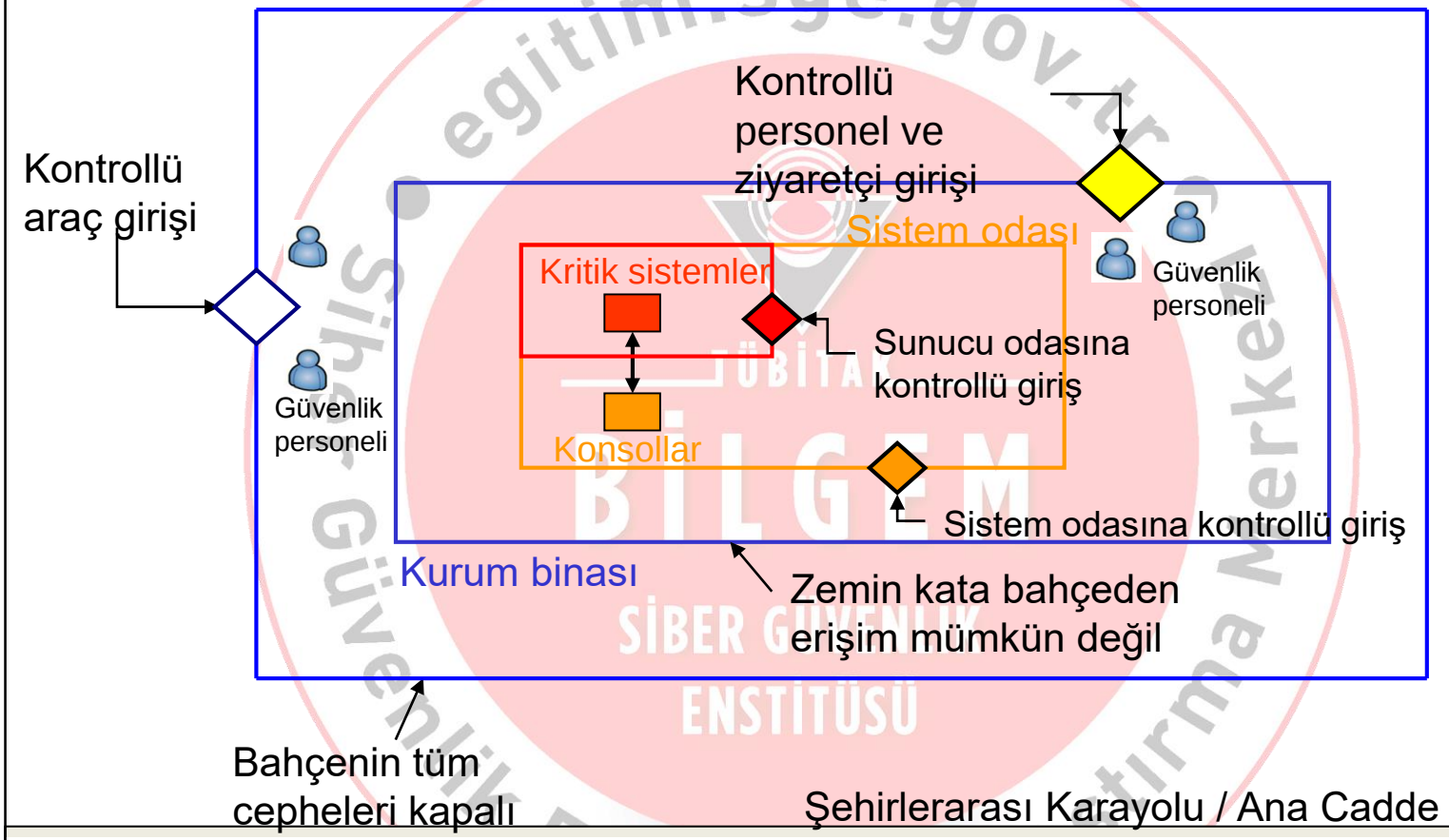
7. Fiziksel ve Çevresel Güvenlik (ISO 27002, 11.x)

