Business value of the operational system security evaluation for the integrator and service provider

Hiroyuki Kaneko
Center for Evaluation of Information Security,
Mizuho Information & Research Institute, Inc.

Background

- Strengthening of corporate governance and improvement of internal management
  - Personal information protection law
    (From a perspective of customer information protection)
  - Unfair Competition Prevention Law
    (From a perspective of intellectual property and confidential information protection)
  - Sarbanes-Oxley (SOX) Act in the U.S.
    (Repercussions to the revision of the Securities Exchange Law in Japan and such)

- Effects on Enterprise Management
  - Compliance
  - Corporate Social Responsibility
  - Value of information assets (assurance of confidentiality, integrity, and interoperability)

  - Greater responsibility of management leadership
  - More detailed and expansive corporate information disclosure

Requirements for Information System

- Customer information
  - Personal information data, possession of private data
- Corporate information
  - Data on management, business, and human resources
  - Data on intellectual property and proprietary technology
- Financial information
  - Accounting data

Pursuit of accuracy, completeness, efficiency, and convenience
Basic security is essential
Issues lies in maintaining a balance.

Providing stable and secure system services

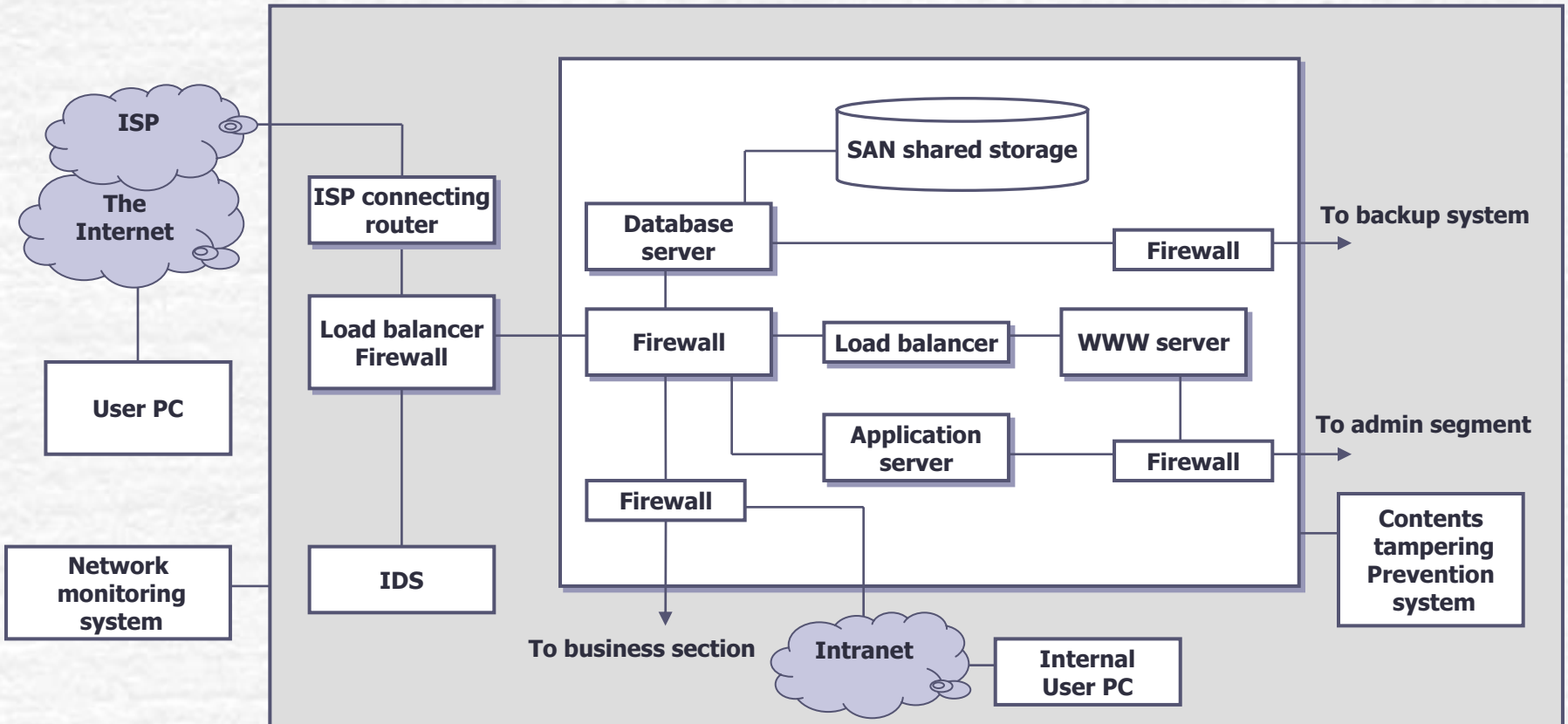
Accountability by top management

Risks vs. Costs
Establish an internal management system.
Major IT flaws often affect management directly.

