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

BİLİŞİM SİSTEMLERİ DENETİMİ VE SAYIŞTAY

AHMET TOPKAYA
SAYIŞTAY BAŞDENETÇİSİ

Bilişim Sistemleri Denetimi Kavramı

- Güncel denetim yaklaşımlarından bir tanesi olan bilişim sistemleri denetimi; işletmelerin sahip oldukları bilişim sistemleri kaynaklarının değerlenmesi sürecidir.

- Bilişim sistemleri denetimi; bir bilişim sisteminin, kurum amaçlarına etkin bir şekilde ulaşılmasını, kaynakların verimli kullanılmasını, varlıkların korunmasını ve veri bütünlüğünün sürdürülmesini sağlayacak şekilde tasarlanıp tasarlanmadığını tespit etmeye yönelik kanıt toplama ve değerlendirme süreci

Bilişim Sistemleri Denetiminin Kurumlara Sağlayacağı Faydalar

- Bilişim Sistemlerin kesintisiz çalışmasını sağlamak,
- Acil durumlar karşısında iş sürekliliğini korumak,
- Teknoloji risklerine karşı önlem almak,
- Teknolojik alt yapının ihtiyaçlarını karşılamada optimum çözüm olup olmadığını ölçmek,
- Bilgi işlem departmanının kişilere bağımlı olmamasını sağlamak,
- Kullanıcıların sistem yada uygulama kaçaklarını görme ve bu kaçakları kötüye kullanma ihtimalini ortadan kaldırmak,
- Bilişim sistemlerinde var olan hatalardan kaynaklanan kurum zararlarını azaltmak,
- Müşteri ve kurum bilgilerinin güvenliğini sağlamak

Bilişim Sistemleri Denetimi ve Sayıştay

Sayıştay; Anayasa (160. madde) ve diğer yasalardan (832 sayılı Sayıştay Kanunu) aldığı yetkiye dayanarak, merkezi yönetim bütçesi kapsamındaki kamu idarelerinin, sosyal güvenlik kurumlarının ve mahalli idarelerin bütün gelir ve giderleri ile mallarını Türkiye Büyük Millet Meclisi adına denetlemek ve sorumluların hesap ve işlemlerini kesin hükme bağlamakla görevli bir yargı ve yüksek denetim kurumudur.

Bilişim Sistemleri Denetimi ve Sayıştay

- 5018 Sayılı Kanun, Sayıştay'a dış denetim organı olarak "Düzenlilik Denetimi" ve "Performans Değerlendirmesi" yapma görevi vermiş ve bu denetimlerin "genel kabul görmüş uluslar arası denetim standartlarına" göre yürütülmesini öngörmüştür.
- Say2000i, Medula, Vedop gibi sistemlerin kamu kurumları tarafından kullanılmaya başlanması
- 2003 Hazine Bilişim Sistemleri Denetimi Raporu
- İngiltere ve İspanya Sayıştay'ı ile yürütülen "Sayıştay'ın Denetim Kapasitesinin Güçlendirilmesi" Eşleştirme Projesi sonucunda "Bilişim Sistemleri Denetimi Rehberi" oluşturuldu.

Bilişim Sistemleri Denetimi ve Sayıştay

- Sayıştay Başkanlığı olarak toplamda 6 kurumda Bilişim Sistemleri Denetimi yapılmıştır.
- Sayıştay Başkanlığı, TUBİTAK UEKAE, Marmara Üniversitesi arasında imzalanan protokol kapsamında "T.C. Sayıştay Başkanlığı Bilgisayar Destekli Denetim Sistemi Yazılımı Projesi" yürütülmektedir.
- Sayıştay Başkanlığı EUROSAI'nin IT çalışma grubunun bir üyesi olarak uluslar arası metodoloji çalışmalarına ve eğitim seminerlerine hem eğitici hem de katılımcı sıfatı ile katılmakta ve INTOSAI'nin IT çalışma grubuna gözlemci sıfat ile iştirak etmektedir.

Sayıştay'ın Bilişim Sistemleri Denetimi Metodolojisi

Bilişim sistemleri denetimi yürütülürken risk tabanlı denetim yaklaşımına uygun olarak şu genel çerçeve izlenir;

- Öncelikle incelenen bilişim sisteminden kaynaklanabilecek riskler belirlenir,
- Bu riskleri minimize edecek kontrol mekanizmaları belirlenir,
- Bu kontrol mekanizmalarının kurumun yapısı göz önünde tutularak oluşturulup oluşturulmadığı, oluşturulmuş ise etkin çalışıp çalışmadığı incelenir,
- İnceleme sonrası, iç kontrollerdeki zayıflıklar değerlendirilir
- Elde edilen bulgular belli bir prosedüre göre raporlanır.

