# IT Security Management and Security Metrics Guide

Prof. Jungduk Kim
Department of Information Systems
Chung-Ang University

- IT Security Management
  - Paradigms & Concepts
  - IT Security Management Processes
- IT Security Metrics Background
  - Definition & benefits using metrics
  - Metrics types & success factors
- Metrics Development & Implementation
  - Metrics development process
  - Establishing performance targets
  - Metrics Program Implementation

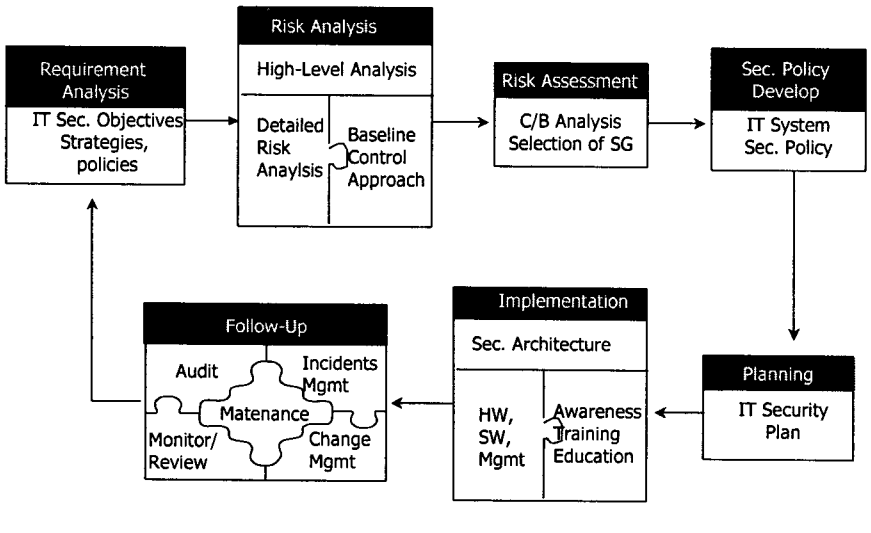
- The 1st wave - Technical
  - Late 50's~ early 80's
    - Technical issues by techies
  - Built in facilities of mainframe OS
    - ACL, User-ids & Passwords
- The 2nd wave - Management
  - Early 80's ~ middle 90's
    - Distr. Computing, Internet, WWW, EC
  - Top Mgmt involvement, ISSO, Organizational structure

