IT and Security Standards
A Practical Approach to Implementation

ISACA San Francisco
October 20, 2005

Mark Lundin, Senior Manager, KPMG LLP
Agenda

- Introductions
- IT and Security Standards Landscape
- Standards Setting Process
- Comparison of Standards
- Use of Standards
- Questions
Introductions
IT and Security Standards
Landscape
So Many Standards

COBIT
ISO 20000
ISO 27001
ISO 27002
ISO 17799
SOX 404
ITGI
PCAOB #2
SysTrust
WebTrust

HIPAA
BS 7799
SAS 70
ISO 21827
BS 15000
CISF

ITIL
ISO 27002
CMM
PCI
ANSI

FFIEC
COSP
SAS 70
SOX 404
ITGI
PCAOB #2
SysTrust
WebTrust

CISP
BS 15000
CMM
PCI
ANSI

HIPAA
BS 7799
SAS 70
ISO 21827
BS 15000
CISF

ITIL
ISO 27002
CMM
PCI
ANSI
COBIT

- COBIT has been developed as a generally applicable and accepted standard for good Information Technology (IT) security and control practices that provides a reference framework for management, users, and IS audit, control and security practitioners.
- COBIT, issued by the IT Governance Institute and now in its third edition, is increasingly internationally accepted as good practice for control over information, IT and related risks.
- Core components include:
  - Framework with high level control objectives
  - Management guidelines
  - Detailed control objectives
  - Audit guidelines
- COBIT (version 4.0), planned for release in November 2005 has been enhanced to provide better integration with other more detailed, guidance such as ITIL ISO 17799.
BS 7799-1 / ISO 17799

- Developed by British Standards Institution (BSI)
- Maintained by ISO/IEC/JTC 1 (Information Technology)/SC 27 (IT Security Techniques)
  - This standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organizational security standards and effective security management practice and to provide confidence in inter-organizational dealings. Recommendations from this standard should be selected and used in accordance with applicable laws and regulations.
- ISO 17799 will be renumbered to ISO 27002 in the future.
BS 7799-2 / ISO 27001

- Developed by British Standards Institution (BSI)
- Maintained by ISO/IEC/JTC 1 (Information Technology)/SC 27 (IT Security Techniques)
- BS 7799-2:2002 Information security management systems - Specification with guidance for use
  - This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS within the context of the organization’s overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof.
BS 7799 / ISO 17799 – Model

Figure 1 — PDCA model applied to ISMS processes
BS 7799 / ISO 17799 – Scope

- Information Security Management System (ISMS)
  - Define scope, policy
  - Risk assessment
  - Address risks
  - Implement and operate
  - Monitor and review
  - Maintain and improve
  - Management commitment

- Security Policy
- Organizational Security
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Control
- Systems Development and Maintenance
- Business Continuity Management
- Compliance
ITIL

- Developed by Office of Government Commerce (UK)
- ITIL is intended to assist organizations to develop a framework for IT Service Management.

**IT Service Management is:**
- a top-down, business driven approach to the management of IT that specifically addresses
  - the strategic business value generated by the IT organization
  - the need to deliver a high quality IT service.
- designed to focus on the people, processes and technology issues that IT organizations face.
ITIL – Scope

- Service Support
- Service Delivery
- Planning to Implement Service Management
- Application Management
- ICT Infrastructure Management
- Security Management
- Software Asset Management
- The Business Perspective: The IS View on Delivering Services to the Business
Developed by British Standards Institution (BSI) based largely on ITIL

Maintained by ISO/IEC/JTC 1 (Information Technology)/SC 7 (Software and System Engineering)

BS 15000-1:2002 IT service management, Part 1: Specification for service management

- This specification defines the requirements for an organization to deliver managed services of an acceptable quality for its customers.

ISO/IEC DIS 20000-1 (ISO version being finalized)
Developed by British Standards Institution (BSI) based largely on ITIL

BS 15000-2:2003  IT service management, Part 2: Code of practice for service management
  - BS 15000-2 represents an industry consensus on quality standards for IT service management processes. These service management processes deliver the best possible service to meet an organization’s business needs within agreed resource levels, i.e. service that is professional, cost-effective and with risks which are understood and managed.

