Financial Sector Regulations Pertaining to Pen Testing

Overview

IT Governance Best Practice

Strategic Alignment - Focuses on ensuring the linkage of business and IT plans; on defining, maintaining and validating the IT value proposition; and on aligning IT operations with enterprise operations.

Value Delivery - It is about executing the value proposition throughout the delivery cycle, ensuring that IT delivers the promised benefits, concentrating on optimizing costs and proving the intrinsic value of IT.

Resource Management - It is about the optimal investment in, and the proper management of, critical IT resources, including information, infrastructure and people.

IT Governance Best Practice

Risk Management - It requires risk awareness by officers, a clear understanding of the appetite for risk, understanding of compliance requirements, transparency about the significant risks, and embedding of risk management responsibilities into the organization.

Performance Measurement - Tracks and monitors strategy implementation, project completion, resource usage, process performance and service delivery. Using, for example, balanced scorecards that translate strategy into action to achieve goals measurable beyond conventional accounting.

IT Risk Management

Involves four major components:

- Assets
- Threats
- Vulnerabilities
- Impact

Types of Risks

The risks are many and include:

- Data theft
- Cyber attacks
- Data integrity
- Disaster recovery and uptime
- Privacy concerns
- Record retention
- Meeting compliance
- Monetary and credit risk
- Natural disasters of all sorts affecting customers and IT operations
- Economic, market, and major customer risks
- Political risks from changing regulation, laws, policies
- Internal turmoil, audit problems, fraud, etc.

Risk Management

What must be considered?

- Relationship among critical assets
- Threats to those assets
- Vulnerabilities that can expose assets
- Must be looked at via operational context

The four basic approaches:

- Vulnerability Assessment
- Information Security Audit
- Information Security Risk Evaluation
- Managed Services Provider

Information Security Risk Evaluation

Focuses on the following four aspects of security:

- Examine corporate security policies to identify strengths and weaknesses to mitigate or create risk.
  - Compares against industry standards or best practices
- Examines all technology systems, reviews policies, and inspection of physical security.
- Examine IT infrastructure for tech vulnerabilities such as:
  - Introduction of malicious code
  - Corruption or destruction of data
  - Denial of service
  - Unauthorized change and access rights, etc, etc
- To help decision making, examine tradeoff and select cost effective countermeasures.

Information Security Risk Evaluation

PRINCIPLES

- Self Direction – Internal Responsibility for Risk Management
- Adaptable Measures – Flexible Evaluation Process
- Defined Process – Standardized Evaluation Procedures
- Continuous Process – Institutionalize Good Security Practices

Improving Security Posture

You must take the following four steps:

- Move away from a reactive, problem based agenda to proactive prevention.
- Look at security from multiple perspectives i.e. business not just technology.
- Embrace a flexible infrastructure that responds to change quickly.
- Initiate an ongoing system to maintain and improve security posture.

Risk Evaluation Activities

Identifying Information Security Risks

Analyze risk to determine priorities. ex. BIA

Plan for improvement by developing protection strategies.

After risk evaluation, the organization should take the following steps:

- **Plan to implement protection strategy**
- **Implement the selected detailed action plan**
- **Monitor plan for progress and effectiveness**
- **Control variations by taking corrective actions**
- **Plan-do-check-act cycle**

Risk Assessment

Information Gathering

Technical Information

Non-Technical Information

You will need both!

Additionally, information regarding control effectiveness should be gathered. Typically, that information comes from security monitoring, including self-assessments, metrics, and independent tests.

Information Gathering

Items that need to be included:

- An identification of information and the information systems to be protected.
- System characterization and data flow analysis.
  - It is important to understand how the institution uses information in its day-to-day operations.
- The outsourcing strategy.
- Classify and Rank Sensitive Data, Systems, and Applications

Data Classification

Institutions should establish an information data classification program to identify and rank data, systems, and applications in order of importance.

Classification should be based on a weighted composite of all relevant attributes.

Threats and Vulnerabilities

This prioritizes the threats and vulnerabilities.

Threats are the events that could cause harm.

