2009/02/20

Information Security Governance and Benchmarking

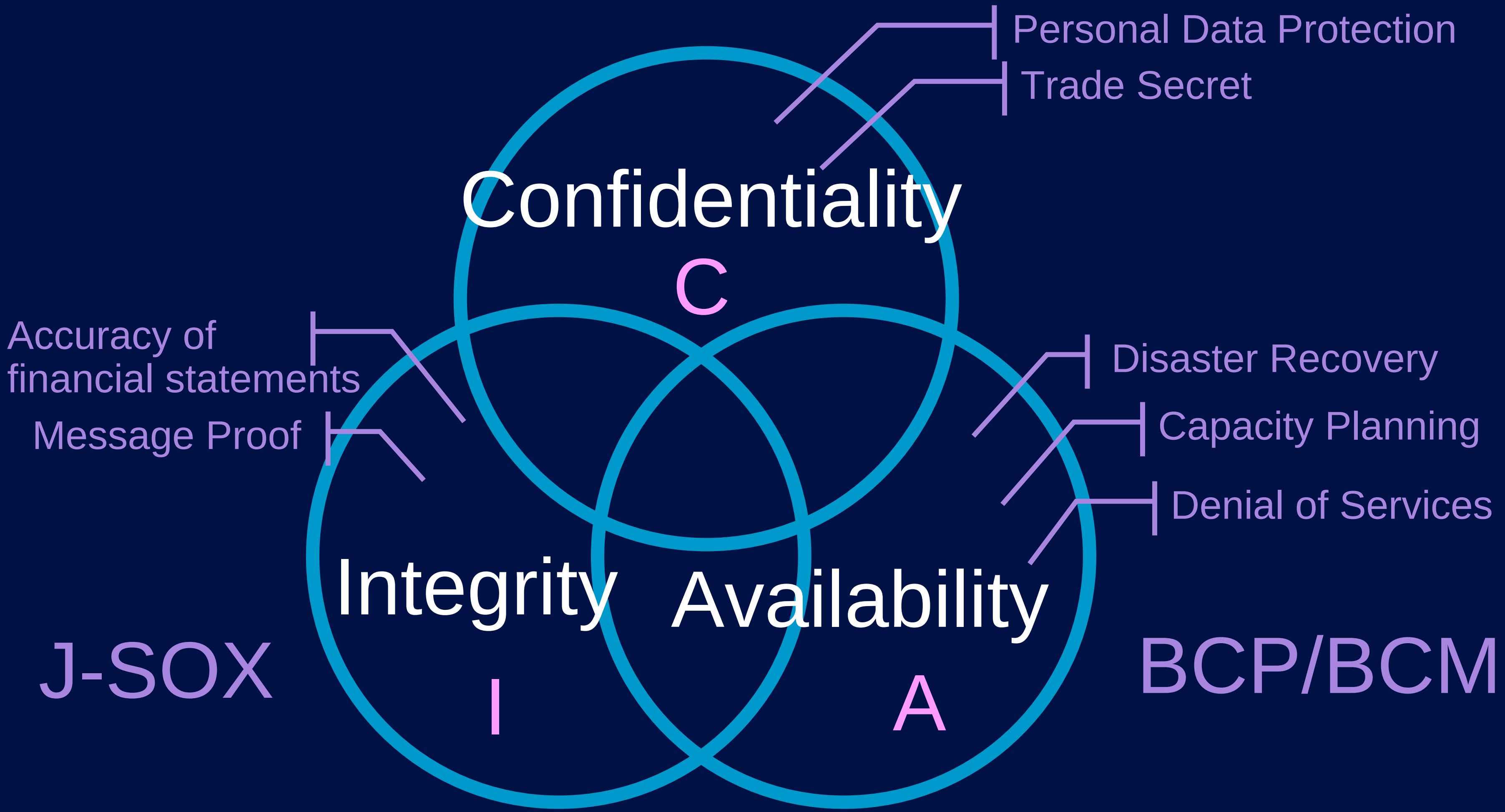
Eijiroh Ohki
Professor, Kogakuin University
eohki@cc.kogakuin.ac.jp

Agenda

Information Security Governance and Benchmarking

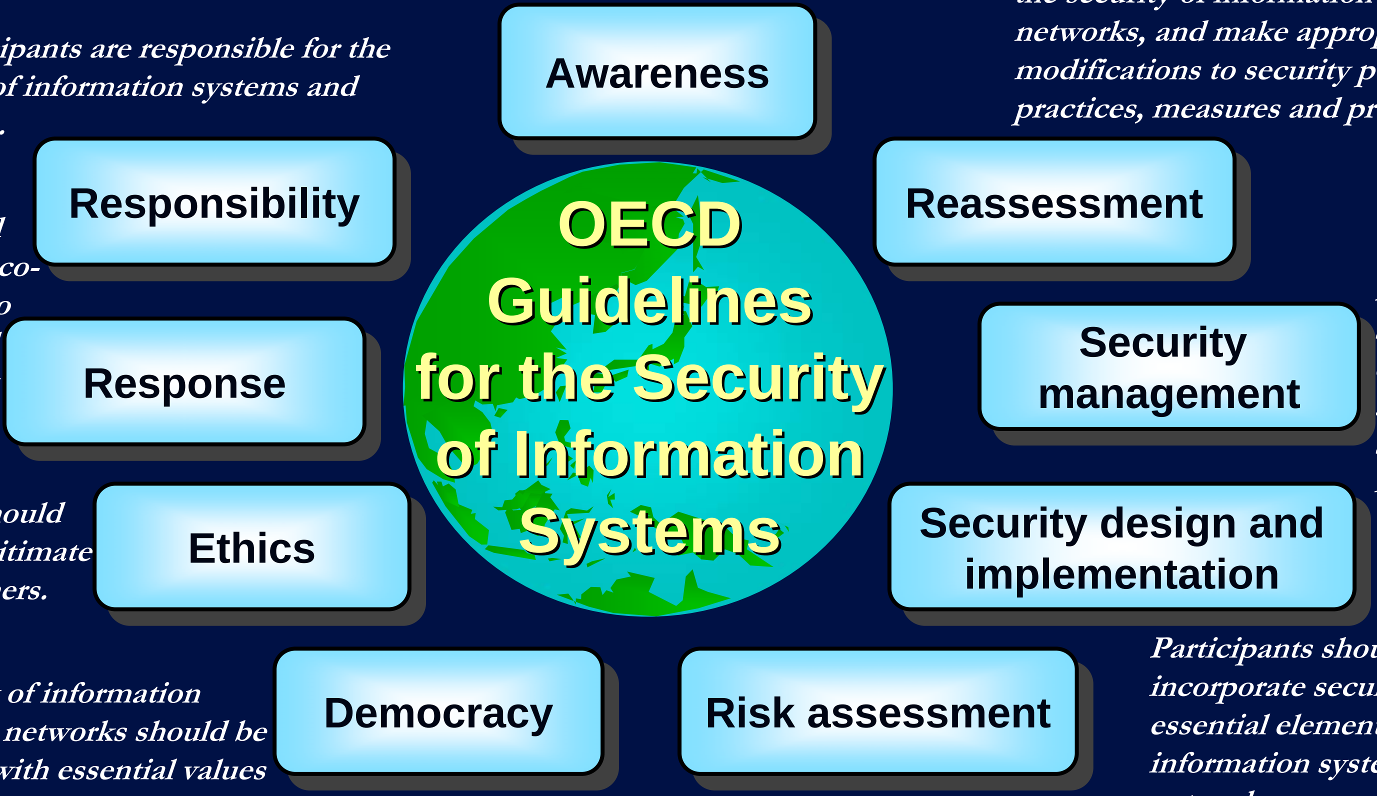
1. Managing Information Security
   - Business and Information Security
   - Security Controls and Management
2. Information Security Governance
   - What is I.S. Governance
   - How to establish I.S. Governance
   - Risk Factors and Risk Treatment
   - Governance Structure
3. Information Security Measures Benchmarking
   - Major issues and three tools
   - What is, How it works, How to utilize