11.1.1 Fiziksel güvenlik sınırı (kötü örnek)

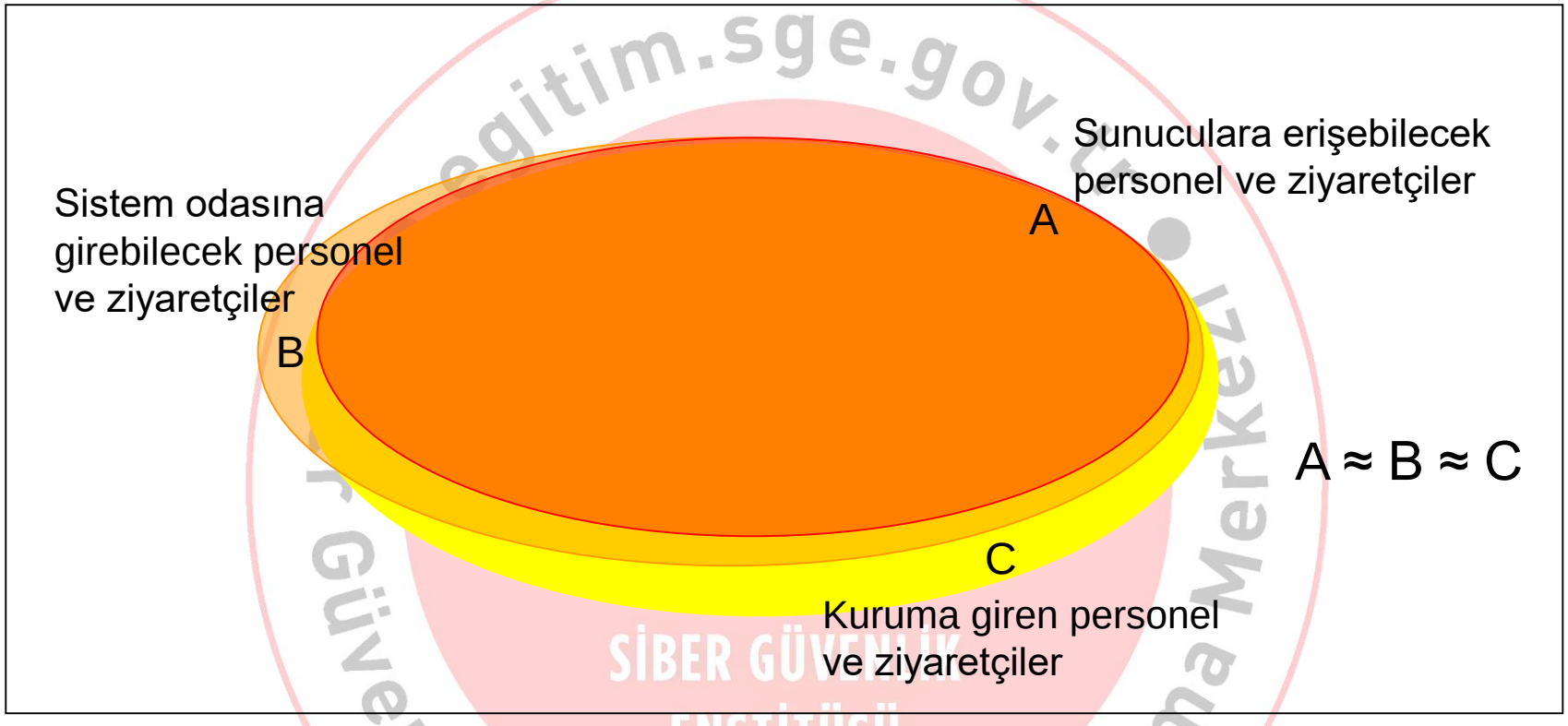


7. Fiziksel ve Çevresel Güvenlik (ISO 27002, 11.x)

11.1.1 Fiziksel güvenlik sınırı (çalışma yapılmış)

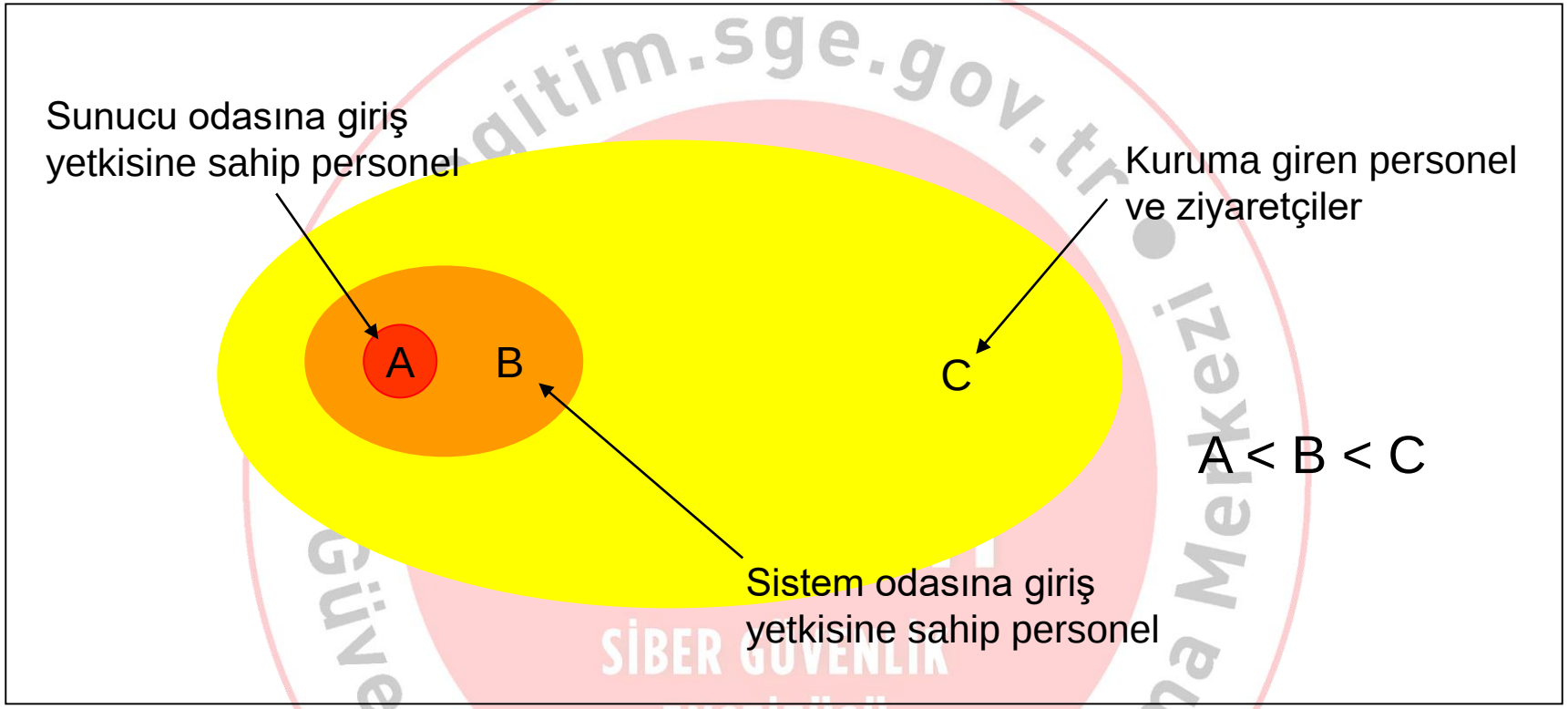


7. Fiziksel ve Çevresel Güvenlik (ISO 27002, 11.x)



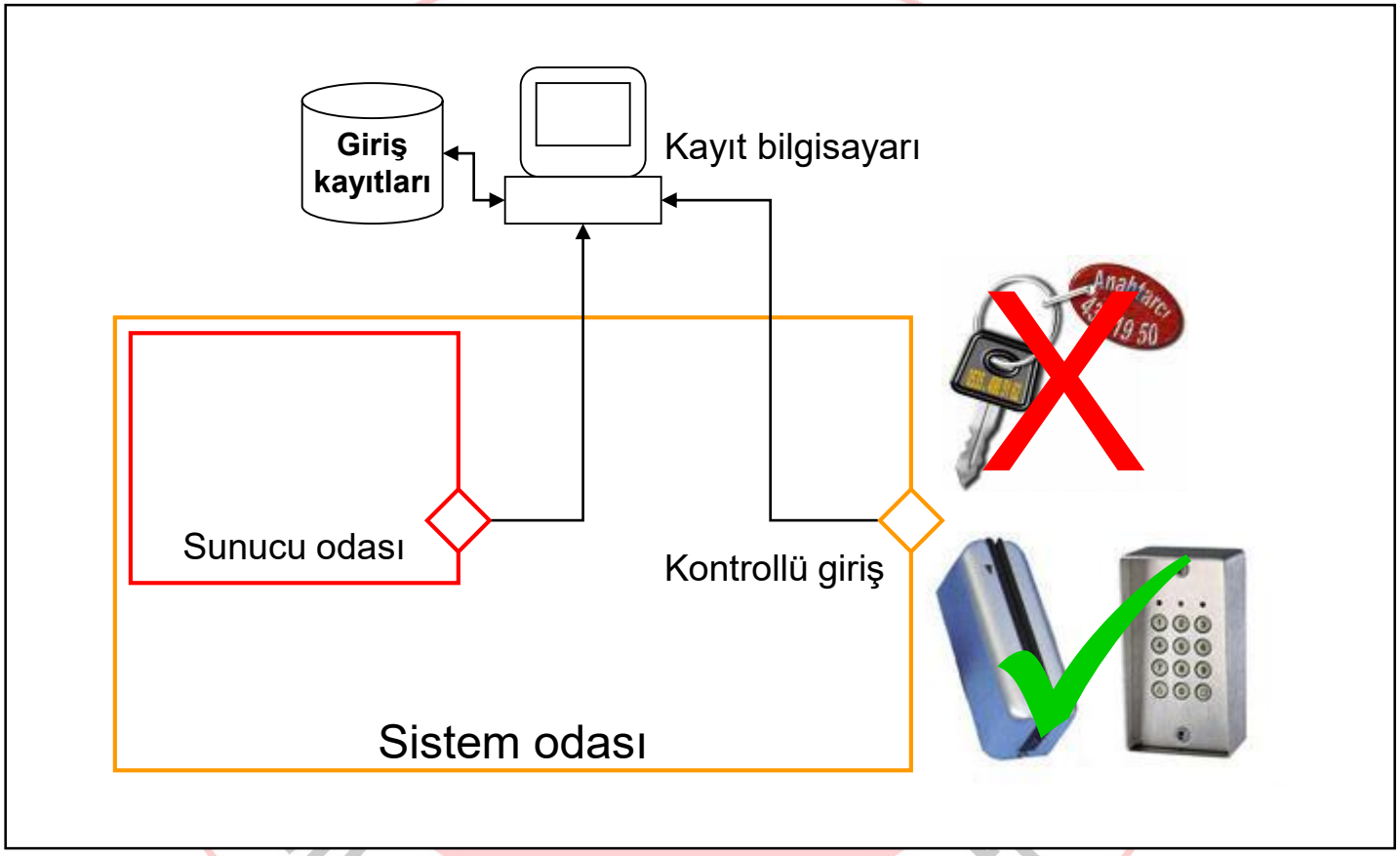
Fiziksel erişim kontrolü (kötü örnek)

