The Approach to Risk & Security Metrics

Predrag Zivic
PEZ@scienton.com

Agenda

Positioning Numerous Standards
Discussing Pros & Cons of Developed Standards
Defining the Baseline for Risk & Security Metrics
Describing the Visual Model
Case Studies

Standards & Mgmt position

Corporate Governance Guidelines (SarbOx, PIPEDA, GLBA)
Management System
Business Process MS. (Why?)
- ISO17799/BS7799
- COBIT
- ISO21827
Maturity Msmt. (What?)
- SSE-CMM (ISO21827)
- NSA Infosec Assess
IT Governance Frameworks – (HOW?)
- CobiT
- GMITS (ISO13335)
- ISO7498-2
- ITIL
- ISO27493-2

Technology Standards – (Application & Automation Tasks)
- CC (ISO15408)
- IT Security
- NSA Guides
Standards & Mgmt position

Corporate Governance Guidelines (SarbOx, PIPEDA, GLBA)

Management System

Business Process MS (Why?)

Maturity Metric (What?)

Technology Standards – (Configuration & Parameters)

CC (ISS14001)

CI Security

NSA Guides

Technology Configuration Metrics

- Metrics & benchmark based on technology configuration
  - www.cisecurity.org
  - www.nsa.gov – SNAC center
  - Others (FIPS, OECD)
- Exact configuration parameters for
  - Routers, switches
  - Windows Systems (NT, 2000, XP)
  - UNIX Systems (Solaris, HP, Linux)

Technology Configuration Metrics (cont’d)

- Pros
  - Excellent technical security details
  - Very specific commands – (IOS, UNIX, NT/2000)
  - Good security configuration education material

- Cons
  - OS version dependent
  - Labor intensive – very little automation
  - Frequent administration staff configuration errors
  - No basis for risk analysis
Technology Configuration Metrics (cont’d)

- **Metrics Pros**
  - Configurations that can be used for audit
  - Can be used to compare configuration baselines

- **Cons**
  - Moving target – OS change requires revisions
  - Difficult to set the metrics baseline – technology dependent
  - Do we really need such strong configuration everywhere? Cost? ROI?

Standards & Mgmt position

- Corporate Governance Guidelines (SarbOx, PIPEDA, GLBA)
- Business Process MS: (Why?)
- Maturity Msrmt. (What?)
- IT Governance Frameworks – (HOW?)
- IT Governance Metrics
  - Metrics based on the IT process controls
  - Guidelines for the Management of IT Security (Part 1-5)
  - IT Infrastructure Lib./ITSM http://www.sage.gov.uk/index.asp?id=2261
  - Control Objectives for Information Technology - http://www.coBIT.org
  - IT process based with IT controls implementation
  - Provide the list of controls and the process for development of controls
  - Define the IT risk analysis processes
IT Governance Metrics (cont’d)

- **Pros**
  - IT process based – Very good lists of process & technology controls
  - Describe the process for risk analysis
  - Very good guidelines to assist security management implementation

- **Cons**
  - Only describe controls applied to IT processes
  - Controls predefined and mixed with technology automation
  - Risk analysis process described at the high level
  - Relation between controls and risk analysis not defined

IT Governance Metrics

- **Metrics pros**
  - Good for the audit process definition
  - Complements technology standards to add to the metrics

- **Metrics Cons**
  - Baseline not clearly defined – goals, technology and process mixed
  - Controls are changing as IT technology and processes change
  - Mixture of controls, processes, and technology does not provide for defined metrics structure
  - Subjective and ad hoc approach to risk & control selection

Standards & Mgmt position

<table>
<thead>
<tr>
<th>Corporate Governance Guidelines (Sarbox, PIPEDA, GLBA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management System</td>
</tr>
<tr>
<td>Business Process MS: (Why?)</td>
</tr>
<tr>
<td>ISO17799/27799/27796</td>
</tr>
<tr>
<td>ISO20000/20010</td>
</tr>
<tr>
<td>ISOxxxxx</td>
</tr>
<tr>
<td>Maturity Msrmt: (What?)</td>
</tr>
<tr>
<td>SSE-CMM (ISO21127)</td>
</tr>
<tr>
<td>NSA/ISAC/Assess</td>
</tr>
<tr>
<td>ISOxxxxx</td>
</tr>
<tr>
<td>CMM (ISO21827)</td>
</tr>
<tr>
<td>ISOxxxxx</td>
</tr>
<tr>
<td>NSA Infosec Assess</td>
</tr>
<tr>
<td>ISOxxxxx</td>
</tr>
<tr>
<td>COSO/COCO</td>
</tr>
<tr>
<td>ISOxxxxx</td>
</tr>
</tbody>
</table>
**Business Process Metrics**