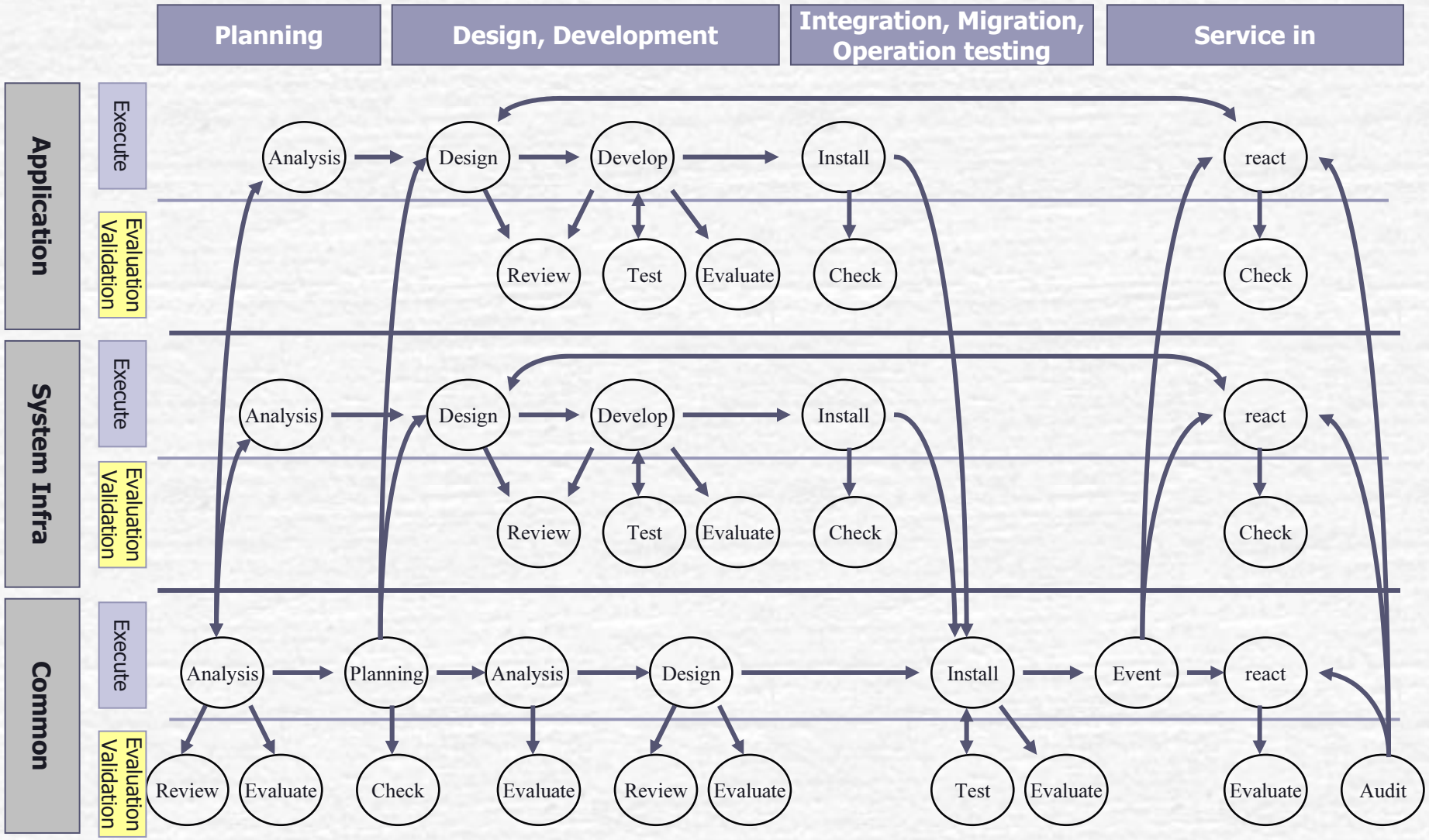
Problem with information systems strike at the core of the company.

Managers must recognize the importance of information systems.