7. Fiziksel ve Çevresel Güvenlik (ISO 27002, 11.x)



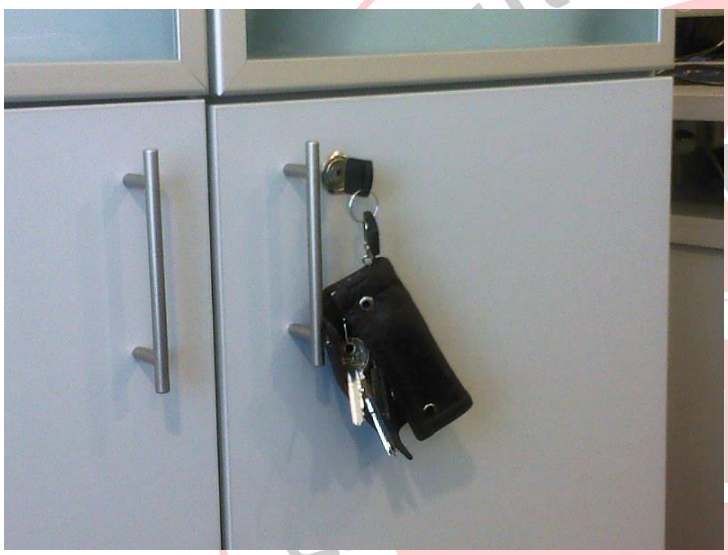
Fiziksel erişim kontrolü (çalışma yapılmış)