Business and Information Security



OECD Security Guidelines *1992, 2002*

"Culture of Security"



OECD Guidelines for the Security of Information Systems

Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

Responsibility

All participants are responsible for the security of information systems and networks.

Response

Participants should act in a timely and co-operative manner to prevent, detect and respond to security incidents.

Ethics

Participants should respect the legitimate interests of others.

Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

Risk assessment

Participants should conduct risk assessments.

Security design and implementation

Participants should incorporate security as an essential element of information systems and networks.

Security management

Participants should adopt a comprehensive approach to security management.

Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

ISO/IEC 27001

Information Security Management Cycle

Establish ISMS

1. Define scope of ISMS
2. ISMS Policy
3. **Risk assessment approach**
4. **Identify Risks**
5. **Assess Risks**
6. **Options for treatment of Risks**
7. Select controls
8. Management approval
9. Statement of Applicability

Plan

Implement & Operate

1. **Formulate Risk treatment plan**
2. **Implement Risk treatment plan**
3. Implement controls
4. Training and awareness programs
5. Manage Operations
6. Manage resources
7. Incident response

Do

Monitor and review

1. Monitoring
2. Regular reviews
3. Measure Controls' effectiveness
4. **Review Risks**
5. ISMS audit
6. Regular Management review
7. Record events

Check

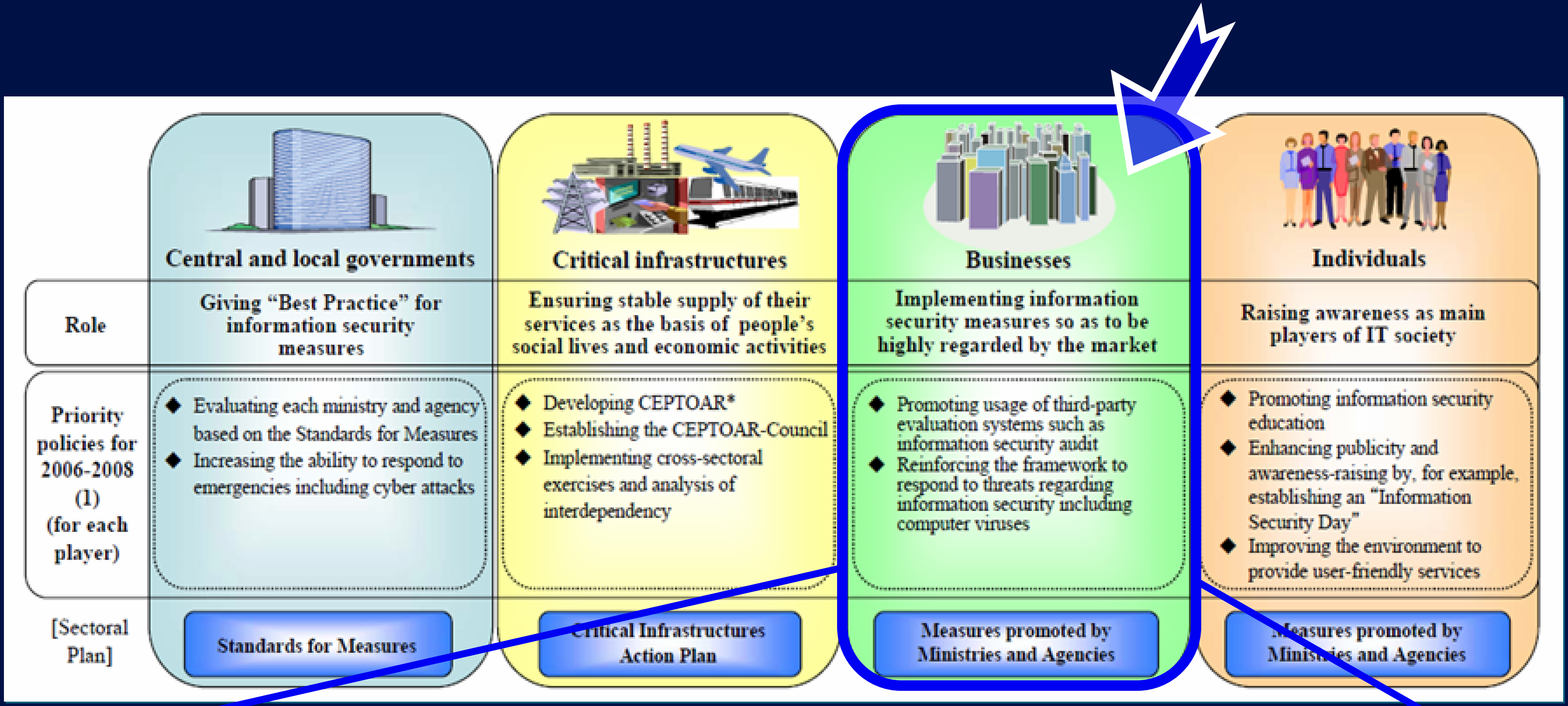
Maintain and improve

1. Implement the identified improvements
2. corrective and preventive actions
3. Communicate
4. Achieve intended objectives