Typical configurations of open system



System life-cycle, development and operation tasks



System risks

System risks	Safety	Business suspension by system down
		Business obstruction by attacks such as hackers
		Leakage of customer information by internal crimes
	Reliability	Business problems by incomplete processing due to system bugs or troubles Mistakes of risk judgment
	Effectiveness, Efficiency	System cannot comply with company's basic principles and strategy
		Unproductive, inefficient system increases costs
	Compliance	Violations of laws
Risks by opening system	Common	System trouble
		Action by internal crime
	Increasing	Theft, seizure, tampering
		Spoofing
	Characteristic	Illegal intrusion
		Business obstruction

Refer to the public material by the Bank of Japan.

Features of an open system

- Pursuit in:
  - Performance
  - Total cost reduction
  - Scalability
- Result in:
  - Complex system configurations
  - Black Box created by existing services and outsourcing
  - Higher system risks
  - Risks always changes
  - System controls and procedures must be made more efficient

Can CC be applied?

- CC can be applied to system security evaluation
  - Security scope via risk analysis
  - Verify security scope by security target
  - Balanced measures between controls and functions
  - System security assurance as a whole
  - Continuous evaluation of system security based on risk management
  - Essential strengthening of security review
  - The ability to adapt to security adds value

Problems of system security

- Lessons learnt from system security problems
  - Security features disabled by application bugs or design errors
  - Security flaws exposed when pushing the system to the limits of its capabilities
  - Data that is meant to be invisible can in fact be accessed
  - No traces remain of blatant violations of system use (such as internal crime)

- Key causes?
  - Insufficient risk analysis
  - Inconsistency of security analysis between each phase
    plan -> design -> develop -> installation -> operation
  - Vague verification of security countermeasures
  - The design or implementation review does not detect system bugs (IT or operation environment)

Problems with analyzing system risk

- Risks always changes
- Due to vulnerabilities of systems or products, changes of operating environments, law revisions, etc.
- RFP concerning security is sometimes vague
- Scope of system security is indefinite and indistinct

- The integrator or system provider often assumes the risks and proposes countermeasures
- The system owner leaves the integrator or provider (guarantees it based on SLA evaluation)
- In reality, countermeasures can be implemented within the budget

Importance of analyzing system risk

- The system owner (entrepreneur = outsourcer) is responsible for continuous risk analysis:
  - User risks vs. Operating risks
- Securely identify actual risks:
  - Repeat the cycle of hypothesis, verification, and review
- Examine measures against risks:
  - Tailored to system operation cycle
  - Robust in the face of changes in risk
- System security evaluation based on risk analysis

Desired approach

- Guideline on continuous security measures for systems
  - System owner (outsourcer), integrator, and system provider cooperate
- CC evaluation methodology
  - Input the risk analysis results into the CC security evaluation
  - Define security scope of the target system in terms of vulnerabilities, threats, and risks, and {objectives = strategy direction}
  - Define scope of security considered acceptable
  - Security target which comprises security model (physical and logical architecture), security scope, and security function set for the target system
  - Evaluate security assurance of the target system using CC evaluation methodology
- Continuous evaluation of system security
  - Clarify the risk via PDCA cycle with continuous gap analysis
  - Don't fix existing implementation easily, don't undervalue the risks
  - It is important to freeze the evaluated security scope of that time
  - Reevaluate affected target range based on the revised security target

Effects of CC application on security issues or accidents

- Cyber attack against Website
  - A DoS attack involves infecting many computers with a virus targeting websites such as government agencies on two or more specific days, causing the website server to crash.
- Data leakage by operations
  - A criminal contacted as a subcontractor engineer for an Internet provider and learned how to access the network and database, and stole data on about 4.5 million individuals.
- Operating data leakage affair
  - A Trojan horse computer virus at a data processing company infiltrated the server and continued sending card data for 1 in every 200 cards out to external servers for a period of almost ten months.

DoS attack on Website

- Issues
  - Outside access
- ST write and evaluate
  -> Identify DoS threat and define appropriate objectives
- Security function requirements
  - Security audit analysis
  - Limitation of multiple simultaneous sessions
  - Fail secure
- Security functions
  - DoS protection mechanism based on signature
    Define packet feature when attacking as data pattern
    Filtering attacking packets
  - DoS protection mechanism based on threshold
    Filtering access packets that exceed unit time threshold

Data leakage by operations

- Issues
  - Access by maintenance personage
- ST write and evaluate
  -> Identify threat by person-in-charge of maintenance and define appropriate objectives
- Security function requirements
  - Access control
  - Encryption
  - Improvement of security environment
- Security functions
  - Encryption of customer information
    Improve confidentiality when data taken out
  - Limit area accessible by maintenance person
    Thorough separation of authority
  - High-security zone

