



Bilgi Teknolojileri Yönetişim ve Denetim Konferansı

BTYD 2010



COBIT® ve Diğer Standartlar ile Karşılaştırılması

Mete Türkyılmaz, MBA, CGEIT, CFE, CISA, MCP
Anadolu Endüstri Holding A.Ş.
Denetim Koordinatör Yardımcısı

COBIT ve Diğer Standartlar ile Karşılaştırması

- ▣ COBIT nedir?
- ▣ COBIT Alanları (Domain)
- ▣ COBIT ve Diğer Standartlar ile Karşılaştırılması\Eşleştirilmesi (Mapping)

COBIT®

- ▣ COBIT 4.1-The Control Objectives for Information and related Technology (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri)
- ▣ COBIT Framework for IT Governance and Control (BT Yönetişim ve Kontrolleri için COBIT Çerçevesi)

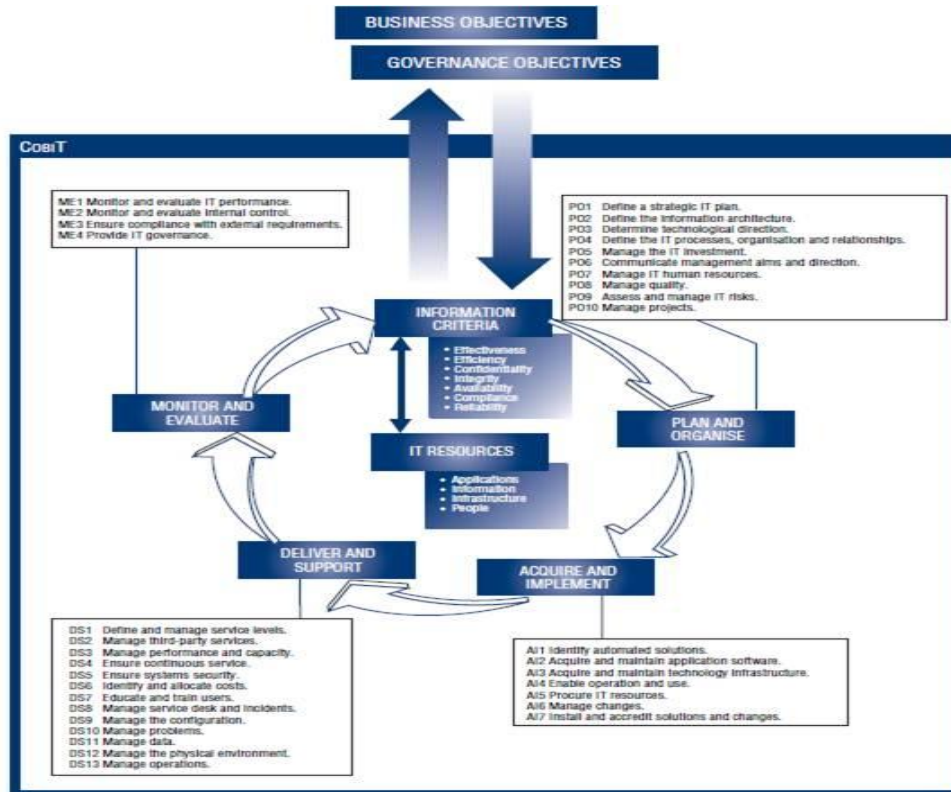
COBIT®



COBIT®



COBIT® ALANLARI (DOMAINS)



PO-Plan and Organise

*IT Assurance Guide: Using COBIT
COBIT Control Practices, 2nd Edition*

APPENDIX II — PLAN AND ORGANISE (PO)

- PO1 Define a Strategic IT Plan**
- PO2 Define the Information Architecture**
- PO3 Determine Technological Direction**
- PO4 Define the IT Processes, Organisation and Relationships**
- PO5 Manage the IT Investment**
- PO6 Communicate Management Aims and Direction**
- PO7 Manage IT Human Resources**
- PO8 Manage Quality**
- PO9 Assess and Manage IT Risks**
- PO10 Manage Projects**

