SOX compliance

BALAZS LENDVAY

Agenda

- Introduction
- What is ISMS
- Frameworks & Standards overview
- SOX detailed review
- Conclusion
- Questions

Information Security Management System

- Centrally managed framework, specific to your business environment
- Set of policies and procedures for systematically managing sensitive data
- Applied to the whole company or to specific data
- Based on a risk assessment across the organization, likelihood and potential impact
- Business management process, not an IT function
- Goal is to minimize risk and ensure business continuity
- Typically addresses employee behavior and processes as well as data and technology

ISMS - Benefits

- Manage information in all its forms
- Technology-based risks and other, more common threats
- Reduces costs (through risk assessment)
- Constantly adapts to changes, controls remain up to date and work properly
- Organizational culture and making processes efficient
- Data Confidentiality, Integrity and Availability
- Timely recovery
- Significantly more resilient to cyber attacks

ISMS - Frameworks

- ISO/IEC 27000 (International Organization for Standardization)
  - Standard and Framework
  - Defines a global approach to security management
- ITIL (IT Infrastructure Library)
  - Defines the processes to be implemented to deliver and support IT services focusing on the business.
- COBIT (Control Objectives for Information and Related Technology)
  - Overlaps with ITIL considerably
  - Up-to-date international set of generally accepted control objectives
  - Focused on controls and metrics
  - Lacks a security component but provides a more global view of IT processes

ISO/IEC 27001:2013 – What is it?

- Requirements for establishing, implementing, maintaining, and improving an Information Security Management System (ISMS)
- Requirements for the assessment and treatment of information security risks
- Does NOT formally mandate specific information security controls
- Management may elect to avoid, transfer or accept information risks
- “Statement of Applicability” (SoA) is not explicitly defined, but mandatory
- Certified compliance with ISO/IEC 27001 is optional (refer to SoA)

ISO/IEC 27002:2013 – What is it?

- Internationally-recognized standard of good practice for information security
- Covers security of all forms of information
- ISO/IEC 27001 formally defines the mandatory requirements for an ISMS
- ISO/IEC 27002 is merely a code of practice/guideline rather than a certification standard
- Recommends information security controls addressing information security control objectives arising from risks to the confidentiality, integrity and availability of information
- Control objectives are at a fairly high level and, in effect, comprise a generic functional requirements specification
- Requires the Statement of Applicability (SoA)
- Forward looking 3 year cycle

SOC - What is it?

- Service Organization Controls Report (SOC)
  - AICPA - American Institute of CPAs - framework for CPAs to examine controls at a service organization
  - Conducted in accordance with Statements on Standards for Attestation Engagements – SSAE 16
- SOC 1
  - Audit of internal controls over financial reporting. If your service provides a number that affects the financial status of your customer, this might apply
  - Description of a service organization's system; suitability of the design of controls
- SOC 2
  - Typically IT focused audit over one, to all five, of the Trust Services Principles (TSP's):
    Security, Availability, Processing Integrity, Confidentiality, Privacy
  - Description of a service organization's system; design and operating effectiveness of controls
  - Point in time report (type I); cover a period of time (type II)
- SOC 3
  - Similar to a SOC 2 audit, less detail, results is mostly used for marketing purposes
- SOC for Cybersecurity

SOX – What is it?

- Sarbanes-Oxley Act of 2002
- Goals:
  - Increase transparency in corporate governance and financial reporting
  - Formalize a system of internal checks and balances
- Applicable to:
  - All publicly held American companies
  - International companies having registered equity or debt securities with the U.S. Securities and Exchange Commission (SEC)
  - Any accounting firm or other third party that provides financial services to either of the above
- Penalties:
  - Penalties for non-compliance: Formal penalties for non-compliance with SOX can include fines, removal from listings on public stock exchanges and invalidation of D&O insurance policies. Under the Act, CEOs and CFOs who willfully submit an incorrect certification to a SOX compliance audit can face fines of $5 million and up to 20 years in jail.
- Takes place once a year. An independent auditor must conduct SOX audits. Company's responsibility
- Applies to any third parties you outsource financial work to – service organizations; SOC report!

SOX - Compliance audit

- Measure of how well your company manages its internal controls.
- **Section 302**:
  - Relates to a company's financial reporting
  - CEO and CFO to confirm that they accept personal responsibility for all internal controls and have reviewed these controls in the past 90 days, including information security infrastructure.
- **Section 404**:
  - Further requirements for the monitoring and maintenance of internal controls related to accounting and financials
  - Requires annual audit of these controls performed by an independent firm. Audit assesses the effectiveness of all internal controls and reports its findings back directly to the SEC.

