CE/CZ 4064 - SECURITY MANAGEMENT ASSIGNMENT

Project 4 :
Information Security Management Assessment Opportunities

Presenters :
Wong Jing Yao (JWONG042)
Huang Peng (PHUANG008)
Au Jit Seah (K1720050K)

INFORMATION SECURITY MANAGEMENT ASSESSMENT

Objectives

- Design an ISMS Assessment method to monitor and review the ISMS to understand the current security posture and set goals to improve information security controls in the subsidiary companies.

Assumptions

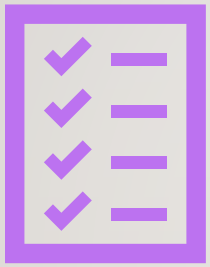
- Set the goals/targets or know the current/previous status of the information security assessments in the subsidiary companies.
- Part of justification process to obtain budget approval to build/acquire, manage and maintain secure information systems.
- Potentially gaining management support to have the company certified in ISO/IEC 27001.

ISMS ASSESSMENT PRINCIPLES

ISO 27002 14 Controls:

- Information Security Policies
- Organization of information security
- Human resource security
- Asset management
- Access control
- Cryptography
- Physical and environmental security
- Operations security
- Communications security
- System acquisition development and maintenance
- Supplier relationships
- Information security incident management
- Information security aspects of business continuity management
- Compliance

ACCESS CONTROL



Business Requirements

Objective: To limit access to information and information processing facilities.

Access control policy

Access to networks and network services

ACCESS CONTROL

User access management

Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.

User registration and de-registration

User access provisioning

Management of privileged access rights

Management of secret authentication information of users

Review of user access rights

Removal or adjustment of access rights

ACCESS CONTROL

System and application access control

Objective: To prevent unauthorized access to systems and applications.

Information access restriction

Secure log-on procedures

Password management system

Use of privileged utility programs

Access control to program source code

INTERNAL ORGANIZATION

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

- Information security roles and responsibilities.
- Segregation of duties
- Contact with authorities
- Contact with special interest groups
- Information security in project management

14 Controls – get the current performance score for each control

Weightage of the control determined by:

Type of control (policy/action/measurements)

Severity of the consequences (severe/minor)

Number of achievable/goals

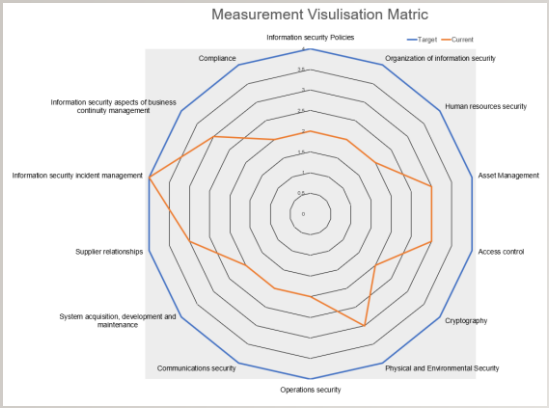
Efforts put

Goal total weighted: the targeted score that each subsidiary company should achieve

Current Total Weighted Score: what level the subsidiary company is currently at

You can identify the room for improvements and which areas to improve from this system

ISMS ASSESSMENT RESULTS



ISMS ASSESSMENT RESULTS

To analyze the results:

- Look at the final overall score to see the overall doing of the company
- Into each subarea and identify the less well-doing one
- In each subarea identify the controls with low scores
- Follow the decisions and measures to see what are the specific actions to take for improvement

Purpose:

- for the subsidiary companies to design, implement, maintain or provide improvements on ISMS
- Provide the main company a reliable measurement matric to analyze their subsidiary companies as a monitoring and assessment tool

ISMS OUTCOMES

Risks

- False sense of security, address only known issues
- Risk assessment is humanly subjective
- Hidden plane of uncertainties (residual risks)
- Compliance takes priority over risk management
- For external audit, risk of "Principal-Agent" problem
- Limited scope of certification

Opportunities

- Adoption of baseline security to address common weaknesses more efficiently
- ISO 27001 Certified (trust assurance symbol), good reputations and public image for branding

ISMS OUTCOMES

Opportunities

- Subsidiary can offer to sell managed security services (eg. Deep Security Services) with the right certifications and experience
- Recover investments by providing security services to both internal and external parties

Justifications

- Recruit certified and technical staff to implement the ISMS
- Propose budget and time frame for measurable deliverables
- Train both IT and non-IT staffs with security awareness programs
- Aim for certifications (eg. ISO 27001)
- New line of business for Managed Security Services

THANK YOU