

BGYS ve BGYS Kurma Deneyimleri

6. Kamu Kurumları BT Güvenliđi Konferansı - 8 Haziran 2011

Fikret Ottekin

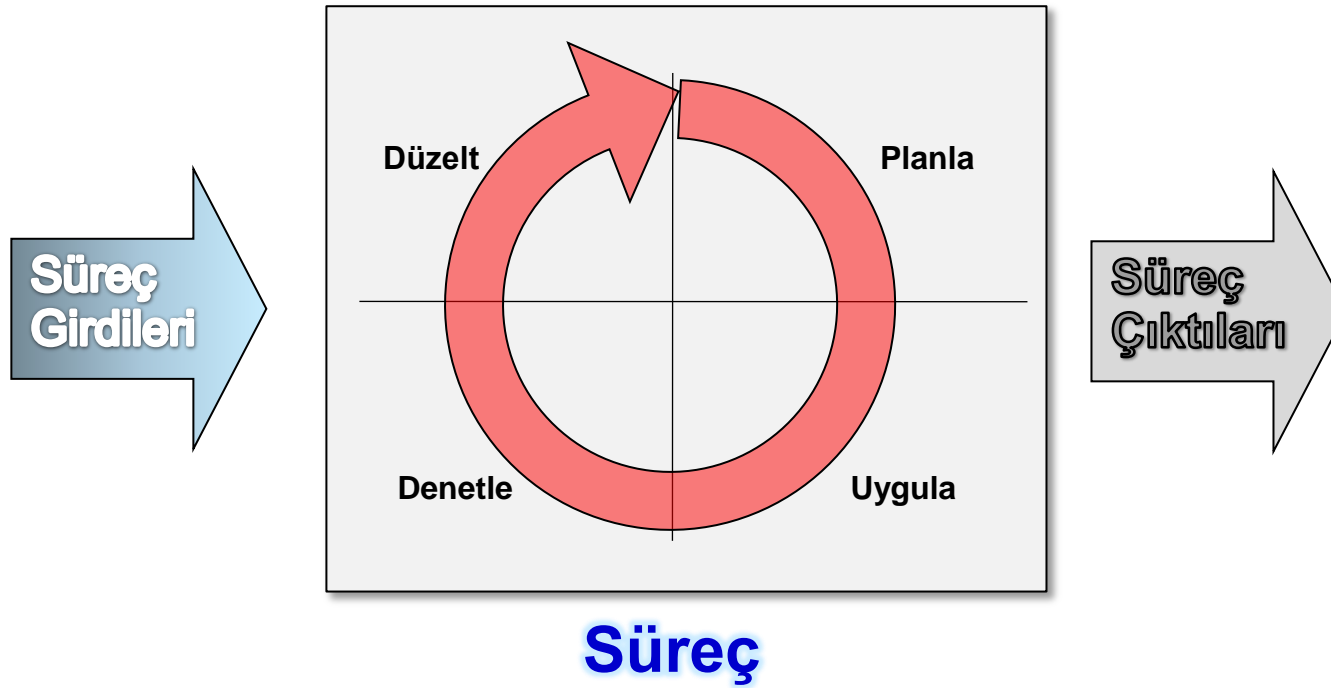


Bilişim Sistemleri Güvenliđi Grubu

ISO 9001 ve ISO 27001

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

Süreç Tabanlı Sistemler



ISO 9001 ve 27001: Girdi ve Çıktılar



	ISO 9001 Kalite Yönetim Sistemi	ISO 27001 Bilgi Güvenliği Yön. Sis.
Süreç Girdileri	- Müşteri memnuniyeti (müşteri ve piyasanın talepleri)	- Kurumun bilgi güvenliği riskleri (yükümlülükler, bilgi varlıkları ve tehditler)
Süreç Çıktıları	- Artan müşteri memnuniyeti (kalitesi artmış ürün/servis)	- Kontrol altına alınmış riskler (gelişen güvenlik anlayışı ve iyileştirilmiş iş süreçleri)

Risk Nedir?



- Seçilen eylemin kayıpla sonuçlanma potansiyeline risk denir. (Wikipedia)
- Potansiyel (Türk Dil Kurumu):
 - Gizli kalmış, henüz varlığı ortaya çıkmamış olan, gizil.
 - Gelecekte oluşması, gelişmesi mümkün olan.
 - Kullanılmaya hazır (güç, yetenek).

Bilgi Güvenliğinde Risk



Botnet



DDoS

WEB Sunucu



Sunucuya ulaşılamıyor

```
Command Prompt
C:\Users\vista>ping google.com
Pinging google.com [209.85.231.104] with 32 bytes of data:
Reply from 10.239.15.1: Destination net unreachable.
Reply from 10.239.15.1: Destination net unreachable.
Reply from 10.239.15.1: Destination net unreachable.
Reply from 10.239.15.1: Destination net unreachable.
Ping statistics for 209.85.231.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

C:\Users\vista>ping google.com
Pinging google.com [209.85.231.104] with 32 bytes of data:
Reply from 209.85.231.104: bytes=32 time=53ms TTL=55
Reply from 209.85.231.104: bytes=32 time=51ms TTL=54
Reply from 209.85.231.104: bytes=32 time=53ms TTL=54
Reply from 209.85.231.104: bytes=32 time=50ms TTL=55
Ping statistics for 209.85.231.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 50ms, Maximum = 53ms, Average = 51ms
C:\Users\vista>
```

- Bilginin gizlilik, bütünlük veya erişilebilirliğinin kaybolma potansiyelidir.

