RİSK YÖNETİMİNDE BAŞARI FAKTÖRÜ "İŞ SÜREKLİLİĞİ YÖNETİMİ"
SUCCESS IN RISKMANAGEMENT: "BUSINESS CONTINUITY MANAGEMENT"

19-20.09.2009
İstanbul Teknik Üniversitesi,
Ayazağa Kampüsü,
Süleyman Demirel Kültür Merkezi

Maslak – ISTANBUL
TÜRKİYE / TURKEY

İSYS Süreçleri ve Yönetim Sistemleri İçindeki Yeri

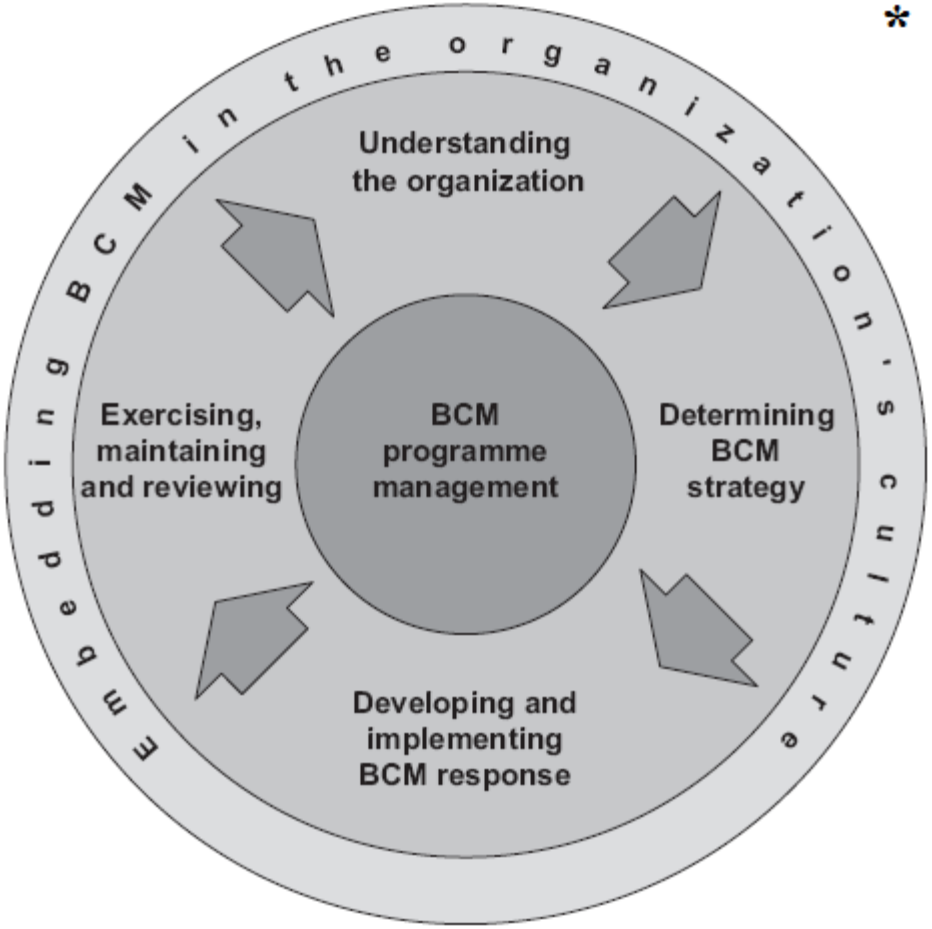
Burak Bayoğlu (CISM, CISA, CISSP)
TÜBİTAK UEKAE
bayoglu@uekae.tubitak.gov.tr

İTÜ/AYM Afet Yönetim Merkezi
ALMANYA YÜKSEKOKULLARI MEZUNLAR DERNEĞİ
Verein der Hochschulabsolventen Deutschlands
DAAD
Deutscher Akademischer Austausch Dienst
German Academic Exchange Service

Sunu Planı

- İSYS Yaşam Döngüsü ve Motivasyon
- COBIT 4.1
- (TS) ISO/IEC 27001
- ITIL v3
- Sonuç

