ACS Education 9th

Consulting

Index

- Overview
- Security consulting methodology

01

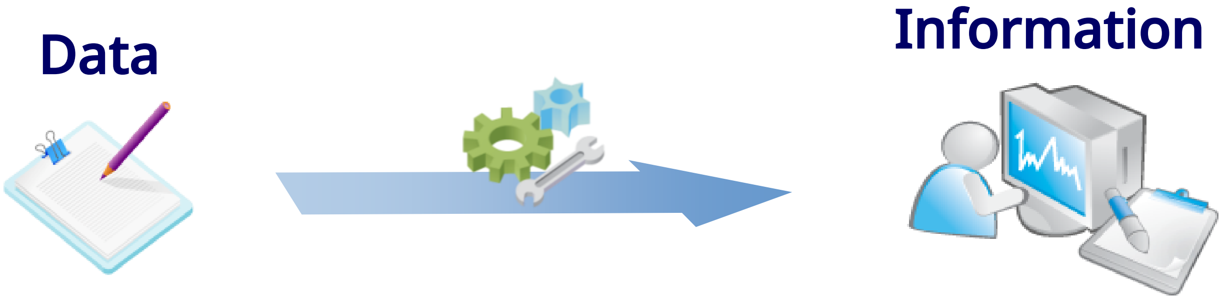
Overview

- Security consulting overview

Security consulting overview

To begin an information security consultation with your client, you must understand some basic concepts. The first step is to know what information needs protecting. Information, like any other critical business asset, is an asset that is valuable to the client and must be properly and continuously protected.

Information is 'knowledge derived from any source.'



Processed data = Information (added value)

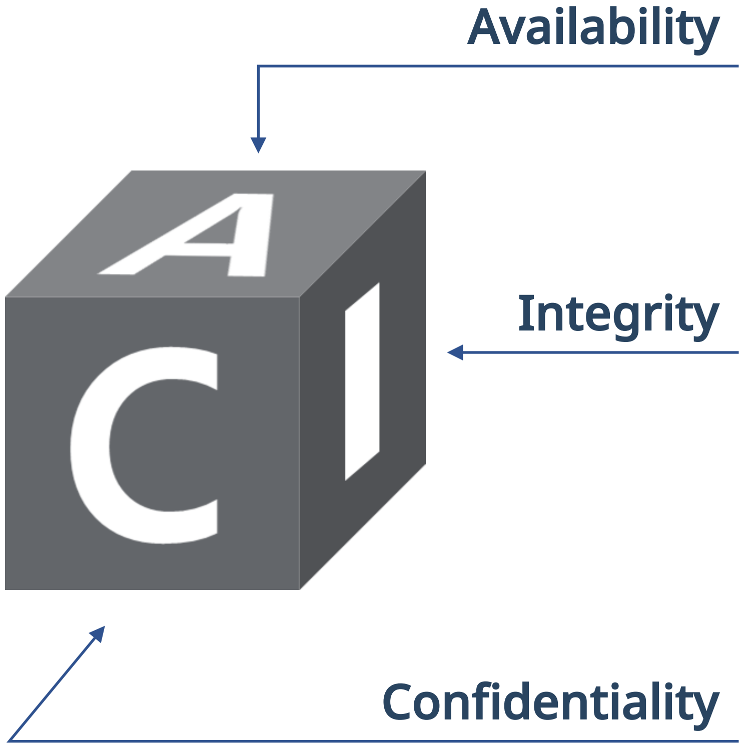
*"Information is an asset which, like other important business assets, has **value** to an organization and consequently **needs to be suitably protected.**"*

ISO/IEC 27001 (2005)

Security consulting overview

Information has inherent qualities. A clear understanding of these characteristics is fundamental to information protection and security controls.

- Qualities of secure information



Availability: Ensure that authorized users have access to information and related assets when they need them (protection from destruction/delay)

Integrity: Ensure the accuracy and completeness of information and processing methods (protection against tampering)

Confidentiality: Ensure that only those who are authorized to access it can do so. (Protection from disclosure)

Security consulting overview

Understanding information

As the value of information becomes more directly tied to a company's competitiveness, the way companies value their assets is changing.

- Accurately value the client's business assets
  - Business valuation is not just about money; you must also factor in information.
- Example of a valuation
  - "Company A provides a service that matches clients with tourist destinations and accommodations through its website.
  - What's its most valuable asset?"

Purpose	Launch of the website	Website installation	Store photos and more	Internal task processing
Pricing	5 million KRW	10 million KRW	10 million KRW	2 million KRW
Remarks	Design by famous creator	Install the latest OS	Archive photos and metadata	Manage customer information

Security consulting overview

Understanding information

Information is clearly subject to management. If you don't manage it, you may not be in business.

- The Importance of Information Management

❖ **Information is the lifeblood of business today.**

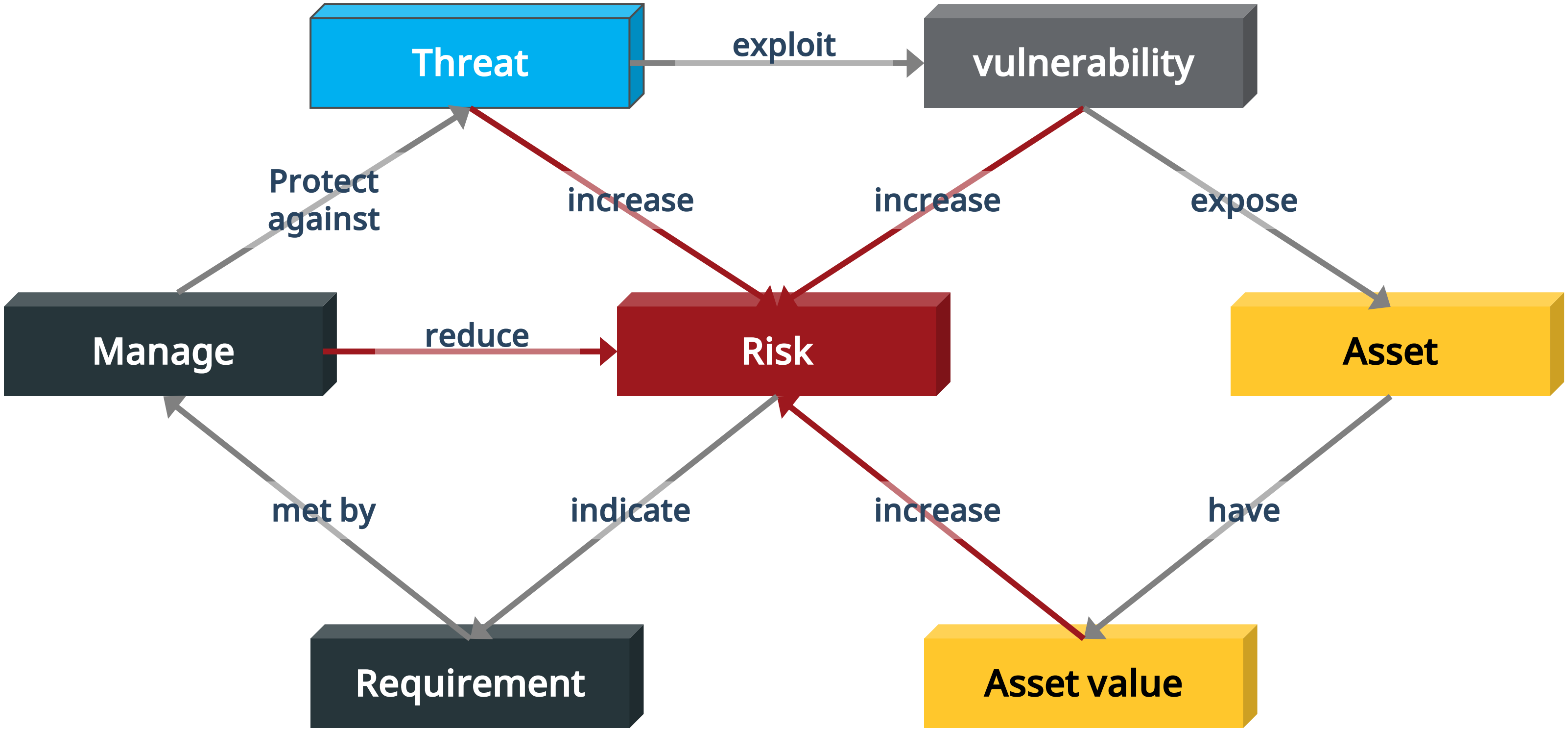
❖ **The very survival & success of your business may depend on it.**

❖ **Information can be sensitive and valuable.**

❖ **It can be critical to your business operations.**

Security consulting overview

To perform information management, it is necessary to recognize the risks associated with information and perform the necessary activities. Therefore, risk management is an integral part of IT. The core of information security consulting is to identify, analyze and evaluate "risks" and create a plan to manage them effectively.

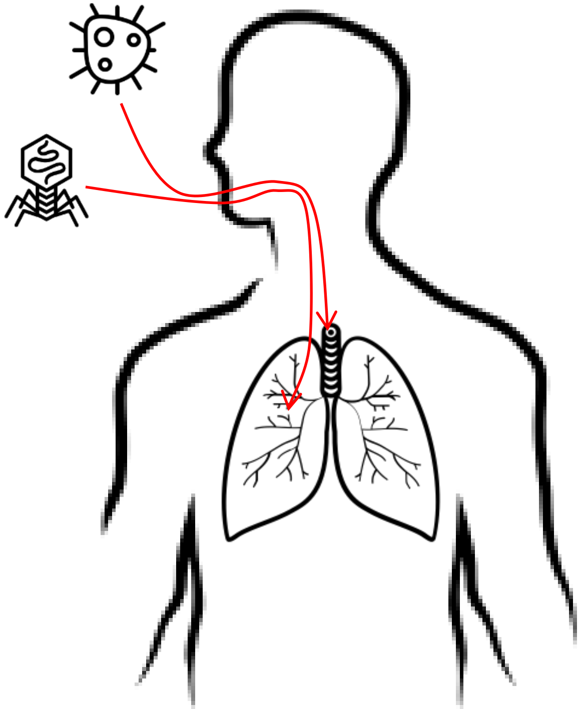


Security consulting overview

Understanding risk

Risk management is the proper control of variables that can affect risk. To do this, you need to understand those variables.

- Variables that can affect risk
  - Asset :
    - An object of protection that represents tangible and intangible economic and non-economic resources of value to the organization.
  - Threat :
    - An event or behavior that has the potential to cause undesirable consequences or damage to an asset.
  - Vulnerability :
    - Preconditions or circumstances for a threat to occur

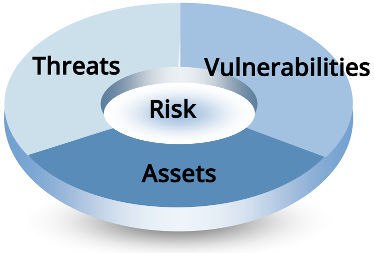


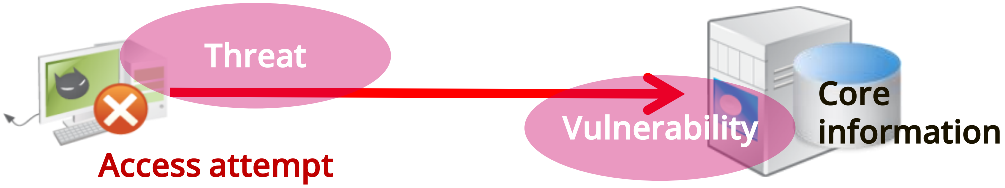
Security consulting overview

"Risk is the potential for an external threat to cause damage (business impact) to an asset by exploiting vulnerabilities that exist within the asset."

- Example risk event scenarios
  - Your server, which is always connected to the Internet, contains sensitive information that unauthorized parties (hackers) want to steal.
  - The server is not patched, sensitive information is not encrypted, and the company's password policy is not followed.

➔ **High risk to information assets due to threats and vulnerabilities**





- **Threats** - Unauthorized (hacker) access attempts
- **Vulnerabilities** - Unpatched
  - Information is not encrypted
  - Violation of corporate password policy

Security consulting overview

"Risk is the potential for an external threat to cause damage (business impact) to an asset by exploiting vulnerabilities that exist within the asset."

- Example risk event scenarios analysis

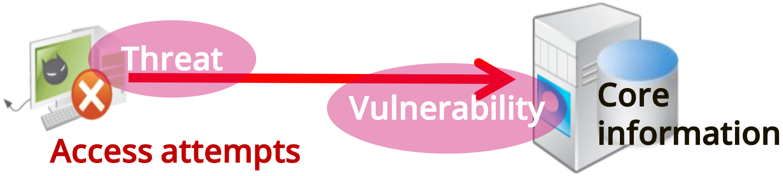
- **Scenario 1** : An instructor prepares a lecture so hard, nearing exhaustion or collapse.
  - ✓ **Asset** : instructor's health **(High)**
  - ✓ **Threat** : clock is ticking, preparing for an intense lecture **(Middle)**
  - ✓ **Vulnerability** : fragile health **(Middle)**

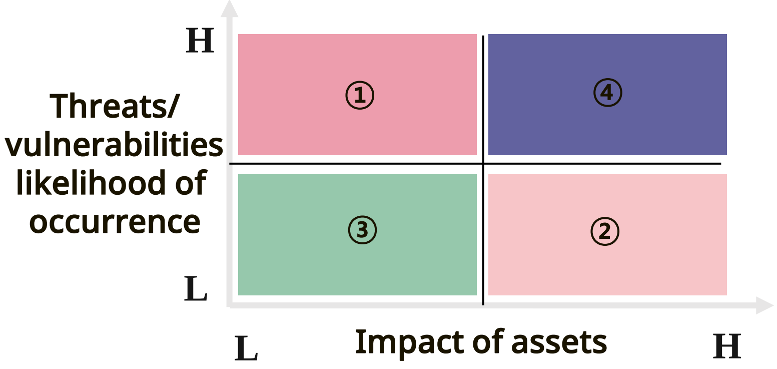
- **Scenario 2** : The ERP system was not developed **using secure coding**, resulting in vulnerabilities.
  - ✓ **Assets** : ERP system **(High)**
  - ✓ **Threat** : failure of programmers to observe secure coding
    Sloppy coding skills (Middle)
  - ✓ **Vulnerabilities** : **programs have inherent limitations**/internal vulnerabilities, resulting
    form the fact that it is created by programmers **(High)**

Security consulting overview

"Risk is the potential for an external threat to cause damage (Business Impact) to an asset by exploiting vulnerabilities that exist within the asset."

- Risk management measures





① **Risk reduction : efforts to reduce threats/vulnerabilities**

For example, applying the latest patch, using DRM for information and enforcing corporate password policy (automation, penalties, etc.)

② **Risk transfer : shift the burden of loss to other areas**

If the risk of the information itself is too great, transfer the risk externally.

③ **Risk acceptance : decide to accept risk, not react to it**

You have applied controls, but the risk still exists, and you accept the risk if it is acceptable.

④ **Risk avoidance : not getting involved in or stepping back from certain risky situations**

You avoid risk by eliminating assets, such as **outsourcing**, due to the high probability and impact of the threat/ vulnerability.

Security consulting overview

Risk

"Risk is the potential for an external threat to cause damage (Business Impact) to an asset by exploiting vulnerabilities that exist within the asset."

- Examples of management actions based on risk event scenario analysis

- **Scenario 1** : An instructor prepares a lecture so hard, nearing exhaustion or collapse.
  - ✓ **Asset** : instructor's health **(High)**
  - ✓ **Threat** : clock is ticking, preparing for an intense lecture **(Middle)**
  - ✓ **Vulnerability** : fragile health **(Middle)**

① Ask the school to reschedule a class.
Adjust the quality of course materials.
Allocate more time to prepare for class.
Increase physical fitness through exercise.

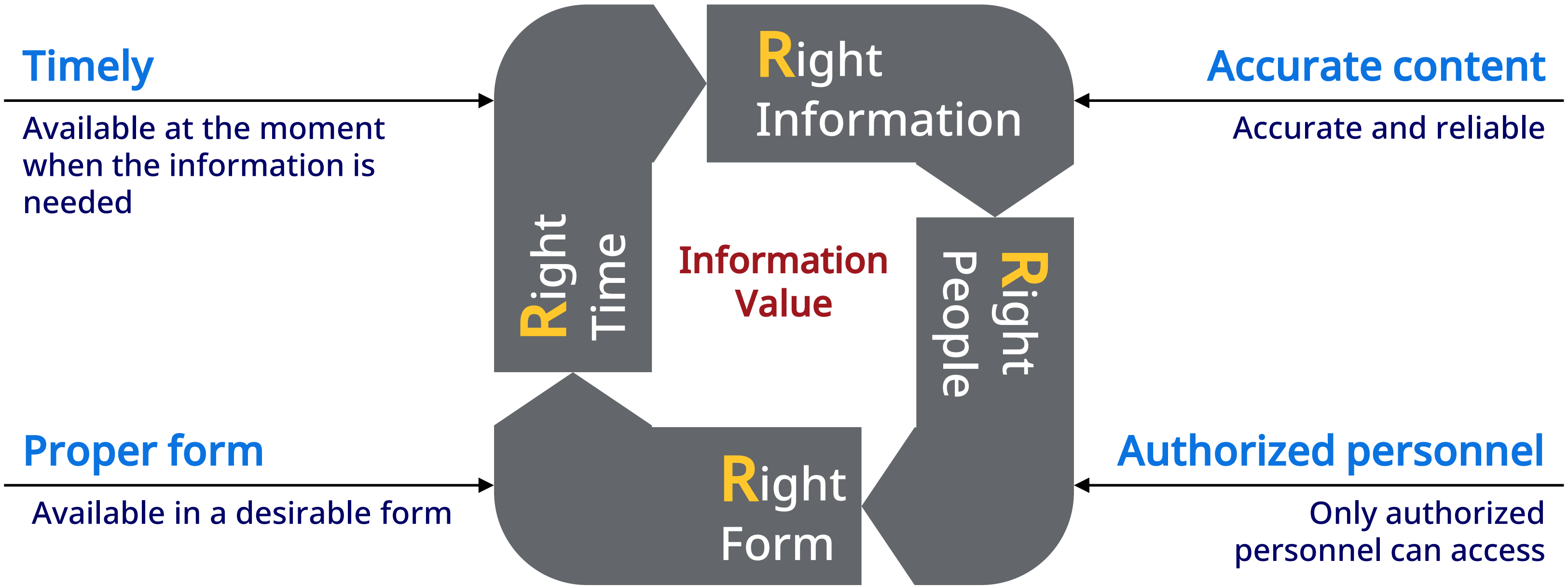
② Enroll in health insurance.
Get a Peer Instructor.