Varlık Envanteri

- Bilgi varlıkları listelenir
 - Bilgi, yazılım, donanım, insan kaynağı, alınan servisler
- Değerlendirilir
 - Bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik değerleri, sahibi ve konumu belirlenir.
- Uzun ve yorucu bir çalışmadır.
 - *Önemli bilgi varlıklarını içeren bir envanter yeterli olabilir.*
- Kurumsal bilgi varlıkları envanteri üstünde yapılan çalışma ile önemli bilgi güvenliği riskleri belirlenir.

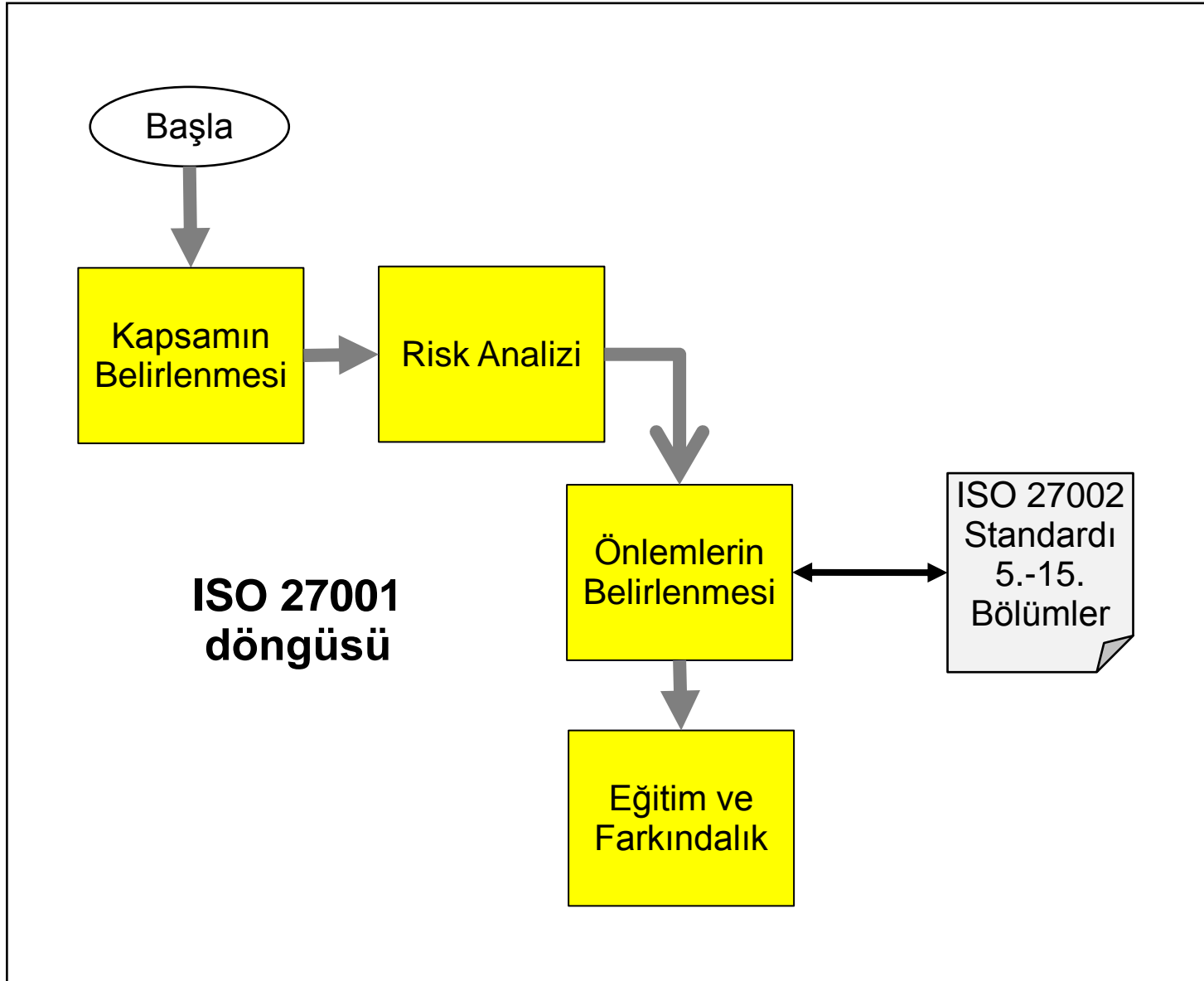
Çeşitli Bilgi Güvenliği Riskleri

Tehdit	Bilgi Varlığı/Açıklık	Risk
Servis dışı bırakma saldırıları	Kurumun WEB Sitesi	WEB sitesinin servis veremez duruma düşmesi - maddi kayıp
İnsani zayıflıklar	USB belleklere ilişkin politika ve eğitim eksikliği / taşıma kolaylığı	Belleklerin kurum dışında kaybolması - kurumsal bilginin açığa çıkması
Sistem odası sıcaklığında ve nem düzeyinde dalgalanmalar	Sunucu sabit diskleri / sınırlı dayanıklılık	Sabit disk arızası - kurumsal bilginin kaybedilmesi
Sistem yöneticilerinin iş yoğunluğu / prosedürsüz çalışması	Güvenlik duvarı kural listesi	Personel hatası - sunucuların Internet'ten saldırıya açık hale gelmesi.