Act

Annex A
Control objectives
and controls

Japan's National Strategy on Information Security
- Priority Policies for FY2006-2008 -

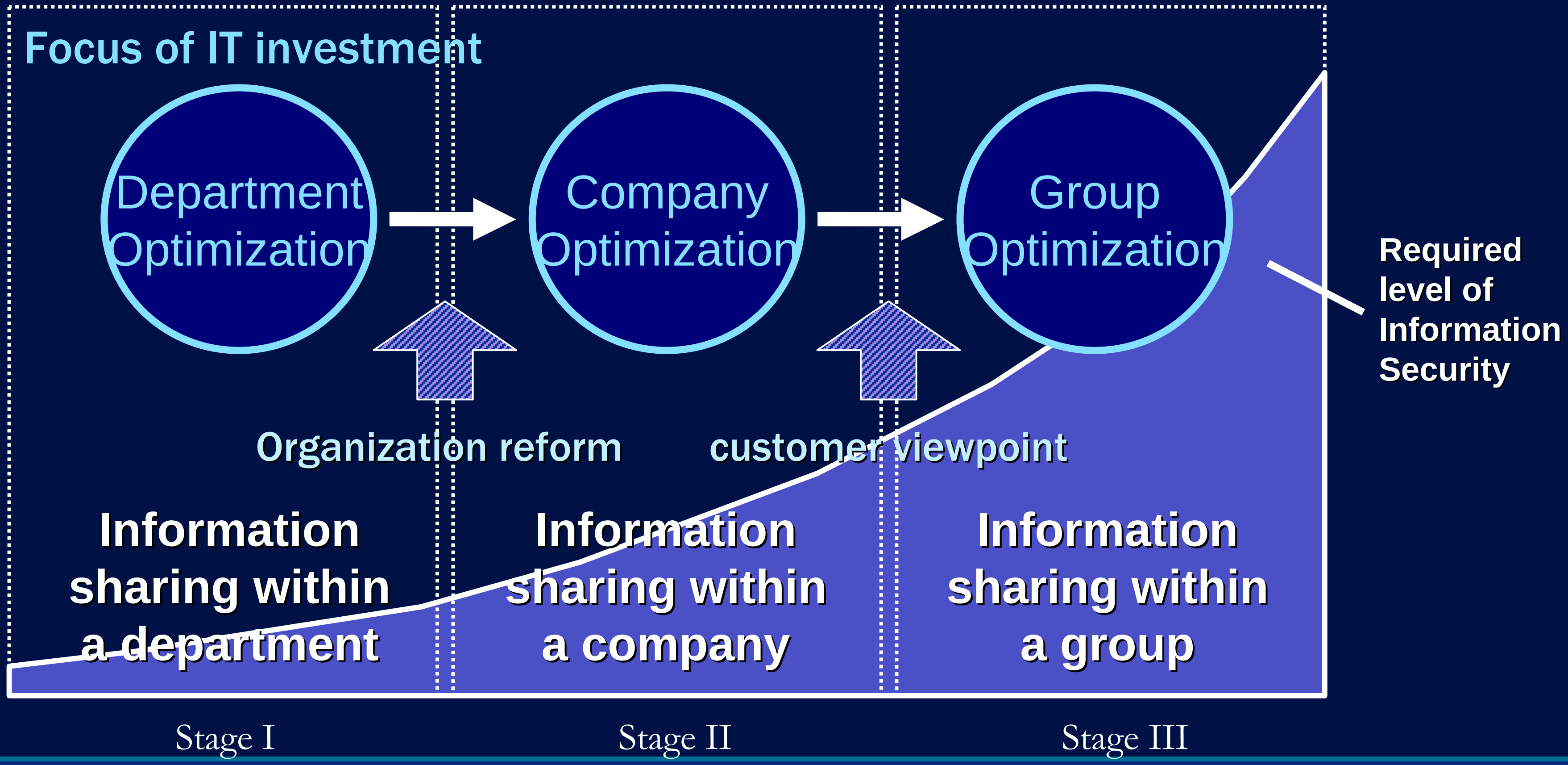


	Central and local governments	Critical infrastructures	Businesses	Individuals
Role	Giving "Best Practice" for information security measures	Ensuring stable supply of their services as the basis of people's social lives and economic activities	Implementing information security measures so as to be highly regarded by the market	Raising awareness as main players of IT society
Priority policies for 2006-2008 (1) (for each player)	◆ Evaluating each ministry and agency based on the Standards for Measures ◆ Increasing the ability to respond to emergencies including cyber attacks	◆ Developing CEPTOAR* ◆ Establishing the CEPTOAR-Council ◆ Implementing cross-sectoral exercises and analysis of interdependency	◆ Promoting usage of third-party evaluation systems such as information security audit ◆ Reinforcing the framework to respond to threats regarding information security including computer viruses	◆ Promoting information security education ◆ Enhancing publicity and awareness-raising by, for example, establishing an "Information Security Day" ◆ Improving the environment to provide user-friendly services
[Sectoral Plan]	Standards for Measures	Critical Infrastructures Action Plan	Measures promoted by Ministries and Agencies	Measures promoted by Ministries and Agencies

Businesses : Implementing information security measures so as to be highly regarded by the market

Security and Stage of IT investment

More comprehensive Information Security Management required as IT investment advances to next stage


Focus of IT investment
Department Optimization
Company Optimization
Group Optimization
Organization reform
customer viewpoint
Information sharing within a department
Information sharing within a company
Information sharing within a group
Required level of Information Security
Stage I
Stage II
Stage III

Importance of End-to-End security

most important information usually shared among companies within a value chain

not only technology measures

every company in the chain needs to establish security management to reduce and maintain risks under allowable level

Agenda

Information Security Governance and Benchmarking

1. Managing Information Security
   - Business and Information Security
   - Security Controls and Management
2. Information Security Governance
   - What is I.S. Governance
   - How to establish I.S. Governance
   - Risk Factors and Risk Treatment
   - Governance Structure
3. Information Security Measures Benchmarking
   - Major issues and three tools
   - What is, How it works, How to utilize

What is Information Security Governance?

To build and operate corporate governance inside companies, taking social responsibility and the mechanism of internal control, which supports corporate governance, from the standpoint of information security into consideration

Source: “Report compiled by the Research Group for Studying What Information Security Should be at Corporations,” Ministry of Economy, Trade and Industry, March 2005.