③ After reducing the likelihood of a collapse by increasing your fitness training and spending more time preparing, embrace the rest.

④ Transfer the course to another instructor.

Security consulting overview

Information protection is about securing the "4Rs" of information to ensure its reliability and increase its value to support the growth and continuity of an organization's business.



Security consulting overview

Understanding the concept of consulting

Consultants put a lot of effort into logic and analysis, report writing and presentation to properly convey their knowledge and experience.

- What is consulting?
  - The dictionary definition is ‘to give advice’.
  - From a consulting business perspective, it means ‘to provide solutions, not just advice’.
    - It is about identifying problems and to getting paid to do things on behalf of a client that the client ‘cannot do’ or ‘does not want to do’.
    - Solutions are 'derived from knowledge and experience’.
    - It's about ‘eliciting information’ from a client and ‘effectively communicating the solution’ using ‘unique tools and techniques’.
      - How it's communicated (reported) makes all the difference!

Security consulting overview

Understanding the concept of consulting

- The perspective of consulting services

"The role of a doctor”

Many enterprise customers want to get an overall picture of their business, including whether it's running smoothly, and they want a prescription.

Objectives : 'vision', 'medium to long term strategy’, 'portfolio', 'restructuring’, 'direction’, etc.

"The role of a detective“

It's to dig into specific areas to solve deeper, more fundamental problems, and improving and innovating processes.

Objectives : 'finance', 'human resources’, 'marketing/sales', 'purchasing’, 'procurement', 'logistics', 'IT', etc.

"The role of a salesperson "

When consulting in the role of doctor or detective, various tasks are identified, and the consultant may be responsible for the detailed development or practical implementation of the tasks.

Objectives : ‘new business development', ‘new customer acquisition', etc.

“The role of an agent”

Often clients and consultants become great partners and work together. However, many times consultants are relegated to low-level, low-level tasks.

Objectives : 'simple order placement', 'contract-based service delivery', etc.

Security consulting overview

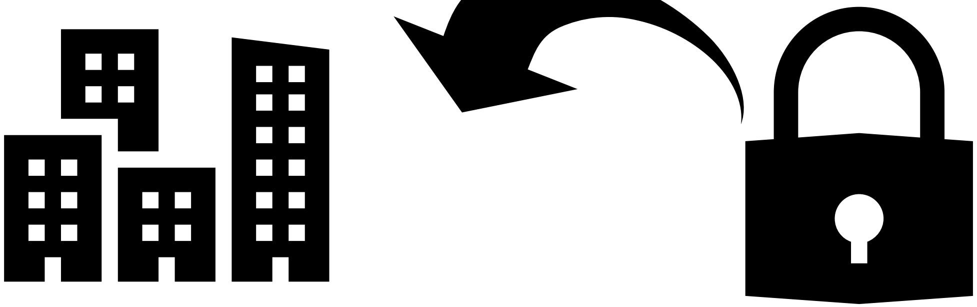
Defining information security consulting

Information security consulting can be defined only after the purpose of "information security" is given to any organization that needs consulting, such as companies, institutions, etc.

- What is information security consulting?
  - Consulting services to protect information assets from "security threats," identify issues that impede the achievement of organizational goals, and develop a response plan that works for the organization.

Who we consult with

Why we consult



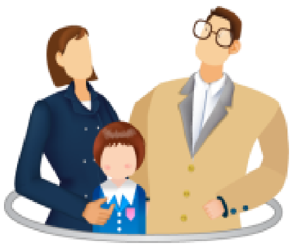
Any organization that needs consulting such as companies and institutions

Providing information protection

Security consulting overview

Customers and consultants

Consulting is all about a client and a consultant, but what is the relationship between the two?



Clients

- Those who have a problem but do not know what it is.
- Those who know the problem and struggles with it.
- Those who are part of a problem but do not know how to solve it.
- Those who know how to solve a problem, but do not have the drive to make it happen.
- **But in the end, they are those who must solve the problem.**

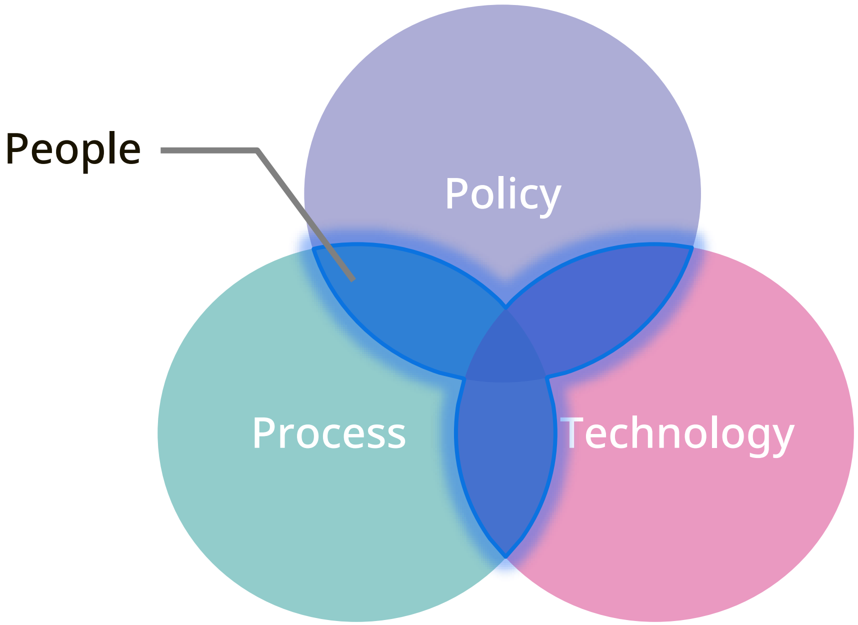
Consultants

- Those who would wrestle with the problem.
- Those who would identify the problem.
- Those who would help a client choose a solution to a problem by providing a rationale for the solution.
- Those who are the driving force behind the execution of a solution.
- **Eventually, they are the ones who are not the parties to the solution, but facilitators of the solution.**

Security consulting overview

Elements of Information Security Consulting

The elements that can be accessed to perform information security consulting can be analyzed and designed in four categories : policy, process, people, and technology.



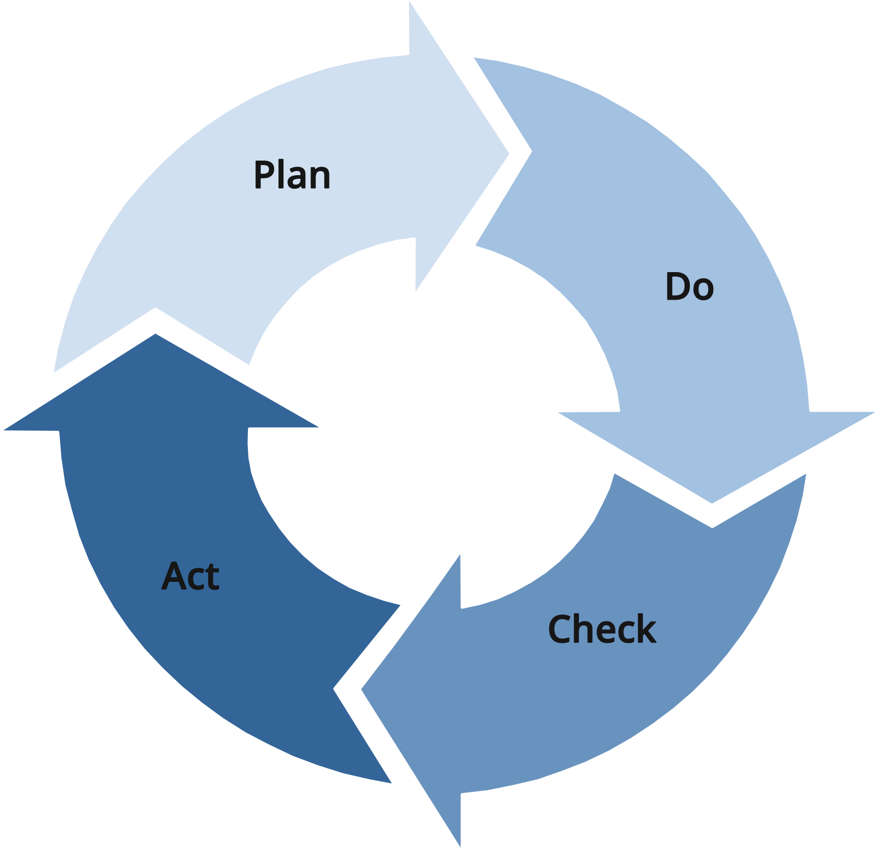
- **3P 1T**

Consultation should be designed to ensure that policies, people, processes, and technology are working appropriately and in harmony to effectively manage information security operations.

Security consulting overview

PDCA Model

The "PDCA cycle" is a management process that involves planning something (Plan), putting it into practice (Do), checking to see if it is right, wrong, or beneficial (Check), and counteracting what went wrong (Act) so that it can be improved from there by executing and verifying a more advanced plan (Act) (originally devised by Schuhart / systematized by Deming).



02

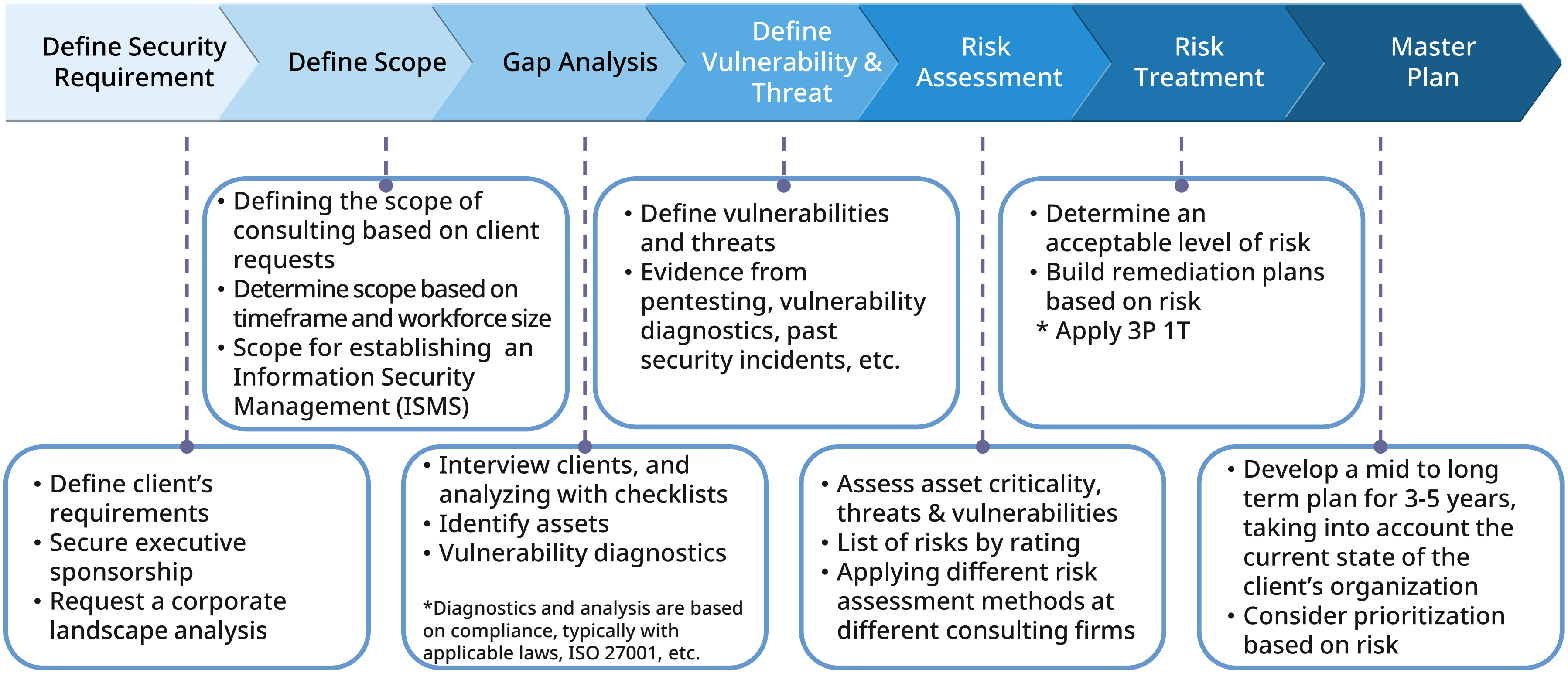
Security consulting methodology

- Overview
- Define security requirement
- Define scope
- Gap analysis
- Define vulnerabilities and threats
- Risk assessment
- Risk treatment
- Master plans

Overview

Information security consulting process

The information security (infosec) consulting process is typically based on the process of establishing an information security management system. You can also customize the methodology based on the performance goals you set for your client's requirements.



Define Security Requirement

- Define client’s requirements
- Secure executive sponsorship
- Request a corporate landscape analysis

Define Scope

- Defining the scope of consulting based on client requests
- Determine scope based on timeframe and workforce size
- Scope for establishing an Information Security Management (ISMS)

Gap Analysis

- Interview clients, and analyzing with checklists
- Identify assets
- Vulnerability diagnostics

*Diagnostics and analysis are based on compliance, typically with applicable laws, ISO 27001, etc.

Define Vulnerability & Threat

- Define vulnerabilities and threats
- Evidence from pentesting, vulnerability diagnostics, past security incidents, etc.

Risk Assessment

- Assess asset criticality, threats & vulnerabilities
- List of risks by rating
- Applying different risk assessment methods at different consulting firms

Risk Treatment

- Determine an acceptable level of risk
- Build remediation plans based on risk

* Apply 3P 1T

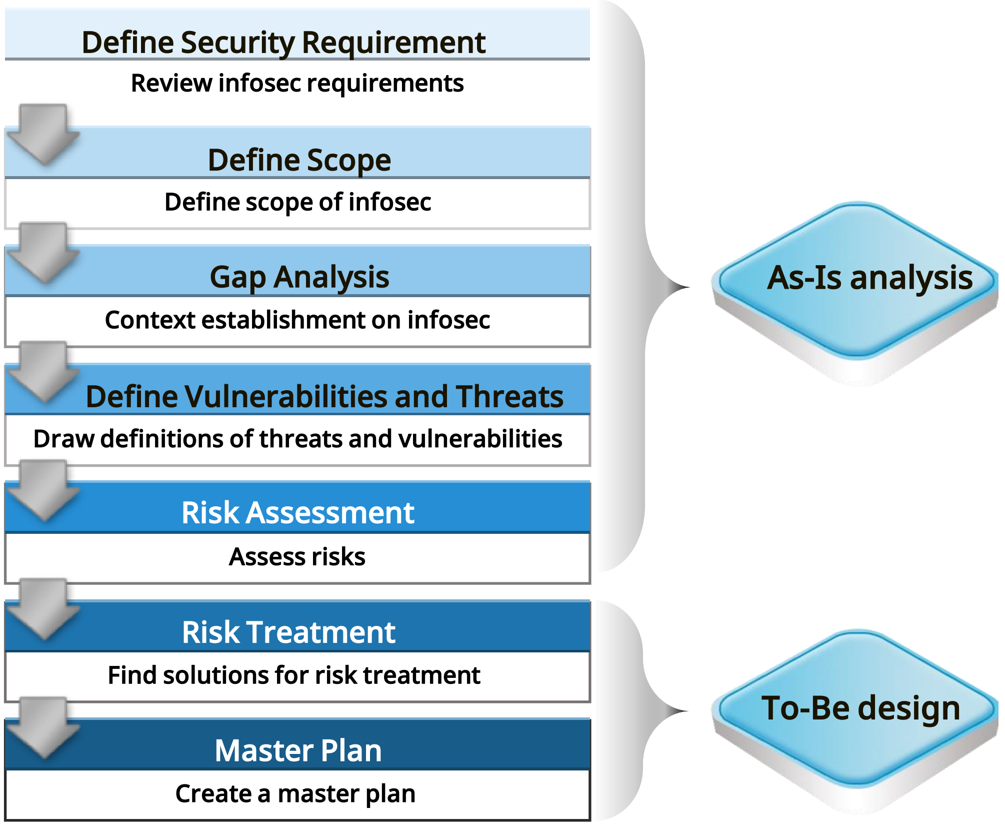
Master Plan

- Develop a mid to long term plan for 3-5 years, taking into account the current state of the client’s organization
- Consider prioritization based on risk

Overview

Information security consulting process

The information security (infosec) consulting process is typically based on the process of establishing an information security management system. You can also customize the methodology based on the performance goals you set for your client's requirements.



Define Security Requirement

Review infosec requirements

Define Scope

Define scope of infosec

Gap Analysis

Context establishment on infosec

Define Vulnerabilities and Threats

Draw definitions of threats and vulnerabilities

Risk Assessment

Assess risks

Risk Treatment

Find solutions for risk treatment

Master Plan

Create a master plan

As-Is analysis

To-Be design

Infosec consulting process?