[See worksheet tabs below to access each section](#)

© 2007 IT Governance Institute. All rights reserved. www.itgi.org

AI-Acquire and Implement

**IT Assurance Guide: Using COBIT
COBIT Control Practices, 2nd Edition**

**APPENDIX III — ACQUIRE AND IMPLEMENT
(AI)**

**AI1 Identify Automated Solutions
AI2 Acquire and Maintain Application Software
AI3 Acquire and Maintain Technology Infrastructure
AI4 Enable Operation and Use
AI5 Procure IT Resources
AI6 Manage Changes
AI7 Install and Accredite Solutions and Changes**

[See worksheet tabs below to access each section](#)

**© 2007 IT Governance Institute. All rights reserved.
www.itgi.org**

DS-Deliver and Support

*IT Assurance Guide: Using COBIT
COBIT Control Practices, 2nd Edition*

APPENDIX IV— DELIVER AND SUPPORT (DS)

DS1 Define and Manage Service Levels

DS2 Manage Third-party Services

DS3 Manage Performance and Capacity

DS4 Ensure Continuous Service

DS5 Ensure Systems Security

DS6 Identify and Allocate Costs

DS7 Educate and Train Users

DS8 Manage Service Desk and Incidents

DS9 Manage the Configuration

DS10 Manage Problems

DS11 Manage Data

DS12 Manage the Physical Environment

DS13 Manage Operations

[See worksheet tabs below to access each section](#)

© 2007 IT Governance Institute. All rights reserved. www.itgi.org

ME-Monitor and Evaluate

**IT Assurance Guide: Using COBIT
COBIT Control Practices, 2nd Edition**

APPENDIX V— MONITOR AND EVALUATE (ME)

ME1 Monitor and Evaluate IT Performance

ME2 Monitor and Evaluate Internal Control


ME3 Ensure Compliance With External Requirements

ME4 Provide IT Governance

[See worksheet tabs below to access each section](#)

© 2007 IT Governance Institute. All rights reserved. www.itgi.org

ISACA-Diğer Standart ve Çerçevesler

- ❑ - **Val IT™** - IT Framework for Business Technology Management
- ❑ **Risk IT** - Framework for Management of IT Related Business Risks
- ❑ **ITAF™** - Information Technology Assurance Framework
- ❑  (BMIS) - Business Model for Information Security