İSYS Yaşam Döngüsü



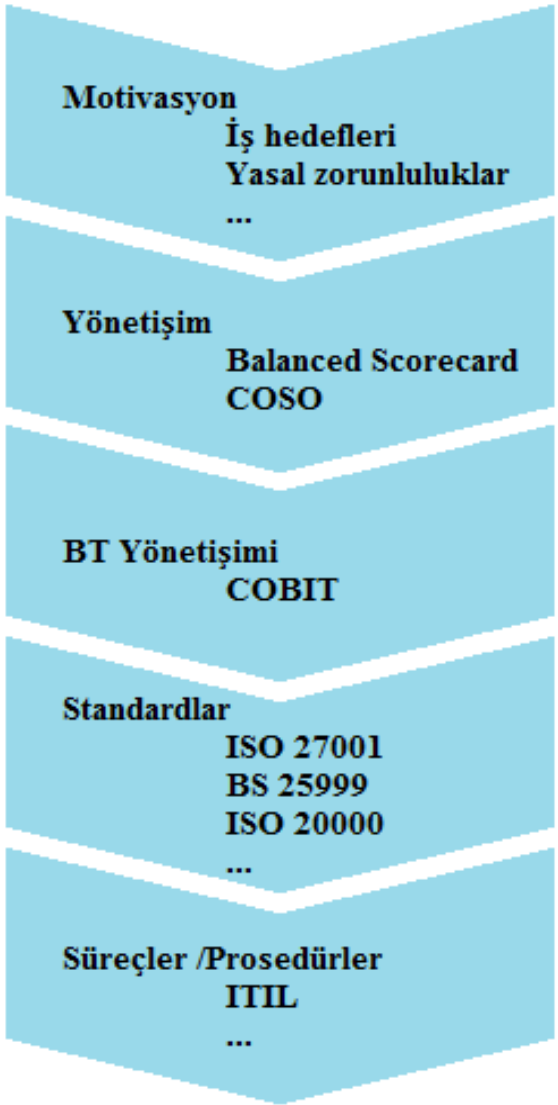
*

* BS 25999-1:2006 sf.9

Motivasyon

- İSYS bir proje değil yaşayan bir süreçtir.
  - Kurulumu proje olabilir.
- Her ihtiyaca cevap veren tek kaynak bulmak mümkün değil.
- Uyumluluk iddiası olabilecek yönetim sistemlerinin etkin kullanımını gereklidir.
  - Neden?

Kaynaklar ve detay seviyeleri



COBIT

- Dört etki alanı
  - PO
  - AI
  - DS
  - ME

- 34 üst seviye kontrol hedefi
  - DS4 – Ensure Continuous Service

COBIT

- DS4 – Ensure Continuous Service
  - 10 detaylı kontrol hedefi
- Kritik iş süreçlerine hizmet veren BT hizmetlerindeki kesintilerin olasılığını ve iş süreçlerine etkisini en aza indirgemeyi amaçlamaktadır.
  - BT süreklilik planlarının hazırlanması
  - Eğitimlerinin verilmesi
  - Testlerinin yapılması
  - Süreklilik planlarının ve bilgilerin dış lokasyonlarda saklanması

DS4 Ensure Continuous Service

- "*An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes.*"
  - Bu tanımla ilgili problem nedir?

DS4 – Detaylı kontrol hedefleri

- DS4.1 IT Continuity Framework / BT Süreklilik Çerçevesi
- DS4.2 IT Continuity Plans / BT Süreklilik Planları
- DS4.3 Critical IT Resources / Kritik BT Kaynakları
- DS4.4 Maintenance of the IT Continuity Plan / BT Süreklilik Planının Devamlılığı
- DS4.5 Testing of the IT Continuity Plan / BT Süreklilik Planının Test Edilmesi
- DS4.6 IT Continuity Plan Training / BT Süreklilik Planı Eğitimi
- DS4.7 Distribution of the IT Continuity Plan / BT Süreklilik Planının Dağıtımı
- DS4.8 IT Services Recovery and Resumption/BT Hiz. Kurtarma ve Devam Ettirme
- DS4.9 Offsite Backup Storage / Dış Lokasyonda Yedekleme
- DS4.10 Post-resumption Review / Kurtarma Sonrası Gözden Geçirme

COBIT DS4 ile ilişkili diğer süreçler

From	Inputs
PO2	Assigned data classifications
PO9	Risk assessment
AI2	Availability, continuity and recovery specification
AI4	User, operational, support, technical and administration manuals
DS1	SLAs and OLAs

Outputs	To	
Contingency test results	PO9	
Criticality of IT configuration items	DS9	
Backup storage and protection plan	DS11	DS13
Incident/disaster thresholds	DS8	
Disaster service requirements, including roles and responsibilities	DS1	DS2
Process performance reports	ME1	

- PO2 Define the information architecture.
- PO9 Assess and manage IT risks.
- AI2 Acquire and maintain application software.
- AI4 Enable operation and use.
- DS1 Define and manage service levels.
- DS2 Manage third-party services.
- DS8 Manage service desk and incidents.
- DS9 Manage the configuration.
- DS11 Manage data.
- DS13 Manage operations.
- ME1 Monitor and evaluate IT performance.