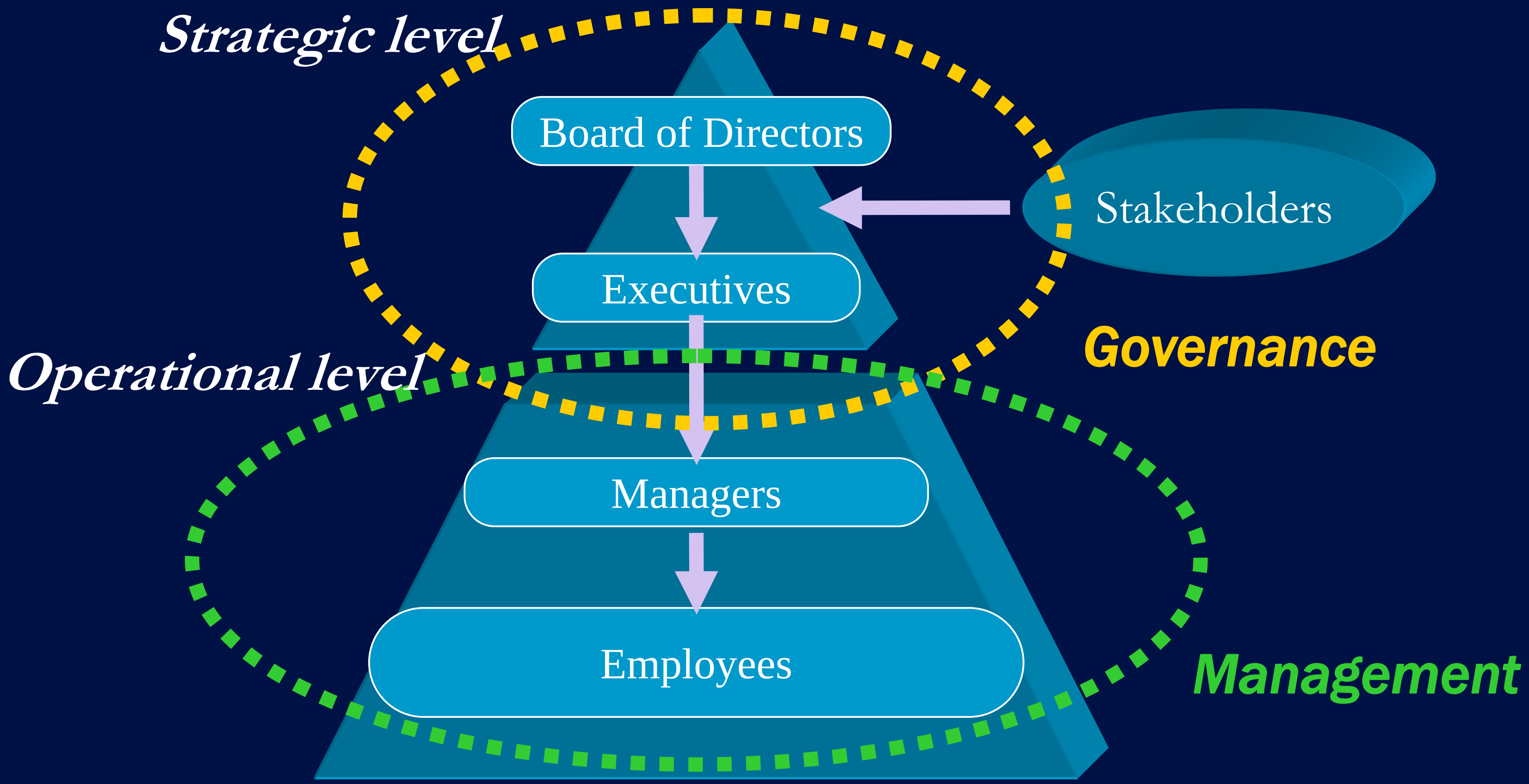
The principal goals of company management are fulfillment of the company’s responsibilities to stakeholders such as shareholders, customers, suppliers, employees, and society, namely, “enhancement of corporate values” and “accomplishment of social responsibility.” Risk management is defined as one of the vital activities that support these missions.

A variety of risks exist. Building and operating a mechanism* to arouse awareness of undertaking activities and thoroughly implementing process activities based on them for the purpose of managing information asset risks is defined as information security governance.

(* Means a mechanism of management decision policy and monitoring the status within the organization and mechanism of disclosure to stakeholders and evaluation by stakeholders.)

Source : Interim Report of the Basic Information Security Problem Committee, Industrial Structure Council June 2008

Governance and Management of Information Security



How to establish IS Governance

1) Define direction and objectives on Information Security clearly

What to be protected ... importance of information assets, Compliance, CSR,

to Which level ... decide allowable residual risk

===> develop Information Security Policy and Standards

2) Establish Internal Control mechanism

Roles and Responsibility... to define allowable risk level, to develop security standards