Operating data leakage affair

- Issues
  - Violation of data maintenance rule
  - Careless security management
- ST write and evaluate
  -> Identify threat concerning maintenance and define appropriate objectives
- Security function requirements
  - Encryption
  - Security observation (data and network)
  - Network connection limitation
- Security functions
  - Encryption of data at processing stage
  - Mechanism for monitoring data (program) integrity
  - Network observation
  - High-security zone

Value of reviews by a third party

- System evaluation by a third party
  - Self review may overlook incompleteness of risk analysis and security target
- Advantages:
  - Standardization of evaluation output
  - Independent and fair verification result by security specialist
- How to use the advantages:
  - Total advantage is obtained by understanding the risk beforehand, and reflecting it in the business plan
  - Difficult to identify advantages in a fix-it-after-the-event corporate culture
  - The necessity of each individual measure is assessed logically through prior analysis and checked against the evaluation frame
  - Long-term cost advantage by improving internal management
- Benefits of using third-party evaluation in business strategy
  - Awareness of the verification logo is fairly low among consumers; it is necessary to evaluate each one on a case-by-case basis

Value for integrator, system provider

- Essential strengthening of security review
  - Incomplete security is prevented beforehand
  - The evaluator desperately looks for incomplete security
- The ability to adapt to security adds value
  - System owner's business strategy
  - Cost balance
  - Reliability
  - Construction of a secure development system
  - Quality of security is greatly improved

Method of applying CC (1)

◈ As RFP:

Phase	Requirements	Investment for acceptance
Planned design	Security scope definition documentation	The review report (arbitrary form) by the evaluation organization is submitted
Specification design	Security requirement specification (as PP) for the system or products	The evaluation report is submitted within a certain period after delivery
Implementation, installation	Adoption of product that has been validated or is in evaluation with CCRA or JISEC	Evidence is submitted as proof of validated product
	System security target	The evaluation report is submitted after installation is completed
	JISEC IT security evaluation of the target system	The certification report is submitted within a certain period after service starts (Based on ST: assurance level is specified by system owner)
Operation commissioning	Execution of security influence analysis	Periodic report of security situation. Additionally, the security influence analysis report is submitted each half year or when the function is changed

JISEC: Japan Information Technology Security Evaluation and Certification Scheme
CCRA: Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security

Method of applying CC (2)

◈ As assurance by integrator or system provider:

Sample for system assurance configuration

Assurance of the entire system

Security Target

- Architecture design
- Function interface specification
- System operation test evidence
- Vulnerability analysis, penetration test result
- System life-cycle controls
- System configuration controls
- System operation manuals
- SLA (service level agreement)

Assurance of applications

- Application development specification
- Application development test evidence
- Development site security
- Development material controls
- Flaw remediation controls

Assurance of Client side

- Agreement with user
- Users manuals

Assurance of system infrastructure

- System infrastructure installation and setting
- Infrastructure maintenance controls
- Infrastructure operational manuals

Shortening the evaluation period and reducing the cost

- Secure development process is improved:
  - Risk analysis and PDCA cycle
  - Security concept designed clearly
  - Close liaison between development and security processes
  - Effective system of reviewing
  - Efficient operation of test environment
  - Concise document that includes necessary information
- Shared understanding of security level
  - Whole of system life-cycle
  - Intention sharing and communication between stake-holders
- Use of validated products
  - Product selection is improved

Concerns of applying CC to system

- CC is incomprehensible for the system integrator
- When CC is applied to the system, is an appropriate IT security evaluation possible?
- Some CC part2 function requirement must drop the abstraction level if there is a concrete security function requirement for the system
- CC part3 assurance requirement can be used as a general approach, but may not be suitable as an evaluation technique

Conclusions

- A framework for continuous analysis and evaluation is a necessary system security measure
- Continuous checking of system security (dynamic security status in relation to ongoing operation, rather than static security status) through risk analysis (gap analysis in continuous evaluation)
- Consistent systematic evaluation and verification can be done throughout the system life cycle by applying CC as a common framework and evaluation method
- CC standardizes the system evaluation result, and is an independent and fair evaluation by a third party
- Current system security countermeasures have been done after the fact. CC brings the benefits of logical and practical evaluation
- It is necessary to refine standard use and evaluation techniques, and accumulate the verification results of the CC system evaluation
- CC can be applied to system security evaluation