ODTÜ BİDB'DE ISO 27001:2005 SERTİFİKASYON SÜRECİ

SUNA KÜÇÜKÇINAR

Uzman

Bilgi Güvenliği Birimi

sunay@metu.edu.tr

İBRAHİM ÇALIŞIR

Mühendis

Bilgi Güvenliği Birimi Yöneticisi

icalisir@metu.edu.tr

Ajanda

- ✓ ISO 27001'e neden ihtiyaç duyduk?
- ✓ Neler yaptık?
- ✓ Ne faydası oldu?
- ✓ Zorluklar neler?
- ✓ Yol planımız nedir?
- ✓ Tavsiyeler
- ✓ Soru-cevap

Neden ihtiyaç duyduk?

- ✓ Bilgi güvenliğinin gün geçtikçe daha çok önem kazanması
- ✓ 9 grup 3 birim var; her birinin BG uygulamaları farklı
  - Farklı gruplar arası BG bağlamında iletişim sağlamak
- ✓ Organizasyon sağlamak, toparlayıcı, düzenleyici olmak
- ✓ Keyfiliği ortadan kaldırmak, standart getirmek
- ✓ Politika prosedür gibi önemli belgeleri düzenlenmesini sağlamak
  - Sadece birkaç tane politika belgemiz vardı.
- ✓ SİSTEM OLUŞTURMAK, SÜREKLİ İYİLEŞME SAĞLAMAK

Aşama 1 - Başlangıç

- ✓ Araştırma
- ✓ Fark Analizi
- ✓ Yönetim Desteği
- ✓ Kapsamın Belirlenmesi
- ✓ Danışmanlık Hizmeti İhale Şartnamesi
  - (Sertifika alınıncaya kadar tüm süreçte danışmanlık + iç/dış sızma testleri)
- ✓ İhale Süreci
- ✓ Danışmanla Çalışmaların Başlaması (Eylül 2013)
- ✓ Proje Planı Oluşturulması

Aşama 2 - Varlık Envanteri

Varlık Envanteri

- ✓ Varlık sınıfları:

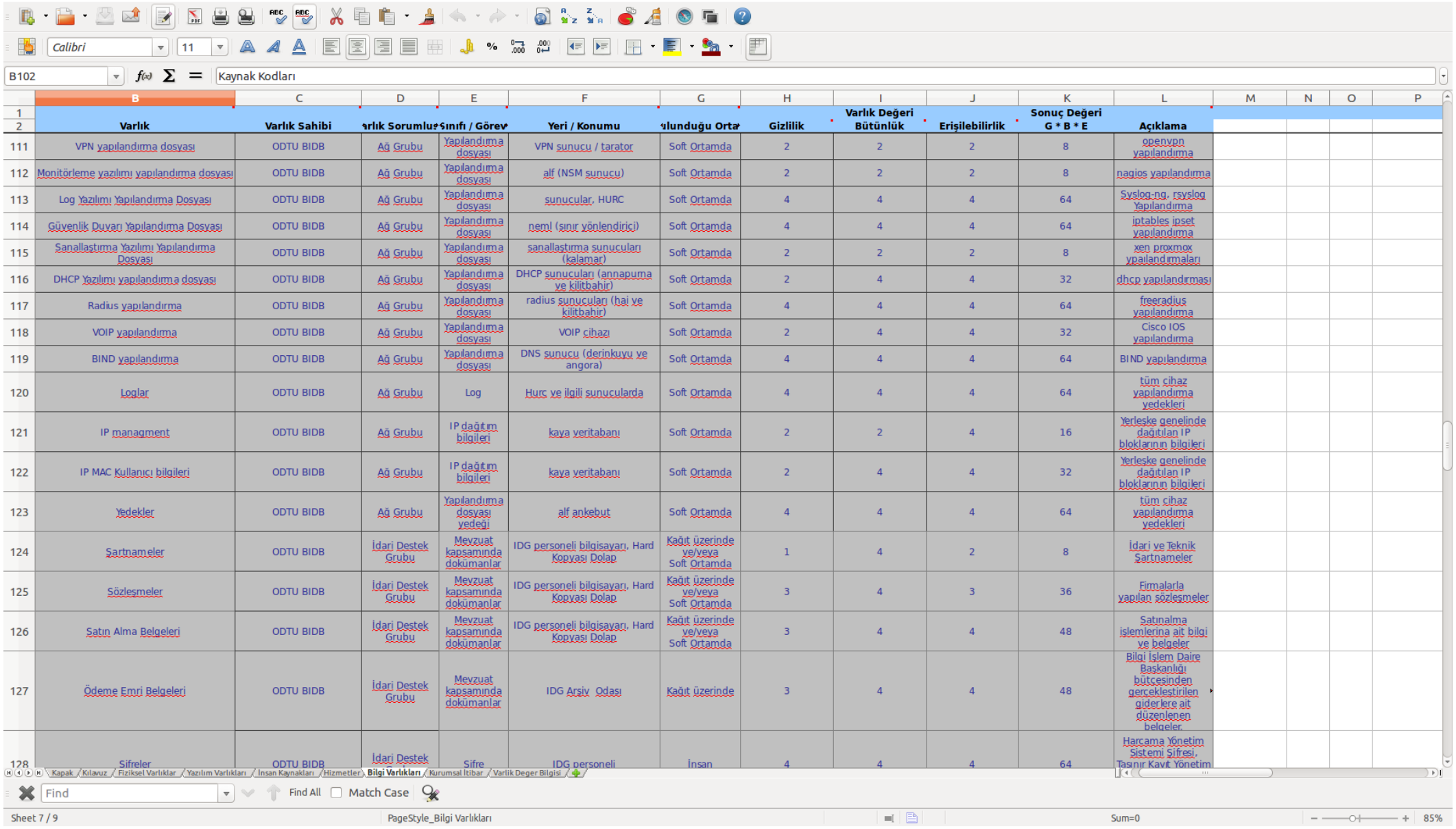
  Fiziksel, yazılım, bilgi, kurumsal itibar, İK, kurumsal hizmetler
- ✓ Varlık listesi oluşturma
- ✓ Varlık Değerlemesi skalasına karar verme
  - Biz 1-5 arası bir değerleme skalası kullanmaya karar verdik.
- ✓ **Gizlilik Bütünlük Erişilebilirlik** değerlerinin belirlemesi
- ✓ Varlık Değerlerini oluşturma = GxBxE
- ✓ Gruplardan toplanan verileri birleştirme, rafine hale getirme
  - Granülite önemli, olabildiğince genelleme yapıldı.
- ✓ 503 satır varlık envanteri
  - 129 fiziksel, 135 yazılım, 31 İK, 13 Hizmet, 193 Bilgi, 2 Kurumsal İtibar

Gizlilik Değeri	Bütünlük Değeri	Erişilebilirlik Değeri	AÇIKLAMA
5	5	5	Çok Yüksek
4	4	4	Yüksek
3	3	3	Orta
2	2	2	Düşük
1	1	1	Çok Düşük

Varlık Değerleri

Güvenlik Hedefi	Çok Düşük	Düşük	Orta	Yüksek	Çok Yüksek
Gizlilik	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan bilginin kritiklik seviyesi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan bilginin kritiklik seviyesi çok az etkiler. Etki kısa vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkmaz. Açığa çıkan bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi açığa çıkar. Açığa çıkan bilginin kritiklik seviyesi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
Bütünlük	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen bilginin kritiklik seviyesi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen bilginin kritiklik seviyesi çok az etkiler. Etki kısa vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişmez. Kontrol dışı değişen bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgi kontrol dışı değişir. Kontrol dışı değişen bilginin kritiklik seviyesi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.
Erişilebilirlik	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen bilginin kritiklik seviyesi kurumu etkilemez.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen bilginin kritiklik seviyesi çok az etkiler. Etki kısa vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilebilir. Erişilebilirliğine zarar gelen bilginin kritiklik seviyesi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.	Varlığa bir zarar gelmesi durumunda kritik bilgiye erişilemez. Erişilebilirliğine zarar gelen bilginin kritiklik seviyesi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.