... to reduce risks below allowable risk level

... to audit, to conduct actions to improve

Name the CSO, CISO and security staffs, provide education and training

Design and Implement Security measures ... build into business processes and ITs

Respond Incidents, Develop and Test Business Continuity Plan

3) Ensure Business Information Security End-to-End

4) Develop Accountability reports to stakeholders

Risk Factors of Information Security

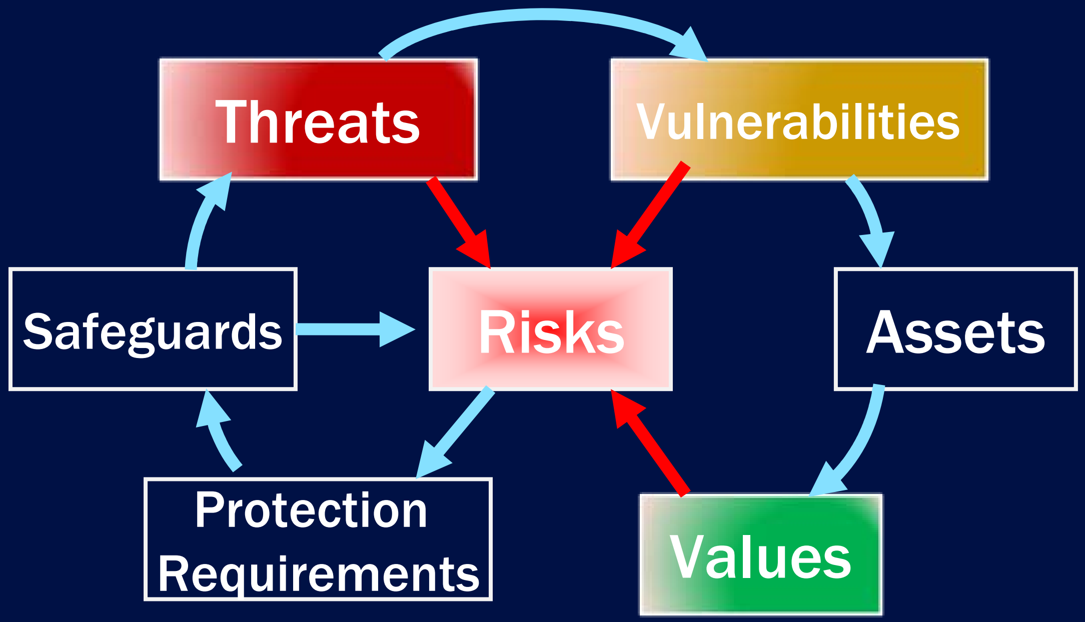
Risk and Business Impact Analysis

- ◆Business Process
- ◆Application
- ◆System
- ◆Network

Necessary Safeguards

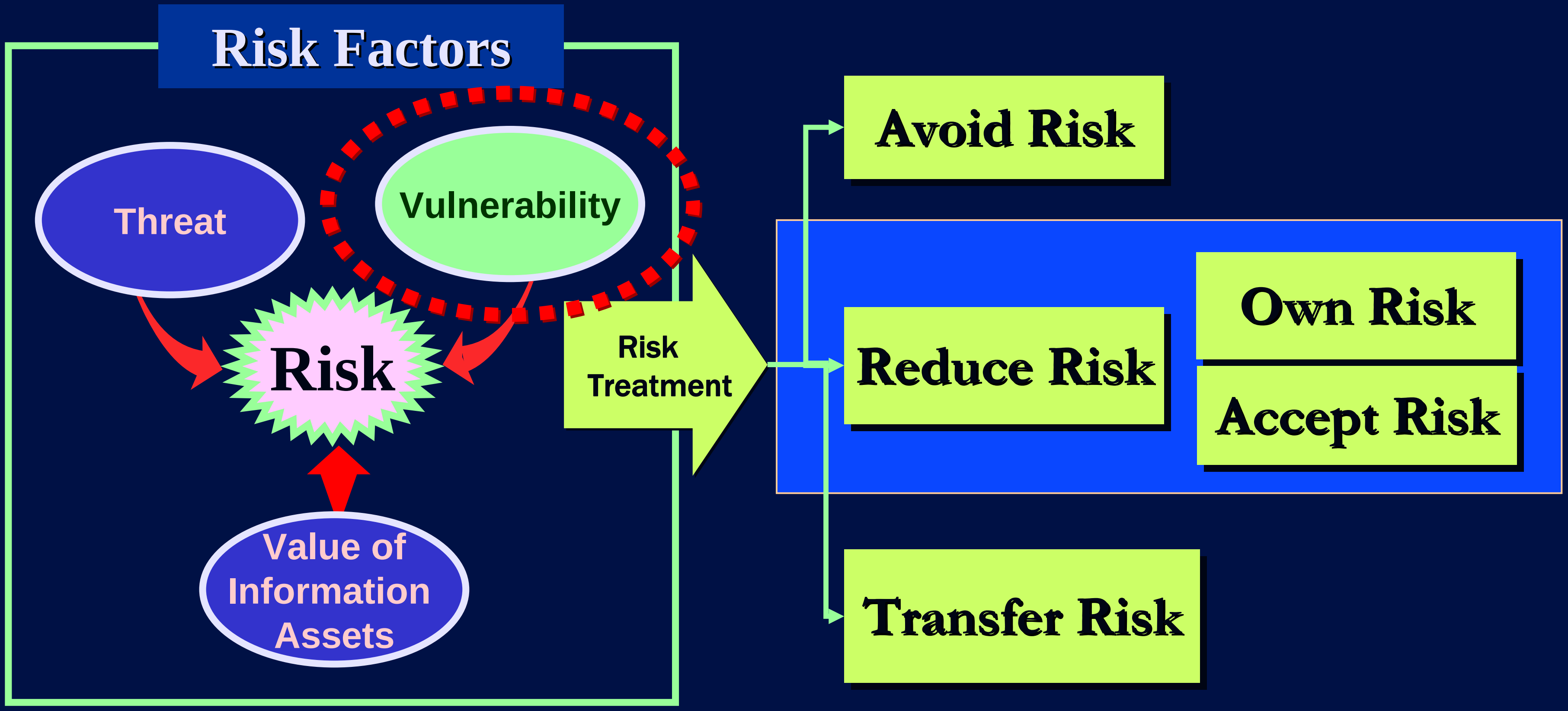
- ◆Risk
- ◆Cost

Risk Factors



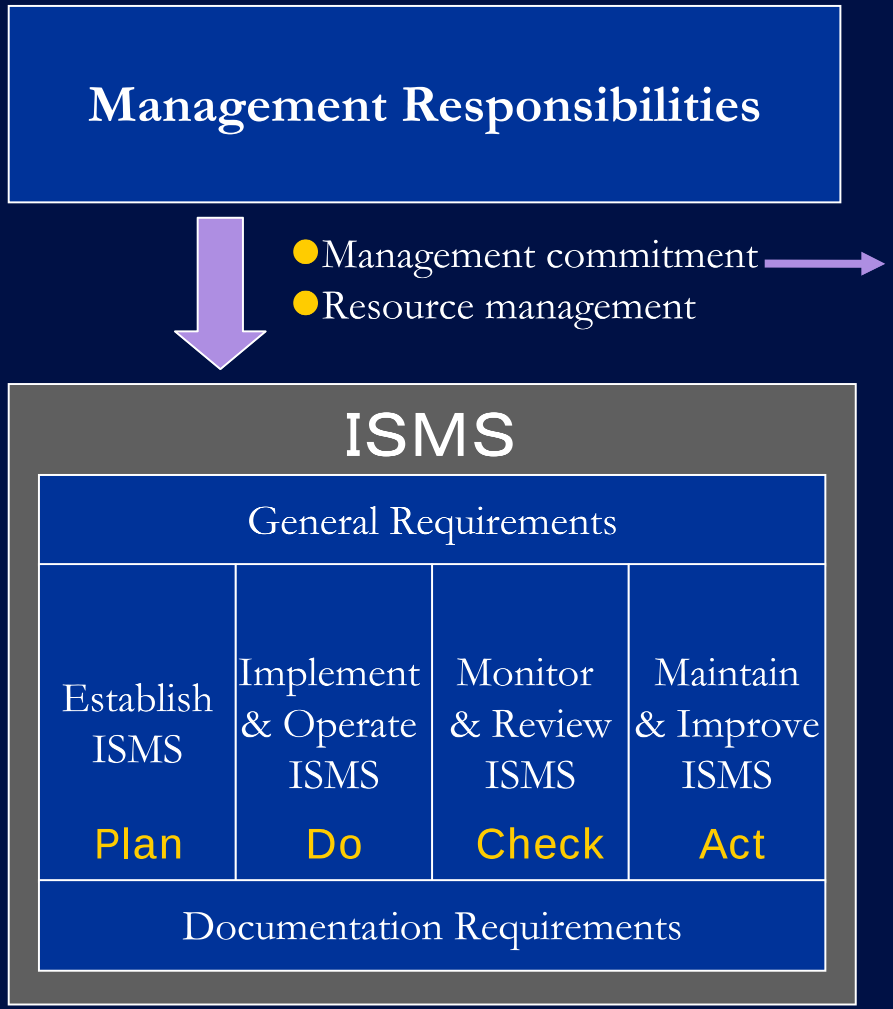
ISO TR 13335 GMITS
Guidelines for Management of
Information Technology Security