"We understand client needs and define the optimal scope of ISMS,

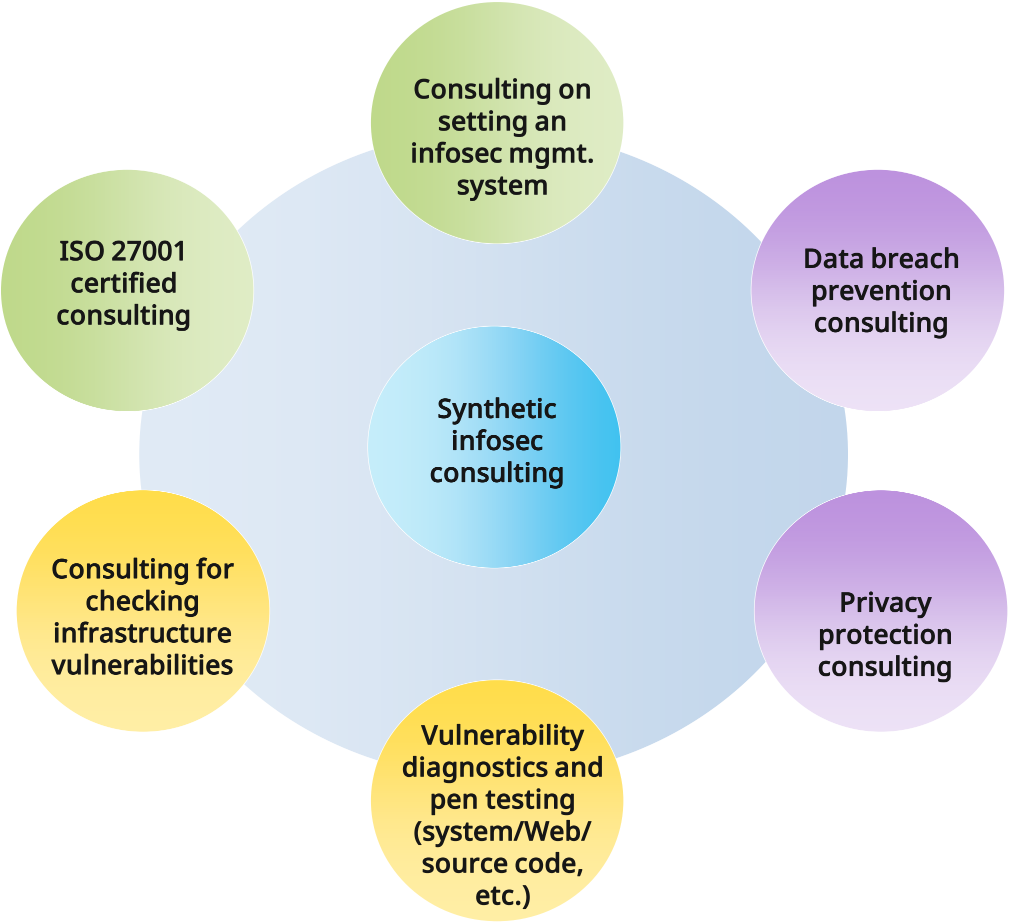
find and define what risks exist,

establish treatment for **unacceptable risks**,

and identify strategies to increase the level of information protection."

Overview

Types of information security consulting


Consulting on setting an infosec mgmt. system

Data breach prevention consulting

Privacy protection consulting

Vulnerability diagnostics and pen testing (system/Web/ source code, etc.)

Consulting for checking infrastructure vulnerabilities

ISO 27001 certified consulting

Synthetic infosec consulting

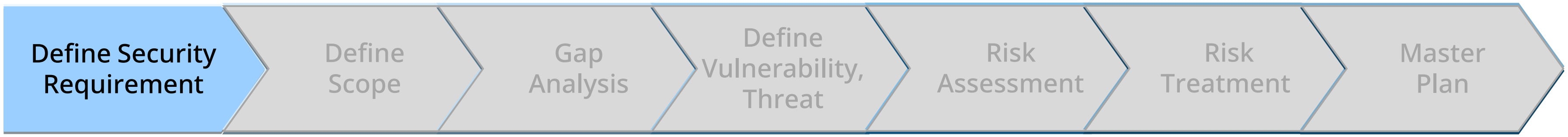
" The types of infosec consulting services are constantly evolving to meet the needs of clients and emerging issues."

However, the consulting process is similar.

Security consulting for OT environments

And more if necessary

Define security requirement



Division	Detail
Overview	• Identify C-suite goals and objectives for infosec • Identify consulting needs of department heads and practitioners in each department
Performance	• Interview C-level executives and heads of departments, etc. • Understand key IT systems and organizational structure, etc. • Reflect the will of top management, department heads, and team leaders in the goals and objectives of consulting projects
Performer	• C-suite, department heads, team leaders • Project representative • Consultant (PM)
Deliverables	• Requirements analysis report

Define security requirement

Conduct interviews to understand security needs

- Interview C-level executives and department heads to gather their information security needs and set the direction for information security consulting.

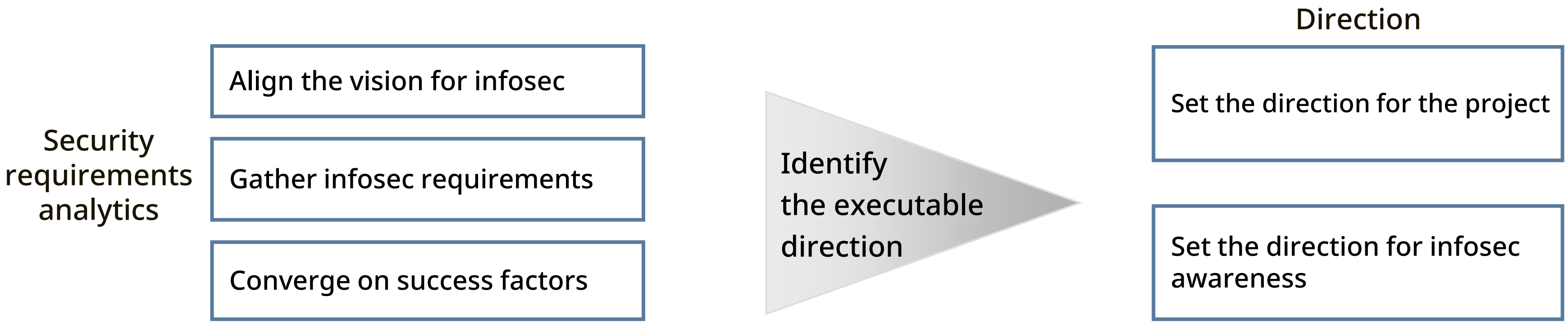
When and who to interview

- Interview Interview schedule: within 4 days after the start of the consulting project (also possible before the start of the project)
- Interviewee : C-suite (CEO, CFO)
  Department heads, TLs, and PMs
  (minimum requirement)
- Interviewer : consultant(s)

Interview topics

- Satisfaction with privacy policies and operational standards
- Privacy-related work history
- Views of key assets
- Views of potential breaches and threats from outside the organization
- Improvements in infosec operation
- Cautions about infosec consulting

How to approach



Security requirements analytics

Align the vision for infosec

Gather infosec requirements

Converge on success factors

Identify the executable direction

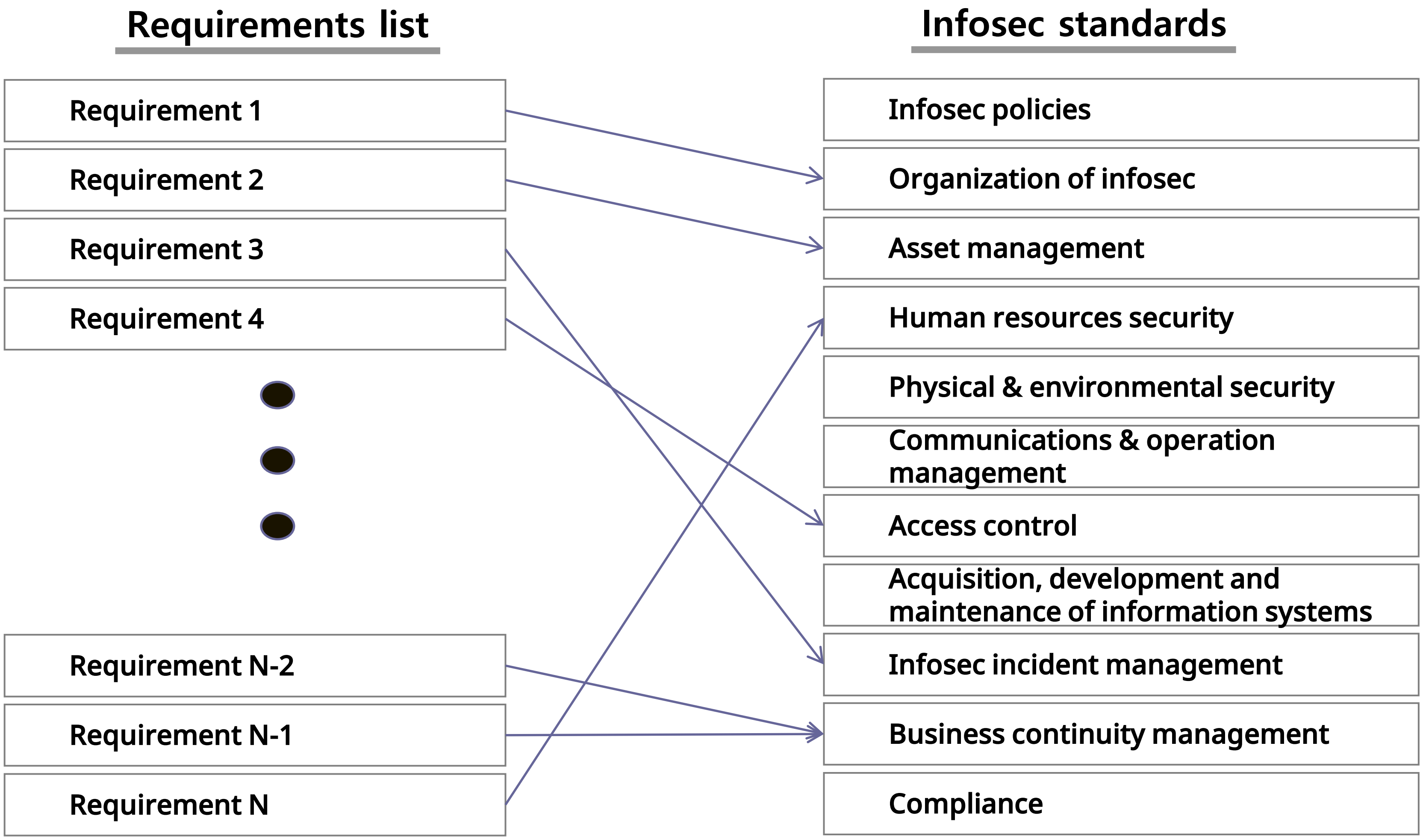
Direction

Set the direction for the project

Set the direction for infosec awareness

Define security requirement

Mapping Infosec standards for security requirements



Requirements list

- Requirement 1
- Requirement 2
- Requirement 3
- Requirement 4

●

●

●

- Requirement N-2
- Requirement N-1
- Requirement N

Infosec standards

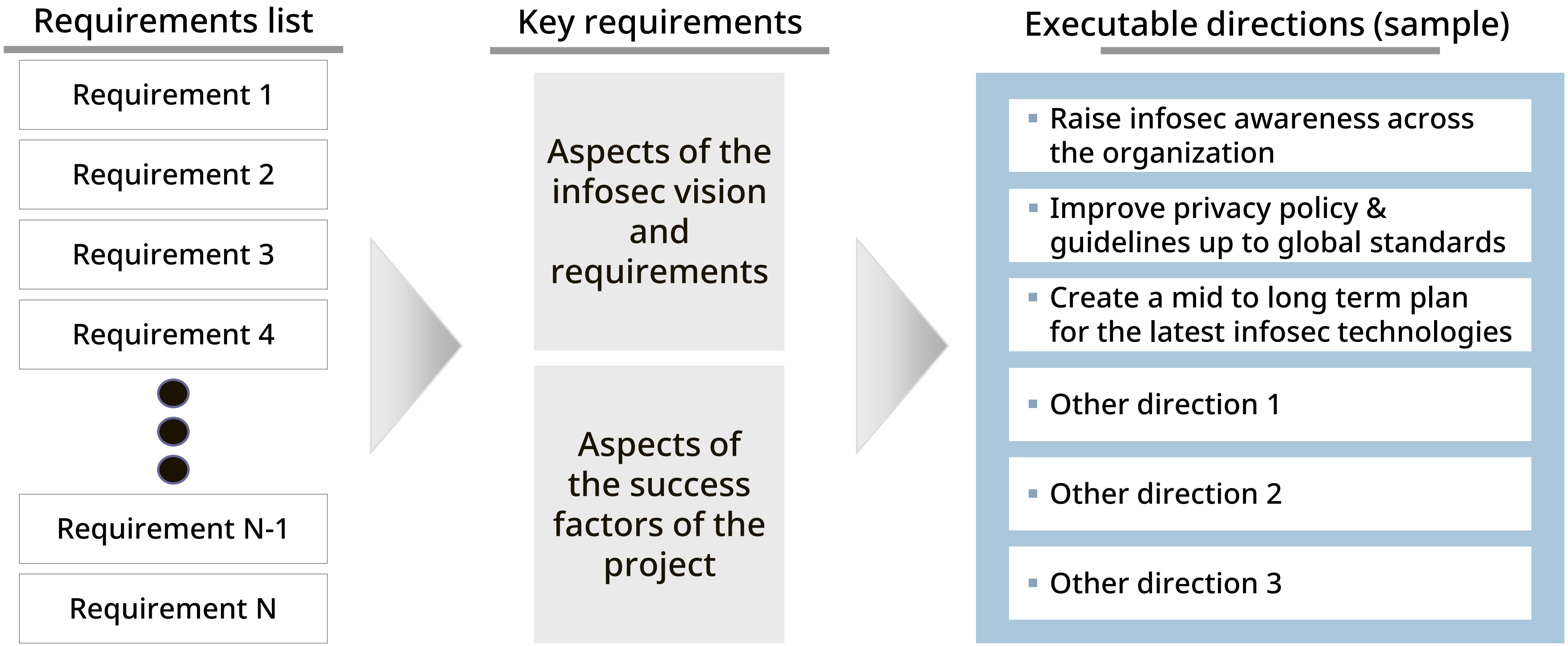
- Infosec policies
- Organization of infosec
- Asset management
- Human resources security
- Physical & environmental security
- Communications & operation management
- Access control
- Acquisition, development and maintenance of information systems
- Infosec incident management
- Business continuity management
- Compliance

(Sample. ISO 27001, 2013)

Impact assessment

Set the direction of your consulting efforts

- Analyzed key requirements in terms of information security vision and needs, project success factors, and derived action items (to-dos) for consulting project



Requirements list

- Requirement 1
- Requirement 2
- Requirement 3
- Requirement 4
- Requirement N-1
- Requirement N

Key requirements

- Aspects of the infosec vision and requirements
- Aspects of the success factors of the project

Executable directions (sample)

- Raise infosec awareness across the organization
- Improve privacy policy & guidelines up to global standards
- Create a mid to long term plan for the latest infosec technologies
- Other direction 1
- Other direction 2
- Other direction 3

Impact assessment

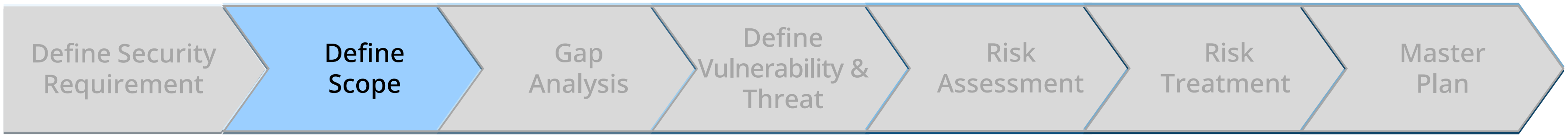
Create a list of requested materials

- List of data requests for environmental analysis (example)

Division	Sub-division	Detail
Organization	• Company-wide organizational chart, and roles & responsibilities	• Understand the organization and the tasks
	• Infosec organizational chart and roles & responsibilities	• Understand infosec organization and how it works
Planning	• Annual infosec plan	• Understand client's infosec goals and business plans
	• Strategic and business plan, including IT	
	• Infosec audit / inspection plan (report)	• Understand audit/inspection status or focus
Policy / guideline	• Privacy policies and guidelines	• Understand policy structure and security control baselines
Information system	• Information systems and N/W diagrams	• Understand the systems and N/W status
	• Infosec system diagram	• Understand infosec system configuration and controls
	• Business systems list and function specifications	• Understand the service history of internal and external systems
	• List of information systems (including a list of security solutions)	• Basis of information assets
Training	• Infosec (& privacy) training syllabus	• Check overall corporate culture
	• Infosec (& privacy) training materials	• Know what to teach in infosec training
Other	Contracts (information security-related outsourcers), pen testing and vulnerability assessment results, and other policy implementation documents	

Define scope

Overview


Define Security Requirement

Define Scope

Gap Analysis

Define Vulnerability & Threat

Risk Assessment

Risk Treatment

Master Plan

Division	Detail
Overview	• Scoping, and taking into account the findings from the phase of defining infosec & privacy requirements
Performance	• Scoping in consultation with your representative • Define the flow of information at the enterprise vs. specific department vs. criticality (sensitivity) level. • Specify organization/people, physical scope, application scope, network scope, etc. • Consider staffing, project duration, etc.
Performer	• Project representatives • Consultant (PM)
Deliverables	• Scoping report

Define scope

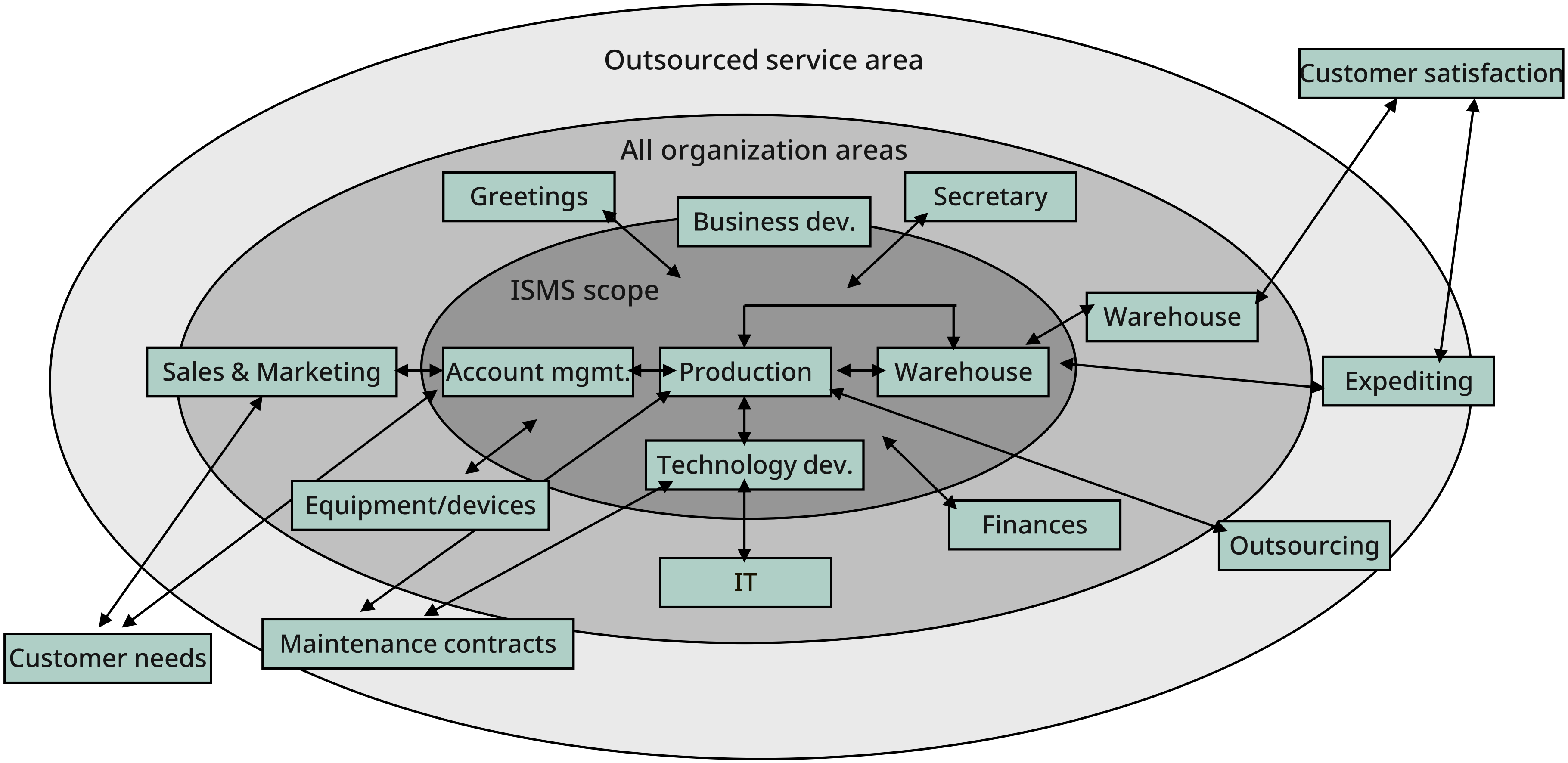
To perform information security consulting, you need to define the scope. This scope should be aligned with the client's needs (both internal and external) and include managing interactions with all partners, suppliers, and customers that are deemed to have an impact on sensitive information.

