Joint Universities Computer Centre Limited
("JUCC")
Information Security Awareness Training- Session Four

Information Security- Perspective for Management

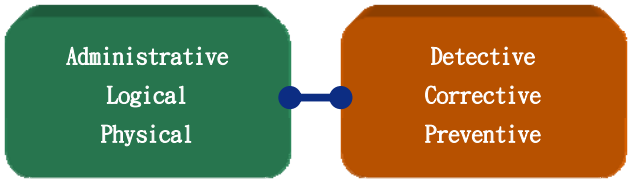
Evaluation of IS Control and Self Assessment

Agenda

- Information Security Control
- Overview of Control Evaluation
- IS Control Evaluation Process
  - Organisation Objectives
  - Scoping
  - Evaluation Programme
  - Execution
  - Reporting
  - Follow-up

Information Security Controls

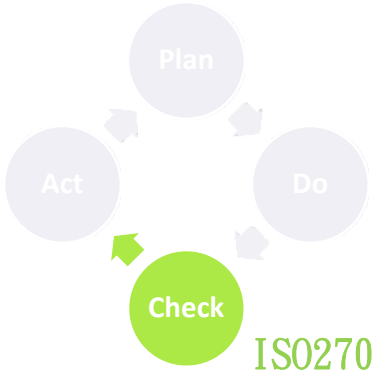
- Implemented to safeguard the security (CIA) of information.
- Should be operationally efficient
- Help meeting business objectives and requirements



Control Evaluation

- **Test of Design** – Evaluate the adequacy and effectiveness of the design of IS controls in place in meeting the relevant university objectives
- **Test of Implementation** – Evaluate whether these controls are implemented effectively
- **Test of Operating Effectiveness** – Assess the operating effectiveness of such controls implemented

Control Evaluation



ISO27001

- Plan and Organize
- Acquire and Implement
- Deliver and Support
- Monitor and Evaluate

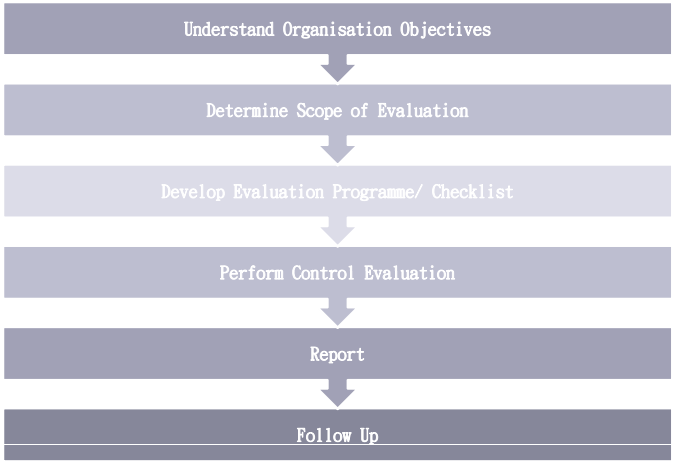
COBIT

Why evaluate controls?

- Highlight areas of weakness
- Identify deviations from organisation objectives
- Maintain a continuous effectiveness and efficiency
- Identify outdated/ obsolete controls
- Ensure legal and contractual compliance
- Provide a better understanding of the daily operations
- Incentive for improvement (evaluation results as KPI)

Who?

- Internal Audit/ Compliance Office
- Information Security Team
- External Auditor
- Control Owners (Self Assessment)

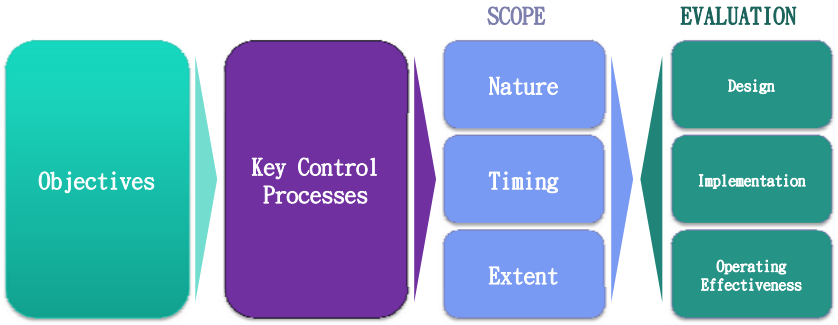


Organisation Objective

- Understand the environment and security requirements
- Identify legal and contractual obligations
- Identify changes to the requirements and obligations
- Obtain an understanding of the IS controls in place
  - Control Owners
  - Processes
  - Historical effectiveness …
- Create a mapping between the organisation objectives/ requirements and relevant departments/ units