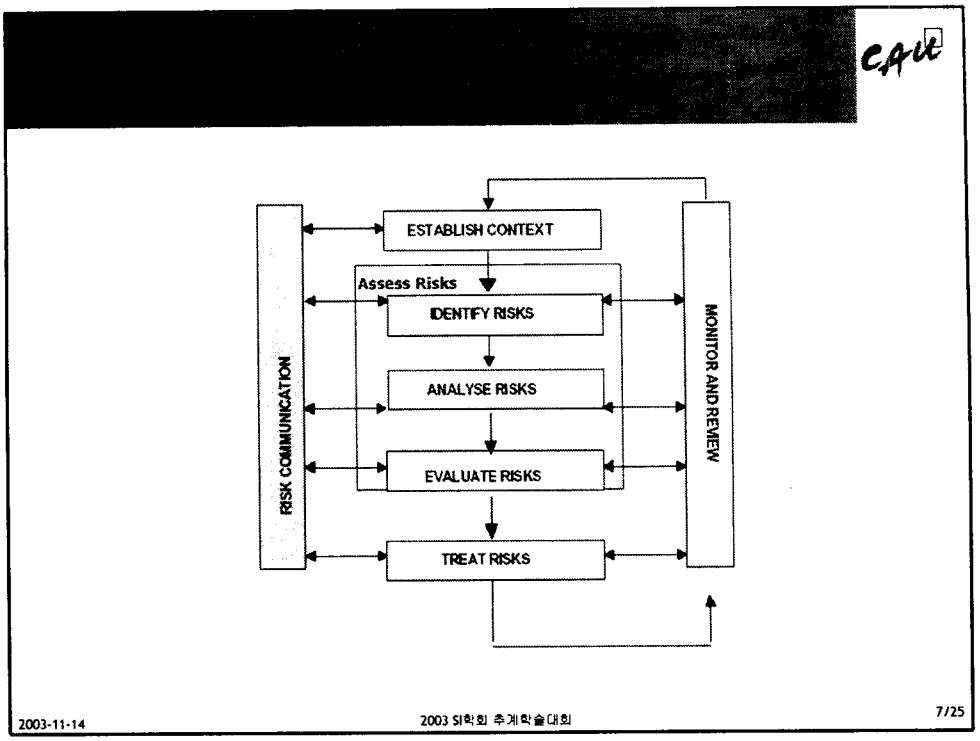


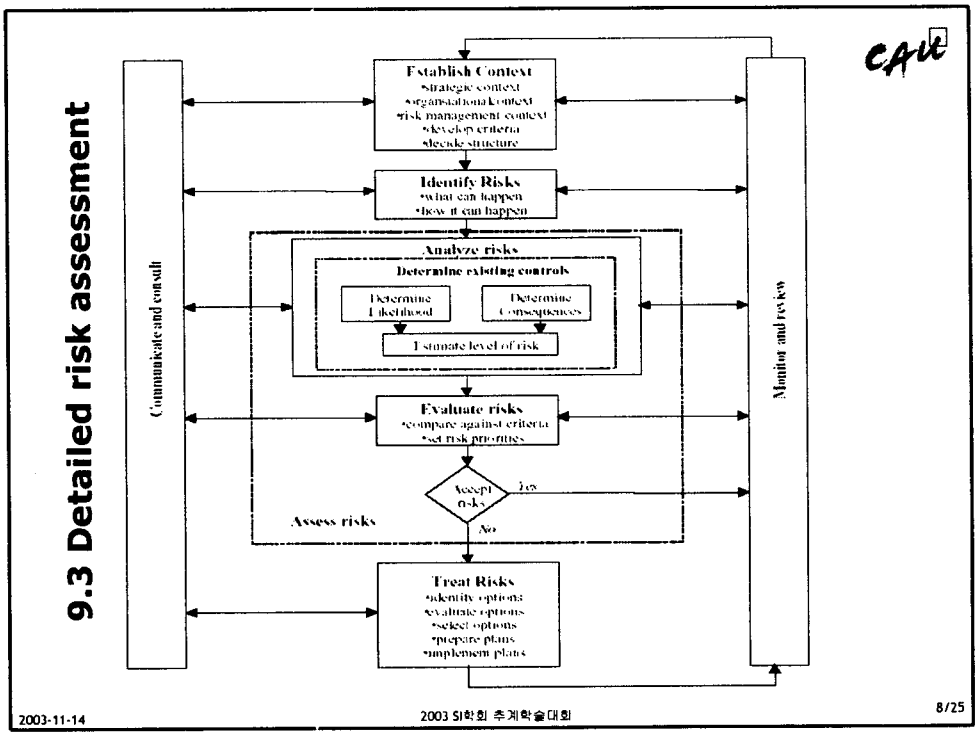
- The 3rd wave - Institutionalization
  - Late 90's ~
    - Corporate wide effort
  - 4 Components
    - Information security standardization
      - "how do I know I am not missing something?"
      - ISO 17799-1(BS 7799-1)
    - International Information Security Certification
      - "how can I prove my infosec preparedness to an EC partner?"
      - BS 7799-2 (240 firms certified, 2003. 8.), ISMS
    - Information Security Culture
      - "My own users may be my biggest enemy?"
      - Human problems, awareness
    - Continuous and dynamic measurement of Infosec
      - "how do I know how well our infosec policies, procedures are complied with?"
      - Mgmt by measurement, metrics

- A comprehensive system of tools and processes used to assure company policy compliance, identify deviations and adjust network computing systems accordingly
- A cycle of pushing controls to the network and collecting risk and threat information from all devices






ESTABLISH CONTEXT
Assess Risks
IDENTIFY RISKS
ANALYSE RISKS
EVALUATE RISKS
TREAT RISKS
RISK COMMUNICATION
MONITOR AND REVIEW
2003-11-14
2003 SI학회 추계학술대회
7/25


9.3 Detailed risk assessment
Establish Context
Identify Risks
Analyze risks
Determine existing controls
Determine Likelihood
Determine Consequences
Estimate level of risk
Evaluate risks
Assess risks
Treat Risks
Communicate and consult
Monitor and review
2003-11-14
2003 SI학회 추계학술대회
8/25

## [illegible]

- How good our information security is?
- How it is compared to other companies?