- Business process governance guidelines
  - Committee of Sponsoring Organization (COCO) – Tradeway Commission
  - ISO9000, ISO14000 and ISO17799/BS7799
  - OECD Governance Guidelines
- Business process controls to create management systems
- Defined management systems can be measured
- The goal is controlled business process

**Business Process Control Metrics**

- Business process controls pros
  - Very good framework for business process improvement
  - Good for management to achieve compliance to legislations and acts (SarbOx, Basel II, HIPAA)
  - Streamlines the control implementation process
- Business process controls cons
  - Very high level controls that apply to the business process
  - Disconnected from technology and operations
  - Risk framework is very ad hoc and high level defined for business processes
  - Very document driven and overwhelming

**Business Metrics**

- Business metrics pros
  - Very good for internal auditors
  - Business and executive management awareness
  - Practices to measure the legislation & act compliance
- Business metrics cons
  - Very high level to measure the controls of the business process
  - No measure of technology and operations
  - Very subjective as there is no clear guideline, just protocols descriptions
Business Process Maturity Metrics

Maturity Models
- SSE-CMM (ISO21827)
- NSA Infosec Assessment - CMM
- CobIT®

Five levels
- Level 1 – Ad hoc performed
- Level 2 – Planned & tracked
- Level 3 – Well defined
- Level 4 – Quantitatively controlled
- Level 5 – Continuously improving

Maturity pros
- Good guidelines for the management system cycles
- Very good definition of business process control implementation
- Excellent executive management guideline tool

Maturity cons
- Very broad in definition of steps and levels
- Organizations can broadly audit levels
- Risk management is done but how?
- Subjective interpretation of terminology and maturity requirements

Maturity metrics pros
- Good to get the understanding of management system
- High-level metrics for executive management
- Process to define the security management system implementation improvement

Maturity metrics cons
- Difficult to measure process implementation
- Very subjective metrics as the level is open to interpretation
- The quality of process is not defined (risk management not defined)
- Only management system maturity is measured
Can we measure risk & security?

What we should look at?
What are our basic business goals & attributes?

Common Metrics Baseline

Information Security Model™
Case Study I
How much security do we have?

Security Strategy Derived From Implemented Tools

Security Software Analysis

- To protect network and to control user access – implement firewall – WE HAVE SECURITY!
- After firewall implementation risk is low – is it?
- Can we see what have we accomplished with the firewall implementation?
- CheckPoint Firewall – Requirements
  - Control access to networks
  - Control access for users
  - Can we use other security controls?
Software Security Analysis Result

- Understand what has been implemented
  - Visualize and understand security system gaps
  - Discover the complementary products to fulfill the gaps
  - Ability to plan budget, resources and time
- Security officers can report this to executives – CxO will understand it
- Ability to optimize and streamline security investment
- Simple approach for security professionals to gain the credibility in the organization

Audit Digest
Summarizing the Audit

Security Strategy Derived From Audit

Audit Digest Requirements

- Client – Insurance Company
  - Audit performed – CIO could not understand the information
  - CIO request:
    1) Compliance with industry standard & industry vertical
    2) Comprehensive report with security strategy vs. 500 page audit
- Solution – Scienton Information Security Model™
  - Used existing audit report in combination with ISM™
  - Summarized and calculated compliance
  - CIO surprised: Good document, but poor ranking for the firm
  - Scienton: Developed short and long term security strategies to improve the firm’s risk compliance ranking
Advantages of the proposed approach

- Quantitative (risk & security metrics), constant in its application and therefore defensible
- Provides a managerial tool necessary for non-technical managers to manage information risk and make appropriate real-time decisions
- Can be tailored for progressive implementation (a long-term vision to be reached in incremental steps, through early and repetitive wins)
- Models privacy as one of its components

ISM™ Risk & Security Modeling Advantages

- An initial risk analysis that can easily be updated and maintained:
  - Takes care of the complexity of the technology environment automatically (cost effective process)
  - Continuous Risk Management and Security Management
- Thorough and standardized: looks into all aspects of security (ISO and CoSIT®)
- Adaptive, scalable and tailored to any industry vertical needs
- Seamless, simple, understandable and visual blueprint for security strategy development

Risk & Security Modeling Summary

- Successful business level modeling
  - Clear findings using Scienton Information Security Model™
  - Calculation of compliance to Governance, Policies & Standards
  - Real-time information for security and risk management strategy
- ROI through:
  - Efficient, reliable risk assessment – quick and standardized
  - Streamlined investment through corporately aligned strategy
  - Clear plan with ability to define budget requirements
  - Optimized & planned implementation = Minimum business risk