ISO/IEC 27001/27002

- PUKÖ Yaşam Döngüsü
- Bilgi güvenliği
  - *iş sürekliliğinin sağlanması, iş risklerinin en aza indirilmesi, yatırım geri dönüşünün ve iş fırsatlarının artırılması amacıyla bilginin her türlü tehdide karşı korunması*
- 11 etki alanı
  - "A.14 İş sürekliliği yönetimi"
    - 5 kontrol

ISO/IEC 27001/27002

- A.14.1.1 Bilgi güvenliğini iş sürekliliği yönetim prosesine dahil etme
- A.14.1.2 İş sürekliliği ve risk değerlendirme
- A.14.1.3 Bilgi güvenliğini içeren süreklilik planlarını geliştirme ve gerçekleştirme
- A.14.1.4 İş sürekliliği planlama çerçevesi
- A.14.1.5 İş sürekliliği planlarını test etme, sürdürme ve yeniden değerlendirme

İSYS ile ilişkili diğer kontroller

- Bilgi güvenliği politikası dokümanında iş sürekliliği yönetimiyle ilgili politika ve diğer dokümanların özet açıklamasının verilmesi. (5.1.1)
- İş sürekliliği planlamasıyla ilgili rollerin ve sorumlulukların tanımlanması. (6.1.3)
- İlgili otoritelerin bağlantı bilgilerinin bulundurulması. (6.1.6)
- İş sürekliliği planlarının varlık envanterinin bir parçası olması. (7.1.1)
- Yeni bilgi sistemleri kurulumu, yükseltmeler, yeni sürüm sistem kurulumu vb. için belirlenecek kabul kriterleri arasında iş sürekliliği anlaşmalarının göz önünde bulundurulması. (10.3.2)

İSYS ile ilişkili diğer kontroller

- Zararlı yazılım saldırıları sonrasında kurtarma amaçlı iş sürekliliği planlarının hazırlanması. (10.4.1)
- İş sürekliliği planlarının gereksinimlerinin karşılanacağından emin olmak üzere sistem yedeklerinin düzenli olarak test edilmesi. (10.5.1)
- Uzaktan çalışma ihtiyacı için iş sürekliliği planlamasının yapılması. (11.7.2)
- Kaybolan ya da hasar gören kriptografik anahtarlarla ilgili iş sürekliliği planlamasının yapılması. (12.3.2)
- Sistemlerde yapılan değişiklikler sonrasında iş sürekliliği planlarının da uygun şekilde güncellenmesi. (12.5.2)

27001 standardından diğer katkılar

- Yönetim sorumlulukları
- Varlık envanteri
  - İş süreçleri
  - Varlık değerleri > RTO/RPO
  - Varlık sahipleri
- Risk analizi
  - İş sürekliliği riskleri

ITIL

- Service Design/Hizmet Tasarımı
- Service Transition/Hizmet Geçişi
- Service Operation/Hizmet İşletme
- Continual Service Improvement/Sürekli Hizmet İyileştirmesi

- IT Service Continuity Management/BT Hizmet Sürekliliği Yönetimi (BT HSY) süreci tanımlanmıştır.

ITIL – BT HSY Amacı

- BT Hizmet Süreklilik planlarıyla, ilgili BT kaynaklarını ve hizmetlerini gerekli durumlarda iş ihtiyacını karşılayabilecek şekilde çalışır hale getirerek kurumun genel İş Sürekliliği Yönetim Sistemi sürecini desteklemek.

- BT kaynaklarının iş süreçlerine olan etkisi ya da iş ihtiyaçlarındaki değişikliklerin planlara yansıtıldığından emin olmak üzere düzenli İş Etki Analizi (Business Impact Analysis) yapılması.

ITIL – BT HSY Amacı

- Düzenli (BT hizmet sürekliliği) risk analizlerinin yapılması.