- Traditionally, infosec is measured on a periodic basis - internal/external audit team
- Infrequent and ad hoc measurement is not acceptable any more - risks are too high
- What is needed is to have a infosec metrics program



## [illegible]

- History
  - IT system-level metrics
  - NIST SP 800-26, Security Self-Assessment Guide for IT Systems
    - 5 mgmt, 9 opec., 3 tech. control topic areas
    - Quantifying critical elements
  - Federal Information Security Management Act (FISMA)
    - Annual report to OMB on implementation and performance level based on annual review
  - IT Security Metrics Workshops (2002. 5)
  - NIST SP 800-55 "Security Metrics Guide for IT Systems" (2003. 7)

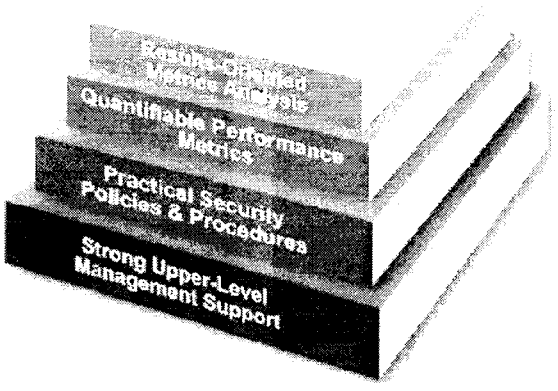
- Tools designed to
  - Facilitate decision making
  - Improve performance & accountability
  - Thru collection, analysis, reporting perf. Data
- IT Security Metrics
  - Must be based on IT security performance goals and objectives
  - Monitor the accomplishment of the goals and objectives by quantifying the level of implementation of the security controls
  - Monitor the effectiveness and efficiency of the controls, analyzing the adequacy of security activities and identifying possible improvement actions



- Things to be considered in development and implementation of IT security metrics program:
  - Metrics must yield quantifiable information (percentages, averages, and numbers)
  - Data supporting metrics needs to be readily obtainable
  - Only repeatable processes should be considered for measurement
  - Metrics must be useful for tracking performance and directing resources

- Improve accountability for security
  - Justify & target investments
    - Can get best value from available resources
- Demonstrate compliance with applicable laws, rules, and regulations
  - Assist for annual FISMA reporting requirement
  - Input into GAO, Inspectors General audits
- Measure the outcomes of security investments and provide quantifiable data that will support allocation of resources for future investments





- Three Types of Metrics
  - Implementation metrics to measure implementation of security policy
  - Effectiveness/efficiency metrics to measure results of security services delivery
  - Impact metrics to measure business or mission impact of security events.

- Which Metrics?
  - depend on the maturity of the security program and the system's security control implementation

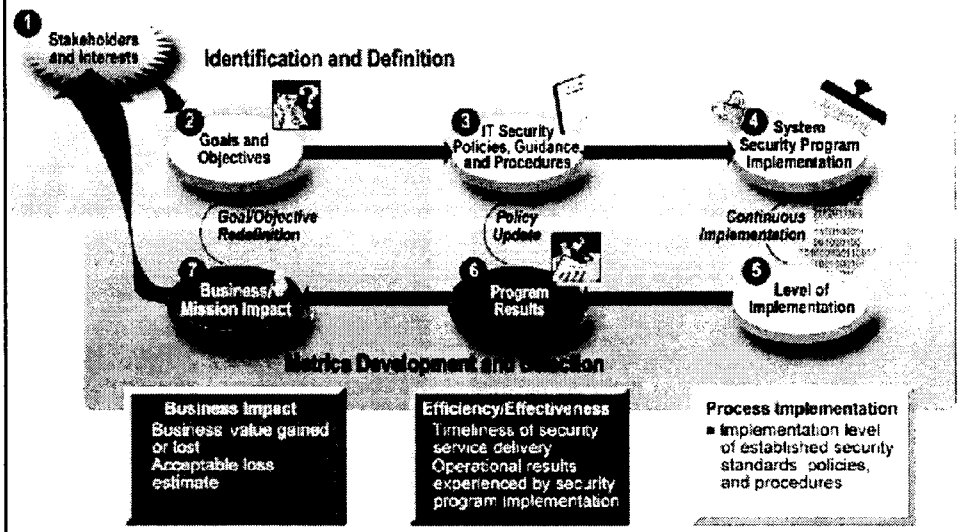


| | Level 1 Policy developed | Level 2 Procedures developed | Level 3 Proc. & ctls implemented | Level 4 Proc. & ctls tested | Level 5 Proc. & ctls integrated |
|---|---|---|---|---|---|
| Metric Types | Goals Defined | Objectives Identified | Implementation | Effectiveness & Efficiency | Impact |
| Collection Automation | None | Low | Medium | High | Full |
| Collection Difficulty | Very high | High | Medium | Medium to Low | Low |
| Data Availability | Non-existent | Some | Can be collected | Available | In Standardized Repository |