7. Fiziksel ve Çevresel Güvenlik (ISO 27002, 11.x)



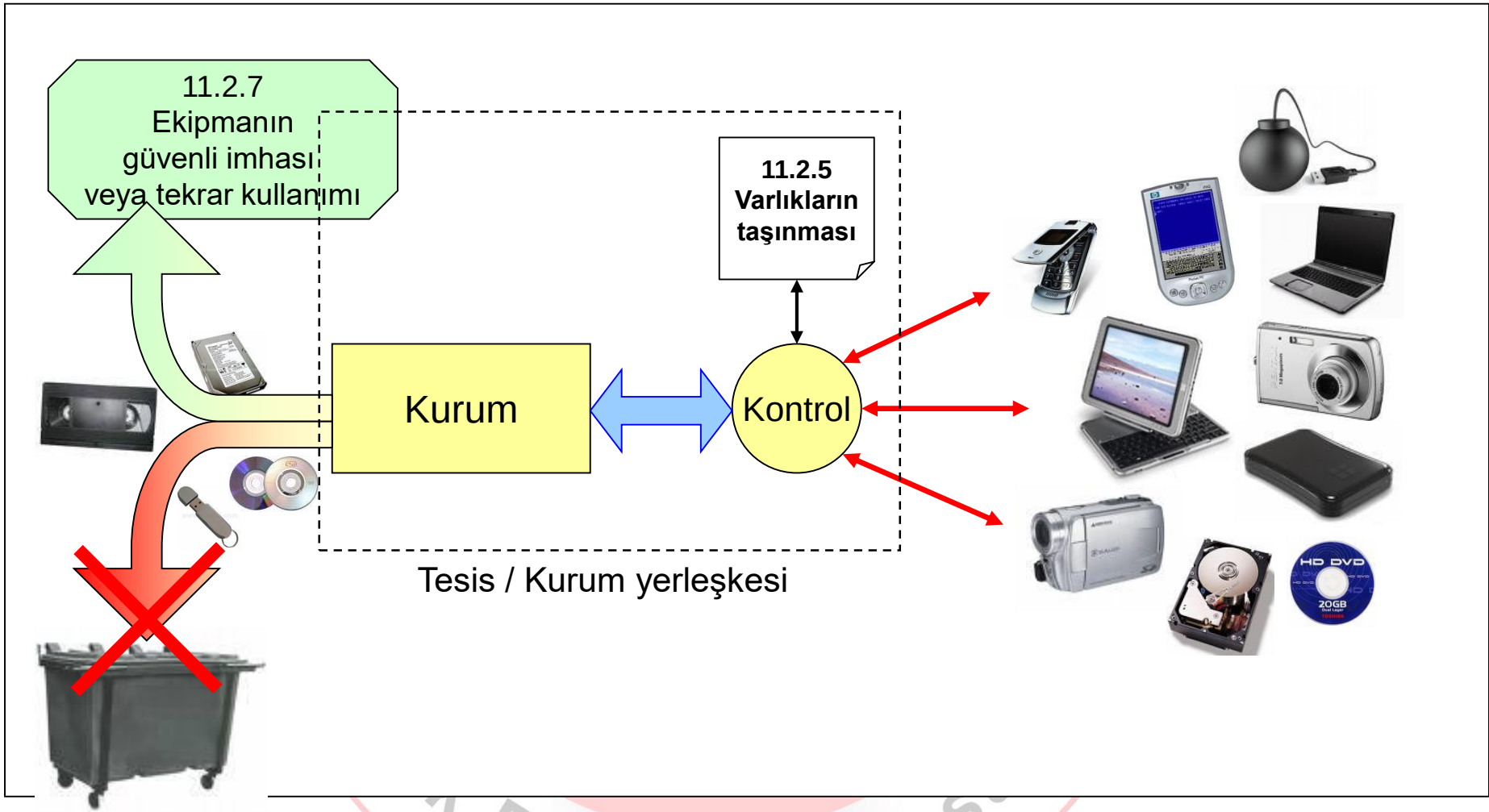
11.1.2 Fiziksel giriş kontrolleri

7. Fiziksel ve Çevresel Güvenlik (ISO 27002, 11.x)



11.2.8 Gözetimsiz kullanıcı teçhizatı

7. Fiziksel ve Çevresel Güvenlik (ISO 27002, 11.x)



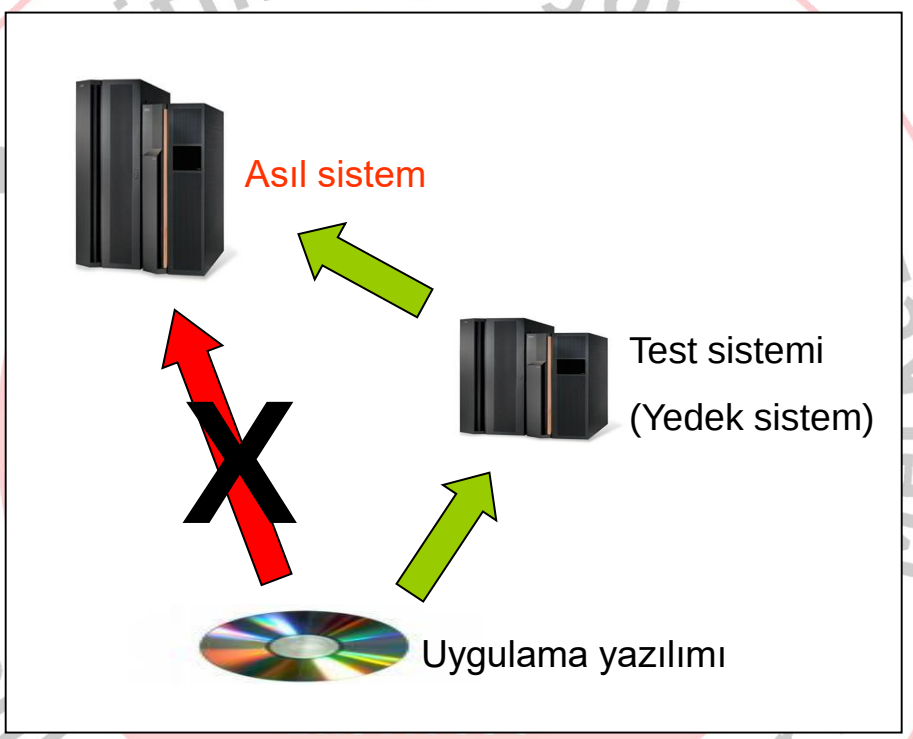
11.2.5 Varlıkların taşınması

11.2.7 Ekipmanın güvenli imhası veya tekrar kullanımı

7. Fiziksel ve Çevresel Güvenlik (ISO 27002, 11.x)

- Ekipmanlar, yeterli erişim kontrolü ve hasar koruma mekanizmaları uygulanmış güvenli alanlarda bulunmalıdır.
- Ekipmanları, kayıp, hasar ve kötü kullanıma karşı koruyacak **yerleşim önlemleri** alınmalıdır.
- Güç kaynakları ve ekipmanların uygun bir şekilde bakımı ve **kablolama güvenliği** sağlanmalıdır.
- **Yerleşke dışına kurulan ekipman** ile bu ekipman ile ilgili bilginin kullanımı ve imhası ile ilgili hususlar göz önünde bulundurulmalıdır.
- Ekipmanı **kurum dışına çıkarma** konusunda bir kontrol mekanizması olmalıdır.
- Ekipmanların kurulu olduğu yerlere dışarıdan erişim olmaması sağlanmalıdır.

8. İşletim Güvenliği (ISO 27002, 12.x)



12.1.4 Geliştirme, test ve işletim ortamlarının birbirinden ayrılması

8. İşletim Güvenliği (ISO 27002, 12.x)

12.3.1 Bilgi yedekleme

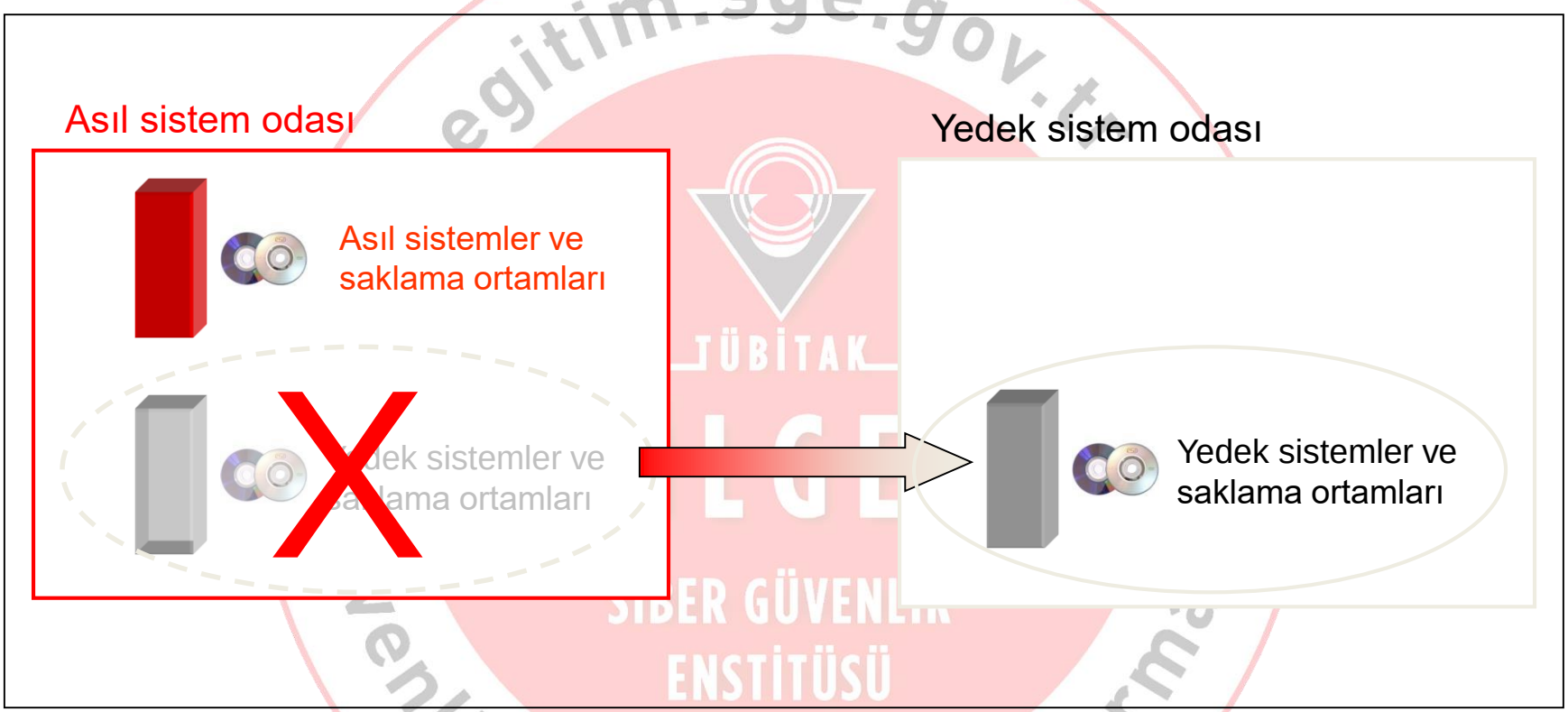
- Yedekleme prosedürleri
- Yedekten geri döndürme prosedürleri

Uygulama-16

- İş sürecinizdeki bilgi, yazılım, donanım varlıklarını göz önünde bulundurun.

- Bu bilgi varlıklarının **yedeklenme ihtiyacını** Varlık Yedekleme.doc dosyasına (“var/yok” şeklinde) kaydedin.