- Define a scope

Include when defining scope	Things to consider
• Activities, features, and services provided to internal and external customers • Physical locations included in the scope (location of external outsourcers is identified by individual contracts / SLAs) • Other information about the organization's operations • Information created, processed, transmitted and stored • Information shared with providers or partners	• Customer data protection level • Level and M/M of consultants engaged • Project duration • Client's data protection requirements • Geographical location of the client's business/third party services • Information about the department(s) that handle sensitive information and where it is stored

Define scope

- Example of the ISMS scope



Define scope

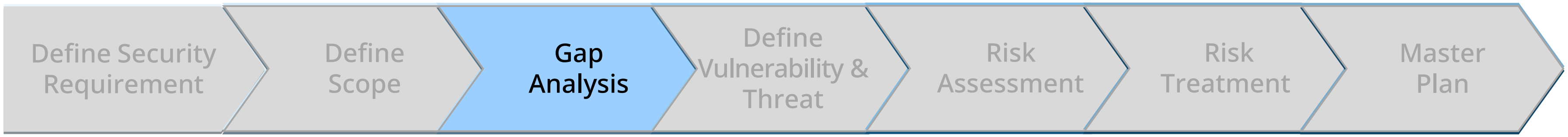
Setting privacy scope based on perspective

- Components

Division	Description	Advantage and disadvantage	
Overarching perspective	Scope across the organization	Pros	• No barriers to organization-wide adoption in the future, but very difficult to achieve organization-wide adoption if only partially implemented • You can deviate from the law of least resistance
		Cons	• Expect non-cooperation and resistance, increasing the risk of project management. • Medium project duration (6-9 months)
Specific department perspectives	Scope only specific departments, such as labs that handle infosec	Pros	• Minimize the path of least resistance • Minimize project management risks • Accelerate delivery of results and outcomes by reducing project duration
		Cons	• Challenges for future organization-wide deployments • The nature of security is such that the negative tends to be emphasized in a specific department that handles infosec. • Difficulty in assessing who owns the information when evaluating assets (IT)
A key information circulating stage perspective	Scope organizations by the stage of production, distribution, storage, disposal of specific info	Pros	• Apply alternatives based on the flow of critical information • Gain control over critical departments
		Cons	• Difficulties with future organization-wide deployments • The rest consider it less important due to the nature of their security and don't distribute it. • Difficulty in being confident that all levels of distribution of sensitive information have been identified and countermeasures taken

Gap analysis

Overview



Define Security Requirement

Define Scope

Gap Analysis

Define Vulnerability & Threat

Risk Assessment

Risk Treatment

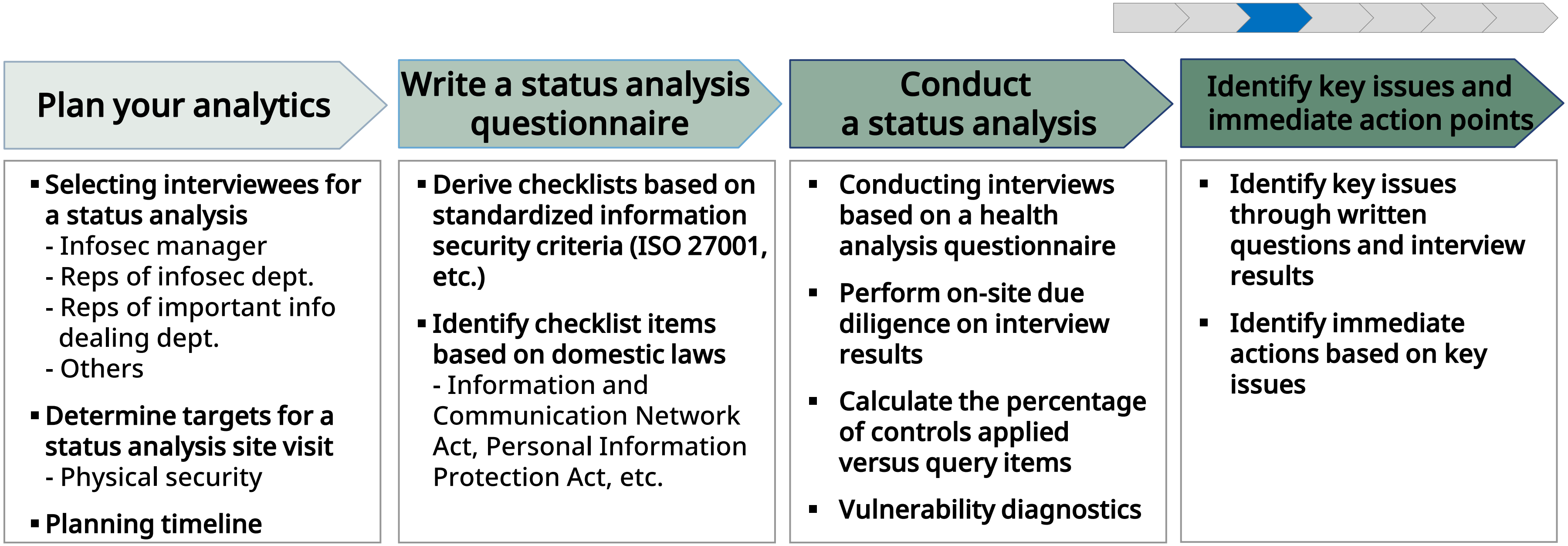
Master Plan

Division	Detail
Overview	• Analyze the current status of an organization's infosec management system using a checklist of control items from ISO27001 and other standards.
Performance	• Identify and categorize the organization's information assets (asset classification criteria are defined based on the organization's environment) • Analyze an organization's security posture to determine if it meets information protection standards such as ISO27001 • Analyze the gap between your current security posture and information protection standards • Conduct interviews with representatives from each of these areas • Gather evidence from the results of vulnerability analyses or interview requests
Performer	• Owner of the asset and contact person defined by infosec area • Consultant(s)
Deliverables	• Asset list / evidence list • Gap checklist • Context establishment report

Gap analysis

Status Analysis Procedure

The goal is to obtain information about the current level of information security as a measure of compliance with standardized information security criteria such as ISO 27001.



Plan your analytics

- **Selecting interviewees for a status analysis**
  - Infosec manager
  - Reps of infosec dept.
  - Reps of important info dealing dept.
  - Others
- **Determine targets for a status analysis site visit**
  - Physical security
- **Planning timeline**

Write a status analysis questionnaire

- **Derive checklists based on standardized information security criteria (ISO 27001, etc.)**
- **Identify checklist items based on domestic laws**
  - Information and Communication Network Act, Personal Information Protection Act, etc.

Conduct a status analysis

- **Conducting interviews based on a health analysis questionnaire**
- **Perform on-site due diligence on interview results**
- **Calculate the percentage of controls applied versus query items**
- **Vulnerability diagnostics**

Identify key issues and immediate action points

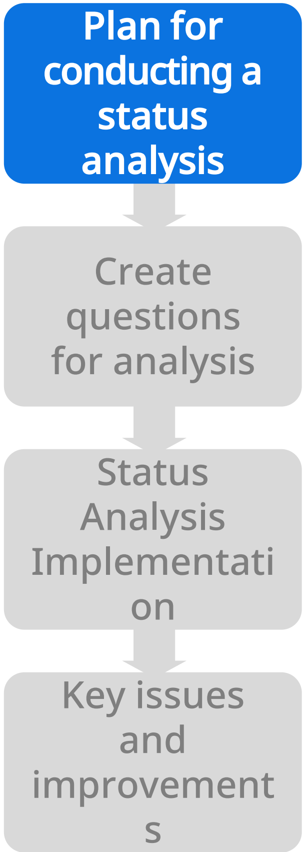
- **Identify key issues through written questions and interview results**
- **Identify immediate actions based on key issues**

If you can't measure it, you can't manage it,
if you can't manage it, you can't improve it.

- Peter Drucker -

Gap analysis

- Plan your analytics



Plan for conducting a status analysis

Create questions for analysis

Status Analysis Implementati on

Key issues and improvement s

When?

- Conduct after an infosec needs analysis
- Duration : depends on scope (mie. 2-3Ws)
- Reporting is also included in the timeframe
- Project duration requires appropriate distribution

Where?

- Where to analyze status?
  - Project room vs dept
- Field trips?
  - Factories vs. regional offices (factories)
- Make the right choice based on project scope and duration

How?

- Choose the right method for your client
  - Will you conduct interviews?
  - Utilize a questionnaire?
  - Question and answer?
- Choose survey methods for status analysis
  - What to choose for data protection criteria?
  - Customize the questionnaire based on the characteristics of the client’s industry

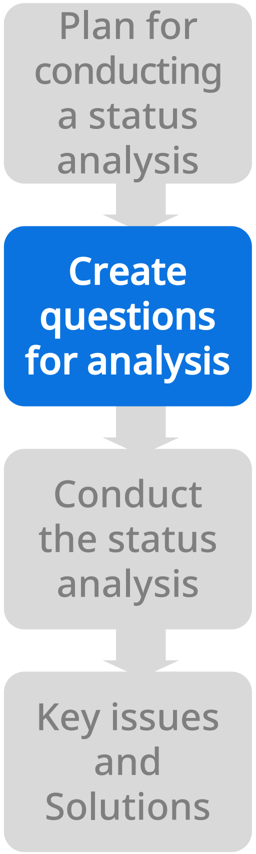
Who?

- (Min. requirement) Information protection leading and related depts
  - Even if it's out of scope, for you to know the status...
- Target depts based on project scope
  - Depts that have sensitive information in your scope
- Team leaders vs. reps

Gap analysis

Write a health analysis query

- Questionnaire example for status analysis (context establishment)


Plan for conducting a status analysis
Create questions for analysis
Conduct the status analysis
Key issues and Solutions

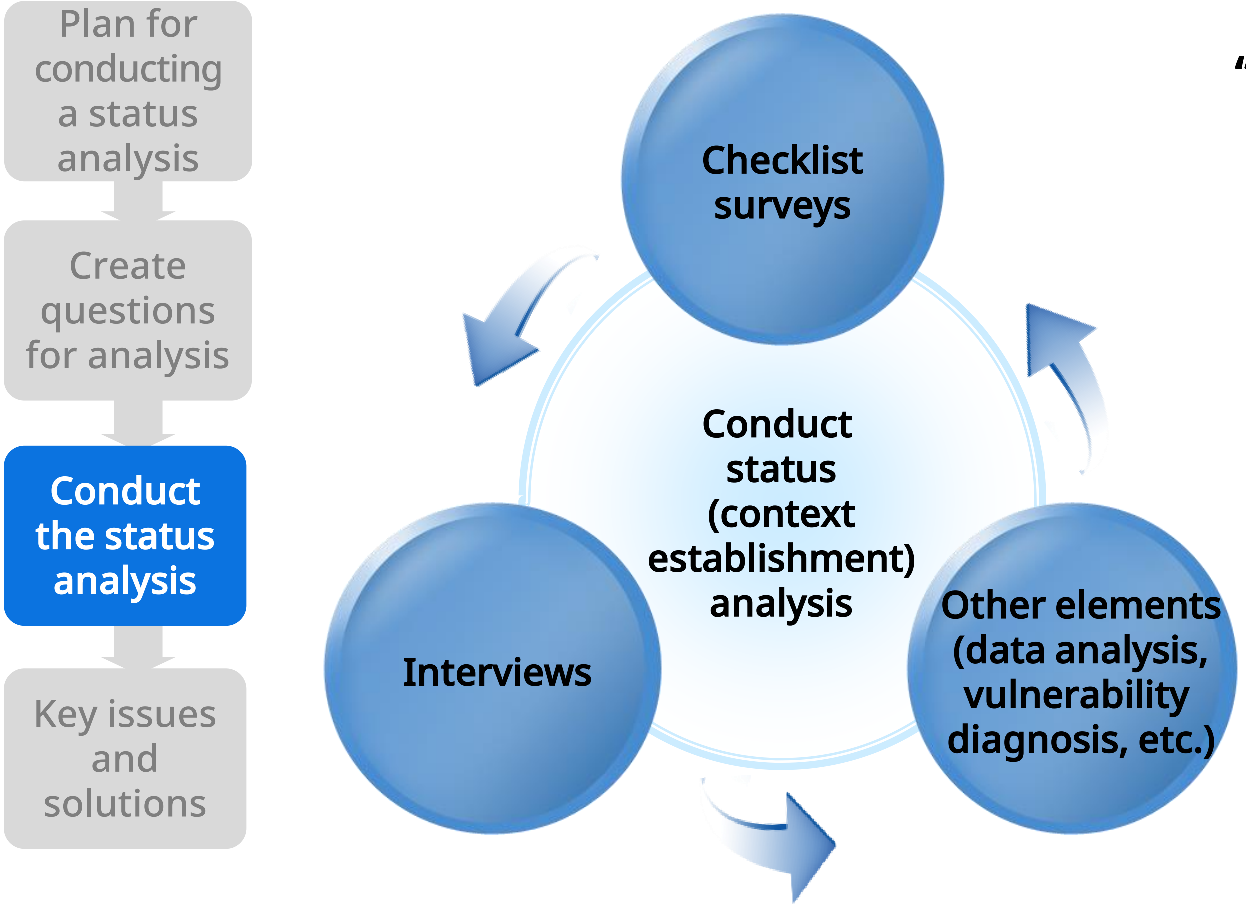
SAMPLE

Cri	Division		Question	Confirm		Reason for rating	Rationale / Record
				Recorded	Fulfiled		
ISO 27001	Secure Zones	A11.1.1-1	Do you have defined policies for the physical security of your workplace?				
		A11.1.1-2	Do you have physical information security controls in place to protect the perimeter of your business?				
		A11.1.1-3	Is each physical security zone separated by criticality?				
	…	…	…	…	…	…	…
Privacy laws	Article 29	1.1	Do you have a privacy policy or internal control plan in place?				
…	…	…	…	…	…	…	…

Gap analysis

Conduct a status analysis (1/3)

- You can conduct the analysis in any combination of the following.



Plan for conducting a status analysis
Create questions for analysis
Conduct the status analysis
Key issues and solutions
Checklist surveys
Conduct status (context establishment) analysis
Interviews
Other elements (data analysis, vulnerability diagnosis, etc.)