Scoping

- To determine how the evaluation process should be carried out
  - **Key controls** in meeting the organisation objectives
  - **Nature | Timing | Extent**



Scoping

Nature

- The evaluation techniques:
  - Observation
  - Inquiry
  - Inspection
  - Knowledge Assessment …

Inspection of system production change documentation.

Observe the physical security of data centre.

Timing

- Regular (annual, perpetual)
- Ad-hoc
- Surprise

Annual IS control evaluation exercise

Perpetual evaluation on rotation basis

Scoping

Extent

- Key controls to be tested
- Degree of assurance required
- Number of deviation expected
- Full population / Sampling

Inspect sample evidence of access activity review by ITD

Full review of firewall ruleset

Evaluation Programme/ Checklist

- Develop standardised testing procedures and requirements
- Develop control testing programmes and checklists for each areas (*People/ Process/ Technology*) of review according to the nature, timing and extent determined

Dept.	Owner	Control Process	Control Frequency	Testing Procedure	Result
IT	Head of Network Operations	Firewall ruleset are reviewed bi-annually for the appropriateness	Bi-annual	Inquire of the Head of Network Operation Inspect the sign-off by HNO for the review carried out on…	…

Evaluation Programme/ Checklist

- Standardise result representation
  - Examples:
    - Effectiveness Scale [1-5]

Effectiveness				
1	2	3	4	5
			✔	

    - Effective / Not Effective

✔ Effective	☐ Not Effective

    - Descriptive Results

Result
The control has been designed effectively to address …

Control Evaluation

- Carry out the control evaluation procedures
- Communicate with control owners for signification matters
  - To verify the applicability
  - To avoid surprise
- Produce documentation/ working paper (if required)
  - For future reference
  - As evidence of review
  - For the use of external auditors/ reviewers
- Evaluation of findings
  - Evaluate residual risks
  - Assign risk rating [H / M / L]

Working Paper
- Risk
- Control Description
- Nature of Control
- Personnel Performing the Evaluation
- Date of Evaluation
- Sampling Technique
- Samples reviewed
- Results
- Findings
- Evaluation/ Risk Rating
- Response of Control Owners
- …

Reporting

- Report to Management
  - **Executive Summary**
    - Objective
    - Scope
    - Methodology
    - Key findings (only major findings, e.g. finding of High & Medium rating only)
    - Conclusion
  - **Findings**
    - Description
    - Risk [Impact & Likelihood]
    - Root Cause Analysis
    - Recommendation
    - Response/ Action Plan

Follow Up

- Identify and agree on a list of control weaknesses and improvement opportunities
- Agree upon the follow-up action with owners
- Decide an actionable target completion date for each follow-up action
- Develop a detailed action plan
- Re-evaluate the control effectiveness subsequent to improvement

Self Assessment

Control Self Assessment

- Self assessment allow control owners to evaluate whether the control processes are:
  - Effective at operation level; and
  - Aligned with the organisation objectives
- The assessment process is usually carried out by employees in the operational areas.
- Execution of self assessment are usually more efficient as the "assessor" already have knowledge of the control processes in place.

Self Assessment

- However:
  - Employees from the functional areas may not have the skill and knowledge in carrying out the assessment
  - Familiarity towards the control process may create blind spots during the assessment
  - Independence threat- If the results of the evaluation are associated with the performance review criteria of the employee, there may be incentive to hide significant evaluation findings

Self Assessment

- Facilitated Self Assessment
  - Internal Audit unit of the university (or external independent auditors) facilitates the control evaluation process by
    - Team meetings; or
    - Questionnaires
  - Controls owners "own" the control self assessment process and carry out the evaluation and assessment process

Summary

- Internal evaluation process is essential to ascertain the **continuous effectiveness** of internal information security controls.
- In practicing **due care**, management should establish sound internal control evaluation process as part of the fundamental information security framework.
- An effectively designed control evaluation process **brings benefits** to the university.

Q&A

?