Denetimin Planlaması Aşaması

1. Kurumun ve Kurumun Bilişim Sistemlerinin Tanınması
2. Sistem Risk Analizlerinin Yapılması
3. Uzman Çalıştırılmasına Karar verilmesi
4. Denetim Stratejisinin Oluşturulması

Sistem Risk Analizlerinin Yapılması

Risk Alanı		Maksimum Risk Puanı	Toplam Risk Puanı	Uygulama Sisteminin Risk Puanlarına Göre Risk Derecesi		
				Yüksek	orta	düşük
1	Önemlilik	360		360-270	270-180	180-90
2	Kritiklik	200		200-150	150-100	100-50
3	Teknik Altyapı	160		160-120	120-80	80-40
4	Karmaşıklık	160		160-120	120-80	80-40
5	Kontrol Çevresi	120		120-90	90-60	60-30
	Genel	1000		1000-750	750-500	500-250

Sistem Kontrollerinin Değerlendirilmesi

- Genel Kontroller
- Uygulama Kontrolleri

Genel Kontroller

Kuruma ait tüm bilişim sistemleri faaliyetlerinin sürekliliğinin sağlanmasına yönelik yapı, yöntem ve prosedürlere ilişkin kontrollerdir. Bu kontroller uygulama yazılımları ve bunlara ilişkin kontroller için güvenli bir ortam oluşturur.

1. Yönetim Kontrolleri
2. Fiziksel ve Çevresel Kontroller
3. Ağ Yönetimi ve Güvenliği Kontrolleri
4. Mantıksal Erişim Kontrolleri
5. İşletim Sistemleri ve Bilgisayar İşlemleri Kontrolleri
6. Veri Tabanı Güvenlik Kontrolleri
7. Sistem Geliştirme ve Değişim Yönetimi Kontrolleri
8. Acil Durum ve İş Sürekliliği Planlaması Kontrolleri

Uygulama Kontroller

Bilgilerin sistemlere ya da programlara tam olarak, zamanında ve sadece bir kere girilmesini, bilgi-işlem ortamında tüm işlem ve süreçlerin istenilen sıra ve düzen içinde gerçekleşmesini, raporların tam ve güvenilir olarak üretilmesini, yetkili kişilere ulaştırılmasını ve uygun şekilde arşivlenmesini sağlayan kontrollerdir.

Uygulama kontrolleri şu alanlarda gerçekleştirilir:

1. Girdi Kontrolleri
2. Veri Transfer Kontrolleri
3. İşlem Kontrolleri
4. Çıktı Kontrolleri

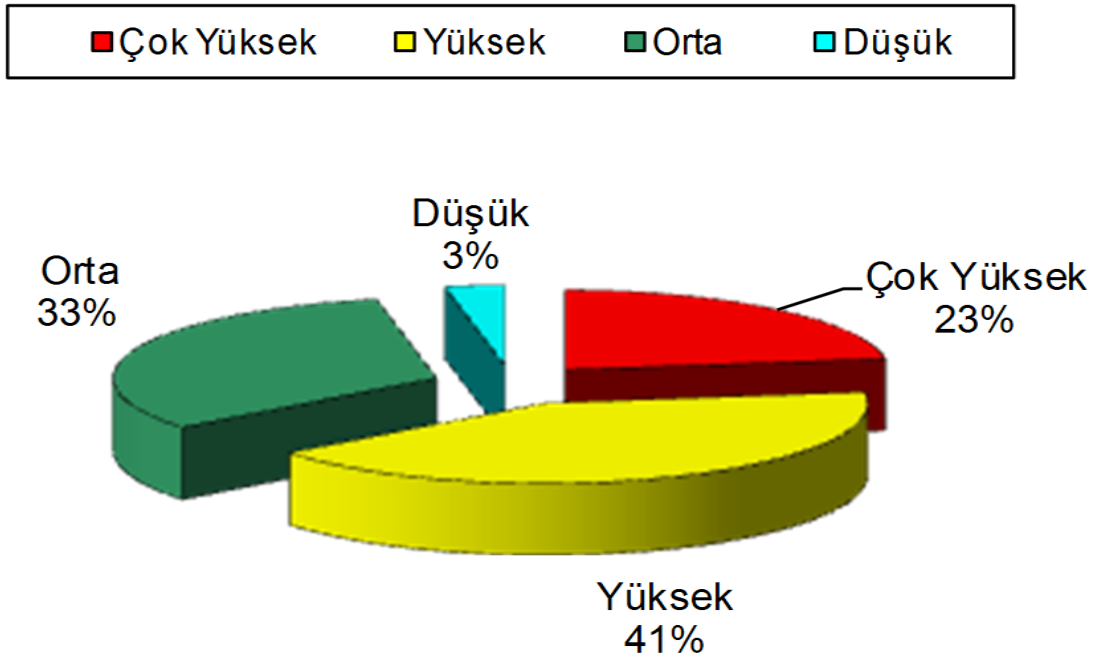
Sistem Kontrollerinin Tamamlanması

1. Kontrol Varlığının Belirlenmesi
2. Kontrol Etkinliğinin Değerlendirilmesi
3. Bulguların Değerlendirilmesi

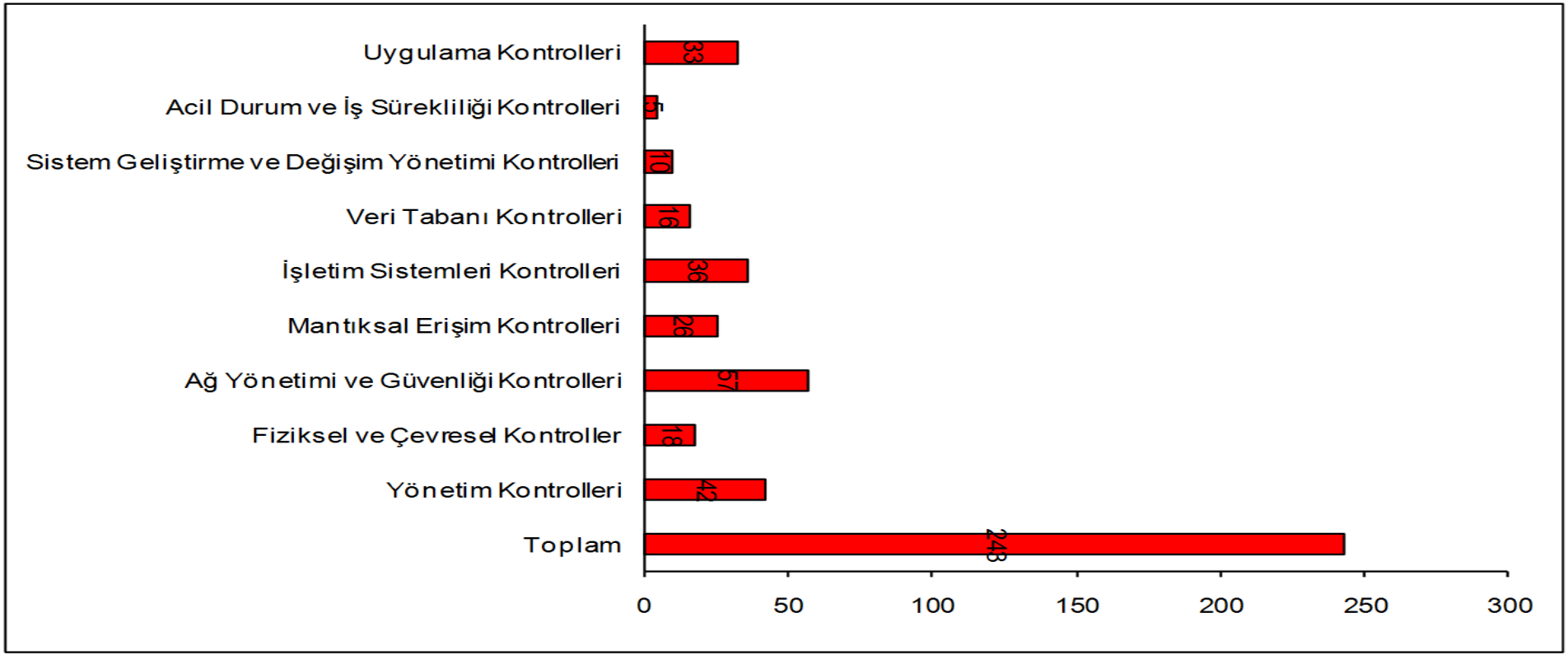
Sonuç ve Değerlendirme

- Görevi kamu kaynaklarının mevzuata uygun olarak verimli, etkin ve tutumlu olarak kullanılıp kullanılmadığını denetlemek olan Sayıştay'ın kurumlarının bilişim sistemleri denetimine ağırlık vermesi yaptığı hukukilik denetiminde bu sistemlerden çıkan verilerin güvenilirliğinin bir anlamda test edilmesidir. Çünkü yapılan denetimlerde bu veriler kullanılmakta olup verilerin hatalı veya yanlış olarak sistemden alınması sonucunda tüm denetim süreci sekteye uğrayabilecektir.
- Sayıştay'ın bilişim sistemleri denetimi kapsamında gerçekleştirdiği pilot denetimlerde aşağıdaki grafiklerde belirtildiği üzere kamu kurumlarımızda hala bilişim sistemleri ile ilgili olarak güvenlik ve güvenilirlik algısının yüksek olmadığı ve kamu kurumlarının bilişim sistemlerinin hala çok yüksek riskler içerdiği görülmektedir. Buda Sayıştay'ın bilişim sistemlerine verdiği önemin ne kadar yerinde olduğunu göstermektedir.

Sonuç ve Değerlendirme



Sonuç ve Değerlendirme



TEŞEKKÜRLER….

AHMET TOPKAYA
SAYIŞTAY BAŞDENETÇİSİ

BTYD 2010

www.btyd.org