ISO Audit and Certification of Trustworthy Digital Repositories

Part II - IT Assessment Methodologies

Bob “Mister” Rogers
mrrogers@ApplicationMatrix.com

PASIG, Austin, TX
Why Risk, Security, and Governance Assessment?

• Trustworthy digital repositories (TDRs) are applicable to every sector of business and government, e.g.,
  – Email and email archives
  – Contracts and business records
  – Electronic medical records
  – Personally identifiable information (PII)
  – Critical infrastructure information (CII)
WHY DOES GOOD DATA GO BAD?
## IT Vulnerability

![Image of a computer screen with the DataLossDB website open, displaying details of various data loss incidents involving credit card numbers and personal information.](image-url)
TDR’s are Only *Part* of the Solution

**People**
- Policies
- Knowledge / Training
- Roles / Access Rights

**Process**
- Retention
- Legal Holds
- Migration
- DR / BCP
- Enforcement

**Technology**
- Application Software
- Security
- Server
- Storage
A “Holistic” Approach is Needed

- Information Governance Reference Model (IGRM)
- CoBiT/Val IT/Risk IT
- ILM2.0 Service Mgt Approach to Information Mgt and automation
- Method for an Integrated Knowledge Environment (MIKE2.0)
- ISM3 Maturity Model
- Security Operations Maturity Architecture (SOMA)
Duty: Legal obligation for specific information

Value: Utility or business purpose of specific information

Asset: Specific container of information
Approaches to Information Security and Management

• **Process oriented** (ISM3, CMMI, Cobit 4.0, ISO9001:2000, ISO20000, ITIL/ITSM)

• **Risk management oriented** (AS/NZS 4360, CRAMM, EBIOS, ISO 27005, MAGERIT, OCTAVE, SP800-30, SOMAP)

• **Controls oriented** (BSI-ITBPM, ISO27000:2005, ISO13335-4)

• **Product oriented** (Common Criteria/ISO15408)

• **Best practice oriented** (ISO/IEC 17799:2005, Cobit, ISF-SoGP)
• Security in Context

• Balance between:
  – business, compliance, and technical needs
  – and limitations, like cost, functionality, privacy, liability and risk

• Process Model
  – Strategic
  – Tactical
  – Operational
A Taxonomy of Cyber Security Risks

- Actions of People
  - Inadvertent
  - Deliberate
  - Inaction

- Systems and Technology Failures
  - Hardware
  - Software
  - Systems

- Failed Internal Processes
  - Process Design or Execution
  - Process Controls
  - Supporting Processes

- External Events
  - Hazards
  - Legal Issues
  - Business Issues
  - Service Dependencies

Source: SEI
Security Control Categories

• Technical
  • Access Control
  • Audit and Accountability
  • Identification and Authentication
  • System and Communications Protection

• Operational
  • Awareness and Training
  • Configuration Management
  • Contingency Planning
  • Incident Response
  • Maintenance
  • Media Protection
  • Physical and Environmental Protection
  • Personnel Security
  • System and Information Integrity

• Management
  • Risk Assessment
  • Planning
  • Security Assessment and Authorization
  • System and Services Acquisition
  • Program Management
Certifying Organizations

- Information Systems Audit and Control Association (ISACA)
  - Certified Information Systems Auditor (CISA)
  - Certified in the Governance of Enterprise IT (CGEIT)
  - Certified in Risk and Information Systems Control (CRISC)
- International Information Systems Security Certification Consortium, Inc. (ISC)²
  - CISSP - Certified Information Systems Security Professional
    - Information Systems Security Architecture Professional (ISSAP)
    - Information Systems Security Engineering Professional (ISSEP)
    - Information Systems Security Management Professional (ISSMP)
For More Information

• Software Engineering Institute
  – A Taxonomy of Operational Cyber Security Risks

• National Institute of Standards and Technology (NIST)
  – Guide for Conducting Risk Assessments (SP800-30 R1)
  – Recommended Security Controls for Federal Information Systems and Organizations (SP800-53 R3)

• INCITS/ISO/IEC
  – ISO27001 Information technology - Security techniques - Information security management systems – Requirements

• Cloud Security Alliance
  – Security Guidance for Critical Areas of Focus in Cloud Computing
Summary

• ISO16363 is a stewardship-focused starting point
• TDR audits/assessments require a broad spectrum risk-based approach
• The stakeholders in commercial and government TDR’s can be a very broad and diverse set of organizations
• Legal and compliance requirements are significant factors