VARLIK ENVANTERİ



	B	C	D	E	F	G	H	I	J	K	L
1								Varlık Değeri		Sonuç Değeri	
2	Varlık	Varlık Sahibi	ırlık Sorumlu	Sınıfı / Görev	Yeri / Konumu	ılunduğu Orta	Gizlilik	Bütünlük	Erişilebilirlik	G * B * E	Açıklama
111	VPN yapılandırma dosyası	ODTU BIDB	Ağ Grubu	Yapılandırma dosyası	VPN sunucu / tarator	Soft Ortamda	2	2	2	8	openvpn yapılandırma
112	Monitörleme yazılımı yapılandırma dosyası	ODTU BIDB	Ağ Grubu	Yapılandırma dosyası	alf (NSM sunucu)	Soft Ortamda	2	2	2	8	nagios yapılandırma
113	Log Yazılımı Yapılandırma Dosyası	ODTU BIDB	Ağ Grubu	Yapılandırma dosyası	sunucular, HURC	Soft Ortamda	4	4	4	64	Syslog-ng, rsyslog Yapılandırma
114	Güvenlik Duvarı Yapılandırma Dosyası	ODTU BIDB	Ağ Grubu	Yapılandırma dosyası	neml (sınır yönlendirici)	Soft Ortamda	4	4	4	64	iptables ipset yapılandırma
115	Sanallaştırma Yazılımı Yapılandırma Dosyası	ODTU BIDB	Ağ Grubu	Yapılandırma dosyası	sanallaştırma sunucuları (kalamar)	Soft Ortamda	2	2	2	8	xen proxmox ypailandırmaları
116	DHCP Yazılımı yapılandırma dosyası	ODTU BIDB	Ağ Grubu	Yapılandırma dosyası	DHCP sunucuları (annapuma ve kilitbahir)	Soft Ortamda	2	4	4	32	dhcp yapılandırması
117	Radius yapılandırma	ODTU BIDB	Ağ Grubu	Yapılandırma dosyası	radius sunucuları (hai ve kilitbahir)	Soft Ortamda	4	4	4	64	freeradius yapılandırma
118	VOIP yapılandırma	ODTU BIDB	Ağ Grubu	Yapılandırma dosyası	VOIP cihazı	Soft Ortamda	2	4	4	32	Cisco IOS yapılandırma
119	BIND yapılandırma	ODTU BIDB	Ağ Grubu	Yapılandırma dosyası	DNS sunucu (derinkuyu ve angora)	Soft Ortamda	4	4	4	64	BIND yapılandırma
120	Loglar	ODTU BIDB	Ağ Grubu	Log	Hurc ve ilgili sunuculardа	Soft Ortamda	4	4	4	64	tüm cihaz yapılandırma yedekleri
121	IP managment	ODTU BIDB	Ağ Grubu	IP dağıtım bilgileri	kaya veritabanı	Soft Ortamda	2	2	4	16	Yerleşke genelinde dağıtılan IP bloklarının bilgileri
122	IP MAC Kullanıcı bilgileri	ODTU BIDB	Ağ Grubu	IP dağıtım bilgileri	kaya veritabanı	Soft Ortamda	2	4	4	32	Yerleşke genelinde dağıtılan IP bloklarının bilgileri
123	Yedekler	ODTU BIDB	Ağ Grubu	Yapılandırma dosyası yedeği	alf ankebut	Soft Ortamda	4	4	4	64	tüm cihaz yapılandırma yedekleri
124	Şartnameler	ODTU BIDB	İdari Destek Grubu	Mevzuat kapsamında dokümanlar	IDG personeli bilgisayarı, Hard Kopyası Dolap	Kağıt üzerinde ve/veya Soft Ortamda	1	4	2	8	İdari ve Teknik Şartnameler
125	Sözleşmeler	ODTU BIDB	İdari Destek Grubu	Mevzuat kapsamında dokümanlar	IDG personeli bilgisayarı, Hard Kopyası Dolap	Kağıt üzerinde ve/veya Soft Ortamda	3	4	3	36	Firmalarla yapılan sözleşmeler
126	Satın Alma Belgeleri	ODTU BIDB	İdari Destek Grubu	Mevzuat kapsamında dokümanlar	IDG personeli bilgisayarı, Hard Kopyası Dolap	Kağıt üzerinde ve/veya Soft Ortamda	3	4	4	48	Satınalma işlemlerine ait bilgi ve belgeler
127	Ödeme Emri Belgeleri	ODTU BIDB	İdari Destek Grubu	Mevzuat kapsamında dokümanlar	IDG Arşiv Odası	Kağıt üzerinde	3	4	4	48	Bilgi İşlem Daire Başkanlığı bütçesinden gerçekleştirilen giderlere ait düzenlenen belgeler.
128	Şifreler	ODTU BIDB	İdari Destek	Şifre	IDG personeli	İnsan	4	4	4	64	Harcama Yönetim Sistemi Şifresi, Taşınır Kayıt Yönetim