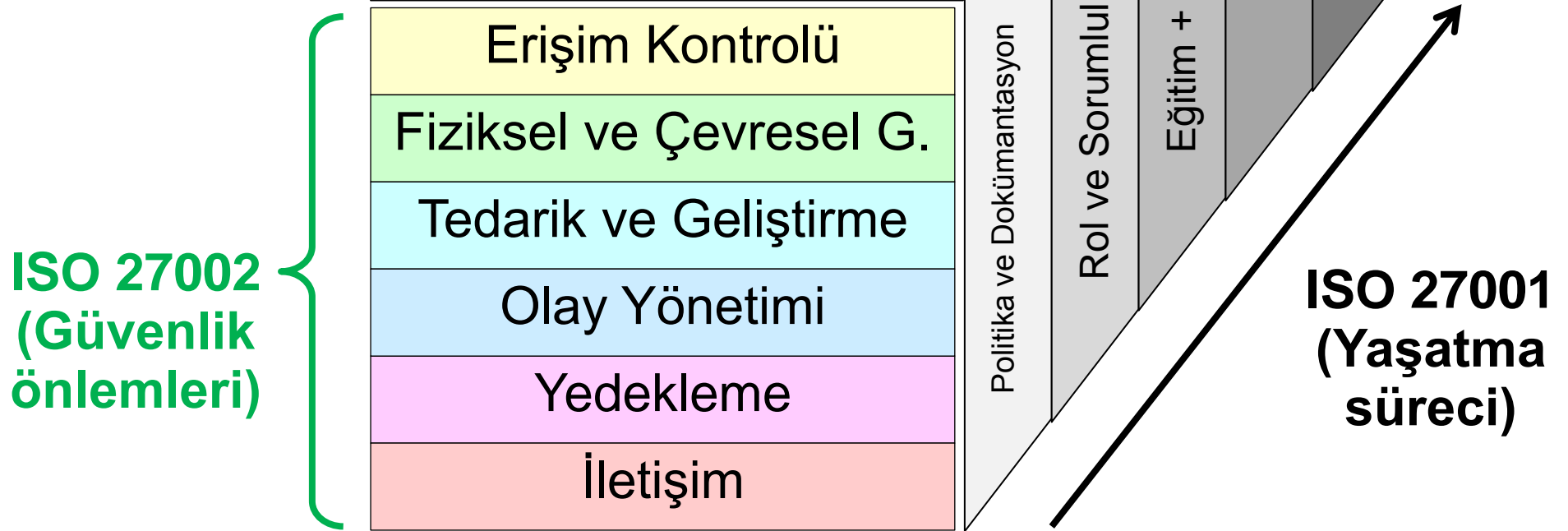
ISO 27001 Süreci, özet



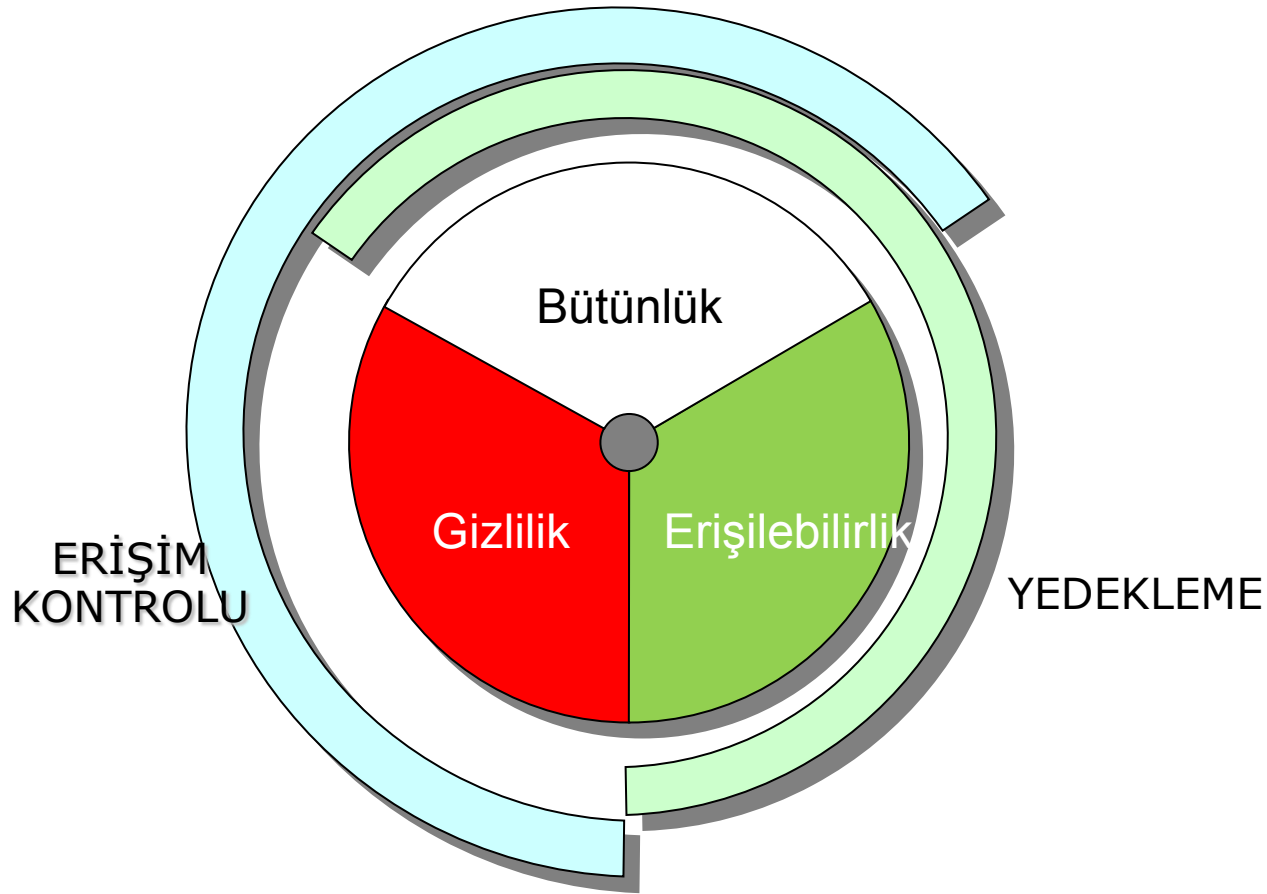
ISO 27001 – 27002 ilişkisi



ISO 27001 – 27002 ilişkisi



ISO 27002: Güvenlik Önlemleri



- ISO 27002, yüzün üstünde önlem içeren bir kılavuzdur. Başlıca önlemler:
 - Erişim Kontrolü **ÖNLEYİCİ** faaliyettir
 - Yedekleme **DÜZELTİCİ** faaliyettir.

Eriřim Kontrol Politikası

Eriřim kontrol politikası tablosu

Kullanıcı ↓	Dizinler					Tesisler		
	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

Yedekleme



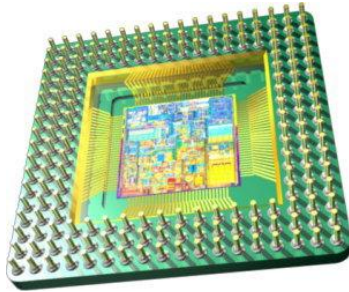
- Yedekleme + yedekten geri dönme prosedüre bağlanmalıdır.
- Gizli bilginin yedeği de gizlidir.