Risk Treatment



- ✓ Acceptable Risk Level
- ✓ Cost effectiveness

ISO/IEC 27001 ISMS Requirements



Management Responsibilities

- Management commitment
- Resource management

ISMS

General Requirements

Establish ISMS — Plan

Implement & Operate ISMS — Do

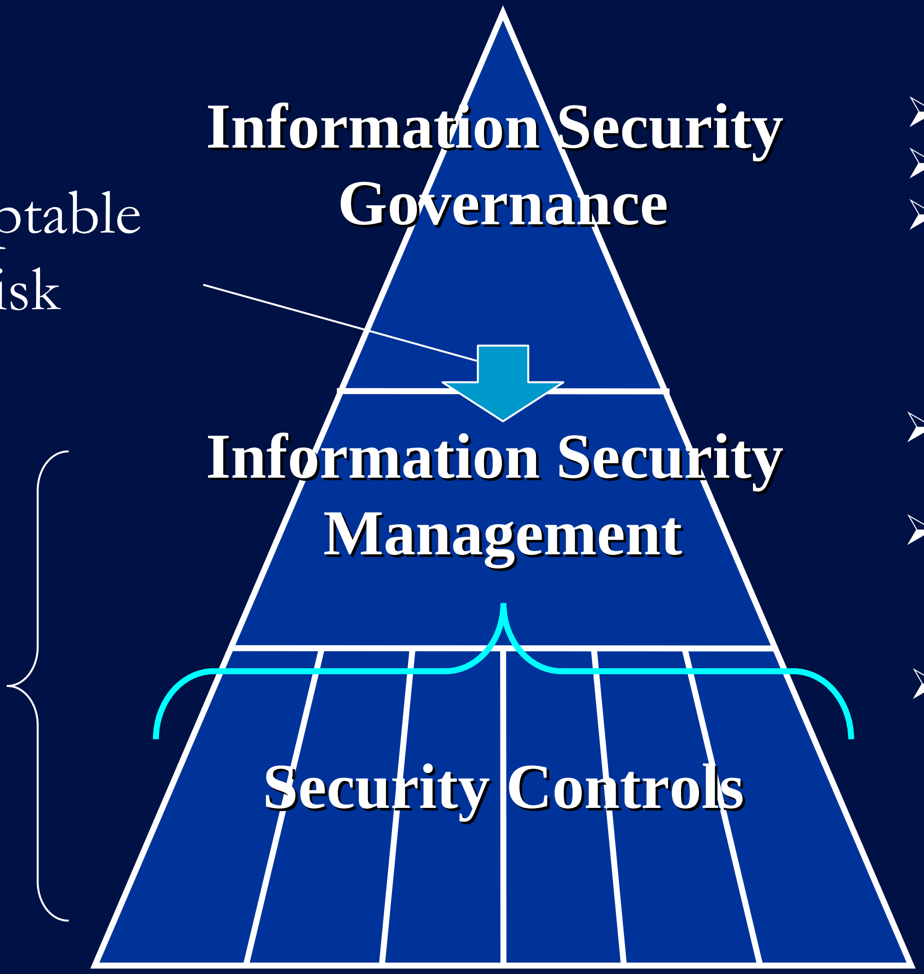
Monitor & Review ISMS — Check

Maintain & Improve ISMS — Act

Documentation Requirements

a. establish an information security policy
b. ensure that information security objectives and plans are established
c. establishing roles and responsibilities for information security
d. communicate the importance
e. provide sufficient resources
f. decide the acceptable level of risk
g. ensure that ISMS internal audit is conducted
h. conduct management reviews

Information Security Governance structure


Information Security Governance
Decide acceptable level of risk
Information Security Management
Realize Risk Reduction
Security Controls

- ➢Direction
- ➢Objectives
- ➢Monitoring

- ➢Establish Management system
- ➢PDCA management cycle

- ➢Sets of Controls
  - ✓ 11 Area
  - ✓ 39 objectives
  - ✓ 133 controls
  - ✓ Many sub-controls

Agenda

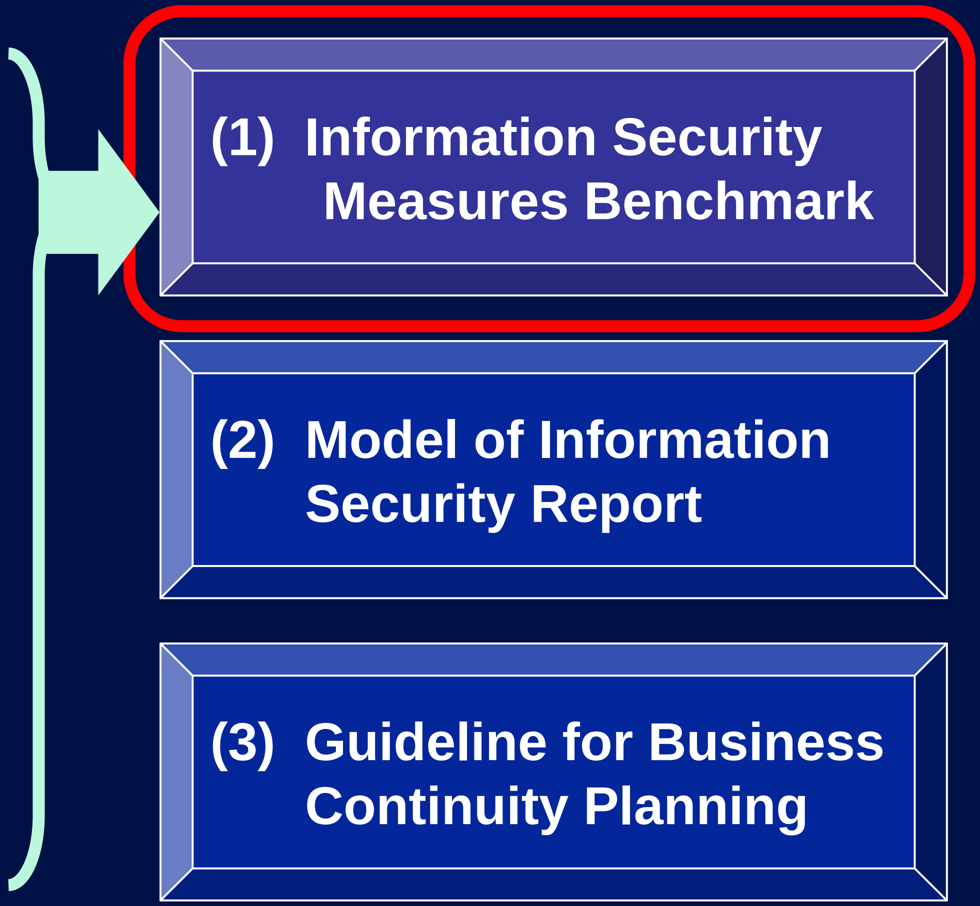
Information Security Governance and Benchmarking