Aşama 3 - Sızma Testleri

İç ve Dış Sızma Testleri

- ✓Danışman firma tarafından gerçekleştirildi
  - Kurum İçi Testler
  - Kurum Dışı Testler
  - DDoS Testi
  - Kaynak Kod Analizi
  - Sosyal Mühendislik Testleri
- ✓Test Sonuçları →
  - Rapor olarak BİDB BGB'ye teslim edildi
- ✓Önlemler
  - Önlemlerin risk tedavi planına dahil edilmesi

Test Sonuçları - Zafiyetler
SQL yerleştirme zafiyeti
XSS çalıştırma zafiyeti
Zayıf güvenlik duvarı kuralları
Eski Apache sürümü kaynaklı zafiyetler
SSL v2 kullanımı
Ön tanımlı SNMP topluluk adı kullanımı
Kolay tahmin edilebilir yönetici yarolası
Güncel olmayan/desteklenmeyen işletim sistemi (IBM AIX 5.2)
Zayıf SSL şifreleme algoritması kullanılması
Eski sürüm PHP kullanımı (5.3.9)

Aşama 4 – Risk Analizi

Risk Analizi

- ✓Neleri risk işleme planına alınan varlıklar
  - Varlık Değeri 27 ve üzeri olan varlıklar
  - GBE değerlerinden herhangi biri 5 olan varlıklar
- ✓Tehditler ve zafiyetler belirlenir
  - Tehdit oluşma olasılıkları belirlenir
  - Tehdit oluşursa varlığa vereceği hasar derecesi belirlenir.
- ✓ RİSK SEVİYESİ = VARLIK DEĞERİ x TEHDİDİN OLUŞMA OLASILIĞI x İŞ HASARININ DERECESİ
  - RİSK SEVİYESİ $_{\text{Kabul Edilebilir}}$ = 27 x 3 x 3 = 243
  - Risk seviyesi > 243 olan varlıklar **Risk Tedavi Planı**na alınır.
- ✓ 226 satır risk analizi

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

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

Aşama 4– Risk Tedavisi

Tespit edilen riskler için yapılabilecekler

- ✓ Riski Azaltma / Önlem Alma
  - İşletim sisteminin güncel versiyonunu kurmak
  - Yazılımın güncel versiyonunu kurmak
  - Administrator/root parolalarını güçlendirmek
  - Ssl v2 değil v3 kullanma
  - En az 128 bit anahtarlama kullanmayı benimseme
  - …..
- ✓ Riskten Kaçınma
  - Aslında aktif olarak kullanılmayan kasanın devre dışı bırakılması
- ✓ Riski Kabul Etme
  - Elektrik İşletme Müdürlüğü nötr hattımızı düzenleyemediği için buradan gelecek tehditleri kabul ediyoruz
- ✓ Risk Transferi
  - Olası bir doğal afet için sigorta yaptırmak gibi….