ISO/IEC DIS 20000-2  (ISO version being finalized)
Figure 1 — Plan-Do-Check-Act methodology for service management processes
Sarbanes-Oxley Act of 2002 (SOX)

Section 302 Management Requirements

- Section 302 requires a company’s management, with the participation of the principal executive and financial officers (the certifying officers), to make the following quarterly and annual certifications with respect to the company’s internal control over financial reporting:
  - A statement that the certifying officers are responsible for establishing and maintaining internal control over financial reporting.
  - A statement that the certifying officers have designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under their supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles.
  - A statement that the report discloses any changes in the company’s internal control over financial reporting that occurred during the most recent fiscal quarter (the company’s fourth fiscal quarter in the case of an annual report) that have materially affected, or are reasonably likely to materially affect, the company’s internal control over financial reporting.

Section 404 Management Requirements

- Requires the SEC to prescribe rules requiring each annual report required by section 13(a) or 15(d) of the Securities Exchange Act of 1934 to contain an internal control report, which shall: (1) state the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting and (2) contain an assessment, as of the end of the most recent fiscal year of the issuer, of the effectiveness of the internal control structure and procedures of the issuer for financial reporting.

- With respect to the internal control assessment required by this section, each registered public accounting firm that prepares or issues the audit report for the issuer shall attest to, and report on, the assessment made by the management of the issuer. Such attestation shall be made in accordance with standards for attestation engagements issued or adopted by the Board. Any such attestation shall not be the subject of a separate engagement.

Source: [http://www.theiia.org](http://www.theiia.org)
COSO

- Developed by the Committee of Sponsoring Organizations of the Treadway Commission
- COSO is a voluntary private sector organization dedicated to improving the quality of financial reporting through business ethics, effective internal controls, and corporate governance.
- COSO was originally formed in 1985 to sponsor the National Commission on Fraudulent Financial Reporting, an independent private sector initiative which studied the causal factors that can lead to fraudulent financial reporting and developed recommendations for public companies and their independent auditors, for the SEC and other regulators, and for educational institutions.
- The National Commission was jointly sponsored by five major professional associations in the United States, the American Accounting Association, the American Institute of Certified Public Accountants, Financial Executives International, The Institute of Internal Auditors, and the National Association of Accountants (now the Institute of Management Accountants).
Internal Control - Integrated Framework (1994)

- Control Environment
- Risk Assessment
- Control Activities
- Information & Communication
- Monitoring


- Internal Environment
  - Objective Setting
  - Event Identification
  - Risk Assessment
  - Risk Response
  - Control Activities
  - Information & Communication
  - Monitoring

- This standard establishes requirements and provides directions that apply when an auditor is engaged to audit both a company’s financial statements and management's assessment of the effectiveness of internal control over financial reporting.

Section 13. Management is required to base its assessment of the effectiveness of the company's internal control over financial reporting on a suitable, recognized control framework established by a body of experts that followed due-process procedures, including the broad distribution of the framework for public comment.

Section 14. In the United States, the Committee of Sponsoring Organizations ("COSO") of the Treadway Commission has published Internal Control – Integrated Framework. Known as the COSO report, it provides a suitable and available framework for purposes of management's assessment.
Section 50. Some controls (such as company-level controls, described in paragraph 53) might have a pervasive effect on the achievement of many overall objectives of the control criteria. For example, information technology general controls over program development, program changes, computer operations, and access to programs and data help ensure that specific controls over the processing of transactions are operating effectively.
ITGI – IT Control Objectives for Sarbanes-Oxley

- This research is intended as a reference for executive management and IT control professionals, including IT management and assurance professionals, when evaluating an organization’s IT controls as required by the US Sarbanes-Oxley Act of 2002 (the “Act”).

Based on COBIT, COSO, SOX 404 and PCAOB#2.

Developed by the IT Governance Institute (ITGI)
- Affiliated with the Information Systems Audit and Control Association (ISACA)
- Established in 1998 as a research think tank in recognition of the increasing criticality of information technology to enterprise success.
ITGI – IT Control Objectives for Sarbanes-Oxley – Scope

- **IT General Controls - Program Development and Program Change**
  - Acquire or develop application system software
  - Acquire technology infrastructure
  - Develop and maintain policies and procedures
  - Install and test application software and technology infrastructure
  - Manage changes

- **IT General Controls - Computer Operations and Access to Programs and Data**
  - Define and manage service levels
  - Manage third-party services
  - Ensure systems security
  - Manage the configuration
  - Manage problems and incidents
  - Manage data
  - Manage operations

- **Company Level Controls**
  - Control Environment
  - Information and Communication
  - Risk Assessment
  - Monitoring

- **Application Controls—Business Cycles**
  - Sales Cycle
  - Purchasing Cycle
  - Inventory Cycle
  - Asset Management Cycle
  - Human Resources Cycle
-- Capability Maturity Model (SSE-CMM)

- Maintained by the International Systems Security Engineering Association (ISSEA) and ISO JTC 1/SC 27 (IT Security techniques)

- The SSE-CMM is a process reference model. It is focused upon the requirements for implementing security in a system or series of related systems that are the information technology security (ITS) domain. Within the ITS domain the SSE-CMM Model is focused on the processes used to achieve ITS, most specifically on the maturity of those processes.

