IT Security and Risk Management

How Information Security Manages Risk

Manny Morales CISSP, CISM, CISA, CSM
Office of the New York State Comptroller

NYSICA June 28, 2012

Topics

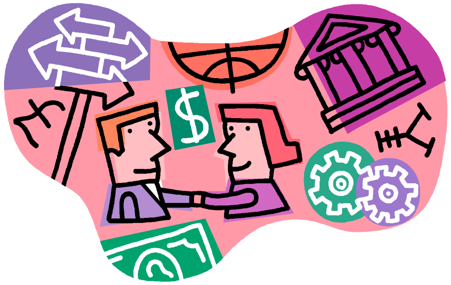
- Information Security Framework
- Risk Management and Assessments
- IT Risk Management Governance
- Secure System Development Lifecycle
- Summary

Information Security Framework

- Policies and Standards
- Security Awareness
- Data Classification
- Data and Network Access Controls
- Privileged Users
- Risk Assessments
- Penetration and Vulnerability Testing
- Business Continuity

General Security Principles

- Confidentiality – Ensuring data is only accessed on a need to know
- Integrity – Ensuring that only authorized changes are made to data and systems
- Availability – Ensuring that data and systems are available when needed



Execution of These Principles

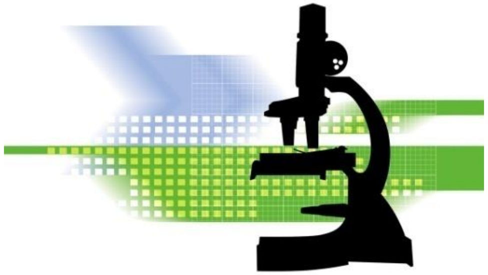
- People – Provide awareness on the Do’s and Don’ts
- Process – Provide the standards and controls for direction
- Technology – An enabler, tools/systems used in compliance to the standards

Security as Business

- ROI
- Establishing a Budget
- Not just IT centric
- Establish security model and supporting frameworks
- Meet business demands
- Identify and Manage Risk
- Marketing and selling

IT Risk Management

- It is a systemic process that is used to identify
  - The threats to a given environment
  - The impact of those threats
  - The likelihood of those threats
  - The mitigation of the threats



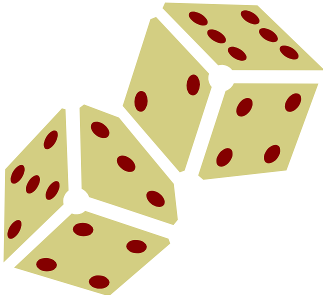
- It is a process for letting management know if an entity is a risk and what is being done about that risk

Common Pitfalls in IT Risk Management

- Inability to manage risk to acceptable levels
- Striking the right balance between risk, cost & effort
- Main challenges relate to governance and the anxiety/resistance to change
- Must demonstrate the value

IT Risks

- It is about understanding what the threats are to your data, organization, business processes, and your infrastructure
- Asking yourself ‘Can it happen’?
- If it can, what should I do?
  - Should I prevent it
  - Should I take the chance it won’t happen
  - Do I wait until it happens, then take action



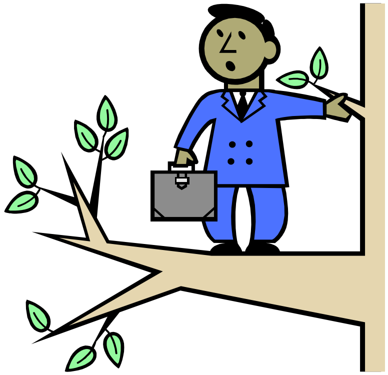
How does it relate to IT Security

- Information risks come in various forms
  - Unintentional – errors, complacency, vulnerabilities
  - Intentional – crime, misuse, Malware

- Use the CIA model as your risk indicator
  - **Confidentiality** – Unauthorized access to data
  - **Integrity** – Unapproved changes
  - **Availability** – No backups

IT Security Risks

- Business Continuity
- Infrastructure Upgrades
- Identity & Access Management
- Physical Access
- Data Classification
- Change Management
- Application Development



If Information risks are ignored, what can happen

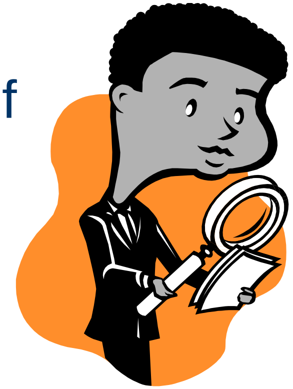
- Loss of reputation – trust factor
- Loss of money – was there financial damage
- Costly – how much did it cost to fix it
- Regulation – did fines have to be paid
- Legal – were laws not followed
- Loss of services – Impact to the business

Why are Risk Assessments so important

- Risk assessments are a formal process of identifying risks with the stakeholders
- It is the best way to get to the heart of the issue(s)
- It provides a process to gather, mitigate, monitor, and report out