Vulnerabilities can be categorized as weaknesses.

- Known vulnerabilities are discovered by testing!

Analyze the probability of different threats causing damage.

You need to look at the potential damage or impact of each threat.

Two general categories:

- Quantitative
- Qualitative

Analytical Methods

Quantitative Method

- Assigning Numerical Measurements.
  - Ex. DoS – Down for 2 hours and your organization generally profits $3000 per hour. Your potential loss is $6000.

Qualitative Method

- Subjective
- Attempts to determine the seriousness of threats and includes the impact.
- Most common in Pen Testing.

Evaluate Controls

Identify controls that mitigate risk.

Generally Categorized by:

- Timing
  - Preventative
  - Detective
  - Corrective
- Nature
  - Administrative
  - Technical
  - Physical

Evaluation must include:

- Controls that Prevent Harm
- Controls that Detect Harm

Evaluate Controls

Evaluation should include:

- Effectiveness of Control
  - Based on non-compliance
- The risks to information held and processed by service providers.
- Independent review of internal controls at service providers and vendors.
- Review of relevant physical access controls.

- These Reviews should be comprehensive and address all data and facilities including remote sites.

Risk Ratings

- Not all threats and risks are equal.
- Institutions have finite resources.

Key - Organize the information and information systems within a logical framework.

Determining the risk rating:

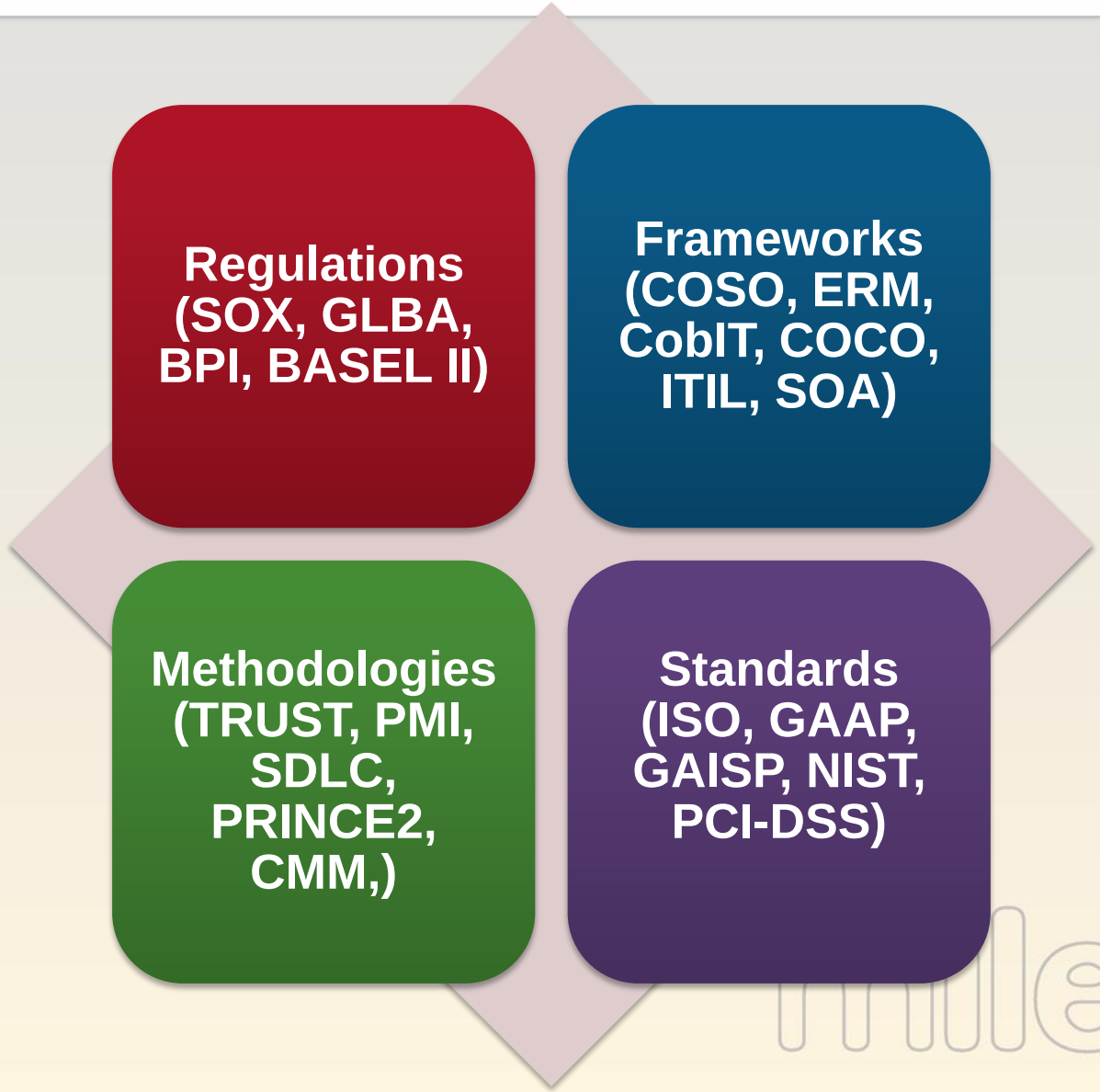
- Probability or Likelihood
- Impact
- Generally High, Medium and Low