- The SSE-CMM describes the essential characteristics of an organization's security engineering process that must exist to ensure good security engineering.
CMM / ISO 21827 – Scope

Security Engineering Process Areas
- PA01 Administer Security Controls
- PA02 Assess Impact
- PA03 Assess Security Risk
- PA04 Assess Threat
- PA05 Assess Vulnerability
- PA06 Build Assurance Argument
- PA07 Coordinate Security
- PA08 Monitor Security Posture
- PA09 Provide Security Input
- PA10 Specify Security Needs
- PA11 Verify and Validate Security

Project and Organizational Process Areas
- PA12 - Ensure Quality
- PA13 - Manage Configuration
- PA14 - Manage Project Risk
- PA15 - Monitor and Control Technical Effort
- PA16 - Plan Technical Effort
- PA17 - Define Organization's Systems Engineering Process
- PA18 - Improve Organization’s Systems Engineering Process
- PA19 - Manage Product Line Evolution
- PA20 - Manage Systems Engineering Support Environment
- PA21 - Provide Ongoing Skills and Knowledge
- PA22 - Coordinate with Suppliers
CMM / ISO 21827 – Capability Levels

Figure 6 - Capability levels represent the maturity of security engineering organizations.
Examples of ISO Standards

The following are examples of standards developed within the TC68/SC2 financial services security working groups:

- ISO/TR13569 Financial services - Information security guidelines
- ISO 15782-1- Certificate management for financial services -- Part 1: Public key certificates
- ISO 19092-2 – Financial Services Biometrics – Part 2: Cryptographic Techniques
- ISO 10126 Banking – Procedures for message encipherment (wholesale) – Part 1: General principles
- ISO 10126-2 Banking – Procedures for message encipherment (wholesale) – Part 2: DEA algorithm
- TR 19038 Banking and related financial services - Part 1-Triple data encryption algorithm modes of operation
Examples of ANSI Standards

Examples of American National Standards Institute (ANSI) standards developed through the Accredited Standards Committee (ASC) X9 (Financial Services) standards organization include:

- ANS X9.19 Financial Institution Retail Message Authentication
- ANS X9.30:1 Public Key Cryptography, The Digital Signature Algorithm
- ANS X9.30:2 Public Key Cryptography, The Secure Hash Algorithm
- ANS X9.31 Digital Signatures Using Reversible Public Key Cryptography for the Financial Services Industry
- ANS X9.49 Secure Remote Access to Financial Services for the Financial Industry
- ANS X9.52 Triple Data Encryption Algorithm Modes of Operation
- ANS X9.62 Public Key Cryptography for the Financial Services ECDSA
- ANS X9.63 Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography
- ANS X9.65 Triple Data Encryption Algorithm (TDEA) Implementation
- ANS X9.79-1 PKI Practices and Policy Framework
- ANS X9.84 Biometric Information Management and Security for the Financial Services Industry
- TG-4 Recommended Notation for DEA Key Management in Retail Financial Networks
- TG-5 Information Security Guideline
- TG-19-1 Triple DES Validation System Procedures
- TG-19-4 Secure Hash Algorithm Validation System (SHAWS): Requirements and Procedures
Examples of Industry Requirements

PCI

Payment Card Industry Data Security Standard (PCI)
- Developed by Visa and MasterCard
- Supercedes Visa’s Cardholder Information Security Program (CISP) and MasterCard’s Site Data Protection (SDP) programs
- This standard is the result of collaboration between Visa and MasterCard to create common industry security requirements.
- Applies to merchants and service providers (i.e., processors and payment gateways)
PCI – Scope

- **Build and Maintain a Secure Network**
  - Install and maintain a firewall configuration to protect data
  - Do not use vendor-supplied defaults for system passwords and other security parameters

- **Protect Cardholder Data**
  - Protect stored data
  - Encrypt transmission of cardholder data and sensitive information across public networks

- **Maintain a Vulnerability Management Program**
  - Use and regularly update anti-virus software
  - Develop and maintain secure systems and applications

- **Implement Strong Access Control Measures**
  - Restrict access to data by business need-to-know
  - Assign a unique ID to each person with computer access
  - Restrict physical access to cardholder data

- **Regularly Monitor and Test Networks**
  - Track and monitor all access to network resources and cardholder data
  - Regularly test security systems and processes.