- Yedekler asıl bilgiden uzakta saklanmalıdır.
- *İnsan kaynağının yedeklenmesi?*

Dokümantasyon

Politika	Ne yapacağım?
Prosedür	Nasıl yapacağım?
Kayıt	Ne yapıldı / Ne oldu?

- Belirlenen güvenlik önlemleri politika ve prosedürlere dönüştürülür.
- Kayıtlar aracılığı ile önlemlerin çalışması izlenir.

Politika ile Yazılım arasındaki farklar



Yazılım

CPU'da çalışır.

(+) CPU'nun yazılımı beğenmemesi tanımlı değildir. Mutlaka çalıştırır.

(-) CPU yazılımdaki hatayı bulamaz / düzeltemez.

Politika / prosedür

İnsanlar tarafından uygulanır.

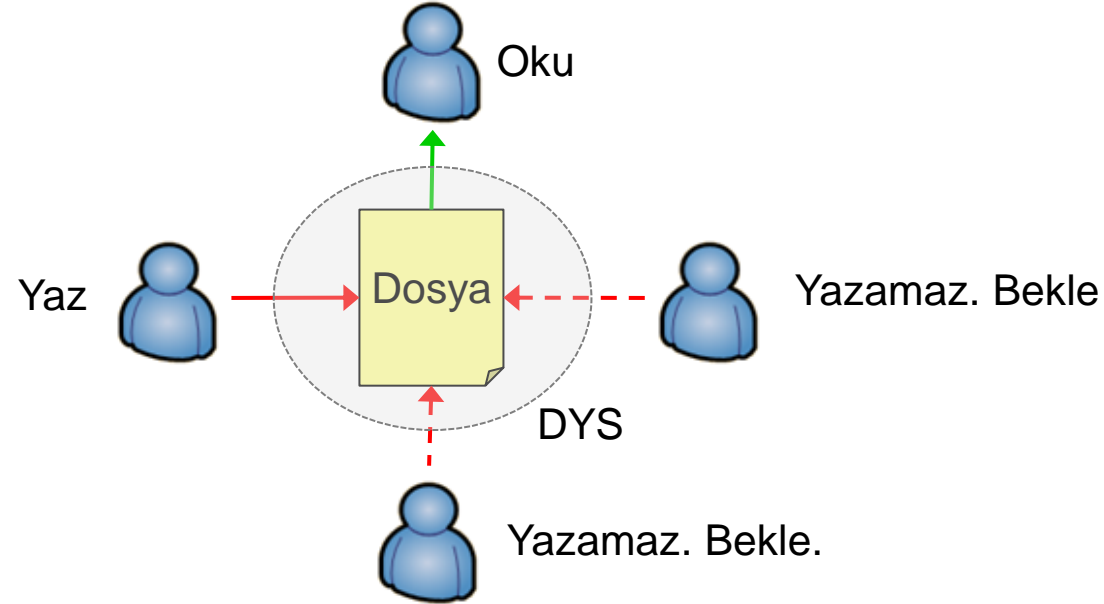
(-) İnsanlar tarafından benimsenmesi gerekir. Yoksa rafta kalır.

