Bilgi Teknolojileri Yönetişim ve Denetim Konferansı

BTYD 2010

ISACA Serving IT Governance Professionals

Türkiye Bilişim Derneği 1971

Türkiye İç Denetim Enstitüsü 1995

eDem TODAİE eDevlet Merkezi

DENETİM BULGULARININ YÖNETİMİ

A.Levend Abay CISM
BT Güvenlik Yönetimi Müdürü
Yapı ve Kredi Bankası AŞ

Gündem

- **Problemin Tanımı**
- **Yaklaşımımız**
- **Standartların Eşleştirilmesi**
- **Yönetim Özeti**

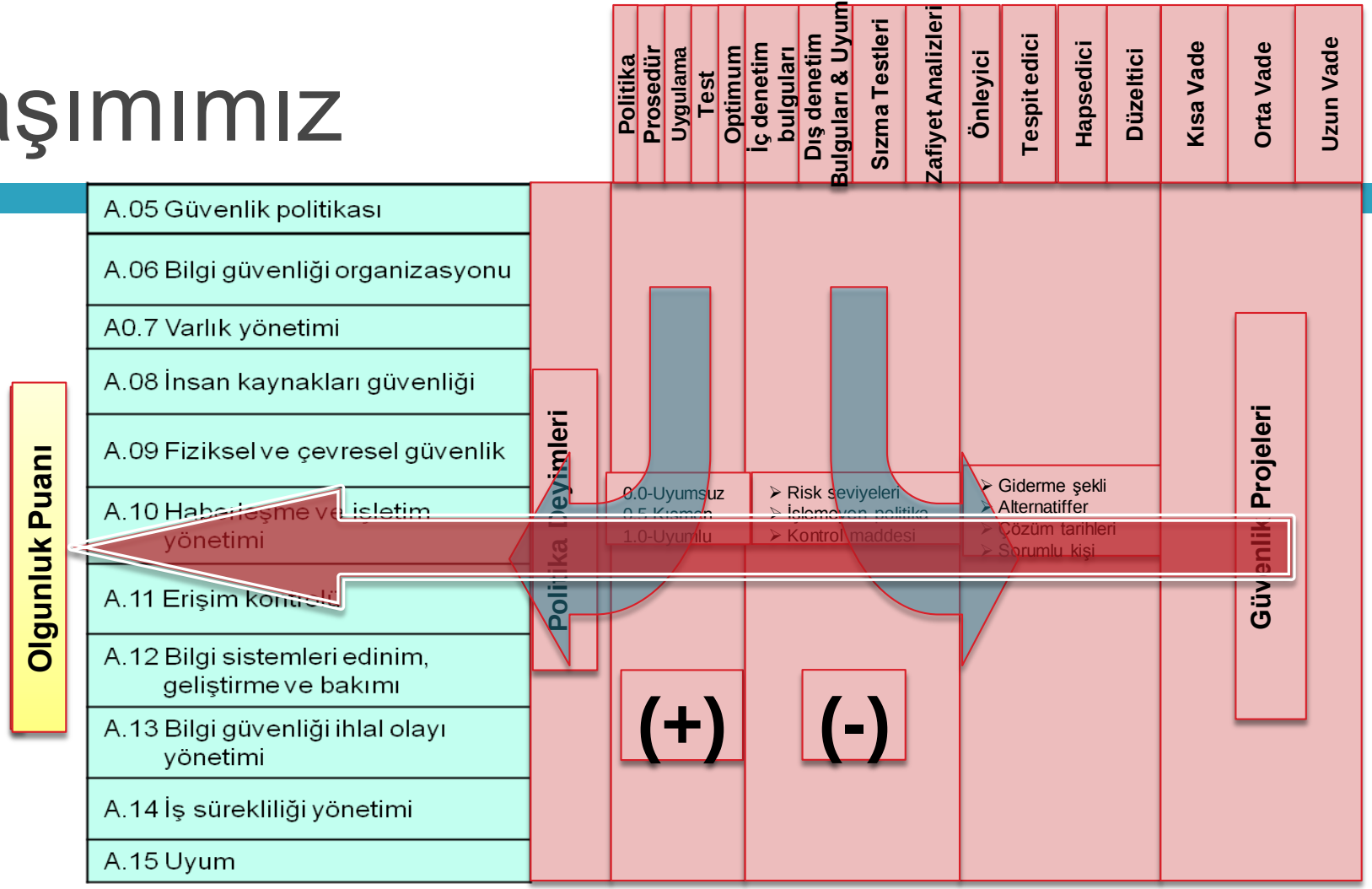
Problemin Tanımı

- **Çok sayıda denetim ve farklı standartlar**
  - BDDK , Holding Denetimi, VISA PIN Security, İç Denetim
  - COBIT, PCI DSS, Tebliğ, ISO 27001, Law 262
- **Farklı ifade edilen benzer bulgular**
  - Bulguların konsolidasyonu
  - Kök sorunun tespiti