"What is important is

from an expert's perspective

to know
(evidence)

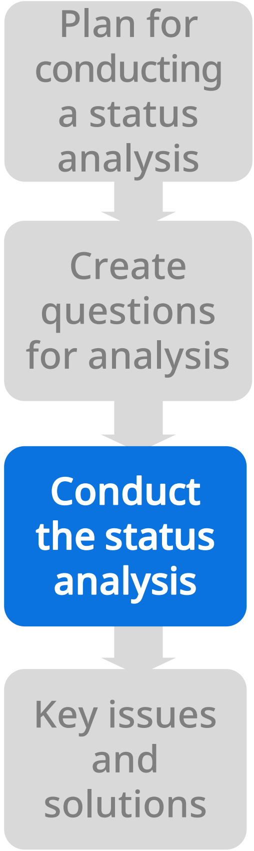
things as they are
(fact)

"as objective as possible."
(baseline)

Gap analysis

Conduct a status analysis (2/3)

- Criteria for evaluating health analytics



Plan for conducting a status analysis

Create questions for analysis

Conduct the status analysis

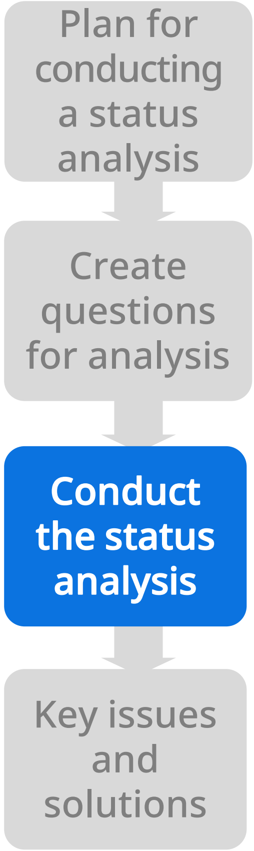
Key issues and solutions

Satisfied	evaluation criteria for test questionnaire	Evaluation criteria for control items
Yes (satisfied)	▪ The control is implemented ▪ Relevant regulations/guidelines/evidence exist ▪ Controls are being substantially implemented	▪ All checkboxes in the control items evaluated as Y
Partial (partially satisfied)	▪ Controls are partially implemented ▪ Relevant regulations/guidelines and supporting data are partially available ▪ Controls are partially implemented	▪ P or N exists among the checkboxes contained in the control items
No (unsatisfied)	▪ Few controls are implemented ▪ Regulations/guidelines, little evidence ▪ Not being implemented in practice	▪ All checkboxes in the control items evaluated to N
Not Applicable (N/A)	▪ Controls are not satisfactory for the job specifications (not applicable)	▪ All checkboxes in the control items rated N/A

Gap analysis

Conduct a Status Analysis (3/3)

- Criteria for evaluating health analytics



Plan for conducting a status analysis

Create questions for analysis

Conduct the status analysis

Key issues and solutions

Control	Y/P/N/NA	Comments
3.1 Information Security Policy	P	
4.1 Information Security Organization	P	
4.3 Outsourcing	N	
5.1 Accountability for assets	NA	
5.2 Information classification		

Apply area-specific statistics

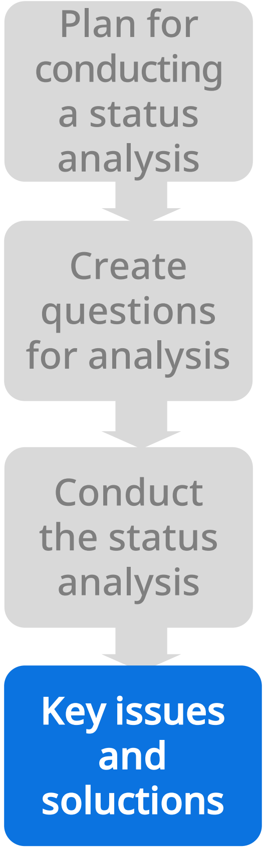
ISMS coverage rate : 71

Domains	Information Security Gap Analysis Results	Evaluation
A.5 Infosec Policy	40% 60%	Good
A.6 Infosec Organization	70% 9% 21%	Good
A.7 Asset classif. and control	80% 20%	Insufficient
A.8 Human security	77% 23%	Good
A.9 Physical/Envir. Security	69.2% 23.1% 7.7%	Good
A.10 Commn. and operations	64.5% 25.8% 9.7%	Good
…		

Gap analysis

Identify key issues and improvements

- Identify improvements based on key issues (example)

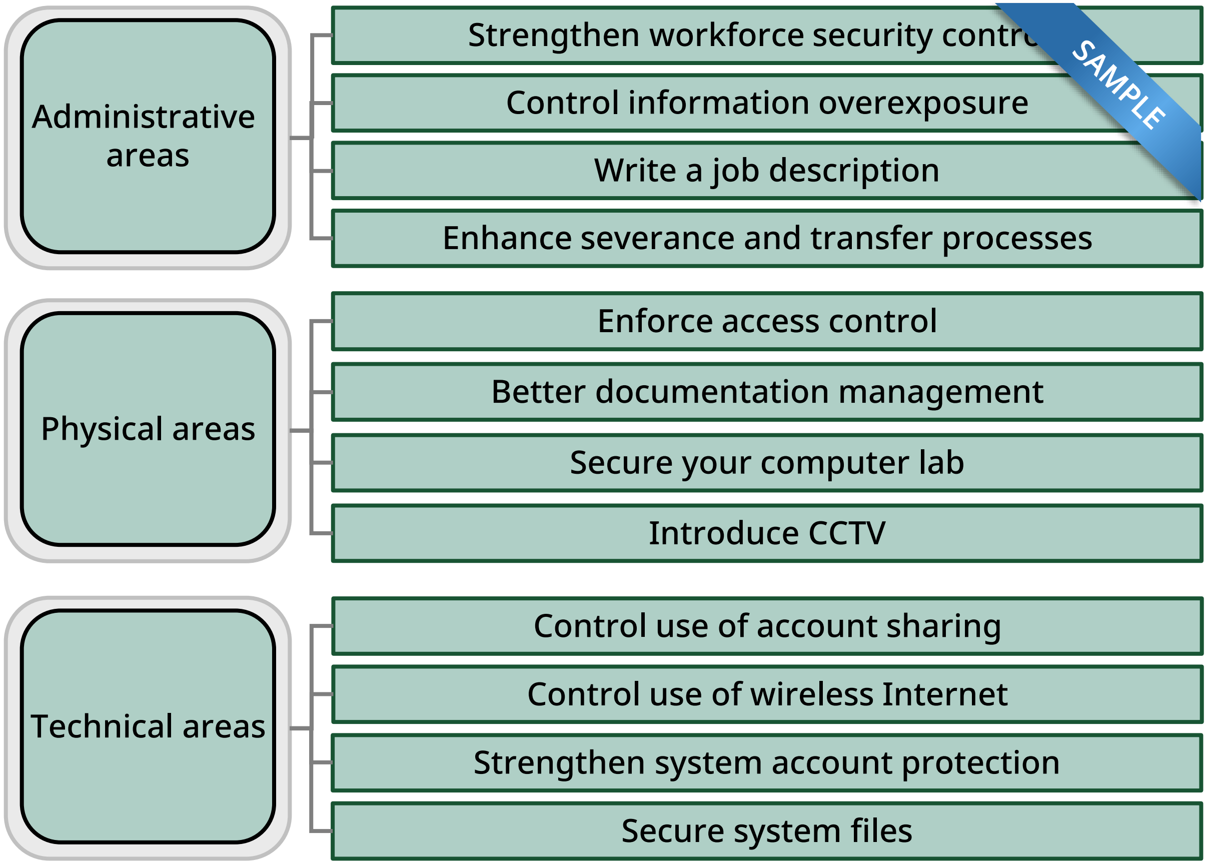


Plan for conducting a status analysis

Create questions for analysis

Conduct the status analysis

Key issues and solutions



Administrative areas

- Strengthen workforce security contr
- Control information overexposure
- Write a job description
- Enhance severance and transfer processes

Physical areas

- Enforce access control
- Better documentation management
- Secure your computer lab
- Introduce CCTV

Technical areas

- Control use of account sharing
- Control use of wireless Internet
- Strengthen system account protection
- Secure system files

Gap analysis

Identify and categorize information assets

All assets that are considered to impact the security of information within the project scope should be identified and can be categorized as follows.

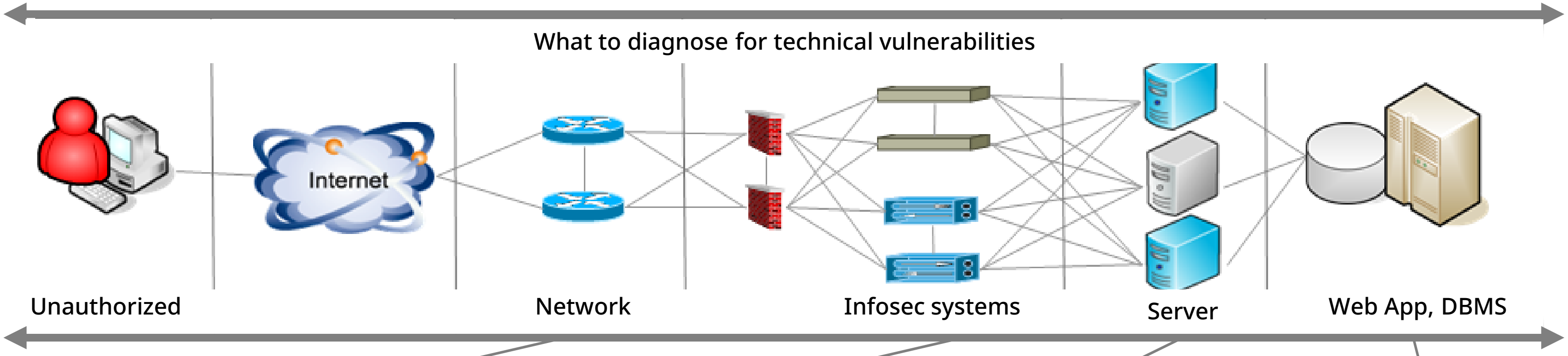
- Information asset classification (example)

Division	Classification	Detail
Information	Sales information, management reporting information, R&D information, etc.	Information in business systems, file servers
Record	Classification standards, offline Documents	Contracts, privacy pledges, etc.
Physical assets	File servers, systems (servers), network equipment, security systems, UPSs, thermo-hygrostats, work PCs, laptops, etc.	Hardware equipment, including IT equipment, PCs/laptops, file servers, etc.
Software	Purchased S/W : Oracle 8i, Windows XP, etc. Self-developed S/W : R&D project system, other business systems	Licensed S/W (Excludes randomly installed S/W, shareware, etc.)
Workforce	Workforce by dept, contractor (outsourced) staff	Contractor staff : include only full-time workers
Company reputation	Trademarks, brand names, and more	IR, tangible and intangible assets that represent your company's image
Service	Maintenance, power, IDC, and more	Equipment maintenance, including networks, servers, PCs, and more Power to physical space

Gap analysis

Gap analysis includes not only the implementation of controls, but also the diagnosis of technical vulnerabilities in each area of the information system.

- Diagnose technical vulnerabilities in each area of the info system


What to diagnose for technical vulnerabilities

Unauthorized

Network

Infosec systems

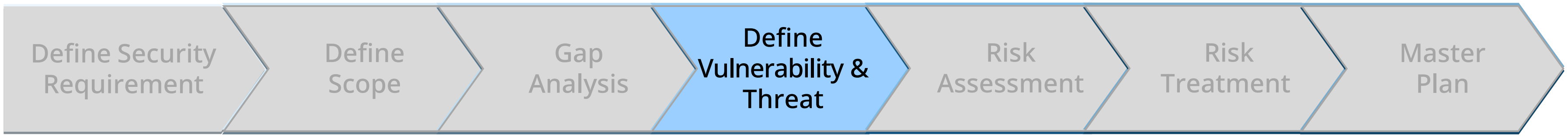
Server

Web App, DBMS

	Diagnostics area: Network	Diagnostics area : security systems	Diagnostics area : server.	Diagnostics: Web, DBMS, etc.
How to diagnose	• Utilize equipment-specific checklists • Manually diagnose configuration information • Interview N/W equipment operations managers • Review operational increments	• Utilize security device-specific checklists • Review security policies (rule sets) • Interview security equipment operations managers • Review operational increments	• Utilize OS-specific checklists • Use OS-specific scripted automated diagnostics or vulnerability scanners • Interview server operations manager • Review operational increments	• Utilize checklists for WEB, DB, and more • Use automated script diagnostics or vulnerability scanners for WEB, DB, etc. • Interview operations Managers • Review operational increments

Define vulnerabilities and threats

Risk assessment-define vulnerabilities and threats



Define Security Requirement

Define Scope

Gap Analysis

Define Vulnerability & Threat

Risk Assessment

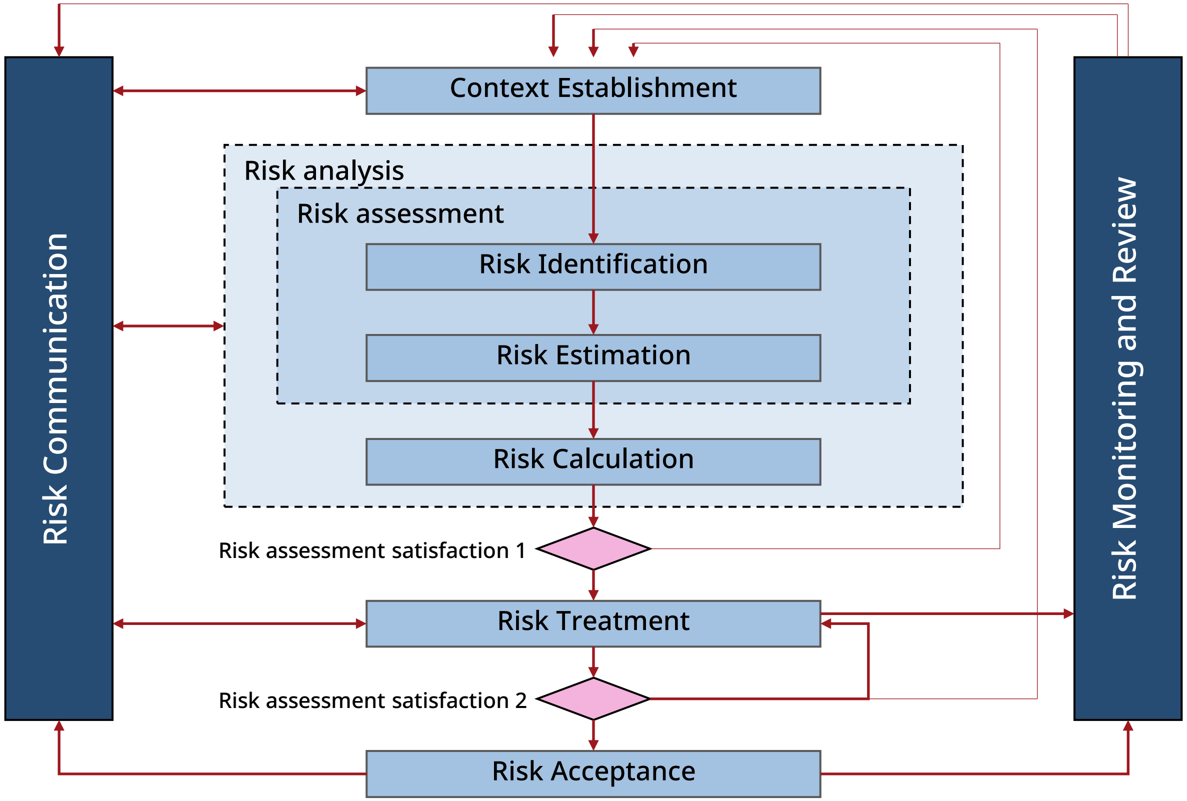
Risk Treatment

Master Plan

Division	Detail
Overview	• Define the threats and vulnerabilities of your information assets through a landscape analysis
Performance	• List asset-specific threats and vulnerabilities identified by the gap analysis • Enumerate relevant threats to each asset, its value, and associated vulnerabilities • Create risk scenarios by mapping assets to threats and vulnerabilities
Performer	• Consultant(s)
Deliverables	• List of vulnerabilities and threats • Risk Assessment Sheet

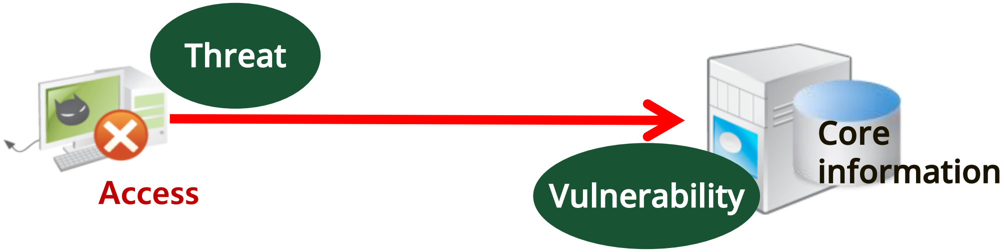
Define vulnerabilities and threats

ISO/IEC 27005 provides a risk management process that is followed in almost all countries and relevant standards.



Define vulnerabilities and threats

- Vulnerabilities are weaknesses, e.g., security flaws in the system.
  - Comparison : vulnerability vs. weakness
  - Threats are anything that could cause damage, harm, or loss to an organization's assets by exploiting those assets' vulnerabilities.



Define vulnerabilities and threats

- Sources of information vulnerabilities and threats

Internal corporate resource

- Security incident reports
- Results of system audits & security reviews
- Observation of business processes & working/operating conditions
- Talks of asset/system owners & users

External database and website resources

- CERT (www.cert.org)
- SANS (www.sans.org)
- CIAC (www.ciac.llnl.gov/ciac)
- AUSCERT (www.auscert.org.au)
- SURFNET (http://cert,surfnet.nl/home-eng.html)
- NIST (http://icat.nist.gov/icat.taf)
- FIRST (www.first.org)
- KISA (www.kisa.or.kr)

Define vulnerabilities and threats

Risk assessment - defining vulnerabilities and threats

- Threat classification examples

Type	Division	Example
Human (intentional)	▪ Theft	▪ Leakage of confidential information, review of system/computer resources
	▪ Communication penetration	▪ Eavesdropping, surveillance, system hacking, infor leakage/deletion/ tampering by viruses, virus dissemination, system shutdown by viruses
	▪ Resource misuse	▪ Info piracy, use of illegal software, and personal use of resources
	▪ Info/System compromise	▪ Deletion/alteration of information, system destruction
	▪ Misuse of authorized access	▪ User misuse of privileges, administrator abuse of privileges, maintenance/ operations personnel abuse of privileges
Human (accident/ mistake)	▪ Lost	▪ Leakage of confidential information, loss of system/computer resources
	▪ Viral infections	▪ Information leakage/deletion/tampering by viruses, virus dissemination, system shutdown by viruses
	▪ Info/system compromise	▪ Deleted/edited information, input errors, system crashes
	▪ Misuse of authorized access	▪ User error, maintenance personnel error, operations personnel error
System	▪ Software failures	▪ Software malfunctions, stops
	▪ Hardware failures	▪ Hardware malfunction, stop
Environment	▪ Internal envir. Disasters	▪ Water damage (broken conduit, vault), fire (arson), air pollution, environmental contamination, extreme temperature rise/drop
	▪ External envir. disasters	▪ Water disaster, fire, earthquake, lightning strike, storm, air pollution, environmental pollution, extreme temperature rise/drop
	▪ Power Failure	▪ Power outage, overvoltage, undervoltage, UPS failure, diesel generator failure
	▪ Communication failures	▪ Service provider's communication service failure, bad line