1. Managing Information Security
   - Business and Information Security
   - Security Controls and Management
2. Information Security Governance
   - What is I.S. Governance
   - How to establish I.S. Governance
   - Risk Factors and Risk Treatment
   - Governance Structure
3. Information Security Measures Benchmarking
   - Major issues and three tools
   - What is, How it works, How to utilize

Three Tools recommended at METI’s study group for Information Security Governance（2005/03）

Major Issues

- Difficult to decide Information Security investment due to lack of risk information
- Security Investment doesn’t have straight link to improve Corporate Value
- Importance of BCP/BCM could not be aware by corporate executives



(1) Information Security Measures Benchmark

(2) Model of Information Security Report

(3) Guideline for Business Continuity Planning

http://www.ipa.go.jp/security/english/benchmark_system.html

Outline of Information Security Measures Benchmark

Input → Self Assessment Result

Provides answers to 40 questions on the Web

i.e. Does your company have any policies or rules for information security and implement them?

Assessment Items (40 Items in Total)

Information Security Measures (25 Items)

- Organizational security
- Physical and environmental security
- Communications and operations management
- Access control, Systems development and maintenance
- Security incidents and malfunctions

Corporate Profile（15 Items）

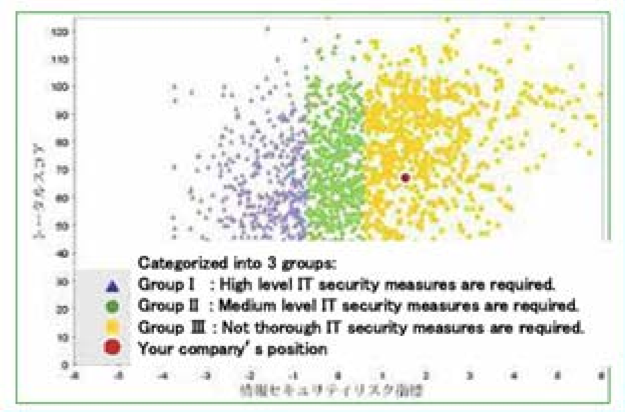
- Number of employees, sale figures, number of basis
- Number of people whose information is held, degree of dependence on Information Technology

1.Displays your company's position using a scatter chart.

2.Compares your organization's score with the desirable security level and the average in your business industry, using a radar chart.

3.Shows your score

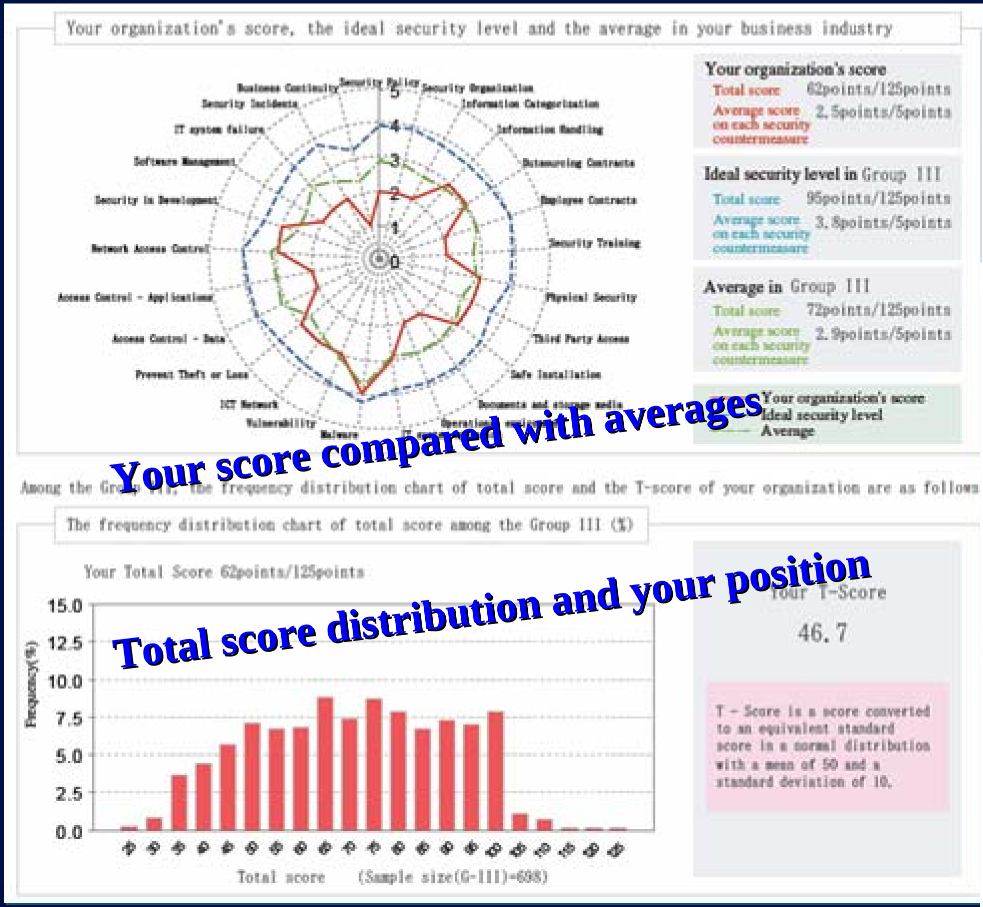
4.Displays recommended security approaches.