Aşama 4– Risk Tedavisi

NO	VARLIK	VARLIK DEĞERİ	Varlık sahibi	ZAAFİYET	TEHDİT	MEVCUT KONTROLLER	TEHDİT GERÇEKLEŞİRSE OLUŞACAK ETKİ	ETKİ SINIFI (G:Gizlilik, B:Bütünlük, E:Erişilebilirlik)	İLAVE KONTROLLER ÖNCESİ			KABUL EDİLEN RİSK	KAÇINILAN RİSK	TRANSFER EDİLEN RİSK	İŞLENECEK RİSK	İLAVE KONTROL
									T.O. OLASILIĞI	HASAR DERECESİ	RİSK DEĞERİ					
1	Sistem Odası	125	SG	Saklama ortamının yetersiz bakımı/yanlış kurulmuş olması	Bilgi sisteminin kırılması			GBE	2	4	1000			*		Kamera sistemi yerleştirilecek
				Nem, toz ve kire açık olma	Toz, zedelenme, donma	Cihazların paketinden çıkarılıp içeri alınması sağlanır, içecekle içeri girilmez, düzenli temizlik yapılır	Cihazın hasar görmesi	BE	2	4	1000			*		Temizlik şirketi haftada iki defa temizlik yaptığını belgeleyecek, Firma ile gizlilik anlaşması
				Voltaj dalgalanmalarına açık olma	Güç kaynağının bozulması	UPS hatlarından besleniyor	Cihazın hasar görmesi	E	2	4	1000				*	Elektrik İşletme Müdürlüğü ya da firma konu hakkında çalışma yapacak
				Sıcaklık dalgalanmalarına açık olma	Meteorolijk olayı	İklimlendirilmiş ortam söz konusu, paratoner var	Cihazın hasar görmesi	E	1	3	375					
				Uygunsuz enerji kablolaması	Güç kaynağının bozulması	Kablolama yeni düzenlendi	Cihazın hasar görmesi	E	2	2	500			*		Elektrik İşletme Müdürlüğü'nden konu hakkında teknik danışmanlık alınacak

Aşama 5 – Belgeler

Standard EK-A listesine göre politika prosedür gibi belgeler oluşturuldu. (28 adet belge)

Politikalar	Prosedürler	Talimatlar
Bilgi Güvenliği Politikası	Bilgi Güvenliği Organizasyonu Prosedürü	Bilgi Sınıflama Talimatı
Varlık Yönetimi Esasları	Doküman ve Kayıt Kontrolü Prosedürü	Olay Açıklık Müdahale Sorumluları ve Talimatları
Personel Güvenliği Esasları	Varlık ve Risk Yönetimi Prosedürü	Yedekleme Talimatı
Fiziksel ve Çevresel Güvenlik Esasları	Düzeltici ve Önleyici Faaliyet Prosedürü	
Haberleşme ve İletişim Esasları	İç Tetkik Prosedürü	
Erişim Kontrol Esasları	E-kimlik Yönetimi Prosedürü	
Ayrıcalık Hakları Yönetim Politikası	İşten Ayrılma Prosedürü	
Erişim Hakları Politikası	Etiketleme Prosedürü	
Parola Yönetimi Politikası		
Temiz Masa Temiz Ekran Politikası		
Uzaktan Erişim Politikası		
VPN Politikası		
Zafiyet Testi Politikası		
Bilgi Sistemleri Edinim Bakım ve Geliştirme Pol.		
Bilgi Güvenliği İhlalleri Yönetim Esasları		
İş Sürekliliği Esasları		
Uyum Esasları		

Aşama 6

- ✓ Prosedür, Politika gibi belgelerin DB onayından geçmesi ve yayınlanması

  http://security.metu.edu.tr

- ✓ Kullanıcı Farkındalığı Eğitimi
  - Danışman firma tarafından verildi.
- ✓ Uygulanabilirlik Bildirgesi
  - EK A maddelerinin yerine getirilmiş hali…
- ✓ İç Denetim
  - Danışman firma tarafından gerçekleştirildi.