- Will you accept the risk?
- Will you mitigate the risk?

Segregation – What happens now?

Important Risk Assessment Practices

Compliance



Many Regulations

Basel II

Original Basel accord in 1988

International accord based on Swiss banking to assure capital protection, data management, & risk management. An international initiative that requires financial services companies to have a more risk sensitive framework for the assessment of regulatory capital. Implementation of Basel II by December 2006.

Key areas are: data capture, reporting and analysis of credit, market, operational risk, and then mitigating perceived risks through business processes, whether automated or performed physically. In other words, IT security is a part of this operational risk mitigation process.

Gramm-Leach-Bliley-Act 1999 Title V

Financial Institutions (banks, ins co's, etc) must protect the confidentiality of an individual's private information.

Required to create, implement, and maintain a comprehensive security program with administrative, technical, and physical safeguards.

Security program must include:

- **Assign designated security program manager.**
- **Conduct periodic risk and vulnerability assessments.**
- **Perform regular testing and monitoring.**
- **Define procedures for change in lieu of test results or changes in circumstance.**

Federal Financial Examination Institution Council - FFIEC

Comprised of the Federal Reserve Board, Office of Comptroller of the Currency, FDIC, Office of Thrift Supervision, and National Credit Union Association Coordination with GLBA 501(B)

Implement security process for the following five areas:

- IT security Risk Assessment
- Information Security Strategy
- Security Controls Implementation
- Security Monitoring
- Security Process Monitoring and Updating

Sarbanes-Oxley Act (SOX 404) 2002

Creation of PCAOB (Public Accounting Oversight Board)

Sets and enforces auditing, attestation, QC, and ethics standards, investigates claims, disciplinary action.

SEC oversees PCAOB and enforces SOX

Requires CEO/CFO certifications (personally liable for financial reporting with up to $20 million dollar in fines/Jail)

Requires internal control monitoring (includes IT security)

Requires records management

Requires whistleblower protection Sec 806

IT Applications and Security

Title IV of the SOX Act, Enhanced Financial Disclosures Section 401- 409, specifically section 404, internal control management.

Internal Control: SOX

SOX: Business or IT Issue?

Financial and related documents are generated from:

- The corporate finance system
- Governance system
- Knowledge management system

CIO and IT department design and operate systems to accomplish the above

SOX is an IT issue, but can be both!

IT Issue for SOX

Data Storage – data warehousing, ERP, CRM, E-mail, record retention/integrity/privacy, data encryption

Transaction systems – Access controls, SOD, password management, DR/BC

Security – penetration testing IPS/IDS, firewalls, I & A, access controls, audit control systems, NAC, security policies, enforcement.

ISO 27002

ISO is a widely accepted set of guidelines and controls for information security.