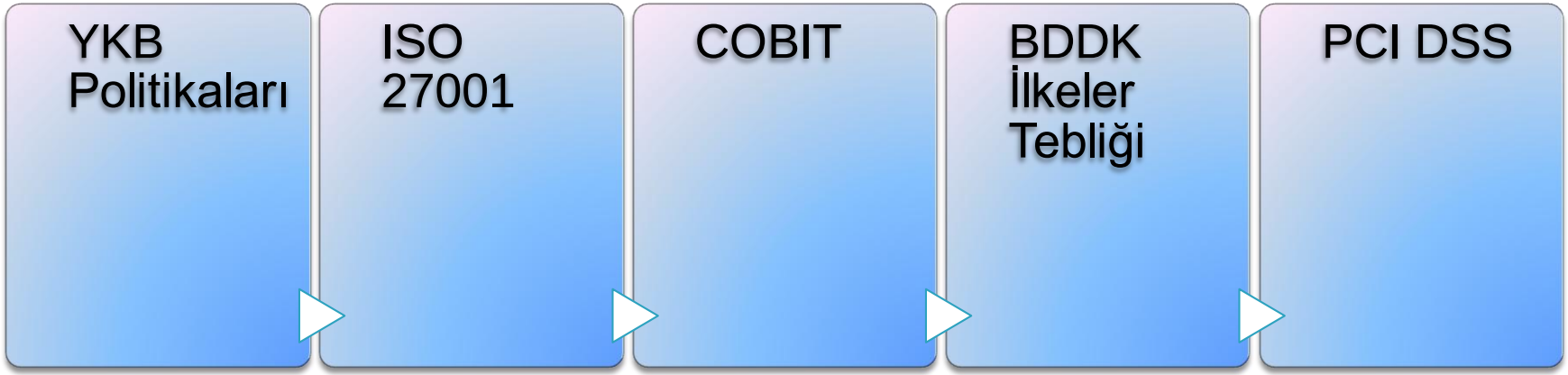
Problemin Tanımı

- **Önceliklendirme ve Planlama**
  - Tekil çözüm yerine paket çözüm
  - Bağımlılıklar / kritiklik seviyeleri
  - Tekrar etmesini önlemek
- **Genel durumu görmek**
  - Güvenlik Olgunluk Seviyemiz
  - En çok hangi alanda uyum sorunumuz var

Yaklaşımımız



Standartların Eşleştirilmesi



YÖNETİM ÖZETİ

KRİTER	OLGUNLUK					KRİTER PUANI
	Politika	Prosedür	Uygulama	Test	Optmum	
A.5 Güvenlik politikası	1.00	0.50	0.25	0.00	0.00	1.75
A.6 Bilgi güvenliği organizasyonu	1.00	0.61	0.47	0.06	0.00	2.15
A.7 Varlık yönetimi	1.00	0.61	0.47	0.06	0.00	2.15
A.8 İnsan kaynakları güvenliği	1.00	0.67	0.67	0.00	0.00	2.33
A.9 Fiziksel ve çevresel güvenlik	1.00	0.68	0.75	0.00	0.00	2.43
A.10 Haberleşme ve işletim yönetimi	1.00	0.11	0.42	0.00	0.00	1.53
A.11 Erişim kontrolü	0.98	0.21	0.48	0.00	0.00	1.67
A.12 Bilgi sistemleri edinim, geliştirme ve bakımı	1.00	0.17	0.43	0.00	0.00	1.60
A.13 Bilgi güvenliği ihlal olayı yönetimi	1.00	0.00	0.13	0.00	0.00	1.13
A.14 İş sürekliliği yönetimi	1.00	0.20	0.10	0.00	0.00	1.30
A.15 Uyum	1.00	0.00	0.58	0.00	0.00	1.58
OLGUNLUK NOTU	1.00	0.34	0.43	0.01	0.00	**1.78**

Teşekkürler

BTYD 2010

www.btyd.org