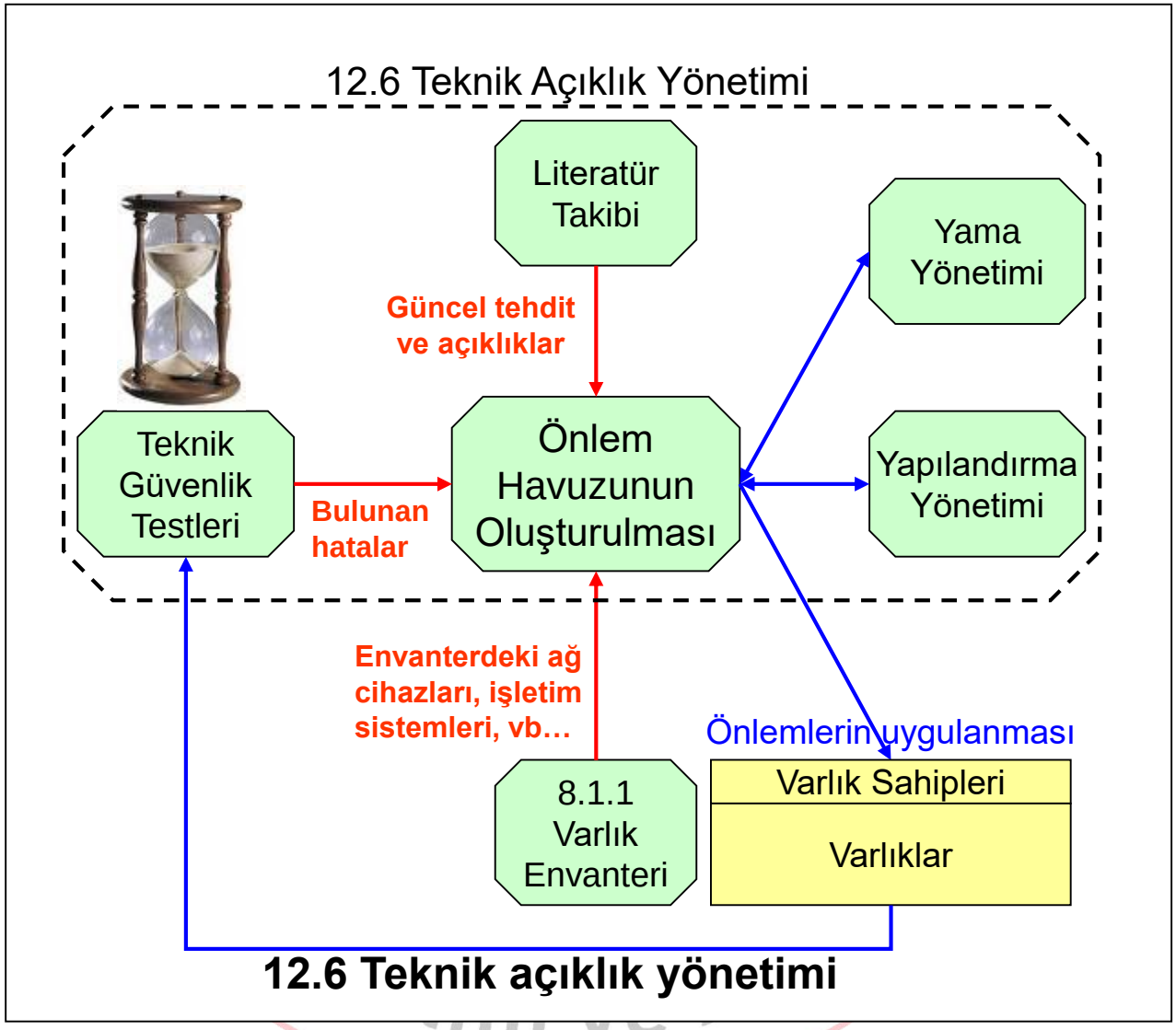
8. İşletim Güvenliği (ISO 27002, 12.x)



8. İşletim Güvenliği (ISO 27002, 12.x)

12.5.1 İşletimsel sistemler üzerine yazılım kurulumu

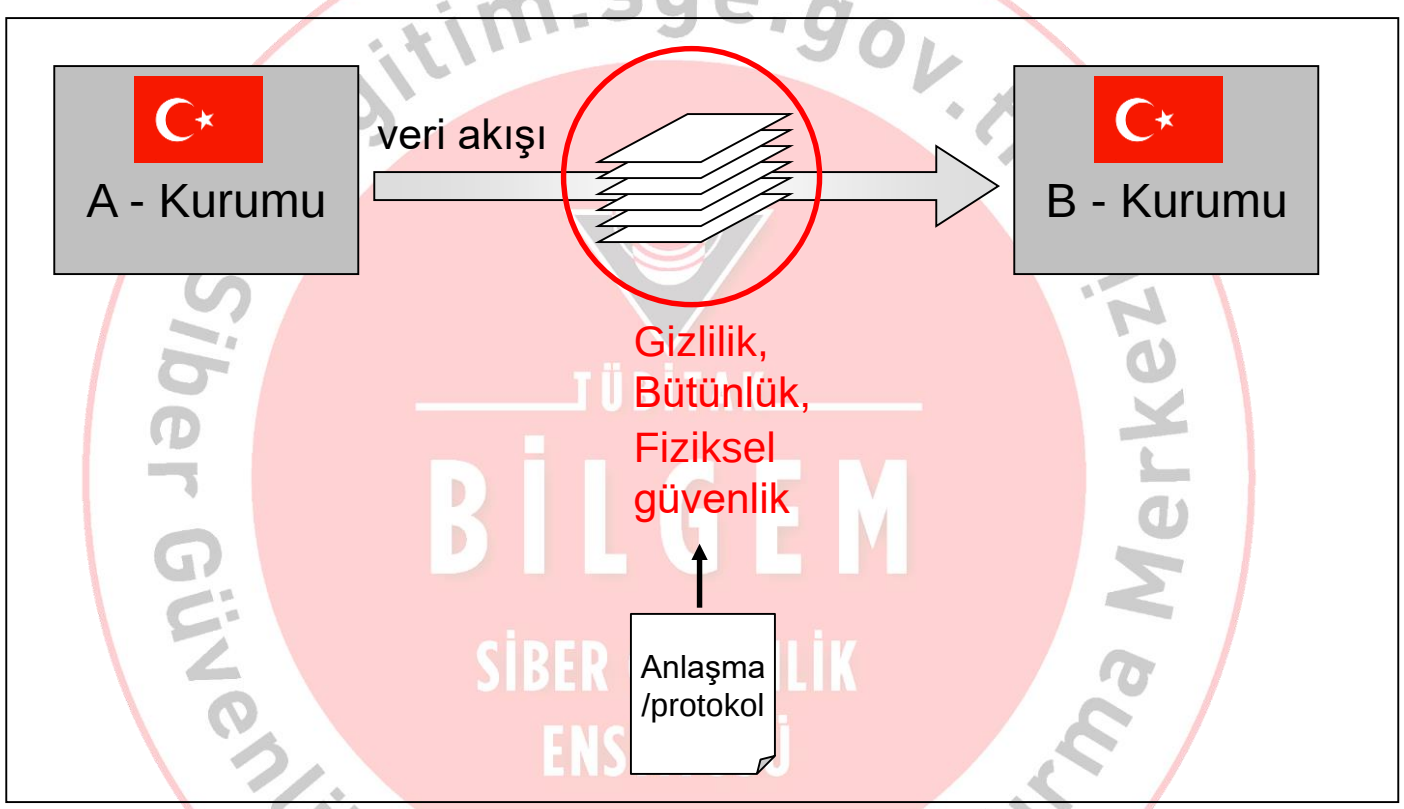
8. İşletim Güvenliği (ISO 27002, 12.x)