Aşama 7 – YGG

Yönetim Gözden Geçirme

- ✓ Katılımcılar
  - Rektör Yardımcı, BİD Başkanı, Grup Yöneticileri, BGB
- ✓ Yapılan Çalışmaların Özeti
  - Varlık Envanteri, Risk Analizi, Risk Tedavi Planı, vs
- ✓ Çalışmalar sonrası yapılacak çalışmalar için öneriler
  - Çıkan sonuçlara göre risk seviyesi yüksek X, Y, Z için önlem alınmalı
- ✓ Yapılacak çalışmalara karar verilmesi
  - X yapılsın (risk azaltma)
  - Y için kaynak ayıramayız, yapılmasın (riski kabul)
  - Z faktörü tamamen ortadan kalksın, risk de oluşturmasın

Aşama 8 - Denetim

- ✓ Denetçi firmanın ihale ile belirlenmesi
- ✓ Denetim 2 gün sürdü
- ✓ Majör Uygunsuzluklar
  - Yok!
- ✓ Minör Uygunsuzluklar
  - Sistem Odası ile ilgili konular (kapısı kapanmayan tape kasası, kapı uygunsuzluğu, vs)
  - Flow toplanmaması
  - Kullanıcı şifresinin post-it ile ekranın kenarına yapıştırılmış olması
  - Kullanıcı bilgisayarlarının denetiminin kendilerinde olması, virüs programını devre dışı bırakabilmeleri

Aşama 9 - Sertifikasyon İşlemleri

- ✓ Firmanın Rapor Hazırlaması
- ✓ Raporun BİDB Yönetimine takdim edilmesi
- ✓ Denetim Sonrası Evrak İşlemlerinin Halledilmesi

Mutlu Son!

CERTIFICATE OF REGISTRATION

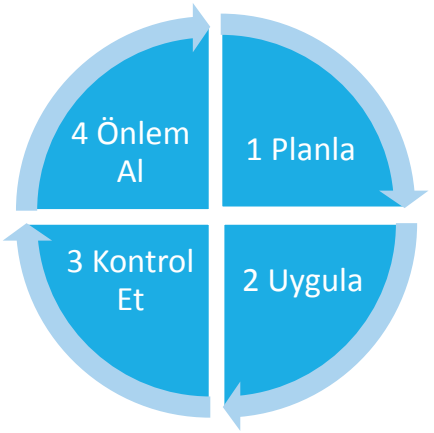
ORTA DOĞU TEKNİK ÜNİVERSİTESİ
BİLGİ İŞLEM DAİRE BAŞKANLIĞI

ISO/IEC 27001:2005

Mu acaba? ☺

Bir BGYS'ye sahip olmanın faydaları

- ✓ Döngüsel yapı
- ✓ Kendimizi tanımamızı sağlaması
- ✓ Yapabileceklerimizi / yapamayacaklarımızı anlamamızı sağlaması
- ✓ SOME kurulumunda kolaylık
  - ISO 27001 belgeniz varsa gerekliliklerin pek çoğunu yerine getirmişsinizdir ve kolayca SOME kurabilirsiniz. Ama tersi doğru değil!
- ✓ Standartlara uygunluk