(+) 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

Yönetim Desteğinin Önemi

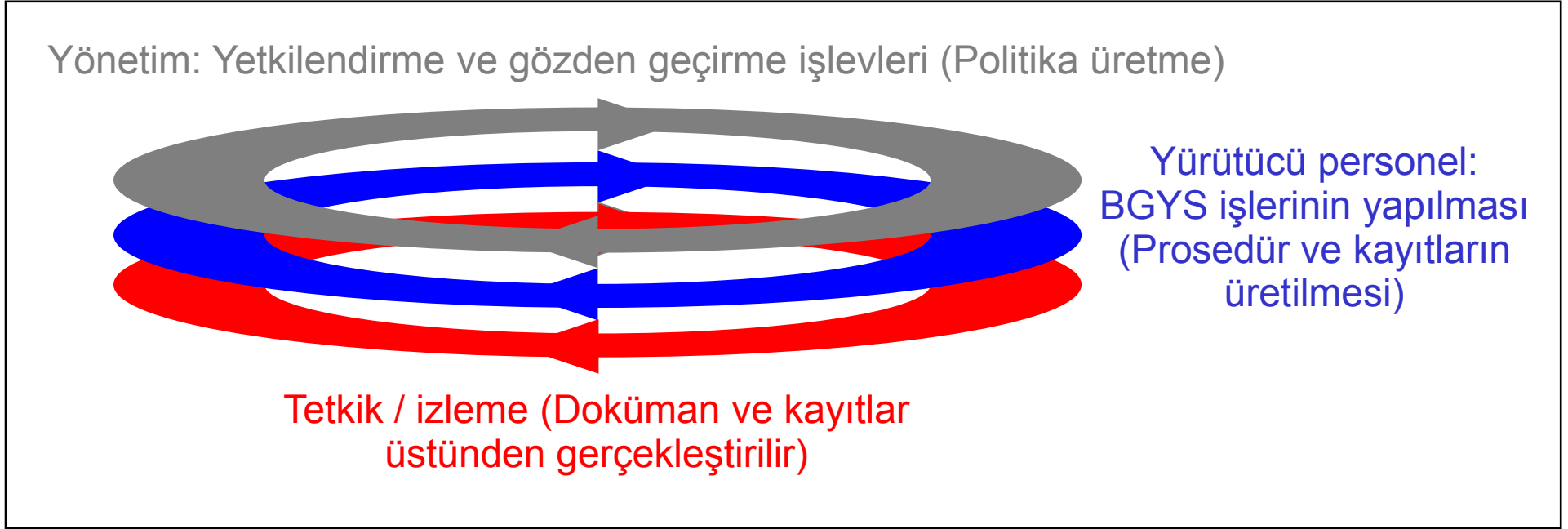
- Hedefi tanımlama
 - *Sertifika hedefi uygun değil: sertifika sebep değil sonuçtur.*
 - *BGYS kurmaya en uygun kurum, ağızı yanmış kurumdur.*
- Kaynak sağlama (insan kaynağı + maddi kaynak)
 - *Sözde değil özde olması gerekir.*
- Belli başlı politikaların belirlenmesi
 - *Kural / kısıtlamaların kurumsal iş süreçlerine uygunluğu*

Yönetim Desteğinin Önemi

- Personel motivasyonu
 - *Değişim ve ek iş yükü çalışanlar tarafından “angarya” olarak algılanabilir.*
 - *Bilgilendirme - ikna*