8. İşletim Güvenliği (ISO 27002, 12.x)

- Dokümante edilmiş işletme prosedürleri
- Değişiklik kontrol süreci
- Kapasite yönetimi
- Geliştirme, test ve işletim ortamlarının birbirinden ayrılması
- **Zararlı yazılımlara karşı prosedürler**
- Yedekleme
- **Kaydetme ve İzleme**
- İşletimsel sistemler üzerine yazılım kurulumu
- **Teknik açıklık yönetimi**
- Bilgi sistemleri tetkik hususları

9. Haberleşme Güvenliği (ISO 27002, 13.x)



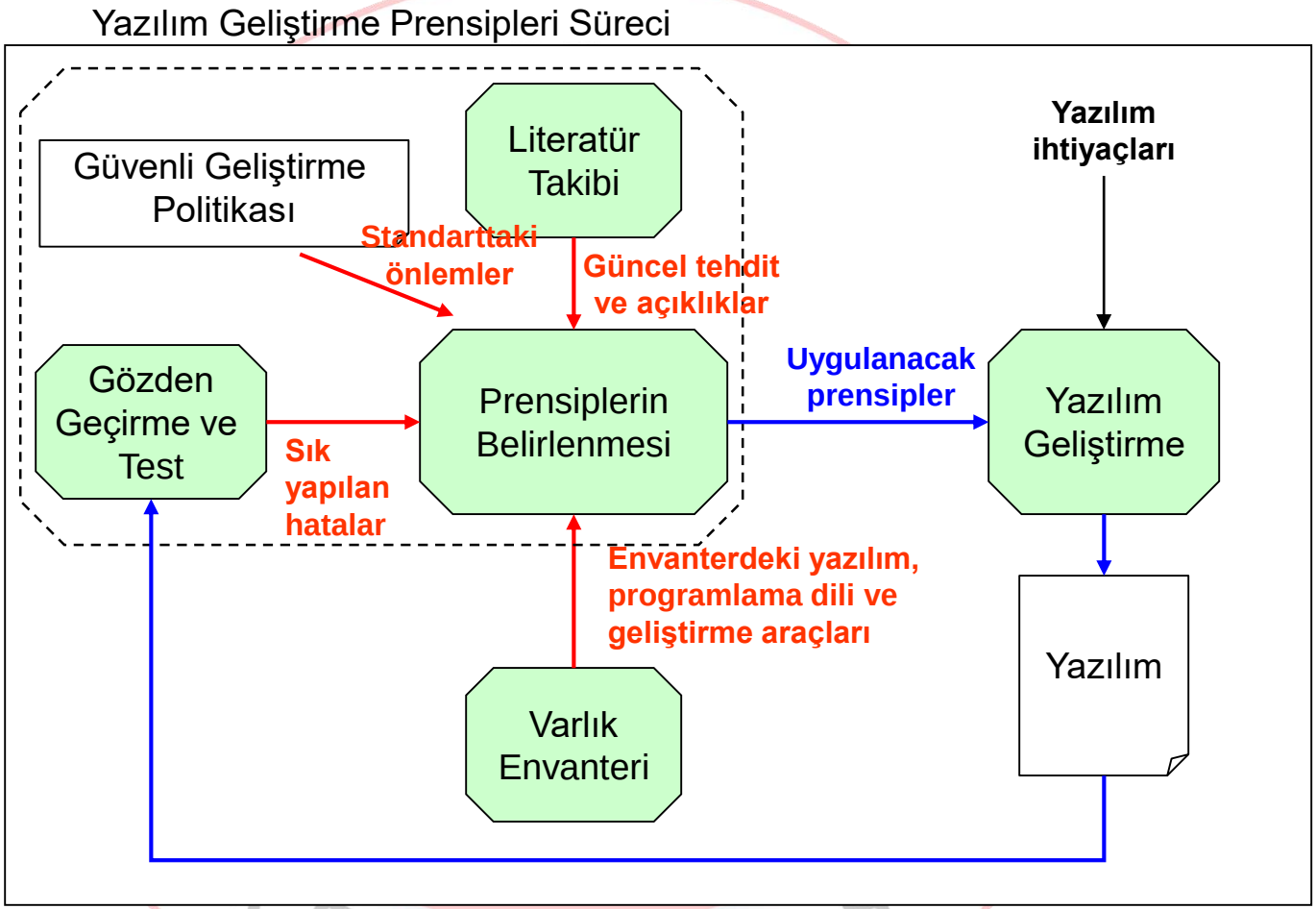
13.2.1- 13.2.2 Bilgi transfer politikaları, prosedürleri ve anlaşmaları

9. Haberleşme Güvenliği (ISO 27002, 13.x)

- Ağ ve ağ hizmetlerinin güvenliği
- Bilgi transfer politikaları ve prosedürleri
  - Posta, e-posta, telefon, faks, video vb .ile yapılan her türlü bilgi iletişimi

10. Sistem Temini, Geliştirme ve Bakımı (ISO 27002, 14.X)

- Bilgi Sistemlerinin güvenlik gereksinimleri, yeni veya var olan bilgi sistemleri sistemleri için analiz edilmelidir.
- Halka açık ağlardaki uygulama hizmetlerinin güvenliği sağlanmalıdır.
- Paralı işlem görülen uygulama hizmetleri korunmalıdır.