Example of Self Assessment Result (Scatter Chart)

Diagnosis Result of
Information Security Measures Benchmark

More than 13,000 usages
as of Dec-2007



Your organization's score, the ideal security level and the average in your business industry

Your organization's score
Total score 62points/125points
Average score on each security countermeasure 2.5points/5points

Ideal security level in Group III
Total score 95points/125points
Average score on each security countermeasure 3.8points/5points

Average in Group III
Total score 72points/125points
Average score on each security countermeasure 2.9points/5points

Your organization's score
Ideal security level
Average

Your score compared with averages

Among the Group III, the frequency distribution chart of total score and the T-score of your organization are as follows

The frequency distribution chart of total score among the Group III (%)

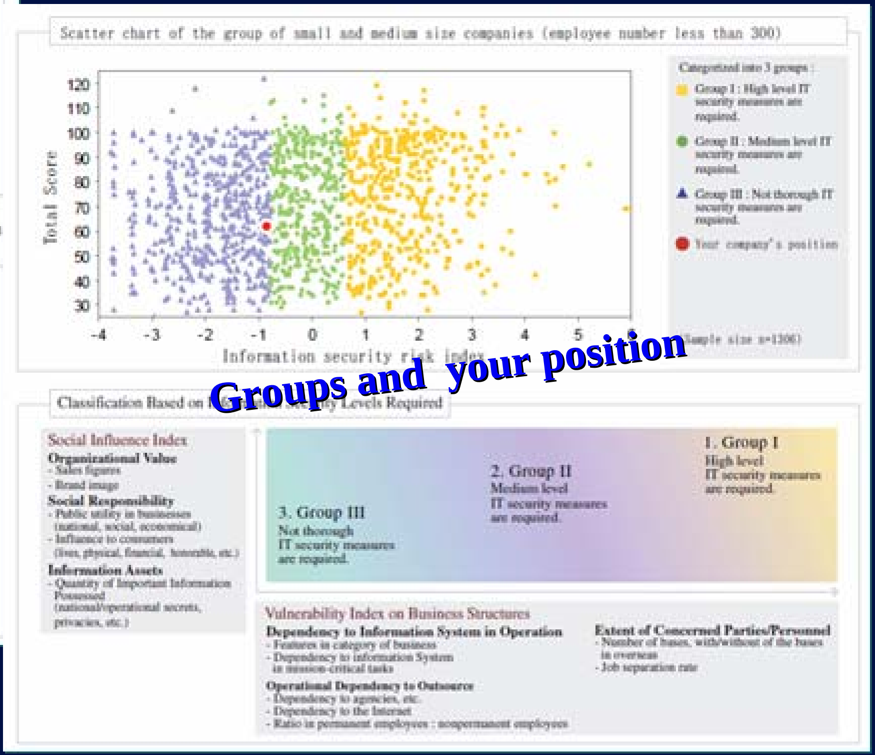
Your Total Score 62points/125points

Your T-Score

46.7

T-Score is a score converted to an equivalent standard score in a normal distribution with a mean of 50 and a standard deviation of 10.

Total score distribution and your position



Scatter chart of the group of small and medium size companies (employee number less than 300)

Categorized into 3 groups :
- 🟨 Group I : High level IT security measures are required.
- ● Group II : Medium level IT security measures are required.
- ▲ Group III : Not thorough IT security measures are required.
- ● Your company's position

(Sample size n=1306)

Groups and your position

Classification Based on Information Security Levels Required

Social Influence Index

Organizational Value
- Sales figures
- Brand image

Social Responsibility
- Public utility in businesses (national, social, economical)
- Influence to consumers (lives, physical, financial, honorable, etc.)

Information Assets
- Quantity of Important Information Possessed (national/operational secrets, privacies, etc.)

3. Group III
Not thorough
IT security measures
are required.

2. Group II
Medium level
IT security measures
are required.

1. Group I
High level
IT security measures
are required.

Vulnerability Index on Business Structures

Dependency to Information System in Operation
- Features in category of business
- Dependency to information System in mission-critical tasks

Operational Dependency to Outsource
- Dependency to agencies, etc.
- Dependency to the Internet
- Ratio in permanent employees : nonpermanent employees

Extent of Concerned Parties/Personnel
- Number of bases, with/without of the bases in overseas
- Job separation rate

Use of IS Measures Benchmark

internally

- for Executives
  - to know your company position in the industry
  - to verify your risk understanding
- for Business Owners
  - to satisfy Business partner requirements
- for business process managers
  - to understand current status, by control area, by department
  - to develop level up plans

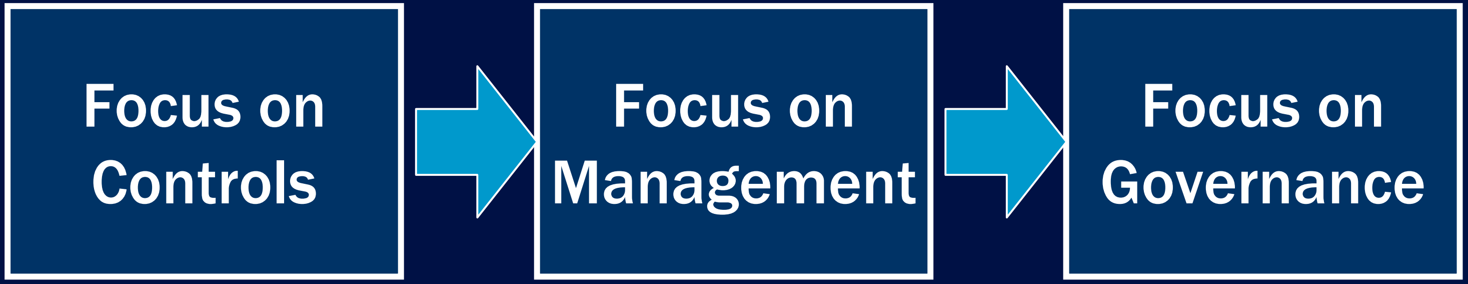
Use of IS Measures Benchmark

externally

- use to grasp group wide security status
  - assess each company within the group in same format, and compare
  - analyze weakness and trends to develop recommendations
- use to lead Business Partners
  - encourage concrete measures
  - develop security terms and conditions
- use to provide consultation
  - executive education materials

Summaries

- Trends of Information Security Program



Focus on Controls → Focus on Management → Focus on Governance

- Explicit risk level agreement
  - define allowable residual risks
  - design and implement security controls to reduce risks to allowable level
  - method to prove controls' effectiveness to reduce risks
  - security audit plan including business partners
- IS Measure Benchmark ... a practical tool