SOC vs ISO summary

- ISO 27001/2
  - Provides best practice framework for establishing an ISMS. Guide for implementing a security program
  - Outlines the organization's conformance to the standard set of requirements
- SOC 2 type II
  - Provides an organization a way to demonstrate that security practices are in place and operating effectively
  - Report outlining the controls that meet the applicable Trust Services Criteria
- Both
  - Provide independent assurance on the service organization's controls that were designed and implemented to meet a specific set of requirements or criteria
  - Internationally recognized standards and are accepted worldwide
  - Allow a service organization to gain significant advantage over competitors

SOC vs SOX Summary

- SOC
  - Audit of internal controls to ensure data security
  - Granular, internal control reports to makes sure the information and data you store is accurate and protected at all times
- SOX
  - Government-issued record keeping and financial information disclosure standards law
  - Doesn’t tell you exactly how to run your record keeping, it does spell out what controls should be in place to provide accurate financial statements
- Both
  - Serve as a protective agent for consumers and organizations
  - Strive for enhanced financial data accuracy and greater internal control support

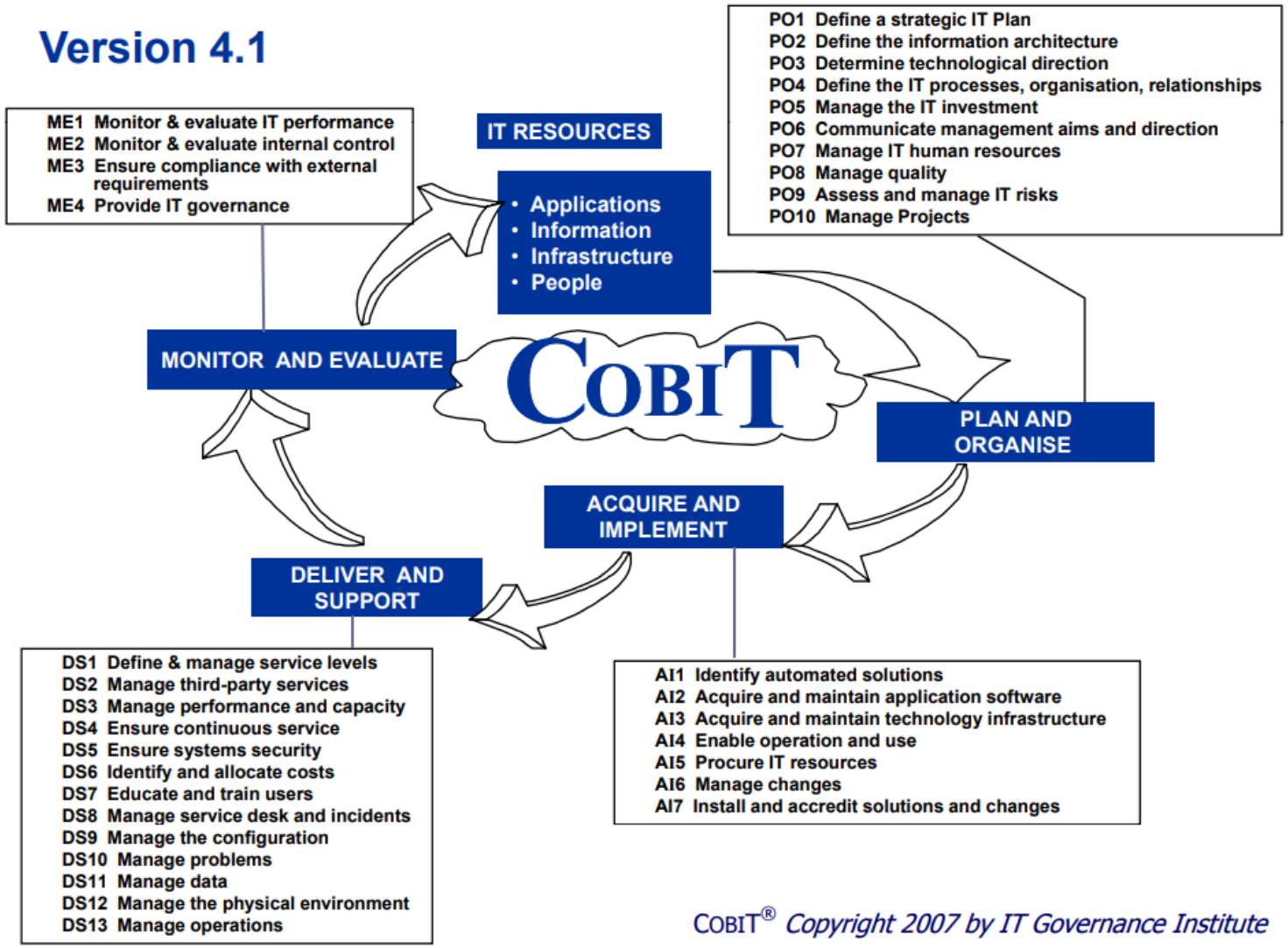
SOX - Important acronyms

- **PCAOB**: The Public Company Accounting Oversight Board. Develops auditing standards and train auditors on the best practices for assessing a company's internal controls. Publishes periodic recommendations and changes to the auditing process.
- **COSO**: Committee of Sponsoring Organizations, a joint organization consisting of representatives from the Institute of Management Accountants (IMA), the American Accounting Association (AAA), the American Institute of Certified Public Accountants (AICPA), the Institute of Internal Auditors (IIA) and Financial Executives International (FEI). Since 1992, COSO has published periodic updates to their internal control framework recommendations this document outlines guidelines for creating and implementing internal controls, and serves as the basis for the auditing standards developing by PCAOB.
- **COBIT**: COBIT (Control Objectives for Information and Related Technology) is a framework published by ISACA. ISACA covers guidelines for developing and assessing internal controls related to corporate information technology. Effectively a more specific version of the COSO framework, it outlines best practices for 34 IT processes. Many organizations will rely on both frameworks when developing a roadmap to SOX compliance.

COSO - Details

- Unified approach for evaluation of the internal control systems
  - Effectiveness and efficiency of operations
  - Compliance with actual laws and regulations
  - Reliability of financial reporting
- COSO framework control components
  - Internal Environment
  - Objective Setting
  - Event Identification
  - Risk Assessment
  - Risk Response
  - Control Activities
  - Information & Communication
  - Monitoring
- Risk Assessment
  - Analysis of risk
  - Consideration of likelihood and impact
  - How risks should be managed
- Risk Response
  - Avoid Risk
  - Accept Risk
  - Reduce Risk
  - Share Risk

Version 4.1



SOX - Audit process

1. Understand and identify the IT environment and systems to be reviewed
2. Perform interviews, walkthroughs, and documentation reviews to gain an understanding on processes
3. Assess appropriateness of existing control environment (control design)