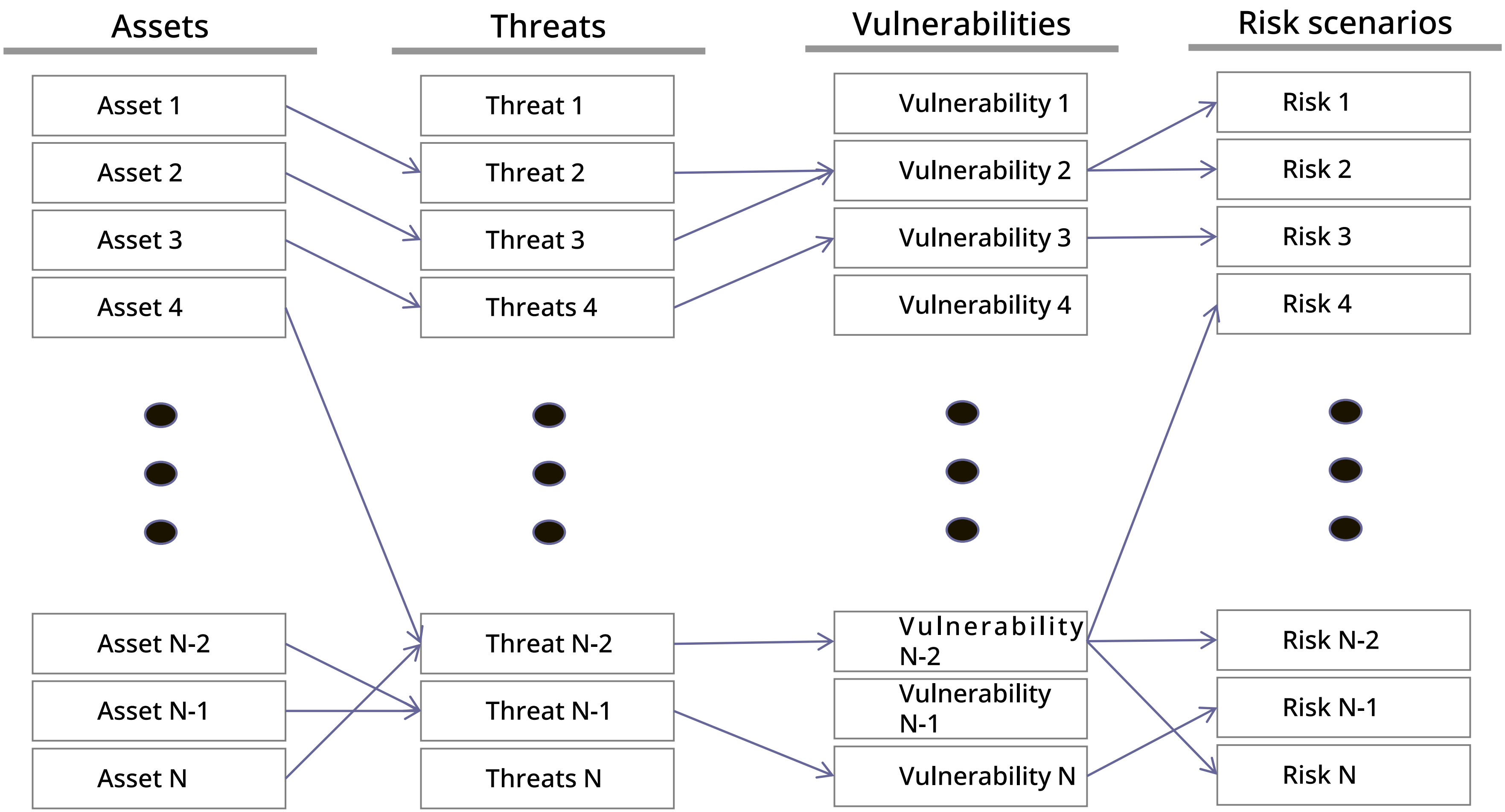
Define vulnerabilities and threats

- Threat classification examples

Type	Division	Example
Admin	▪ Operational vulnerabilities	▪ Lack of/inadequate business procedures, inadequate IT and security budgets, inadequate maintenance of equipment, lack of/inadequate training on system operations, backup resources and systems and services, lack of/inadequate business continuity planning, lack of/inadequate procedures for moving assets in and out, and lack of/inadequate asset classification.
	▪ Weaknesses in infosec mgmt.	▪ Lack of infosec organization/dedicated staff, infosec policies/guidelines, incident mgmt. procedures, security audits, discipline for security violations, and infosec requirements in outsourcing and third-party contracts; inadequate assignment of security responsibilities and authorizations, lack of/inadequate infosec training
	▪ Human vulnerabilities	▪ Absence/inadequate use of staff, lack of supervising regular and third-party employees, lack of infosec awareness, inadequate hiring procedures
Technical	▪ Computer/ commn. related vulnerabilities	▪ Lack of/inadequate authentication mechanisms, access controls, audit trails, complex user interfaces, improper disposal and reuse of storage media, lack of/inadequate change controls, inadequate protection of password tables, inadequate software patch mgmt
	▪ Infosec system-related vulnerabilities	▪ Lack of/inadequate information protection systems (antivirus, firewall, IDS, cryptographic products, etc.), poor management of information protection system upgrades, etc., and poor cryptographic key management.
	▪ System dev.-related vulnerabilities	▪ Unsegregated dev/test/op facilities, insufficient enforcement of security requirements, and lack of change control/shape management
Physical/ Envir.	▪ Physical vulnerabilities	▪ Absence of access control systems/staff, lack of locks on doors/windows, improper location of equipment, etc.
	▪ Environmental vulnerabilities	▪ Lack of constant temperature and humidity, lack of HAVC systems, lack of fire suppression, and location vulnerable to flooding

Define vulnerabilities and threats

- Risk scenarios

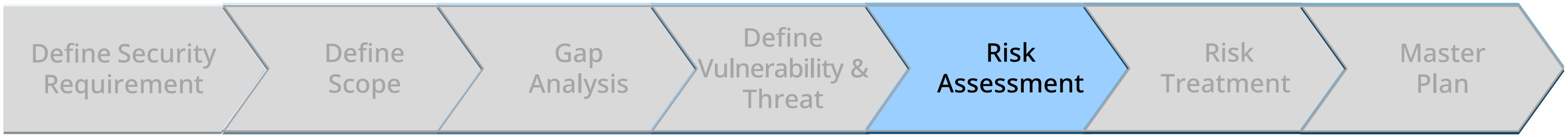


Define vulnerabilities and threats

- Risk scenarios

Division	Classif.	Sub-classif.	Threat and vulnerability	Element (C, I, A)			Dept.	Rep.
Info	App info	Business System	Lack of criteria for critical and sensitive information to protect, such as encryption, can lead to information leakage	C				
			Administrators can look up the passwords of regular users. This allows them to impersonate users and leak information.	C				
			Potential for information leakage by sharing business system administrator account with business system IT personnel	C				
			Potential for information leakage/modification/deletion due to lack of information about the discovery of vulnerabilities in business systems and inability to verify that vulnerable business systems have been properly remediated	C	I	A		
			Potential for information leakage/tampering/deletion by over-granting users write, delete, and view privileges	C	I	A		
			Potential for lawsuits if you fail to destroy customer information provided to you to serve a customer after the service has ended and you no longer have a reason to keep it	C				
			Information leakage/tampering/deletion due to lack of or inadequate management procedures, such as immediate removal of retiree/transfer privileges	C	I	A		
			Potential for information leakage due to vacancies (vacation, training, etc.) of business system users and sharing of access IDs (accounts) among people in the team (more than one person using the same ID)	C				

Risk assessment



Define Security Requirement

Define Scope

Gap Analysis

Define Vulnerability & Threat

Risk Assessment

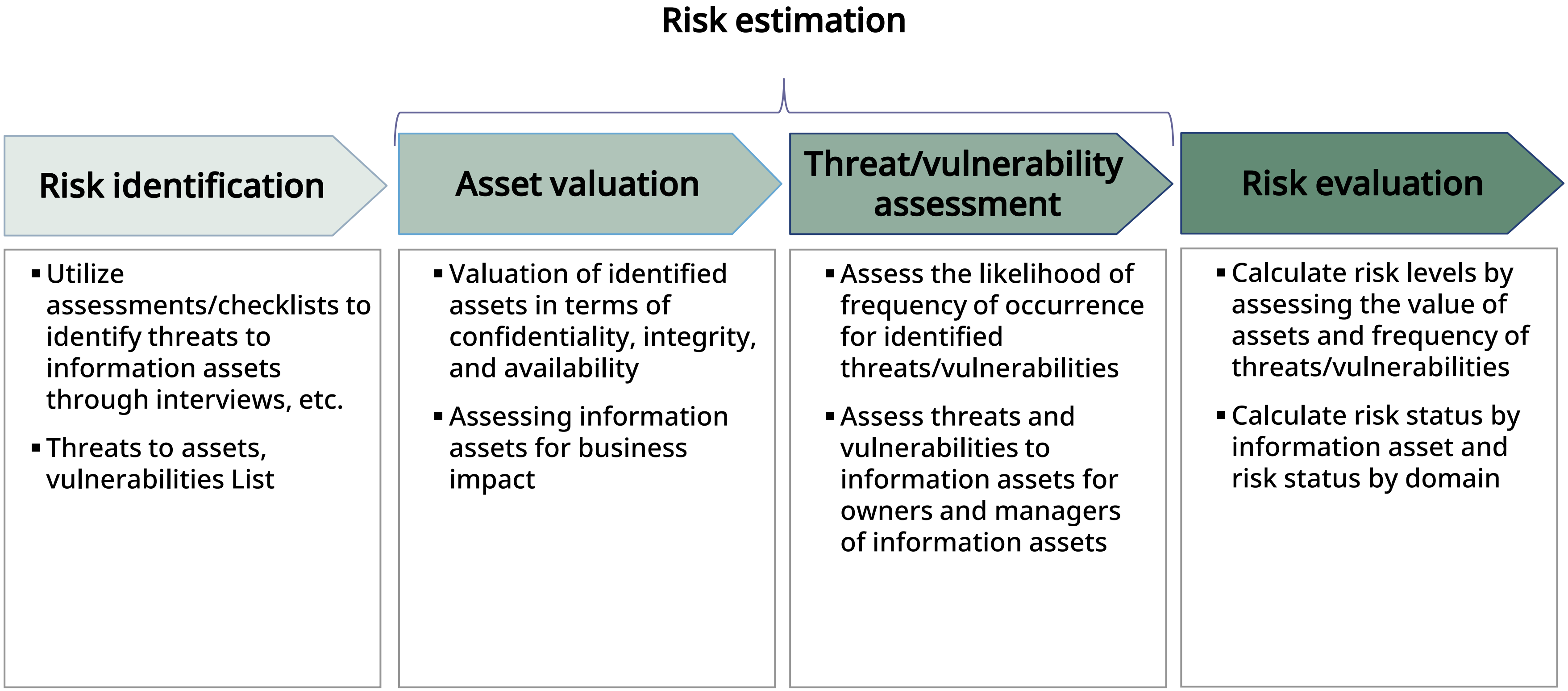
Risk Treatment

Master Plan

Separation	Details
Overview	• Calculate risk by estimating the value of information assets and then assessing the level of risk posed by the threats and vulnerabilities in those assets.
Performance	• Assess by the information asset owner or the person most knowledgeable about the value of the asset • Calculation of confidentiality, integrity, and availability risk based on information asset risk scenarios • Choose the right methodology for your organization's size and level of security requirements is critical to risk assessment • Analyze risk by asset/area based on the risk assessment
Performer	• Information asset owner • Consultant(s)
Deliverables	• Risk analysis report

Risk assessment

The risk level is calculated by assessing the expected damage if an information asset is breached, tampered with, or deleted, and by evaluating the likely frequency of occurrence of the threats and vulnerabilities posed by key information assets at that time.



Risk estimation

Risk identification

- Utilize assessments/checklists to identify threats to information assets through interviews, etc.
- Threats to assets, vulnerabilities List

Asset valuation

- Valuation of identified assets in terms of confidentiality, integrity, and availability
- Assessing information assets for business impact

Threat/vulnerability assessment

- Assess the likelihood of frequency of occurrence for identified threats/vulnerabilities
- Assess threats and vulnerabilities to information assets for owners and managers of information assets

Risk evaluation

- Calculate risk levels by assessing the value of assets and frequency of threats/vulnerabilities
- Calculate risk status by information asset and risk status by domain

Risk assessment

Calculating risks

- Assess information assets, quantify risk using threat/vulnerability analysis results
- Calculate risk for confidentiality, integrity, and availability
- Calculate risk status by information asset and risk status by domain

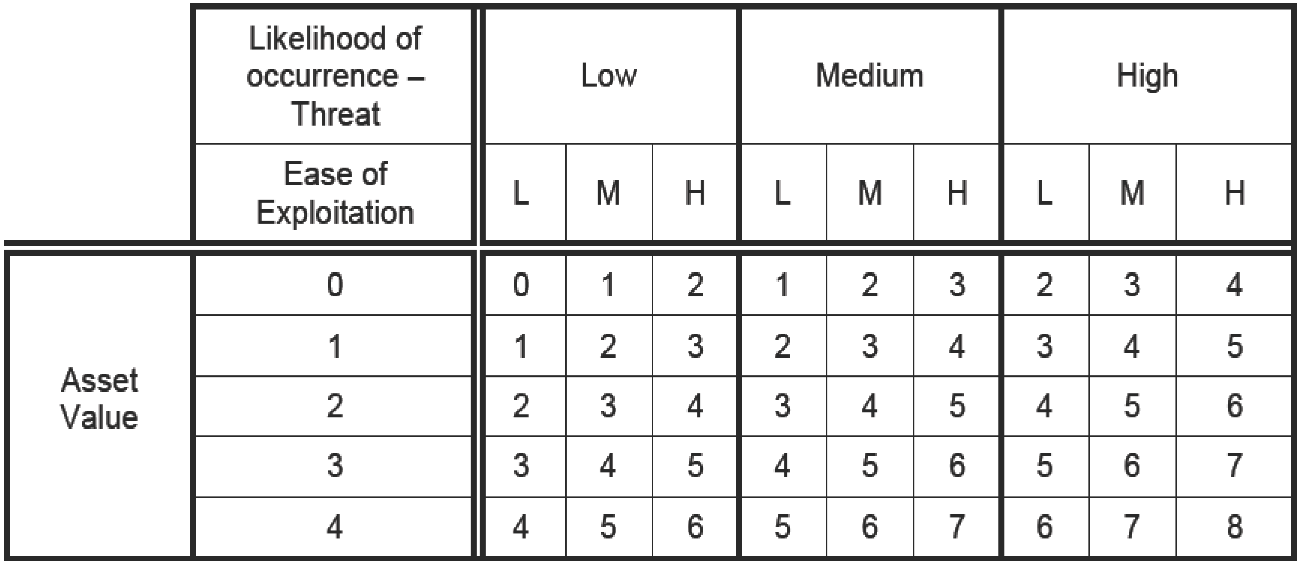
- The assessment includes
  - The value of the asset
  - The level of associated vulnerabilities
  - The likelihood of relevant threats
  - Existing and planned controls that protect the asset

Risk assessment

The traditional Risk Value calculation is

Asset Value + (x) Threat Value + (x) Vulnerability value

Table E.1 a)



	Likelihood of occurrence – Threat	Low			Medium			High		
	Ease of Exploitation	L	M	H	L	M	H	L	M	H
Asset Value	0	0	1	2	1	2	3	2	3	4
	1	1	2	3	2	3	4	3	4	5
	2	2	3	4	3	4	5	4	5	6
	3	3	4	5	4	5	6	5	6	7
	4	4	5	6	5	6	7	6	7	8

- Advantages and disadvantages
  - Advantages : threat and vulnerability assessments can be fine-tuned in detail
  - Disadvantages : hard for assessors to accurately understand and assess threats & vulnerabilities

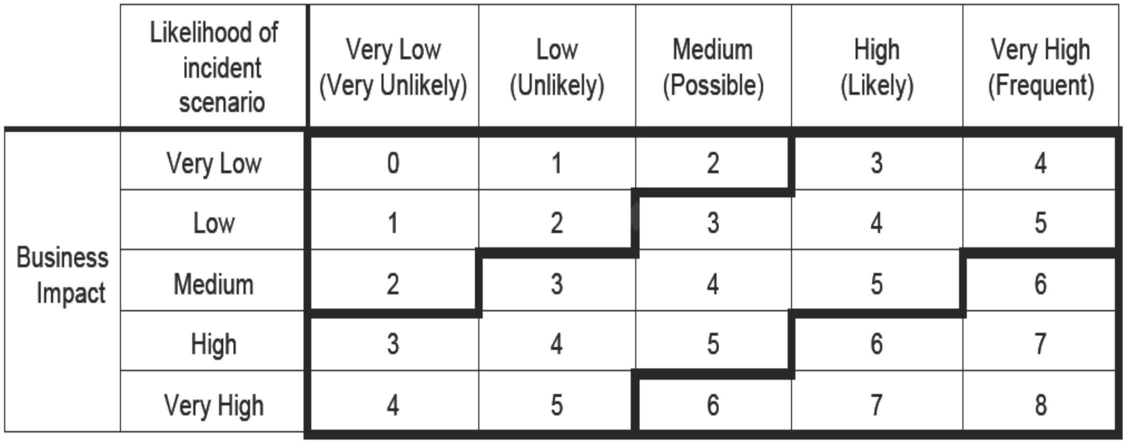
Risk assessment

Risk Scenario Risk Value formula =

Asset Value + (Concern1) x 2)

- Risk scenario : concepts such as threat value and vulnerability value, risk value can be derived without distinguishing between threats and vulnerabilities, which is defined as concern, and the value that indicates the degree of concern is called concern value.