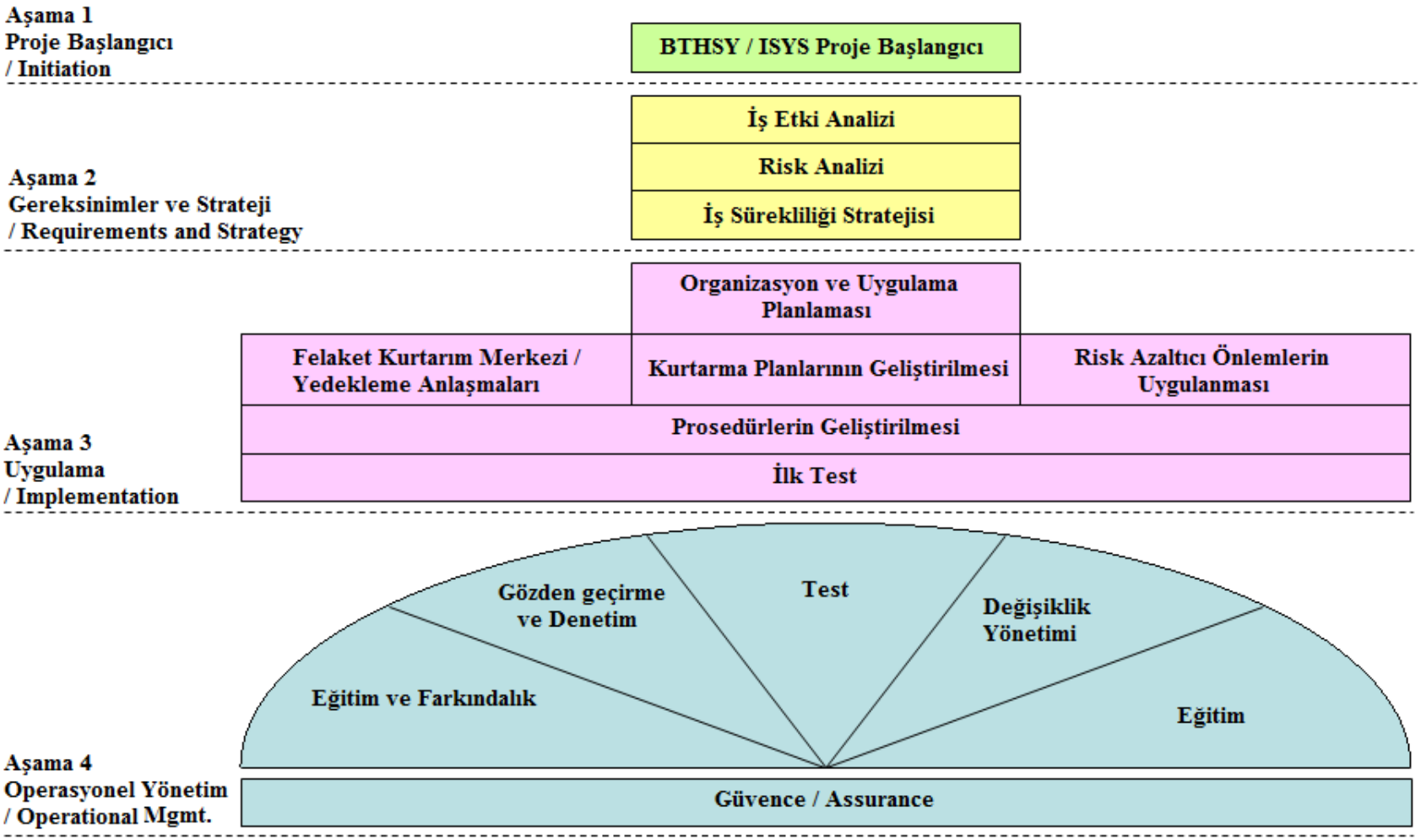
- BT hizmet sürekliliği ve kurtarma çalışmaları konusunda diğer departmanlara tavsiyeler verilmesi, rehberlik edilmesi.

- BT hizmetlerinin erişilebilirliğini arttırıcı proaktif önlemlerin maliyet etkin olduğu sürece uygulanması.

ITIL – BT HSY ile ilişkili diğer ITIL süreçleri (başlıcaları)

- Hizmet Seviyesi Yönetimi/Service Level Management
- Değişiklik Yönetimi/Change Management
- Problem Yönetimi/Problem Management
- Erişilebilirlik Yönetimi/Availability Management

BT HSY Yaşam Döngüsü



Sonuç

- İSYS kurulumu için göz önünde bulundurmamız gereken önemli kaynaklar/standartlar vardır.

- BS25999 Standardı ana çerçeve olmak üzere ilgili kaynakların en baştan ele alınması ile, daha maliyet etkin ve etkili İSYS kurulumu gerçekleştirilebilir.

Dinlediğiniz için teşekkür ederim.

SORULARINIZ ... ?