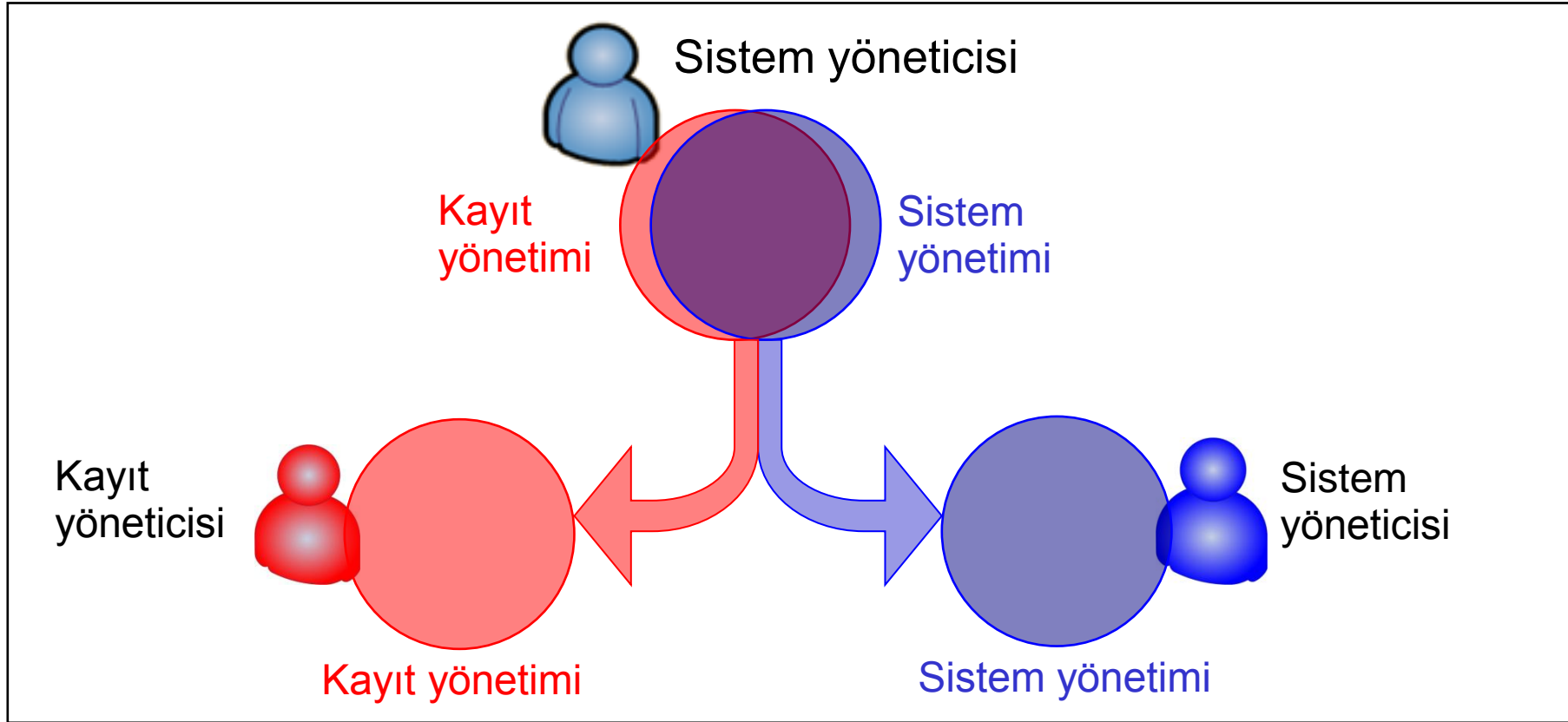


Görevler Ayrılığı



- İşin **yapılması** ile yetkilendirilmesi birbirinden ayrılmalıdır. *(ISO 27002, 10.1.3 Görevler Ayrılığı)*
- Tetkikçiler kendi **yaptıkları** işi **tetkik** edemezler. *(ISO 27001, 6. İç Tetkik)*
- Yasama/**Yürütme**/**Yargı** => Yetkilendirme/**Yürütme**/**Tetkik**

Sistem Yöneticilerinin Durumu



- Sistem yöneticilerinin yaptıkları işlemlere ilişkin kayıtlara erişememeleri,
- Kayıt yöneticilerinin sistem üstünde işlem yapamaması gerekir.

Tetkik

- Tetkikçiler gerçeği hızla algılayan yetkin insanlardır.
 - *Kurumun açıklarını / problemlerini paylaşmak saklamaya çalışmaktan hem daha kolay, hem daha faydalıdır.*
- Tetkik edilen tarafın “ateşi çıkar” (en iyi olasılık).
 - *Ödevinizi yapın.*
 - *Tetkik sonucunu serinkanlılıkla karşılayın. BGYS bir süreçtir. Geçseniz de tekrar tetkik edileceksiniz.*

Düzeltilici – Önleyici Faaliyetler

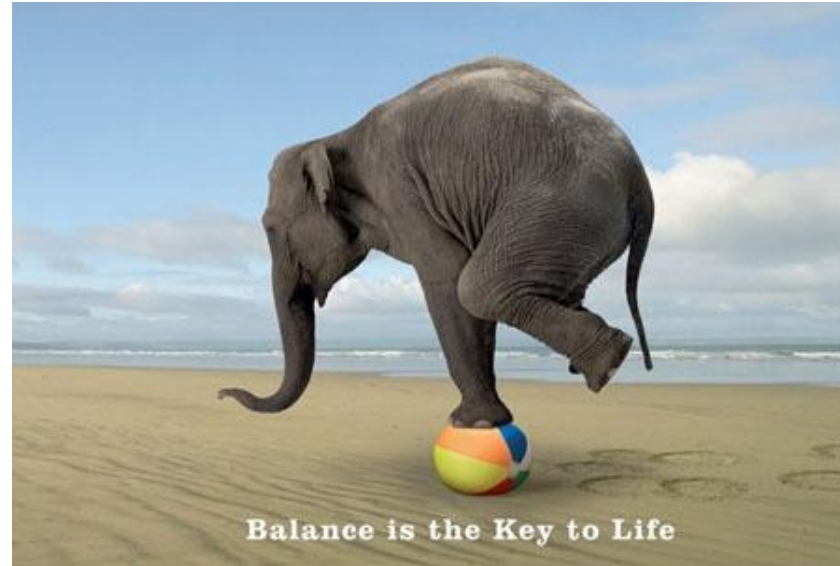
- Tetkik bulgularının **düzeltilici faaliyetlere** dönüştürülmesi gerekir.
- Kök neden analizi
 - Problemi değil probleme neden olan şeyi ortadan kaldırmak.
 - *(Yazılımdaki bir “bug”ı düzeltmek değil “bug” üreten geliştirme sürecini düzeltmek gibi)*
- Diğer kurumların yaşadığı olaylar veya risk analizi sonucunda **önleyici faaliyetler** belirlenebilir.