Methods of finding your IT Security risks

- Reactive approach
  - Audits
  - Incidents
- Current approach
  - Internal Controls - Timing is not always the best
  - Non-structured assessments – Not always all inclusive
- Proactive approach
  - Structured risk assessment in the beginning phase of any plan to produce or upgrade a product or service



Where do I start

- If you wait, will they come? Not really
- Need to get the message out
- Need to work with the following groups:
  - Project Management
  - Architecture
  - IT Operations
  - Governance Board
  - Security
  - Audit

Performing a Risk Assessment

- Know what the new/upgrade service or product is
- You need to work with the Project Manager and the Sponsor
- Agree on the problem, don’t start on solutions
- Gather the business stakeholders, designers, IT support, and security personnel
- Facilitate a Risk Assessment

Risk Conflicts

- There could be times that one of the issues will not get resolved in the time expected
- Need to try to work it out, you can’t drop an issue
- Can’t resolve, need for an escalation
- Management could accept the risk, if so, it needs to be documented

IT Risk Management Workgroup

- Internal committee established as part of the OSC Governance process
  - Representation from various IT and non-IT departments
- The focus is to identify high level IT Risks
  - At enterprise or major line of business
  - Identify the issue, threat, and likelihood
  - Who or what does it affect
  - Assign owner, identify mitigation effort

IT Risk Management Workgroup

- What are the inputs
  - Audits, Internal and External
  - Internal Control Assessments
  - Security testing results
  - IT Infrastructure issues , (e.g., Outages, Maintenance costs)
  - Service level metrics
  - IT Risk assessments
  - IT Project reports

IT Risk Management Workgroup

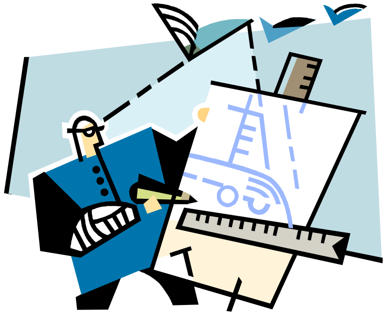
- Chartered in early 2011
- Committee meets every 6 months
- Reviews the inputs
- Comes up with the high level risk(s) that best matches the issue(s).
- Presents to the governance board
- Assess feedback
- Tracks issue

Secure System Development Framework

- Why was this needed
  - More applications/systems are Internet based
  - Most of your breaches are application based
  - Many times application/systems were developed without security or security was brought in late
  - Security testing was not being performed as part of the development process
  - The cost to fix vulnerabilities can be expensive

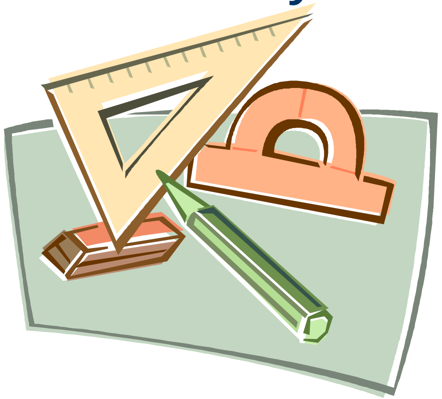
Secure System Development Framework

- How did we get to a Framework
  - Set the goal to make it work within the OSC business model
  - Presented the issue to the governance board
  - Created a project team
  - Used industry and federal government best practices
  - Used models from the private sector
  - Used internal processes to identify gaps



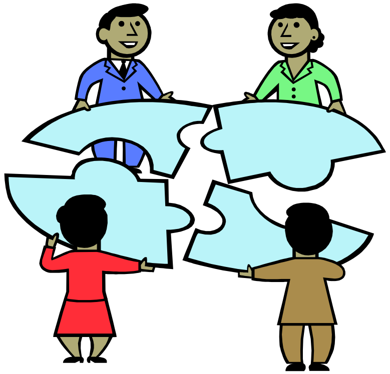
Secure System Development Framework

- What did we produce
  - New standards for development and testing
  - High level framework identified the security tasks that need to be completed
  - Templates, guidance documentation produced
  - Required risk assessments to be done in the early stages
  - Accreditation and certification process established



Secure System Development Framework

- How did we make it work
  - Made it part of the Project Management process
  - Present to senior management for acceptance
  - Made presentations to multiple groups
  - Pilot some projects
  - Streamline the process
  - Constant diligence



Compliance with IT controls

- Have regular security testing done
- Follow-up on risks
- Network with peers
- Work with Audit and Internal Controls
- Perform compliance reviews
- Keep management informed

Summary

- Planning, execution, and follow-up are the three ingredients to success
- Get the business involved, IT is a sub-set
- Objective is to manage IT risk to an acceptable level, there is no such thing as zero risk
- Report on progress through the proper management channels

Final Thoughts

Thanks

- If you would like to reach me, contact: mmorales@osc.state.ny.us