Controls based on essential legislative requirements or common best practice for information security.

Essential Controls Include:

- Data protection and privacy of personal information.
- Safeguarding company information.
- Intellectual property rights.

- ANSI=USA
- BSI=UK

ISO 27002: Control Components

Background on PCI

In 1999, VISA International developed the Cardholder Information Security Program (CISP), became mandatory June 2001.

Mastercard - Site Data Protection Program (SDP).

American Express - Data Security operating Policy (DSOP).

Discover - Discover Information Security Compliance (DISC).

In December 2004, a new standard but based on CISP, offers unified approach and is adopted by all credit card companies to protect credit card holder data. PCI Security Standard Council (PCI SSC) owns, develops, maintains PCI Standard.

PCI is also standard required outside US for Visa Account Information Security (AIS).

All merchants, service providers that store, process, or transmit credit card data must comply with PCI.

Credit card associations and non government agencies are enforcing PCI compliance via penalties and fines.

Dirty Dozen

Requirement 1	• Install and maintain a firewall configuration to protect cardholder data.
Requirement 2	• Do not use vendor supplied defaults for system passwords and other security parameter.
Requirement 3	• Protect stored cardholder data.
Requirement 4	• Encrypt transmission of cardholder data across open, public networks. • WEP cannot be used.
Requirement 5	• Use and regularly update anti-virus software or programs.
Requirement 6	• Develop and maintain secure systems and applications.

Dirty Dozen

Requirement 7	• Restrict access to data by business need-to-know.
Requirement 8	• Assign a unique ID to each person with computer access.
Requirement 9	• Restrict physical access to cardholder data
Requirement 10	• Track and monitor all access to network resources and cardholder data.
Requirement 11	• Regularly test security systems and processes. Requirement 11.3 is clarified to explicitly mandate internal AND external penetration testing of networks AND applications.
Requirement 12	• Maintain a policy that addresses information security for employees and contractors.

Change Control and Auditing

PCI "Dirty Dozen" focuses on change control and auditing in several requirements. Examples:

- Requirement 1 – install and maintain firewall configuration to protect data.
  - 1.1.1 – establish firewall configuration standards that include formal process for approving and testing all external network connections and changes to the firewall configurations.
- Requirement 6 – develop and maintain secure systems and applications.
  - 6.4 – follow change control procedures for all system and software configuration changes.

An audit self-assessment questioner is recommended:

- **www.pcisecuritystandards.org/saq/index.shtml**

Total Cost of Compliance

Includes:

- Costs related to process, technology, and people are understood.
- Each gap, risk control, area and internal control systems area are analyzed in detail.

For each Initiative or ongoing process:

- Requirements for resources
- Time frame
- Deliverables
- Budget
- Control measures

"With respect to PCI compliance, in many cases it cost about 40% more than they estimated," Brink said.

- **“PCI compliance costs often underestimated, study finds” 2007**

Total Cost of Compliance

Complying with government regulations consumes $1.4 Trillion

- **$1,028 billion federal mandates, $343 billion state & local government mandates**
- **14.9% of the economy - $4,680 per man, woman and child**
- **http://mwhodges.home.att.net/regulation.htm**

The data reveals that for non-accelerated filers, the total average first-year cost for management assessment and additional audit fees is $78,474, which is 13.8% less than the $91,000 cost the SEC initially predicted.

- **http://www.reuters.com/article/pressRelease/idUS166700+09-Jan-2008+BW20080109**

The study found that in many cases, companies are consistently underestimating the costs associated with compliance, said Derek E. Brink, vice president and research director at Aberdeen. Even the best-in-class organizations are underestimating the costs, he said.

What does this mean to the tech?

1. Some regulations such as PCI require Pen testing as part of the normal requirements.
2. The others require the C-Level management to be liable for areas of negligence when looking at security.
3. You, as the tech, at worst could loose your job for negligence but the CEO, CIO and such could personally have to pay for breaches or spend time in jail.
4. If the organization is performing Pen tests on a regular basis you are no longer negligent.

Review