BGYS Kurarken: Danışman Desteđi



- Danışmandan beklenenler:
 - *Uzak görüşlü olmak, liderlik ve teknik destek*
 - *ISO 27001 uyumluluđunu kovalarken dozu kaçırmamak (İş süreçlerine ve insan kaynađına dikkat!)*

BGYS Kurarken Dengeyi Gözetmek



- **Gizlilik** ile **erişilebilirlik** arasında denge.
 - *Gizli bilgiyi koruma uğruna iş süreçlerini fazla yavaşlatmak kurumda hayatı çekilmez hale getirebilir.*
- ISO 27001 uyumluluğu ile iş gücü arasında denge.
 - *Kurulan sistemin eksiklerini ISO 27001 standardına dengeli bir şekilde yaymak.*

BGYS Kurarken: Problemler

- Kurmak çalıştırmaktan zordur. Çünkü:
 - Yapılacak iş fazla. (Politikaları oluşturmak güncellemekten çok daha zor)
 - Personel deneyimsiz.
- Risk analizinin gerçekçi bir biçimde yapılması
 - Risklerin görevli personel tarafından saklanması riski
 - Kendi iş yükünü azaltmak için
 - Yönetimin reaksiyonundan çekindiği için
 - *9001'deki kadar belirgin bir şekilde müşteriden geri besleme gelmiyor.*

BGYS Kurarken: Uzun ince bir yol



- Orta büyüklükte bir kuruma BGYS kurulması 12-24 ay sürmektedir.
- Ülke birliğinin / yönetim desteğinin kaybolduğu dönemler yaşanabilir.

Mutlu Son


THE INTERNATIONAL CERTIFICATION NETWORK
CERTIFICATE
IQNet and
TSE
hereby certify that the organization
MERKEZİ FINANS VE İHALE BİRİMİ - CENTRAL FINANCE AND CONTRACTS UNIT
ESKİŞEHİR YOLU 4.KM. 2.CAD. (HALKBANK KAMPÜSÜ) NO:63 C-BLOK 06580 SÖĞÜTÖZÜ
- ANKARA / TÜRKİYE
has implemented and maintains a
which fulfills the requirements of the following standard
TS ISO / IEC 27001
Scope of the certificate is given in annex.
Date of Revision: 25-03-2011
Date of Certificate: 25-03-2011
Valid Until: 25-03-2014
Registration Number : TR-BYS-032/11


Michael Drechsel
President of IQNet




Aykut KIRBAŞ
Head of Personnel and System
Certification Center



IQNet Partners*:
AENOR Spain, AFNOR Certification France, AIB/Viascert International Belgium, ANCE Mexico, APCER Portugal,
CISQ Italy, CQC China, CQM China, CQS Czech Republic, Cso Cert Croatia, DQS Holding GmbH Germany, DS Denmark,
ELOT Greece, PCAV Brazil, FONDORISHA Venezuela, HKQA Hong Kong China, ICONTEC Colombia, IMC Mexico,
Inspecta Certification Finland, IRAM Argentina, JQA Japan, KPC Korea, MSZT Hungary, NENKO AS Norway, NSAI Ireland,
PCBC Poland, Quality Austria Austria, KR Ruzsza SI, Israel, SIQ Slovenia, SIRIM QAS International Malaysia, SQS Switzerland, SRAC Romania, TEST
St Petersburg, Russia, TSE Turkey, YUQS Serbia.


IQNet is represented in the USA by: AFROR Certification, CISQ, DQS Holding GmbH and NSAI Inc.
* The list of IQNet partners is valid at the time of issue of this certificate. Updated information is available under www.iqnet-certification.com

069

 **TÜRK STANDARDLARI ENSTİTÜSÜ** 
BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ BELGESİ
Kuruluş Adı ve Adresi
Organisation Name and Address
MERKEZİ FINANS VE İHALE BİRİMİ - CENTRAL FINANCE AND CONTRACTS UNIT
ESKİŞEHİR YOLU 4.KM. 2.CAD. (HALKBANK KAMPÜSÜ) NO:63 C-BLOK 06580 SÖĞÜTÖZÜ - ANKARA TÜRKİYE

KAPSAM: TS ISO / IEC 27001
- AVRUPA BİRLİĞİ TARAFINDAN TÜRKİYEDE FİNANSE EDİLEN PROGRAMLAR ÇERÇEVESİNDE GERÇEKLEŞEN İHALELERİN
BÜTÇELEME, İHALEYE ÇIKMA, SOZLEŞME İMZALAMA, ÖDEME, MUHASEBE VE MALİ RAPORLAMA HİZMETLERİ

SUNUMU
SCOPE: TS ISO / IEC 27001
- AS AN INDEPENDENT BODY, HAS THE SOLE RESPONSIBILITY OVER THE OVERALL BUDGETING, TENDERING, CONTRACTING,
PAYMENTS, ACCOUNTING AND FINANCIAL, AND REPORTING ASPECTS OF THE PROCUREMENT OF SERVICES, SUPPLIES, WORKS
AND GRANT IN THE CONTEXT OF EU FUNDED PROGRAMMES IN TURKEY




Belge No / Certificate No	Belge Tarihi / Date of Certificate	Geçerlilik Tarihi / Valid Until	Revizyon Tarihi / Date of Revision
BYS-032/11	25.03.2011	25.03.2014	25.03.2011

Bu belge belgelendirme şartlarına uygunluk sağlandığı sürece geçerlidir.
This certificate is valid provided that compliance with the certification requirement is maintained.