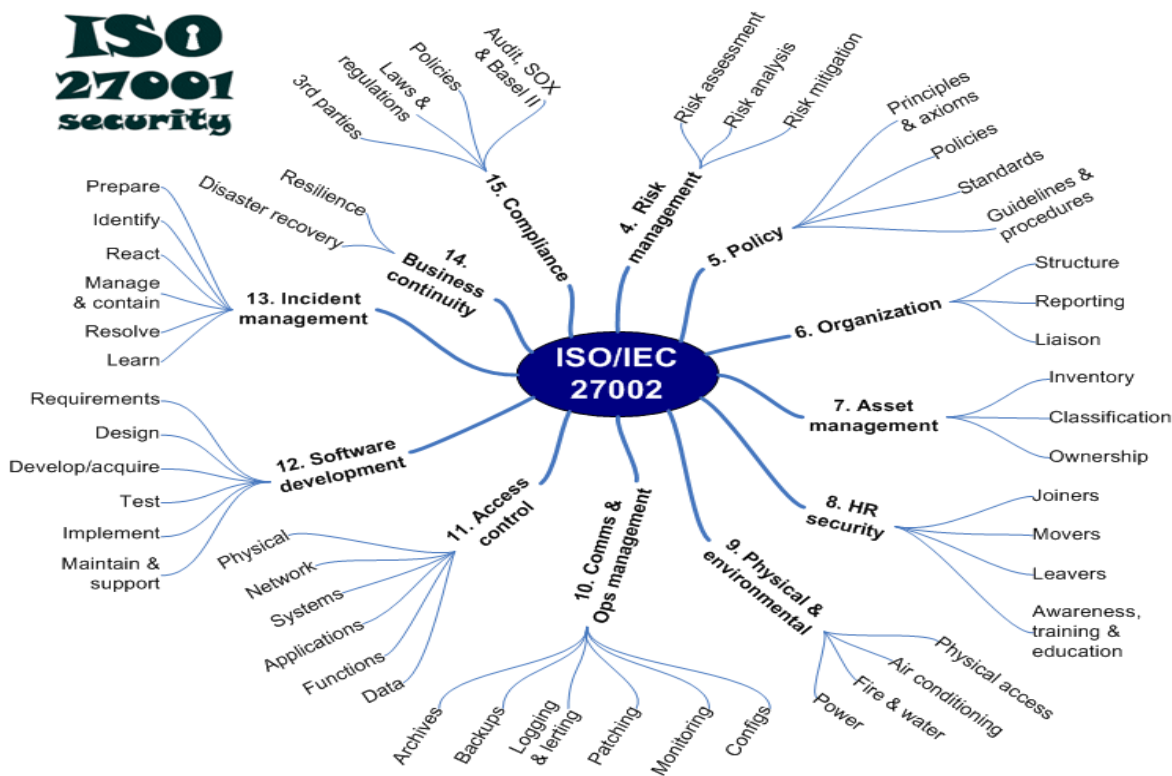
Diğer Çerçeve ve Standartlar

- ▣ ITIL® v3
- ▣ TOGAF 8.1-9.0
- ▣ ISO\IEC 27002-ISO\IEC 27001 (ex. ISO\IEC 17799)
- ▣ NIST SP800-53-Recommended Security Controls for Federal Information Systems
- ▣ CMMI®
- ▣ COSO

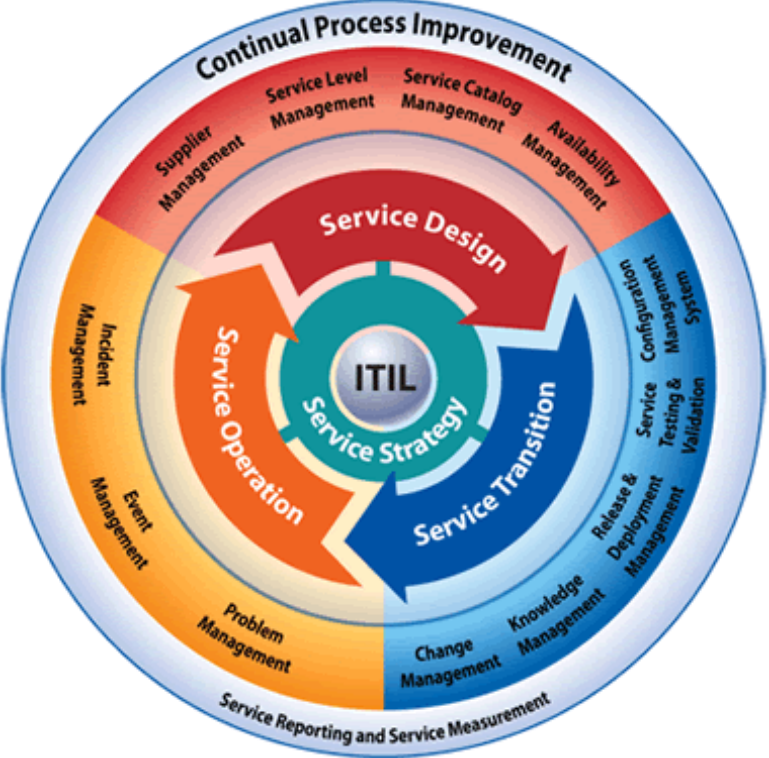
Diğer Çerçeve ve Standartlar

- PMI-*PMBOK*®
- PRINCE2
- MPMM
- NSA-INFOSEC, ISF-*The Standard of Good Practice for Information Security*
- theIIA-GTAG (GAIT Methodology-a risk-based approach to assessing the scope of IT general controls)