4. Validate existing controls to assess control operating effectiveness

SOX – ITGC domains

1. Access to Programs and Data
2. Program Development
3. Program changes
4. Computer operations

SOX – ITGC – Access to programs and data

- Policies and procedures
- Physical and environmental security
- Logical access to systems and data
- Security configurations, e.g. password controls, lockout screens
- User Management
- Principle of Least Privilege (POLP)
- Segregation of Duties (SoD)
- Monitoring of access

SOX – Examples - Access

- User Access (DS5)
  - Users and their system activity should be uniquely identifiable
  - User access requests, modifications, and removals should be documented and approved
  - Terminated users should have access removed timely
  - Access levels should based on a user's job duties (least privilege principle)
  - Remote access should rely on secure protocols

SOX – Examples - Access

- Logical Security (DS5)
  - Confidentiality, integrity, and availability over systems and data
  - Strong authentication controls should prevent user accounts from being compromised
  - File shares should be adequately restricted to appropriate users
  - Patches/system updates should be applied timely
  - Network services should be closed unless necessary for business reasons
  - Anti-virus software should be installed and up-to-date
  - Sensitive data should be encrypted

SOX – ITGC – Program development & Program changes

- Having a record of what was changed, in addition to when it was changed and who changed it
- Documentation and Training over program development process
- Controls over Program Changes (e.g.: approvals, checkpoints)
- Transfer to live
- Maintenance activities
- Change Requests
- Software Development Life Cycle (SDLC)

SOX – Examples

- Change Management (AI6 & AI7)
  - Addresses how an organization modifies system functionality to meet business needs
  - Requests for changes should be documented and follow defined change management procedures
  - Emergency changes should follow a defined process
  - Changes should be properly tested (in separate environments) to ensure functionality meets defined requirements
  - Controls should restrict migration of program changes to production by authorized and appropriate individuals.

SOX – ITGC – Computer Operations

- Organization of IT function
- Service Level Agreements
- Business Continuity and Disaster Recovery Plans
- Network Management
- Backups and Recovery

Conclusion

- Frameworks complement each other
  - You can supplement the IT operational process strengths of ITIL with the critical success factors (CSF)
  - and key performance indicators (KPI) of COBIT,
  - and both can make good use of the security processes and controls defined in ISO
- COBIT and ISO also provide
  - guidance, key indicators, and controls for the definition of service-level agreements,
  - capacity planning, availability management, and business continuity, which complement ITIL service delivery processes
- Mapping, mapping, mapping…

Questions?

References

http://www.iso27001security.com/

https://linfordco.com/blog/soc-2-security-vs-iso-27001-certification/

https://www.ssae-16.com/

https://www.aicpa.org/InterestAreas/FRC/AssuranceAdvisoryServices/DownloadableDocuments/OtherMapping/Trust_Services_Map_to_ISO_27001.xlsx

http://www.sox-online.com/coso-cobit-center/original-coso-framework/

https://www.csoonline.com/article/220639

http://www.isaca.org/chapters7/Sacramento/NewsandAnnouncements/Documents/Overview_of_SOC_Reports_-_ISACA_Presentation_2-21-13_.pdf