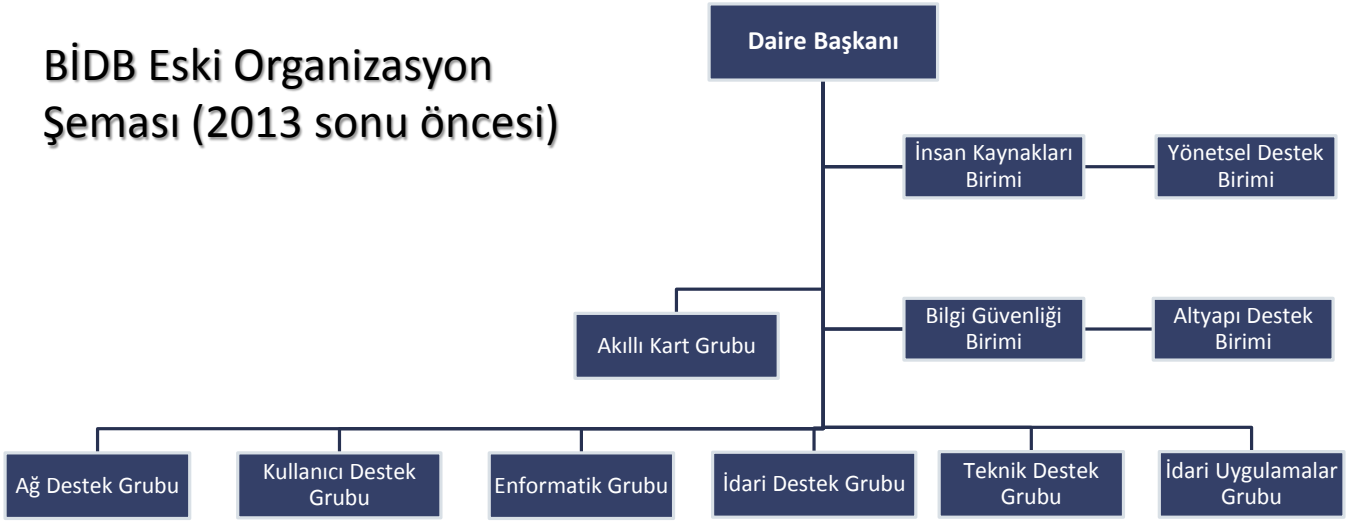


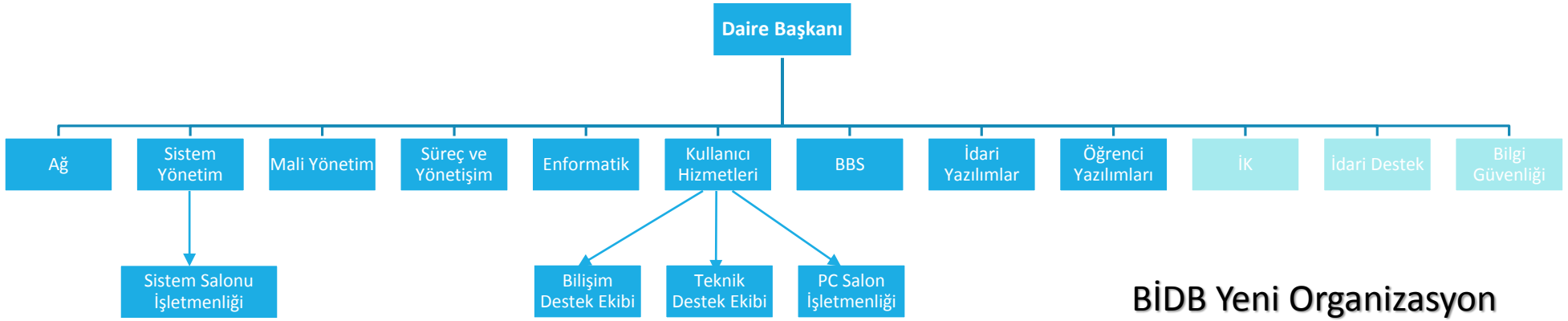
BGYS Döngüsü

Zorlandığımız Konular

- ✓ Genel:
  - Danışman değişikliği
  - Organizasyonel Yapının Değişmesi
    - Adaptasyon Süreci
    - Varlık sahipliklerinin değişmesi
  - Yeni danışmanla çalışmalara sağlık sorunları nedeni ile ara verilmesi
- ✓ Çok fazla paydaşla uğraşma zorluğu (9 Grup + 3 Birim)
- ✓ Asli görevlerin yanı sıra BGYS işlerinin ek yük getirmesi
- ✓ Çok fazla politika vs metni üzerine uğraşma
- ✓ Bir BGYS yazılımı kullanmamamız

BİDB Eski Organizasyon Şeması (2013 sonu öncesi)





BİDB Yeni Organizasyon Şeması (2013 Sonu)

Yol Planı

- ✓ BGYS Yazılımı Almak
  - Yazılım satın alınıyor.
- ✓ ISO 27001:2013 versiyonuna geçiş
  - Eylül 2015 son tarih
- ✓ Yeni bir döngüye geçiş / ya da iyileştirmelere devam etmek

Tavsiyeler

- ✓ Kapsamınızı iyi belirleyin.
- ✓ Detaylarda kaybolmayın.
- ✓ Mümkünse BGYS yazılımı kullanın.
- ✓ Danışman çalışacaksanız;
  - Danışman size yol göstersin ki bir sonraki döngüde zorlanmayın.

Teşekkürler!

Soru ve Cevaplar

Sorularınız için: security@metu.edu.tr