## Background & Success Factors

- o Organizational Considerations
  - Participation from system stakeholders and others concerned
- o Manageability
  - 5 - 10 metrics per stakeholder at a single time
  - Change management
- o Data Management Concerns
  - Data gathering and reporting should be standardized for quality and validity of data
  - Non-intrusive as possible and used for correction
  - Establishing security metric program costs money, but maintaining it needs not cost too much



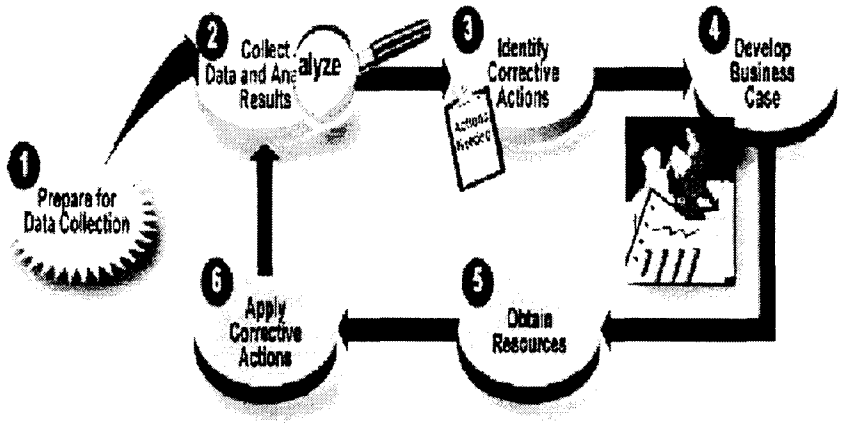


| | |
|---|---|
| **Performance Goal** | State the desired results of implementing one or several system security control objectives/techniques that are measured by the metric. When using NIST SP 800-26, this item will list a critical element, as stated in 800-26. |
| **Performance Objective**[1] | State the actions that are required to accomplish the performance goal. When using NIST SP 800-26, this item will list one or more subordinate questions, as stated in 800-26. Multiple performance objectives can correspond to a single performance goal. |
| **Metric** | Define the metric by describing the quantitative measurement(s) provided by the metric. Use a numeric statement that begins with the words "percentage," "number," "frequency," "average," or other similar terms. |
| **Purpose** | Describe the overall functionality obtained by collecting the metric. Include whether a metric will be used for internal performance measurement or external reporting, what insights are hoped to be gained from the metric, regulatory or legal reasons for collecting a specific metric, if such exist, or other similar items. |
| **Implementation Evidence** | List proof of the security controls' existence that validates implementation. Implementation evidence is used to calculate the metric, as indirect indicators that validate that the activity is performed, and as causation factors that may point to the causes of unsatisfactory results for a specific metric. (Sections 4.1.3, IT Security Policies, Guidance, and Procedures Review; 4.1.4, System Security Program Implementation Reviews; and 4.1.5, Metrics Development and Selection, contain a discussion of what information can be used to identify appropriate implementation evidence for individual metrics. Section 5.2, Collect Data and Analyze Results, contains a discussion and a list of common causation factors.) |
| **Frequency** | Propose time periods for collection of data that is used for measuring changes over time. Suggest time periods based on likely updates occurring in the control implementation. (Section 4.3, Feedback Within Metrics Development Process, contains a discussion on the frequency of metric data collection.) |
| **Formula** | Describe the calculation to be performed that results in a numeric expression of a metric. The information gathered through listing implementation evidence serves as an input into the formula for calculating the metric. |
| **Data Source** | List the location of the data to be used in calculating the metric. Include databases, tracking tools, organizations, or specific roles within organizations that can provide required information. (Section 3.4.3, Data Management Concerns, contains a discussion on metrics data sources.) |
| **Indicators** | *Provide information about the meaning of the metric and its performance trend.* Propose possible causes of trends identified through measurement and point at possible solutions to correct the observed shortcomings. State the performance target, if it has been set for the metric and indicate what trends would be considered positive in relation to the performance target. (Section 4.2, Establishing Performance Targets, contains a discussion about the relationship of performance targets and the indicators.) Describe how the information gathered through listing implementation evidence is to be used as input into the analysis of indicators. The implementation evidence serves for validating performance of security activities and pinpointing causation factors. |