- **Maintain an Information Security Policy**
  - Maintain a policy that addresses information security
Examples of Industry Requirements


- This booklet provides guidance to examiners and organizations on determining the level of security risks to the organization and evaluating the adequacy of the organization’s risk management.

Topics covered include:
- Security Process
- Information Security Risk Assessment
- Information Security Strategy
- Security Controls Implementation
- Security Testing
- Monitoring and Updating
Examples of Industry Requirements

HIPAA

  - This final rule adopts standards for the security of electronic protected health information to be implemented by health plans, health care clearinghouses, and certain health care providers.
  - This final rule implements some of the requirements of the Administrative Simplification subtitle of the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

- The scope includes:
  - Administrative safeguards
  - Physical safeguards
  - Technical safeguards
  - Organizational requirements
  - Policies and procedures and documentation requirements
SAS 70

- Statement of Auditing Standards (SAS) No. 70, Service Organizations
- Audit reporting framework for service organizations defined by AICPA
- Type 1 report covers design and controls placed in operation
- Type 2 adds tests of operating effectiveness
- Report structure:
  - Auditor’s opinion
  - Service provider’s description of controls
    - Overview of operations
    - Control objectives
    - Supporting control procedures
    - COSO components
  - Auditor’s tests of operating effectiveness and results
  - Other information

Typical IT control objective topics include, but are not limited to:
- Systems development
- Change management
- Logical access
- Physical access
- Operations management
- Job processing
- Communications security
Trust Services
(WebTrust/SysTrust)

- AICPA/CICA Trust Services Criteria:
  - Security
  - Availability
  - Processing Integrity
  - Online Privacy
  - Confidentiality

- There are four levels of requirements:
  - Policies
  - Communications
  - Procedures
  - Monitoring

- The WebTrust reporting framework is focused on online systems whereas SysTrust applies to any type of system.

- WebTrust for Certification Authorities (WebTrust for CAs) applies specifically to public key infrastructure (PKI) / certification authority (CA) systems and includes requirements for CA Business Practices, CA Environmental Controls, CA Key Life Cycle Management, and Certificate Life Cycle Management.
Standards Setting Process
ISO Technical Committees

There are over 200 ISO technical committees:
- JTC 1 Information technology
- TC 1 Screw threads
- TC 2 Fasteners
- TC 3 Limits and fits
- TC 4 Rolling bearings
- TC 5 Ferrous metal pipes and metallic fittings
- TC 6 Paper, board and pulps
- TC 8 Ships and marine technology
- TC 10 Technical product documentation
- ...
- TC 68 Financial services
- TC 69 Applications of statistical methods
- TC 70 Internal combustion engines
- ...
- TC 227 Springs
- TC 228 Tourism and related services
- TC 229 Nanotechnologies

Committees are structured as follows:
- Technical Committee
  - Subcommittees
    - Working groups

For Example:

- ISO/IEC JTC 001 Information technology
  - SC 07 - Software and System Engineering
  - SC 27 - IT Security Techniques
  - SC 37 - Biometrics