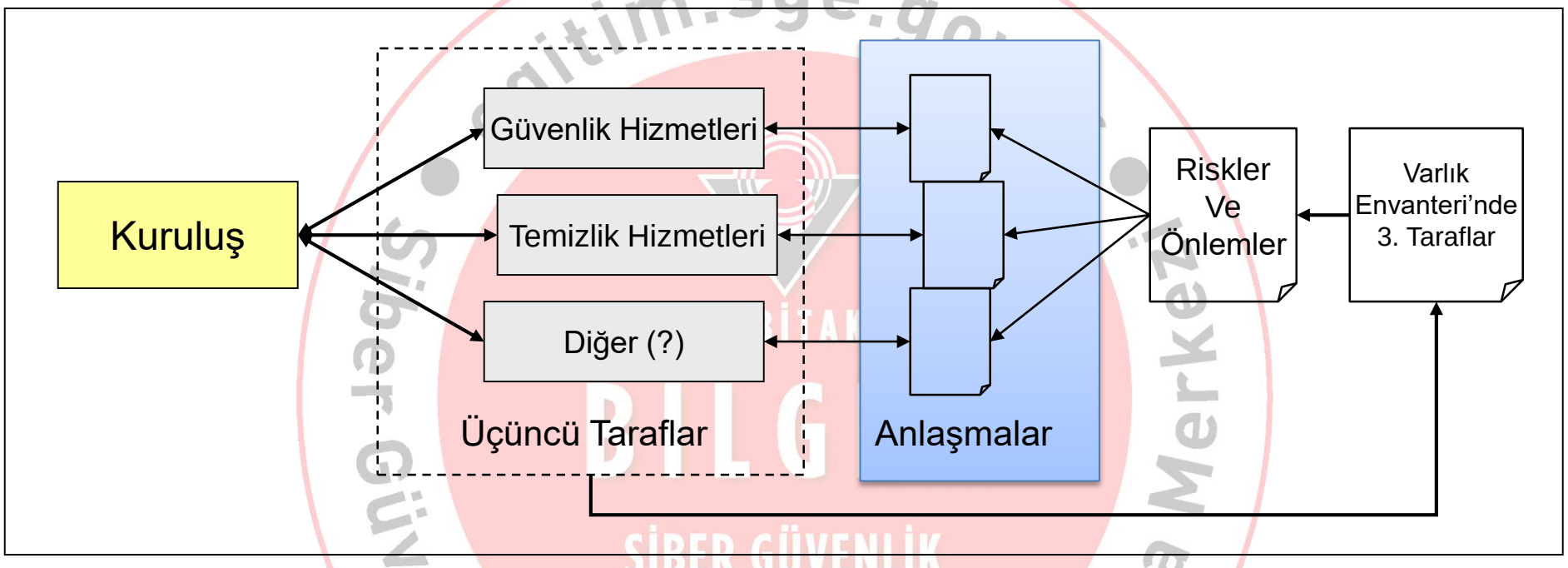


14.2.5 Güvenli sistem mühendisliği prensipleri

10. Sistem Temini, Geliştirme ve Bakımı (ISO 27002, 14.X)

- Geliştirme ve destek süreçlerinde güvenlik
  - Güvenli Geliştirme politikası/prensipleri
  - Kontrollü sistem ve yazılım değişiklikleri
  - Güvenli geliştirme ortamı
  - Sistem güvenlik testleri
  - Sistem kabul testleri
- Test verisinin korunması

11. Tedarikçi İlişkileri (ISO 27002,15.X)



15.1.1 Tedarikçi ilişkileri için bilgi güvenliği politikası

11. Tedarikçi İlişkileri (ISO 27002,15.X)

- Kuruluşun bilgi ve iletişim olanaklarını sağlayan tedarik zincirindeki bilgi güvenliği gereksinimleri tedarikçi ile kararlaştırılarak yazılı hale getirilmelidir.
- Tedarikçi anlaşmalarında bilgi güvenliği hususları ifade edilmelidir.

11. Tedarikçi İlişkileri (ISO 27002,15.X)

- Kuruluş, tedarikçilerden alınan hizmetler, düzenli aralıklarla izlemeli, gözden geçirmeli ve tetkik etmelidir.

- Tedarikçiler tarafından sağlanan hizmetlerdeki değişiklikler yönetilmelidir.

12. Bilgi Güvenliği Olay Yönetimi (ISO 27002, 16.x)

16.1 Bilgi güvenliği ihlal olaylarının ve iyileştirmelerin yönetimi

12. Bilgi Güvenliği Olay Yönetimi (ISO 27002, 16.x)

- Güvenlik olayları ve zayıflıkları bildirilmelidir.
- **Güvenlik olayları** yönetimi ve iyileştirmeleri ile ilgili sorumluluklar ve **prosedürler** tanımlanmalı,
  - Güvenlik olayları ile ilgili kanıtlar toplanmalıdır.
- Yaşanan bilgi güvenliği olayları analiz edilmeli, olayların tekrarını önlemek üzere kök nedenler değerlendirilmelidir.

13. İş Sürekliliği Yönetiminin Bilgi Güvenliği Hususları (ISO 27002, 17.x)

17.1 Bilgi güvenliği sürekliliği

İş Sürekliliği Planlaması

- İş süreçlerinin kesintiye uğramasını engelleyecek ayrıntılı **iş sürekliliği yönetimi planı** oluşturulmalıdır.
- Sonuçları strateji planında yer alacak bir **etki analizi** çalışması yapılmalıdır.
  - İş sürekliliği yönetimi süreci belirlenen kritik süreçleri kapsamalıdır.
- İş sürekliliği planlarının **bilgi güvenliği boyutu** gözden kaçırılmamalıdır.
- İş sürekliliği planları test edilmeli ve sürekli olarak gözden geçirilmelidir.

Tartışma-7

- İş süreciniz için Hedef Kurtarma Noktasını (“Recovery Point Objective”) belirleyin.

- İş süreciniz için Hedef Kurtarma Zamanı (“Recovery Time Objective”) süresini belirleyin.

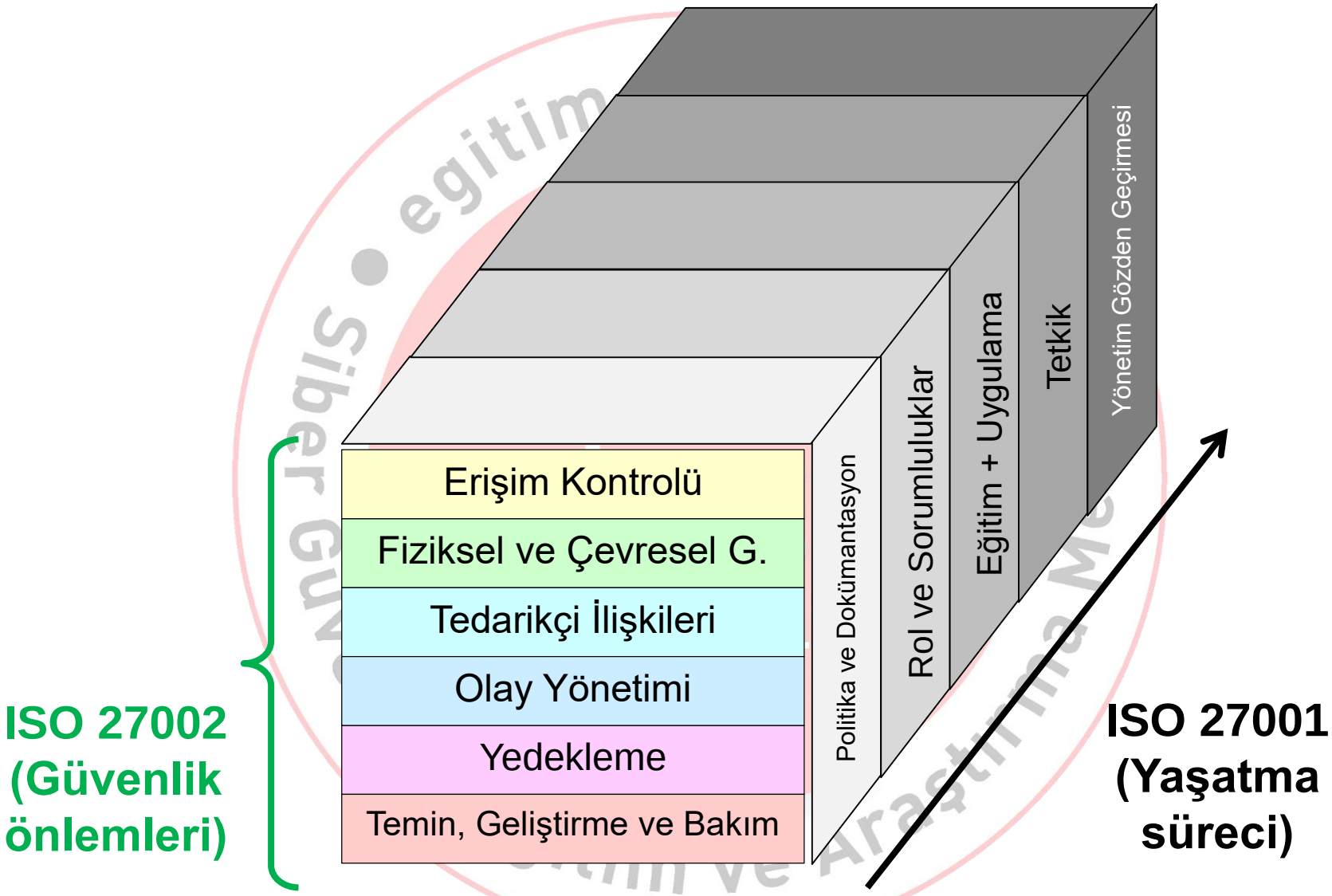
Bilgi İşleme Sistemlerinin Yedekliliği (ISO 27002, 17.2)