Table E.1 b)

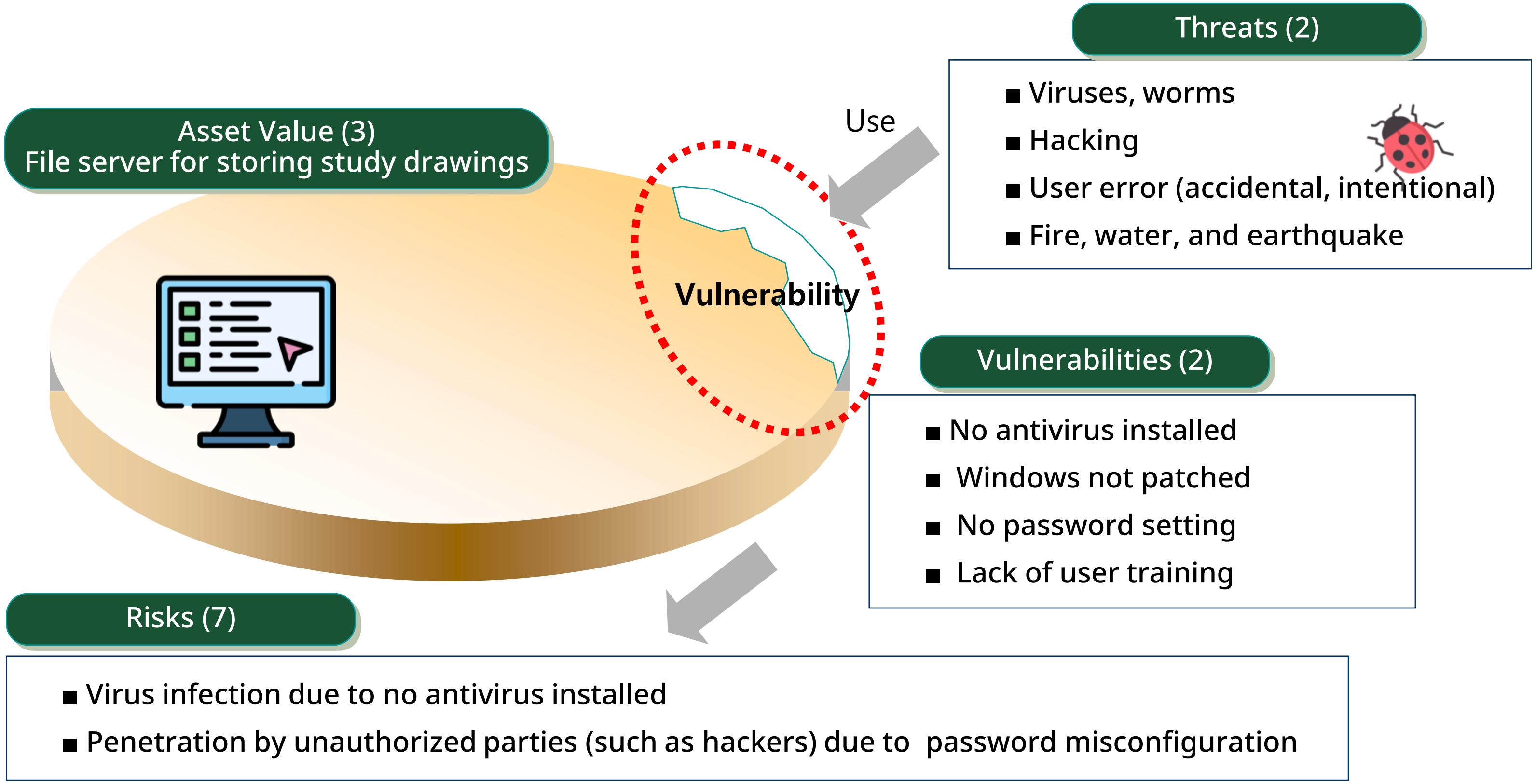


	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

- Advantages and disadvantages
  - Advantages : threat and vulnerability assessments can be fine-tuned in detail
  - Disadvantages : hard for assessors to accurately understand and assess threats & vulnerabilities

Risk assessment

- Threats exploit vulnerabilities to cause damage to assets.



Asset Value (3)
File server for storing study drawings

Threats (2)

- ■ Viruses, worms
- ■ Hacking
- ■ User error (accidental, intentional)
- ■ Fire, water, and earthquake

Vulnerabilities (2)

- ■ No antivirus installed
- ■ Windows not patched
- ■ No password setting
- ■ Lack of user training

Risks (7)

- ■ Virus infection due to no antivirus installed
- ■ Penetration by unauthorized parties (such as hackers) due to password misconfiguration

Risk assessment

Traditional risk value calculation methods

- Risk of information leakage or tampering due to a virus infection on a fileserver that does not have antivirus installed (Risk Scenario Attributes C, I)
  - Risk (7) = Asset value (3) + Threats (2) + Vulnerabilities (2)

Threat level		Low (1)			Medium (2)			High (3)		
Vulnerability level		L(1)	M(2)	H(3)	L(1)	M(2)	H(3)	L(1)	M(2)	H(3)
Asset value	L(1)	3	4	5	4	5	6	5	6	7
	M(2)	4	5	6	5	6	7	6	7	8
	H(3)	5	6	7	6	7	8	7	8	9

Group Co.	Group Name	Asset value			Threat	Thr Value	vulnerabilities	Vul Value	Risk Value		
		C	I	A					C	I	A
Client-IF-0001	Information in fileservers	3	3	1	Newly infected and leaked/tampered with	2	No antivirus installed	2	7	7	5

Risk assessment

How to calculate risk value for risk scenarios

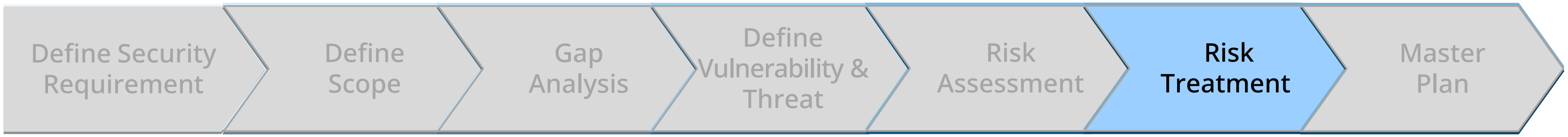
- Risk of information leakage or tampering due to a virus infection on a fileserver that does not have antivirus installed (Risk Scenario Attributes C, I)
  - Risk (7) = Asset value (3) + (Risk scenario (2) X 2)

Division		Confidentiality			Integrity			Availability		
Asset value		L(1)	M(2)	H(3)	L(1)	M(2)	H(3)	L(1)	M(2)	H(3)
Risk scenarios x 2	L(1)x 2=2	3	4	5	3	4	5	3	4	5
	M(2)x2=4	5	6	7	5	6	7	5	6	7
	H(3)x2=6	7	8	9	7	8	9	7	8	9

Group Co.	Group Name	Group value			Concern Co.	Concern	Concern Value	Risk Value		
		C	I	A				C	I	A
Client-IF-0001	Information in fileservers	3	3	1	Concern-01	New viruses infected and leaked/tampered with due to no antivirus installed	2	7	7	5

Risk treatment

Control system extablishment – reducing risks



Define Security Requirement

Define Scope

Gap Analysis

Define Vulnerability & Threat

Risk Assessment

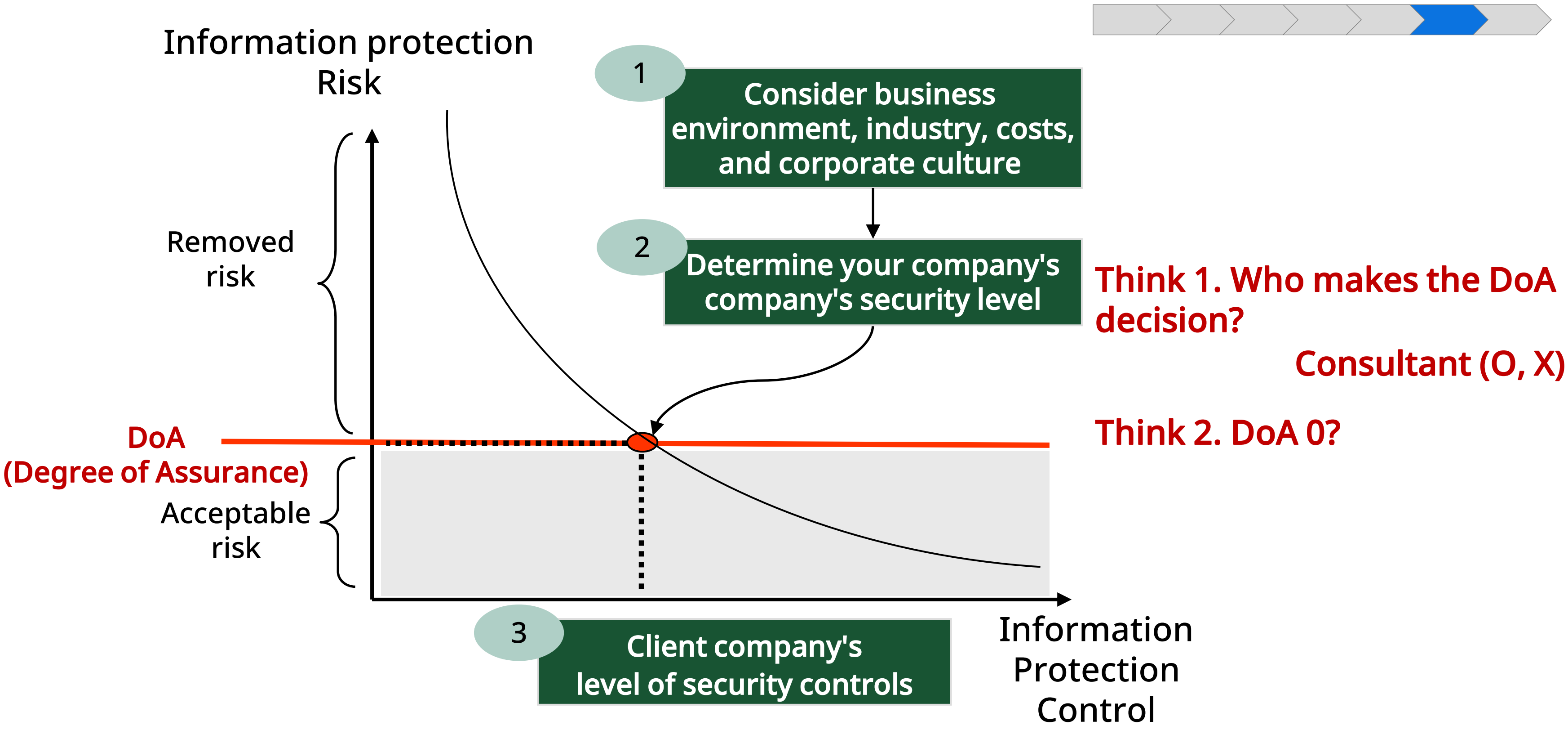
Risk Treatment

Master Plan

Division	Detail
Overview	• Define the level of "risk to be managed" based on the risk assessment and manage the risk to reduce it to an "acceptable risk" level.
Performance	• Determine Degree of Assurance (DoA) (Acceptable Risk vs. Unacceptable Risk) • Select controls for unacceptable risk • Determine 3P 1T or management, physical, and technical improvements to reduce risk • Compare selected controls with other information security countermeasures to identify effective improvements
Performer	• Project representative(s) • Consultant(s)
Deliverables	• Risk treatment plan • Privacy policy, guidance for improvements (draft)

Risk treatment

Degree of Assurance (DoA) is the level of risk an organization is willing to accept for risks identified in risk analysis.


Information protection
Risk
Removed risk
DoA
(Degree of Assurance)
Acceptable risk
1
Consider business environment, industry, costs, and corporate culture
2
Determine your company's company's security level
3
Client company's level of security controls
Information Protection Control

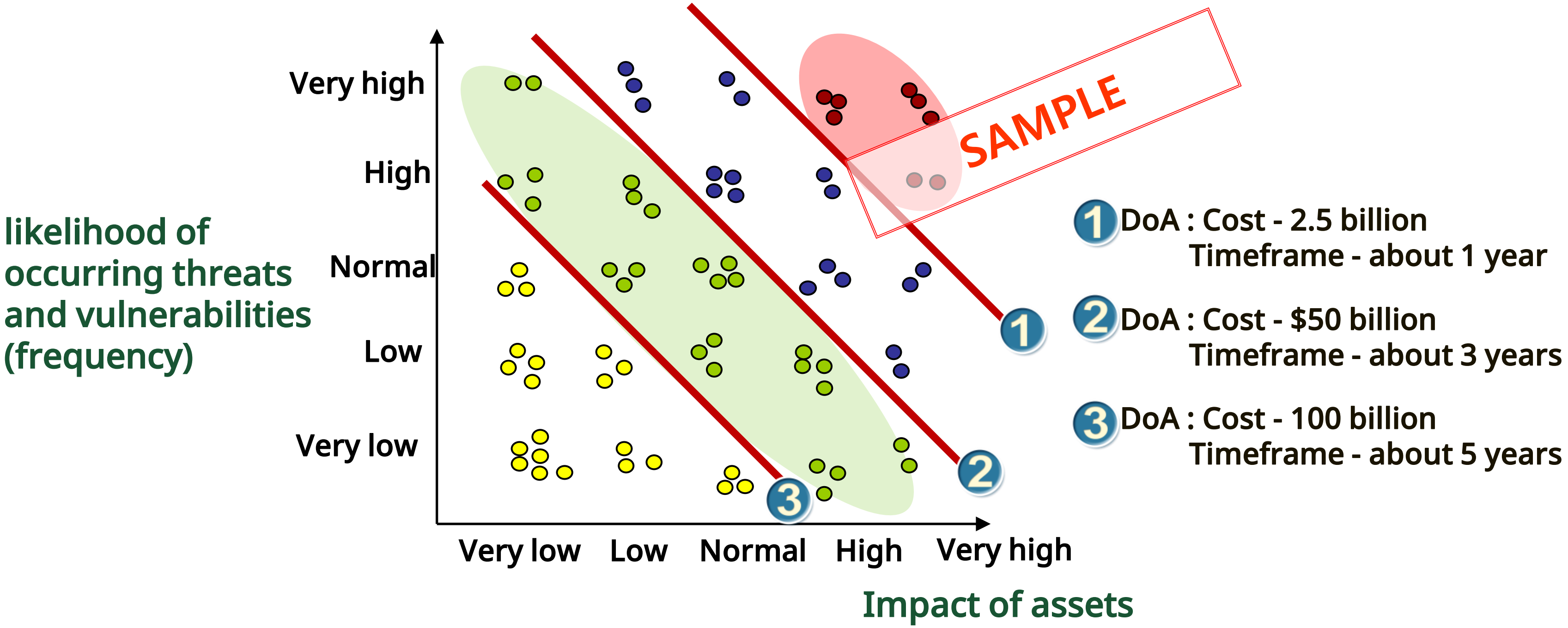
Think 1. Who makes the DoA decision?

Consultant (O, X)

Think 2. DoA 0?

Risk treatment

- How does a consultant determine DoA in infosec consulting?
  - Method 1 : Verbally discuss with the customer
  - Method 2 : Present a risk number that requires action
  - Method 3 : Outline the cost and timeframe of actions to be taken according to the DoA setting



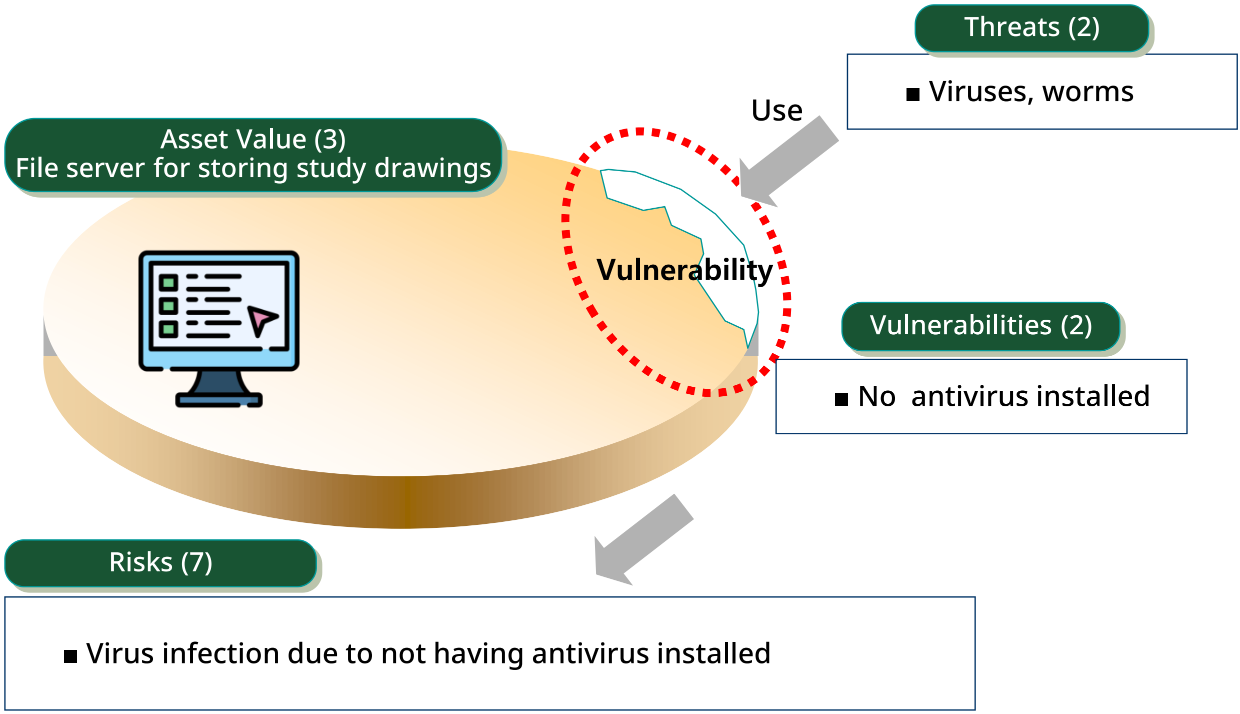
1 DoA : Cost - 2.5 billion
Timeframe - about 1 year

2 DoA : Cost - $50 billion
Timeframe - about 3 years

3 DoA : Cost - 100 billion
Timeframe - about 5 years

Risk treatment

Degree of assurance



Threats (2)

- Viruses, worms

Use

Asset Value (3)
File server for storing study drawings

Vulnerabilities (2)

- No antivirus installed

Risks (7)

- Virus infection due to not having antivirus installed

Threat level		Low (1)			Medium (2)			High (3)		
Vulnerability level		L(1)	M(2)	H(3)	L(1)	M(2)	H(3)	L(1)	M(2)	H(3)
Asset value	L(1)	3	4	5	4	5	6	5	6	7
	M(2)	4	5	6	5	6	7	6	7	8
	H(3)	5	6	7	6	7	8	7	8	9

Risk treatment

- Reduce risks

Threat Level		Low (1)			Medium (2)			High (3)		
Vulnerability Level		L(1)	M(2)	H(3)	L(1)	M(2)	H(3)	L(1)	M(2)	H(3)
Assets Value	L(1)	3	4	5	4	5	6	5	6	7
	M(2)	4	5	6	5	6	7	6	7	8
	H(3)	5	6	7	6	7	8	7	8	9

- Threat level reduction: 1
  - Install Viruswall
- Vulnerability level reduction: 0 or 1
  - Strengthen policy enforcement, awareness training, and antivirus installation