ISO\IEC 27002-ISO\IEC 27001



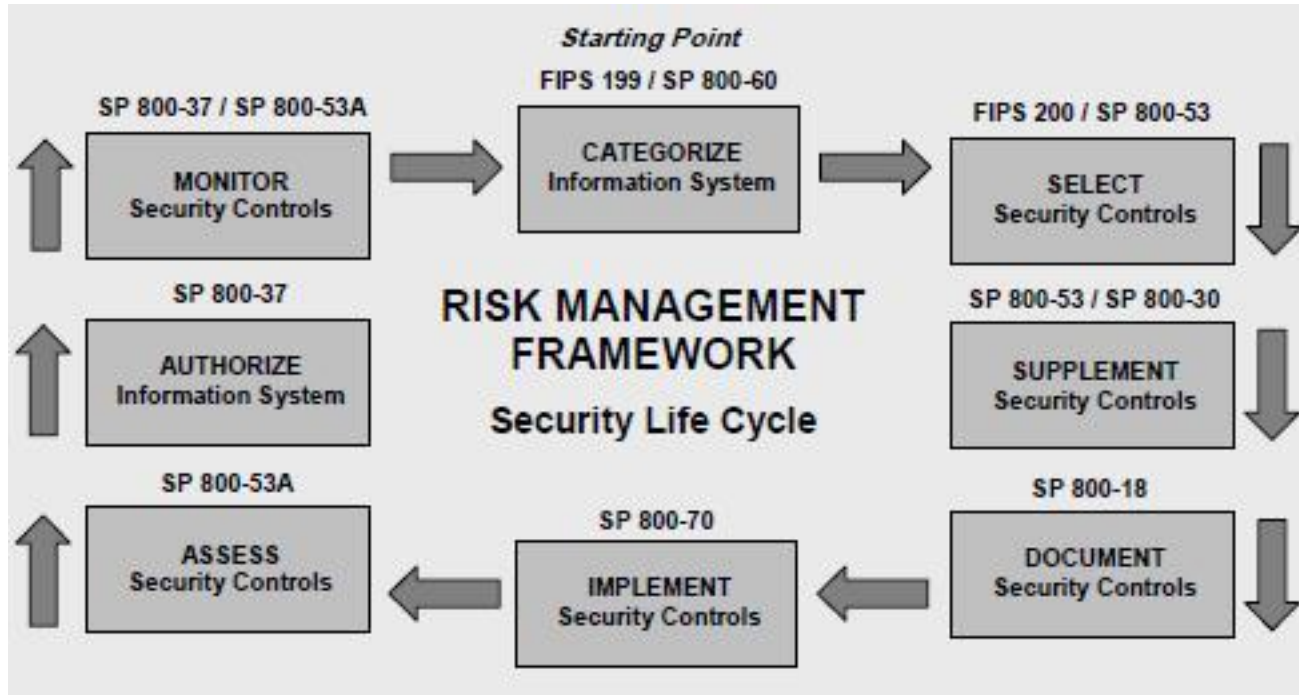
ITILv3



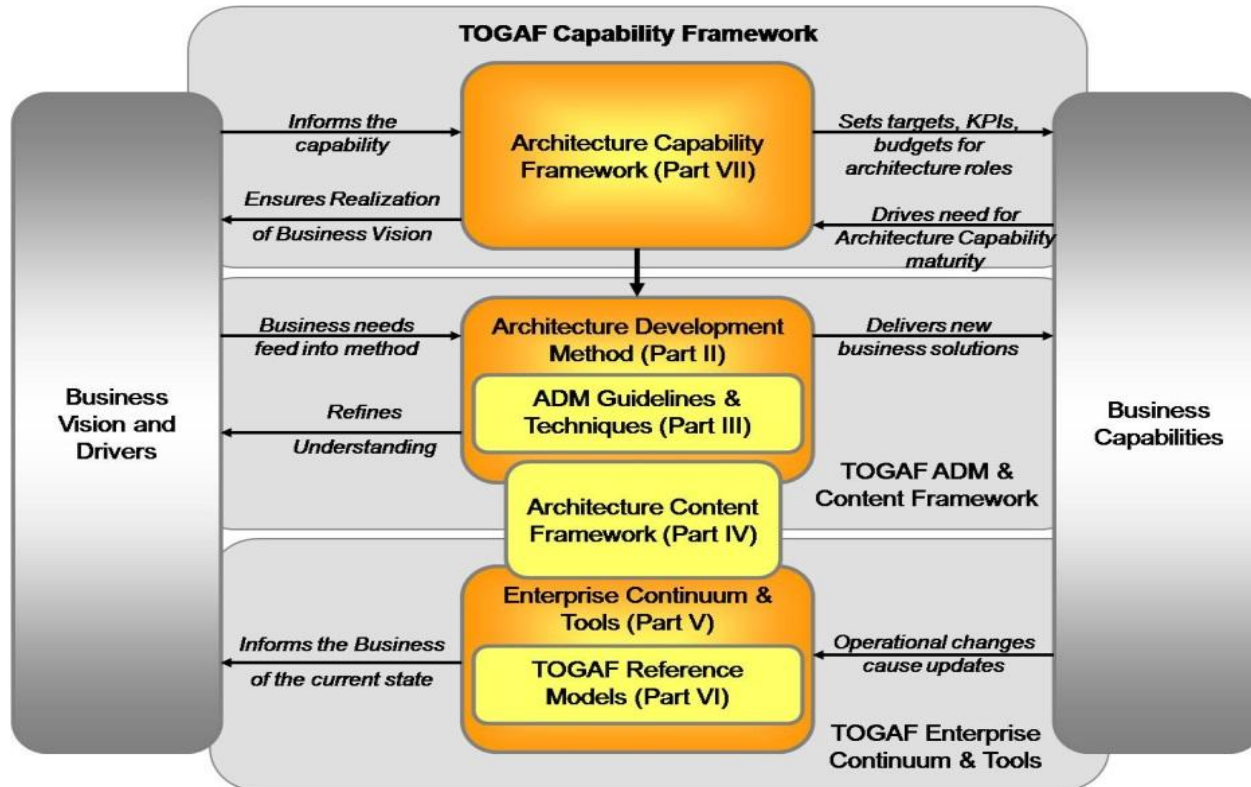
COSO



NIST SP800-53



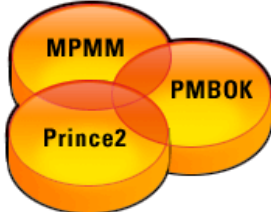
TOGAF 8.1-9.0



CMMI®



PMBOK-PRINCE2-MPMM



theIIA-Global Technology Audit Guides (GTAG)

- PG GTAG-15: Information Security Governance
- PG GTAG-14: Auditing User-developed Applications
- PG GTAG-13: Fraud Prevention and Detection in an Automated World
- PG GTAG-12: Auditing IT Projects
- PG GTAG-11: Developing the IT Audit Plan
- PG GTAG-10: Business Continuity Management
- PG GTAG-9: Identity and Access Management
- PG GTAG-8: Auditing Application Controls
- PG GTAG-7: Information Technology Outsourcing
- PG GTAG-6: Managing and Auditing IT Vulnerabilities
- PG GTAG-5: Managing and Auditing Privacy Risks
- PG GTAG-4: Management of IT Auditing
- PG GTAG-3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment
- PG GTAG-2: Change and Patch Management Controls: Critical for Organizational Success
- PG GTAG-1: Information Technology Controls



Regülasyonlar

- The Sarbanes–Oxley Act (Sarbox\SOX)
- The Gramm–Leach–Bliley Act (GLB)
- PCI Data Security Standard (PCI DSS)
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules
- BASEL II-III



Teşekkürler :-)

BTYD 2010

www.btyd.org