Sistem Belgelendirme Müdürü
System Certification Director

Personel ve Sistem Belgelendirme Merkezi Başkanı
Head of Personnel and System Certification Center


Mustafa ÖLÇER


Aykut KIRBAŞ

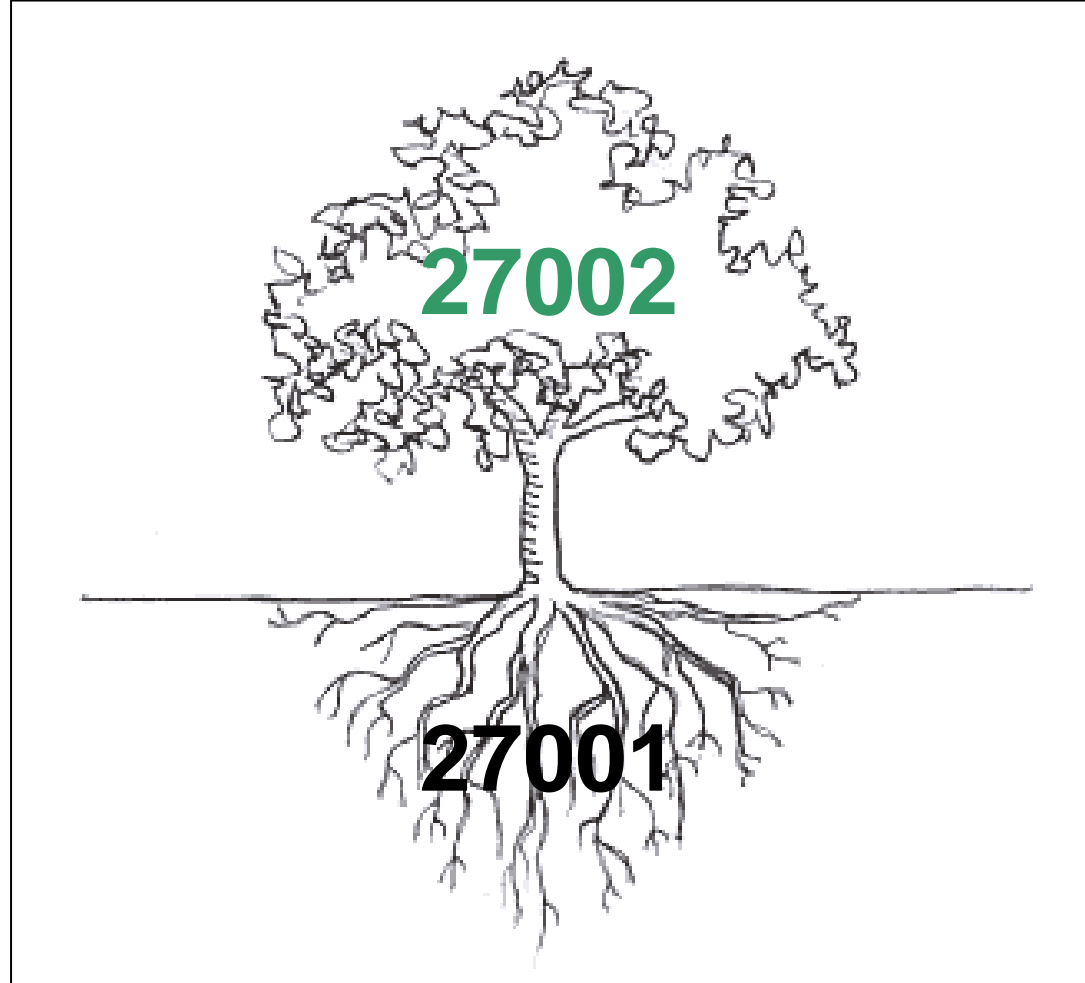



Partner of
THE INTERNATIONAL CERTIFICATION NETWORK

Özet

- Bilgi güvenliği standartlarının detaylarında kaybolmamak gerekir.
 - *Asıl amaç kurumun işlerini düzene sokmaktır.*
- Dönüşümün zaman alacağı unutulmamalı.
 - *Orta vadede (>1 yıl) olumlu sonuçlar alınabilir.*
- 9001, 27001 ve 27002 standartlarını karıştırın.
 - *(45 TL +%8 KDV www.tse.org.tr)*

Sonuç



Güvenlik önlemleri

Yaşatma süreci

Sorular?



Fikret Ottekin

fottekin@uekae.tubitak.gov.tr

TÜBİTAK - UEKAE

Bilişim Sistemleri Güvenliği Grubu

www.bilgiguvenligi.gov.tr