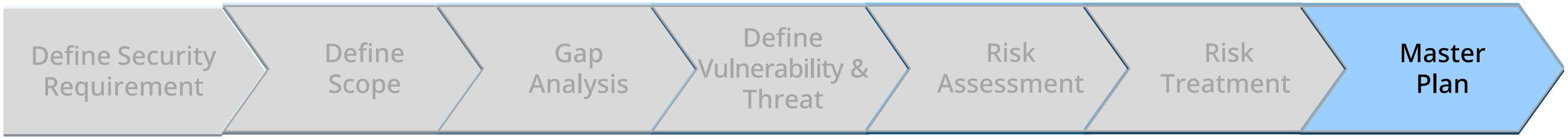
'Acceptable level of risks'

Threat level		Low (1)			Medium (2)			High (3)		
Vulnerability level		L(1)	M(2)	H(3)	L(1)	M(2)	H(3)	L(1)	M(2)	H(3)
Asset Value	L(1)	3	4	5	[illegible]	5	6	5	6	7
	M(2)	4	5	6	[illegible]	6	7	6	7	8
	H(3)	5	[illegible]	[illegible]	6	7	8	7	8	9

'Accept residual risks'

Security master plans

Information security master plan


Define Security Requirement → Define Scope → Gap Analysis → Define Vulnerability & Threat → Risk Assessment → Risk Treatment → **Master Plan**

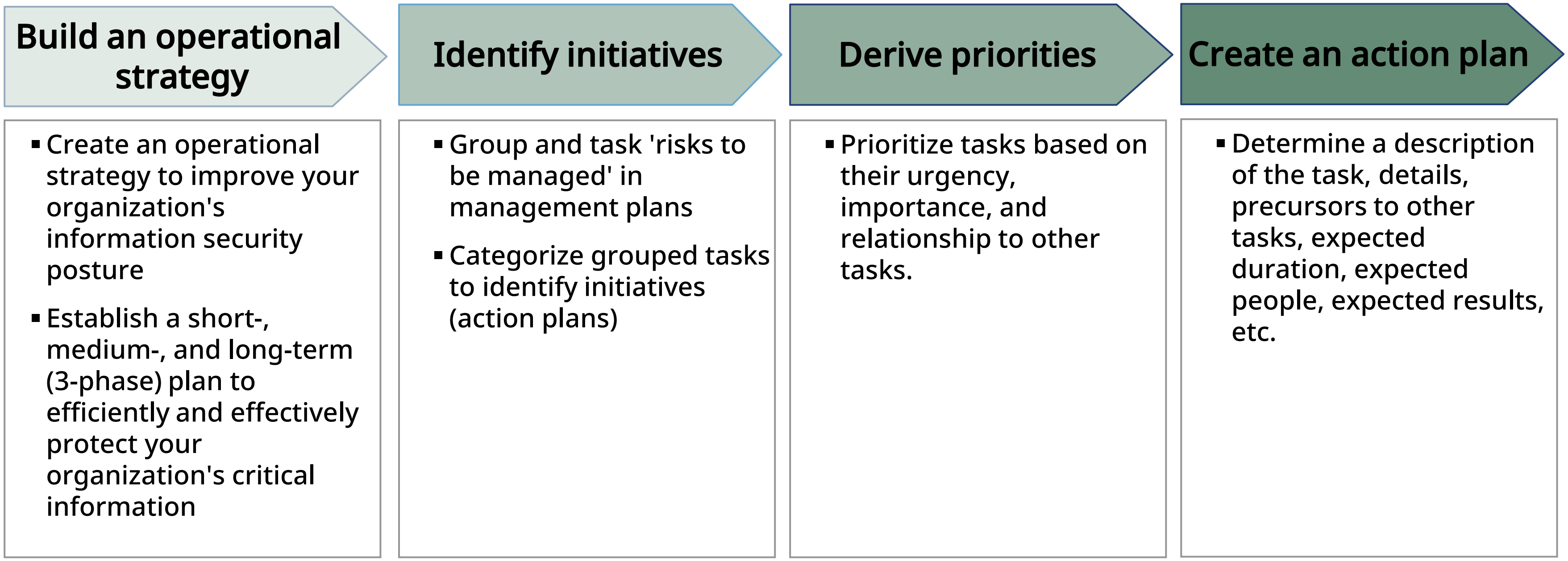
Separation	Details
Overview	• Create an action plan to implement based on the results of the risk treatment
Performance	• Establish a step-by-step strategy for operating the information security management system and define • implementation (drive) tasks to achieve the goal • Prioritize your work Create a milestone schedule • Create an implementation plan for each task (antecedent relationship between tasks, expected duration, expected manpower, expected impact, task description, etc.)
Performer	• C-suite, department heads, team leaders • Project representative(s) • Consultant(s)
Deliverables	• Master plan

Security master plans

Information security master plan

Information security master planning is an activity that defines the security strategy and vision to effectively support the organization's information security objectives, analyzes the current state and requirements for business and information technology, identifies challenges, and establishes a roadmap.

- The master plan should detail functional and technical requirements to a level that can be implemented once established, and include a deployment strategy and implementation plan.



Build an operational strategy

- Create an operational strategy to improve your organization's information security posture
- Establish a short-, medium-, and long-term (3-phase) plan to efficiently and effectively protect your organization's critical information

Identify initiatives

- Group and task 'risks to be managed' in management plans
- Categorize grouped tasks to identify initiatives (action plans)

Derive priorities

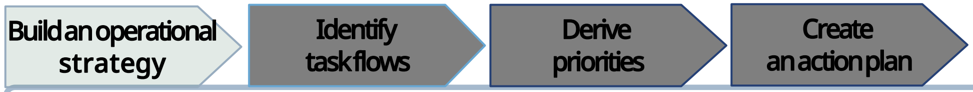
- Prioritize tasks based on their urgency, importance, and relationship to other tasks.

Create an action plan

- Determine a description of the task, details, precursors to other tasks, expected duration, expected people, expected results, etc.

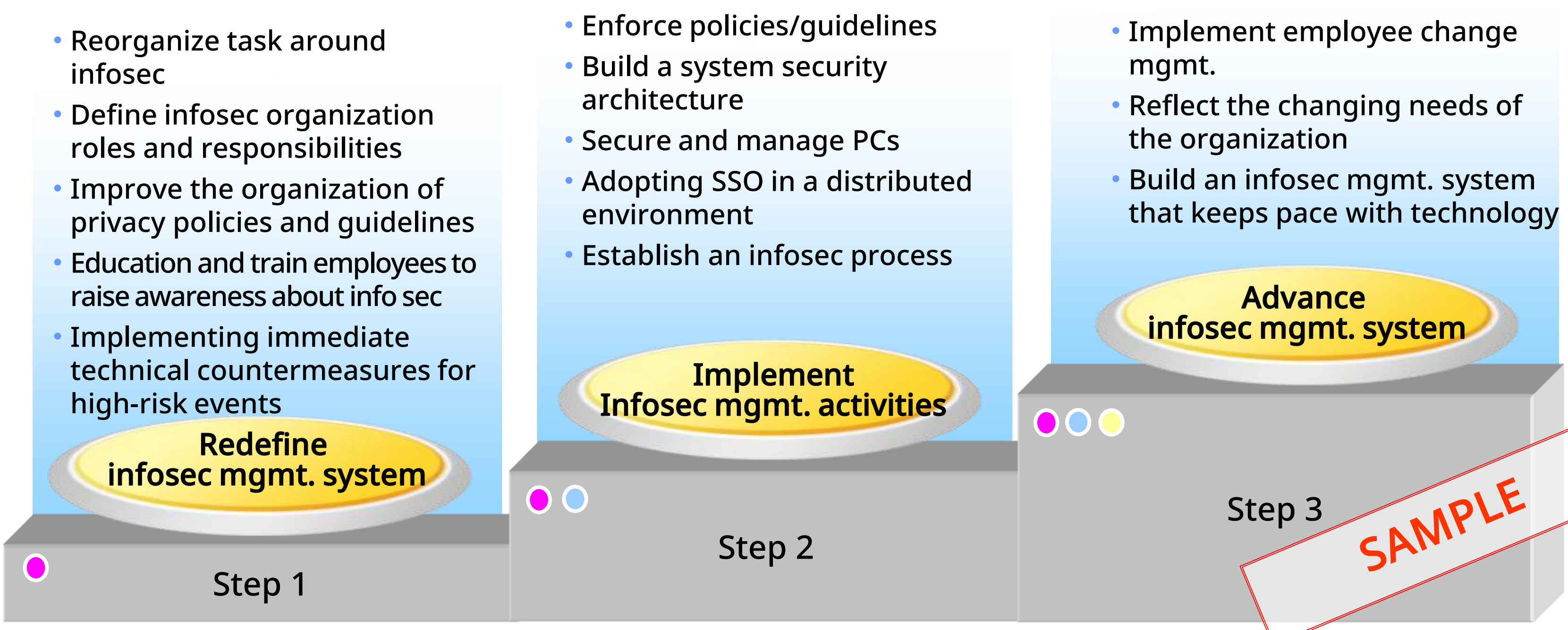
Security master plans

Building an operational strategy



Follow a phased information security operations strategy

- ✓ **Phase 1. Define an information security management system**
- ✓ **Phase 2. Implement ongoing information security management activities** and,
- ✓ **Phase 3. Enter the advanced stage of the information security management system** and and strengthen external credibility



Redefine infosec mgmt. system

- Reorganize task around infosec
- Define infosec organization roles and responsibilities
- Improve the organization of privacy policies and guidelines
- Education and train employees to raise awareness about info sec
- Implementing immediate technical countermeasures for high-risk events

Implement Infosec mgmt. activities

- Enforce policies/guidelines
- Build a system security architecture
- Secure and manage PCs
- Adopting SSO in a distributed environment
- Establish an infosec process

Advance infosec mgmt. system

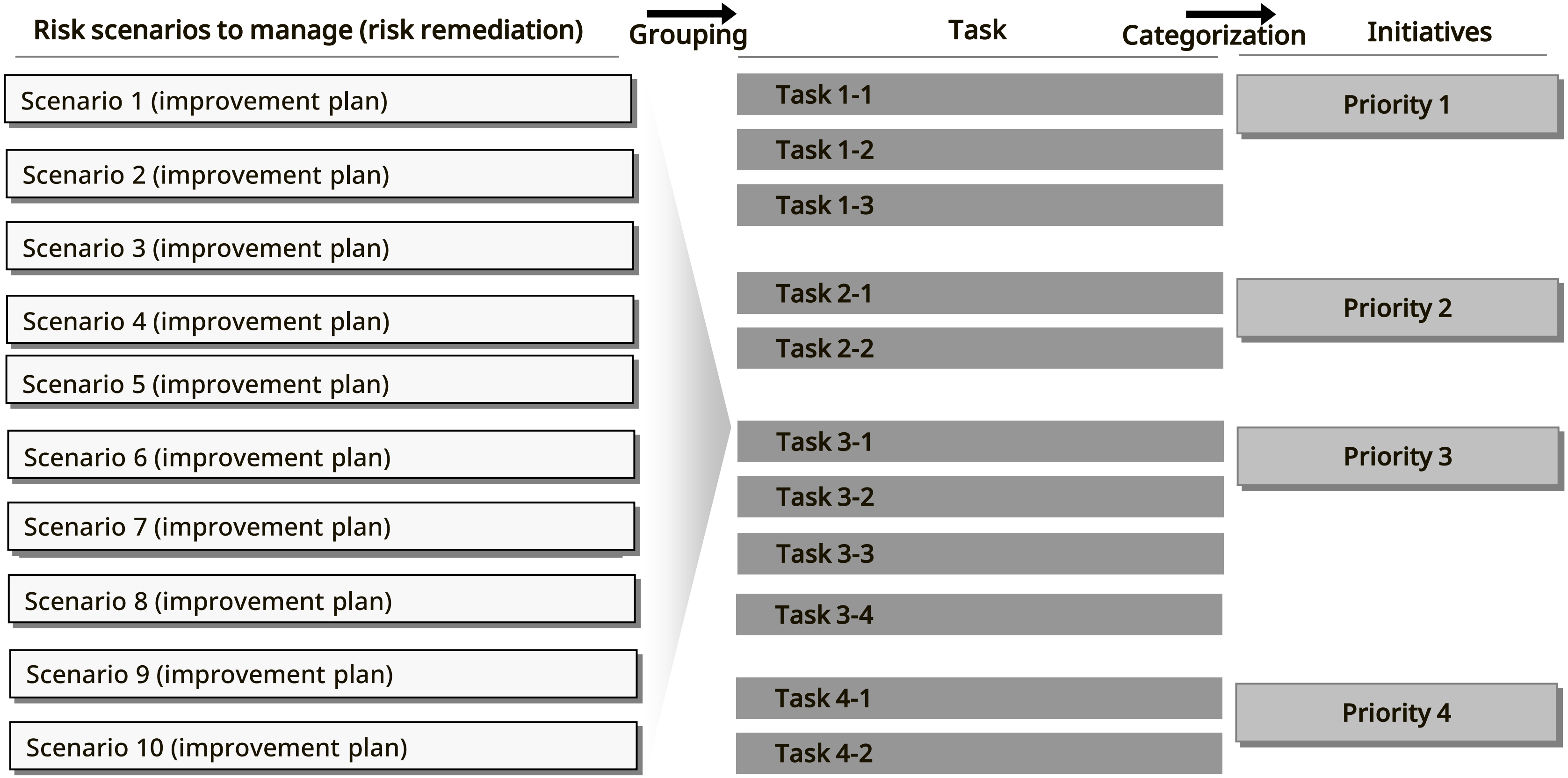
- Implement employee change mgmt.
- Reflect the changing needs of the organization
- Build an infosec mgmt. system that keeps pace with technology

Security master plans

Building an operational strategy

Build an operational strategy → Identify task flows → Derive priorities → Create an action plan

Derive activities by grouping countermeasures for prioritized risk scenarios identified through risk assessment, and establish tasks to improve information protection issues by separating them into areas.



Risk scenarios to manage (risk remediation)

Grouping

Task

Categorization

Initiatives

Scenario 1 (improvement plan)

Scenario 2 (improvement plan)

Scenario 3 (improvement plan)

Scenario 4 (improvement plan)

Scenario 5 (improvement plan)

Scenario 6 (improvement plan)

Scenario 7 (improvement plan)

Scenario 8 (improvement plan)

Scenario 9 (improvement plan)

Scenario 10 (improvement plan)

Task 1-1

Task 1-2

Task 1-3

Priority 1

Task 2-1

Task 2-2

Priority 2

Task 3-1

Task 3-2

Task 3-3

Task 3-4

Priority 3

Task 4-1

Task 4-2

Priority 4

Security master plans

Building an operational strategy

Build an operational strategy → Identify task flows → Derive priorities → Create an action plan

- **Prioritize sectors and set prioritization**

■ Security : evaluate whether implementing the countermeasure will significantly improve the security rating.

■ Urgency : evaluate how urgent the task needs to be implemented from a security perspective compared to other tasks.

■ Applicability : evaluation items on whether the investment cost of implementing the countermeasure is reasonable and whether it will be applied stably.

■ Rank 1 : 14 to 15 total points

■ Rank 2 : 12 to 13 total points

■ Rank 3 : 10 to 11 total points

■ Rank 4 : 8 to 9 total points

- **How to prioritize the initiatives (action plans)**

1) Prioritization of initiatives is assessed by security, urgency, and applicability.

2) There are five rating levels with points for each level.
- Very High : 5 points,
- High : 4 points,
- Medium : 3 points,
- Low : 2 points,
- Very Low : 1 point

3) The priority score is calculated as follows
Priority Score = Sum of evaluator scores per category

Division		Subtask	Security	Urgency	Applicability	Total Score
Improvement	1	Improving policies/guidelines	4	5	5	15
	2	Improve PC privacy guideline	4	5	3	12

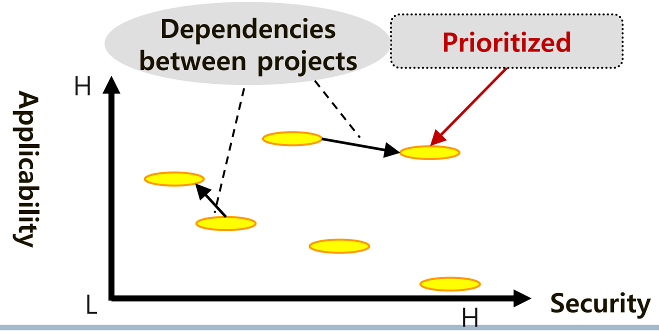
Security master plans

Building an operational strategy

Build an operational strategy → Identify task flows → Derive priorities → Create an action plan

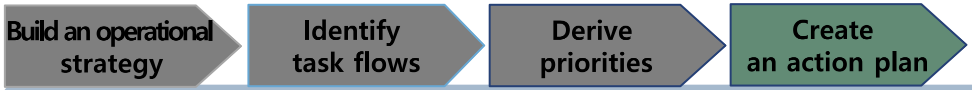
- Rating criteria

Criteria	Security	Urgency	Applicability
VH	The threat is so high that urgent action is required, or security improvements are across the board.	When security is urgent (immediacy)	Low investment, easy to implement
H	Level of security threat is high and need a quick fix	Security should be implemented but this needs short-term plans (less than a year)	Required investment is less than $100 million, or if it's somewhat easier to apply
M	Moderate risk, medium-term treatment required, or security improvements cover multiple areas.	There is a targeted deployment plan to secure (more than one year but less than two)	Required investment is less than 1-3 billion or requires some level of effort to implement
L	Level of security threat is low	Security should be implemented and this needs the mid-term plan (at least 2 but no more than 3 years)	The investment cost will be 300-500 million, or the application is difficult due to technical factors or application conditions.
VL	Level of security threat is very low, or the security enhancement applies only to a specific area.	Security should be implemented and this requires planning for the long term (3+ years)	Requires investment is large (500 million or more), or application is technically and logistically challenging.



Security master plans

Building an operational strategy


Build an operational strategy
Identify task flows
Derive priorities
Create an action plan

- Create a roadmap for the initiatives (example)

Duration / What's next	Year 1	Year 2				Year 3				Cost
	Q4	Q1	Q2	Q3	Q4	Q1	Q2	Q3	Q4	
Adopt an integrated security management system				■	■					0000
Intrusion Prevention System Redundancy	■									0000
Introducing a patch management system		■								0000
Secure your development		■								0000
Secure your PC			■							0000
Secure your system				■				■		0000
Secure your network					■					0000
Secure your applications			■							0000
Enhance data security						■	■			0000
Strengthen your incident response		■								0000
Labor	1.0MM	2.5MM	1.0MM	2.5MM	1.0MM	2.5MM	1.0MM	2.5MM	0MM	