- İhtiyaç duyulan erişilebilirlik seviyesini karşılamak amacıyla sistem yedekliliği sağlanmalıdır.
- Yedek sistem veya mimarilerden çalışma test edilmelidir.

14. Uyum (ISO 27002, 18.x)

- İlgili **yasal gereksinimler** belirlenmeli ve takip edilmeli
- **Fikri mülkiyet hakları** ve benzeri yasal düzenlemeler
- Kayıtlar ve kişileri tanımlayan bilgiler uygun olarak korunmalıdır
- Güvenlik politikasına uyum, periyodik gözden geçirmelerle sağlanmalıdır

Özet: Bilgi Güvenliği Standartları



Denetim ve Sertifikasyon

Denetim Türleri

1. İç Denetim (kurum adına yapılır)

2. Dış Denetim (sertifikasyon makamı yapar)

   2.1 Ön denetim (isteğe bağlı)

   2.2 Belgelendirme denetimi

      2.2.1 Dokümantasyon denetimi
      2.2.2 Uygunluk denetimi

   2.3 Sürekli (periyodik) denetim (sertifikayı aldıktan sonra yılda bir)

   2.4 Tekrar denetim (sertifika süresi dolduktan 3 yıl sonra)

   2.5 Takip denetimi (SM'nin yaptığı denetimlerde uygunsuzluk çıkarsa)

Denetim ve Üslup

Detektif Clouseau

Peter Sellers (1925-1980)

- Tetkikçiler gerçeği hızla algılayan yetkin insanlardır (Clouseau interrogates the staff).
  - *Kurumun açıklarını / problemlerini paylaşmak saklamaya çalışmaktan hem daha kolay, hem daha faydalıdır.*

Denetim ve Üslup

- Tetkik edilen tarafın “ateşi çıkar” (en iyi olasılık).
  - *Ödevinizi yapın.*
  - *Tetkik sonucunu serinkanlılıkla karşılayın. BGYS bir süreçtir. Geçseniz de tekrar tetkik edileceksiniz.*

Dokümantasyon Denetimi

- Hedef,
  - Kurumda bulunması gereken BGYS dokümantasyonunu kontrol etmek ve
  - İkinci seviye denetim (uygunluk denetimi) için bilgi toplamaktır.

Dokümantasyon Denetimi

- BGYS, standardın ***dokümantasyon gereksinimleri*** açısından değerlendirilir.
- Denetçiler spesifik prosedürleri derinlemesine incelemez.
- Standardın tanımladığı ***zorunlu dokümanlar*** gözden geçirilir, yeterli miktarda politika, prosedür ve çalışma talimatı incelenir.
- Kurumda veya kurum dışında gerçekleştirilebilir.

Uygunluk Denetimi

- Hedef;
  - ***Kuruma ait BGYS'nin ISO 27001 gereksinimlerine uygunluğu***
  - Kuruma ait BGYS'nin işlerliği
  - Kurumun kendi hedeflerine, politikalarına ve prosedürlerine bağlılığı denetlenir
  - Kurumda gerçekleştirilir
  - BGYS'nin uygulandığının ve işletildiğinin doğrulanması için örnekler incelenir. (Örn: Kayıtlara bakılır)
  - Kayıtların prosedürlere uygunluğu denetlenir
- Baş tetkikçi **bulguları kurum yetkilileri ile paylaşır**.
- Denetimler sırasında uygunsuzluklar ortaya çıkmışsa kurum 3 ay içerisinde bunları düzeltmelidir.

Minör Uygunsuzluk

- ISO 27001 standardında tanımlanan bir gereksinimin,
  - kurumsal BGYS sürecinin durmasına veya
  - iş süreçlerini güvence altında tutma kabiliyetini yitirmesine

  neden olmayacak şekilde bulunmaması veya çalışmaması,
- Ürün veya hizmetin kullanıcıya
  - iş göremez veya
  - kurumsal yükümlülükleri sağlayamaz

  durumda ***ulaşma olasılığını*** ortaya çıkaracak haller.

Minör Uygunsuzluk Örnekleri

- Örnek Minör Uygunsuzluklar
  - *İş Sürekliliği Planı'na göre altı ayda bir yapılması gereken senaryo bazlı tatbikatın yapılmaması*
  - Güvenlik politikasının belirtilmiş süre içinde gözden geçirilmemesi
  - *Bazı dokümanların sınıflandırmasının yapılmamış olması*
  - Virüs tespit ajanlarının güncel olmaması

Majör Uygunsuzluk

- ISO 27001 standardında tanımlanan bir gereksinimin,
  - kurumsal BGYS sürecinin durmasına veya
  - iş süreçlerini güvence altında tutma kabiliyetini yitirmesine

  neden olacak şekilde bulunmaması veya çalışmaması,
- Ürün veya hizmetin kullanıcıya
  - iş göremez veya
  - kurumsal yükümlülükleri sağlayamaz

  durumda ***ulaşmasına*** neden olacak haller.

Majör Uygunsuzluk Örnekleri

- *BGYS'de herhangi bir yönetim liderliğinin gözlenmemesi*
- Risk analizi yapılmadan kontrollerin belirlenmesi
- *Güvenlik politikasının olmaması*
- Güvenlik rol ve sorumlulukların tanımlanmaması
- *İş sürekliliği planının olmaması*
- Fikri mülkiyet haklarına uyulmaması
- *Personele eğitim verilmemiş olması*

Gözlem

- ISO 27001 Standardında yer alan gereksinimlerin karşılanması ile ilgili gözlenen ancak yukarıdaki kategorilere girmeyen eksiklerdir.
- Herhangi bir yaptırım gerektirmez
- Örnek:
  - Risk değerleme rehberinde tehdit etki derecelerinin tarifinde "yüksek", "orta" ve "düşük" ifadeleri geçmektedir. Bu ifadeler daha somut olarak açıklanmalıdır.

Denetim Egzersizleri

– Denetim Egzersizleri.xls dokümanında yer alan 30 adet olay/duruma karşılık gelen ISO 27001 standart maddesini bulunuz (Süre: 1,5 saat).

TÜBİTAK

Teşekkürler