- TC 68 Financial Services
  - SC2 Financial Services Security
    - WG4 Information Security Guidelines for Banking
    - WG8 Certificate Management for Financial Services
    - WG11 Encryption Algorithms Used in Banking Applications
    - WG13 Security in Retail Banking
<table>
<thead>
<tr>
<th>STAGE</th>
<th>00</th>
<th>20</th>
<th>60</th>
<th>SUB-STAGE</th>
<th>90</th>
<th>99</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Registration</td>
<td>Start of main action</td>
<td>Completion of main action</td>
<td>92 Repeat an earlier phase</td>
<td>93 Repeat current phase</td>
<td>98 Abandon</td>
</tr>
<tr>
<td>00 Preliminary stage</td>
<td>00.00 Proposal for new project received</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>10 Proposal stage</td>
<td>10.00 Proposal for new project registered</td>
<td>10.20 New project ballot initiated</td>
<td>10.60 Voting summary circulated</td>
<td>10.92 Proposal returned to submitter for further definition</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20 Preparatory Stage</td>
<td>20.00 New project registered in TC/SC work program</td>
<td>20.20 Working draft (WD) study initiated</td>
<td>20.60 Comments summary circulated</td>
<td></td>
<td>20.98 Project deleted</td>
<td>20.99 WD approved for registration as CD</td>
</tr>
<tr>
<td>30 Committee Stage</td>
<td>30.00 Committee draft (CD) registered</td>
<td>30.20 CD study ballot initiated</td>
<td>30.60 Comments/voting summary circulated</td>
<td>30.92 DC referred back to Working Group</td>
<td>30.98 Project deleted</td>
<td>30.99 CD approved for registration as DIS</td>
</tr>
<tr>
<td>40 Enquiry stage</td>
<td>40.00 DIS registered</td>
<td>40.20 DIS ballot initiated: 5 months</td>
<td>40.60 Voting summary dispatched</td>
<td>40.92 Full report circulated: DIS referred to TC or SC</td>
<td>40.93 Full report circulated decision for new DIS ballot</td>
<td>40.98 Project deleted</td>
</tr>
<tr>
<td>50 Approval stage</td>
<td>50.00 FDIS registered for formal approval</td>
<td>50.20 FDIS ballot initiated: 2 months. Proof sent to secretariat</td>
<td>50.60 Voting summary dispatched. Proof returned by secretariat</td>
<td>50.92 FDIS referred back to TC or SC</td>
<td>50.98 Project deleted</td>
<td>50.99 FDIS approved for publication</td>
</tr>
<tr>
<td>60 Publication Stage</td>
<td>60.00 International Standard under publication</td>
<td>60.60 International Standard published</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>90 Review stage</td>
<td>90.20 International Standard under periodical review</td>
<td>90.60 Review summary dispatched</td>
<td>90.92 International standard to be revised</td>
<td>90.93 International Standard confirmed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>95 Withdrawal Stage</td>
<td>95.20 Withdrawal Ballot initiated</td>
<td>95.60 Voting summary dispatched</td>
<td>95.92 Decision not to withdraw International Standard</td>
<td></td>
<td></td>
<td>95.99 Withdrawal of International Standard</td>
</tr>
</tbody>
</table>
Comparison of Standards
# High Level Standards Roadmap

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>COSO</td>
<td>BS 7799-1/ ISO 17799</td>
<td>ITIL BS15000-2/ ISO 20000-2</td>
<td>CMM/ ISO 21827</td>
<td>ITGI-SOX</td>
<td>ISO various ANSI various</td>
<td></td>
</tr>
<tr>
<td>Certification/ Audit Criteria/ Requirements</td>
<td>BS 7799-2/ ISO 27001</td>
<td>BS 15000-1/ ISO 20000-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Regulatory/ Industry Requirements</td>
<td>PCI FFIEC HIPAA</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audit Framework</td>
<td>SAS 70 &amp; Trust Services</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>WebTrust for CAs</td>
<td></td>
</tr>
</tbody>
</table>
Use of Standards / Putting it All Together
Putting It All Together

- Standards can be used as:
  - a guide for defining internal control objectives and developing internal policies
  - a guide for assessing current controls against an industry standard
    - Design vs. effectiveness
    - In place vs. not in place
    - Levels of maturity
  - a basis for external certification / audits
  - a guide for defining requirements for third parties (e.g., security requirements, service level agreements)
  - a basis for assessing compliance with agreements
A Standards-Based Approach

Feedback Loop

Consider:
- New risks
- New requirements
- Organizational changes
- Refining existing requirements
- Automated vs. manual controls
- Continuous improvement

Define Control Objectives That Address Business Risks

Define Requirements

Define Specific Controls and Specific Procedures

Measure Compliance

Address Significant Non-Compliance Issues

Use the most relevant standard as a foundation and add relevant incremental requirements of other standards, regulations, etc. as needed.
Risks

- Avoid the endless cycle of mapping.
- Avoid the temptation to address obscure topics.
- Avoid the tendency to search for something that “sort of” meets the requirement.
- Avoid unclear measurement criteria
For More Information

Please contact:

Mark A. Lundin
Senior Manager, Risk Advisory Services
KPMG LLP
55 Second Street
San Francisco, CA 94105
Office: 415-963-5493
Cell: 925-864-1054
Email: mlundin@kpmg.com