CAIT

- Indicator line of the metric form
- Establish a goal by which success is measured
- Setting performance targets differ for types of metrics
  - Implementation metrics - relatively easy
  - Efficiency, Effectiveness, impact metrics - complex
    - Target first, actual measurement, then adjust target
    - Measurement first, use it as a baseline, then set appropriate targets
    - Historic data helps
    - Expert recommendations and standards within the industry






| Critical Element | Metric | OMB Guidance Reference |
|---|---|---|
| 1.1 | Percentage of systems that had formal risk assessments performed and documented | LC.1.c |
| 2.1 | Percentage of total systems for which security controls have been tested and evaluated in the past year | LC.1.g |
| 3.1 | Percentage of total systems that have the costs of their security controls integrated into the life cycle of the system | LC.1.f |
| 4.1 | Percentage of total systems that have been authorized for processing following certification and accreditation | LC.1.e |
| 5.2 | Percentage of current security plans | LC.1.d |
| 9.2 | Percentage of systems that have a contingency plan | LC.1.h |
| 9.3 | Percentage of systems for which contingency plans have been tested in the past year | LC.1.i |
| 13.1 | Percentage of employees with significant security responsibilities who have received specialized training | LC.3.c (denominator) and LC.3.d (numerator) |
| 14.1 | Percentage of agency components with incident handling and response capability | LB.8.c (numerator) |
| 14.2 | Number of incidents reported externally to FedCIRC or law enforcement | LB.9.c |

| | |
|---|---|
| **Critical Element** | 1.1 Is risk periodically assessed? |
| **Subordinate Question** | 1.1.2 *Are risk assessments performed and documented on a regular basis or whenever the system, facilities or other conditions change?* |
| **Metric** | Percentage of systems that had formal risk assessments performed and documented |
| **Purpose** | *To quantify the number of risk assessments completed in relation to the organization's requirements.* |
| **Implementation Evidence** | 1. Does your agency maintain a current inventory of IT systems?<br>? Yes ? No<br>2. If yes, how many systems are there in your agency (or agency component, as applicable)? _____<br>3. *Of the systems in your current inventory, how many systems have had risk assessments performed and documented in the following time frames?* (Select the nearest time frame for each system; do not count the same system in more than one time frame.)<br>*Within past 12 months*_____ *Within past 2 years*_____ *Within past 3 years*_____<br>4. For any system that underwent a risk assessment, list the number of systems after the reason(s) that apply:<br>Scheduled risk assessment_____ Major change in system environment_____<br>Major change in facilities_____ Change in other conditions (specify) _____<br>5. For any system that has not undergone a risk assessment in the past 3 years, list the number of systems *after the reason(s) that apply:*<br>No policy _____ No resources_____ System tier level does not require _____<br>System previously not defined_____ New system _____<br>Other (specify) _____ |
| **Frequency** | Semiannually; annually |
| **Formula** | At agency level: Sum of risk assessments on file for each time frame (Question 3) / IT systems in inventory (inventory database) (Question 2)[5] |



| | |
|---|---|
| **Data Source** | Inventory of IT systems that includes all major applications and general support systems; risk assessment repository |
| **Indicators** | This metric computes the percentage of systems that have undergone risk assessments over the last three years (which is normally the required maximum time interval for conducting risk assessments). To establish the distribution of time for risk assessment completion, the number of systems listed for each time frame is computed. The total within three years should equal 100 percent of all required systems. Systems that are not receiving regular risk assessments are likely to be exposed to threats. Question 4 is used to validate the reasons for conducting risk assessments and to ensure that all systems are accounted. Question 5 is included to determine the reason risk assessments were not performed. Defining the cause will direct management attention to the appropriate corrective actions. By documenting and tracking these factors, changes can be made to improve performance by updating the security policy, directing resources, or ensuring that new systems are assessed for risk as required. |

CAVE


김정덕, 중앙대학교