Joint Universities Computer Centre Limited (“JUCC”)

Information Security Awareness Training - Session Five

End User Security, IS Control Evaluation & Self- Assessment

End User Self Assessment

Agenda

- Control Evaluation
  - Test of Design
  - Test of Implementation
  - Test of Operating Effectiveness
- Control Evaluation Methodology and Techniques
- Self Assessment
  - Control Self Assessment
  - Access Review
  - Review of System Update and Patch Level
  - Review of Anti-virus Signature Update
  - Reporting

End User Computing (“EUC”) Controls

- Implemented to **safeguard** the security (CIA) of information
- Ensure that a standard **corporate policy** is in place to govern the lifecycle of critical EUC data (e.g. spreadsheets and access databases)
- Assist the organisation in meeting **business objectives**

Control Evaluation

- **Test of Design**

Evaluate the adequacy and effectiveness of the design of controls in place in meeting users' requirements

Example: Evaluate if the established user access rights confer with their roles

- **Test of Implementation**

Evaluate whether these controls are implemented effectively

Example: Evaluate if sign off procedures exist for approving program changes are properly signed off upon each request

- **Test of Operating Effectiveness**

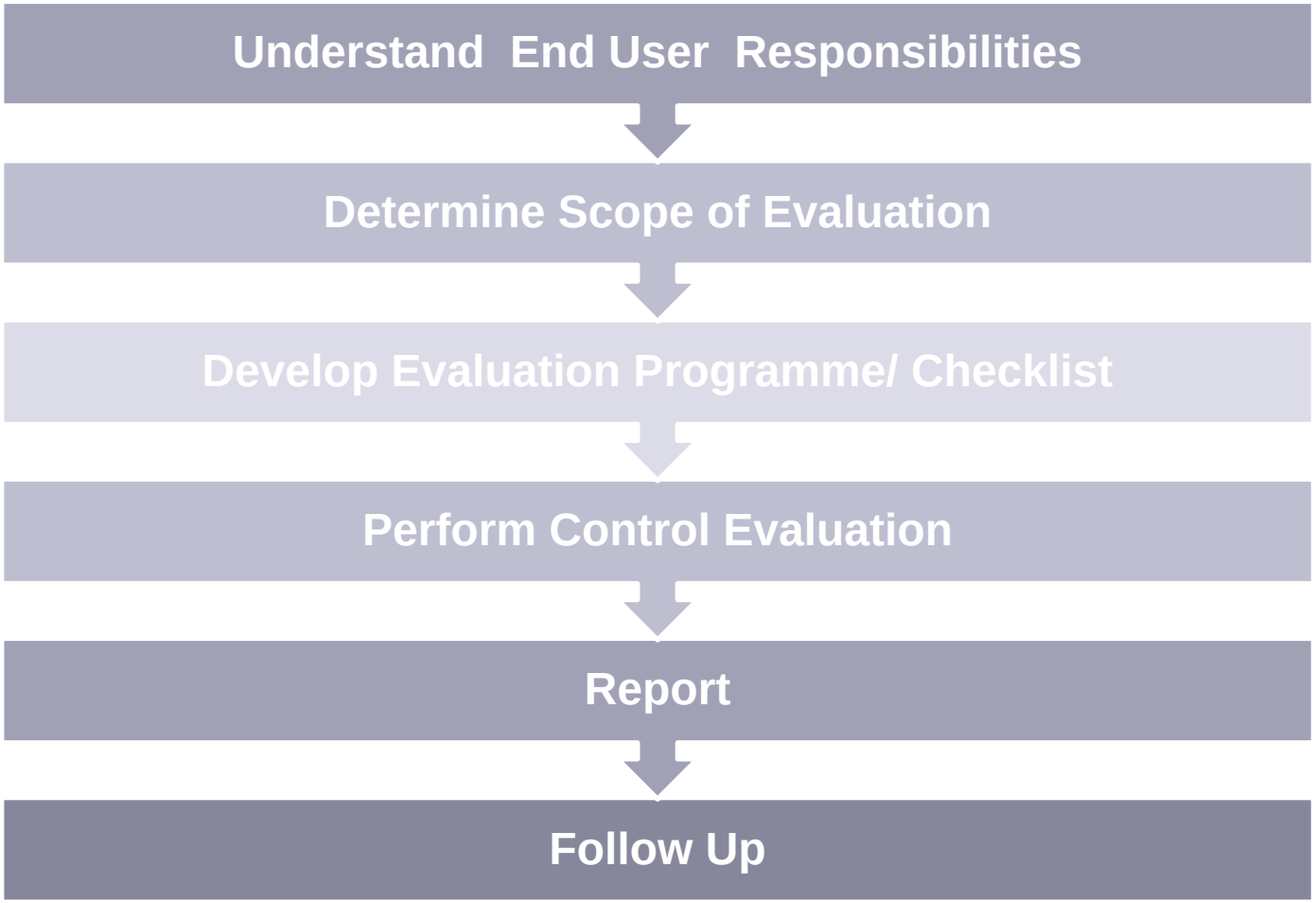
Assess the operating effectiveness of such controls implemented

Example: Evaluate if program changes are properly signed off upon each request

Why self assessment?

- Identify deficiencies and highlight areas of weakness
- Cultivate user awareness and security culture among end users
- Maintain a continuous monitoring process
- Ensure timely update on obsolete controls
- Ensure consistent legal and contractual compliance
- Provide a better understanding of the daily operations

Control Evaluation Methodology and Techniques

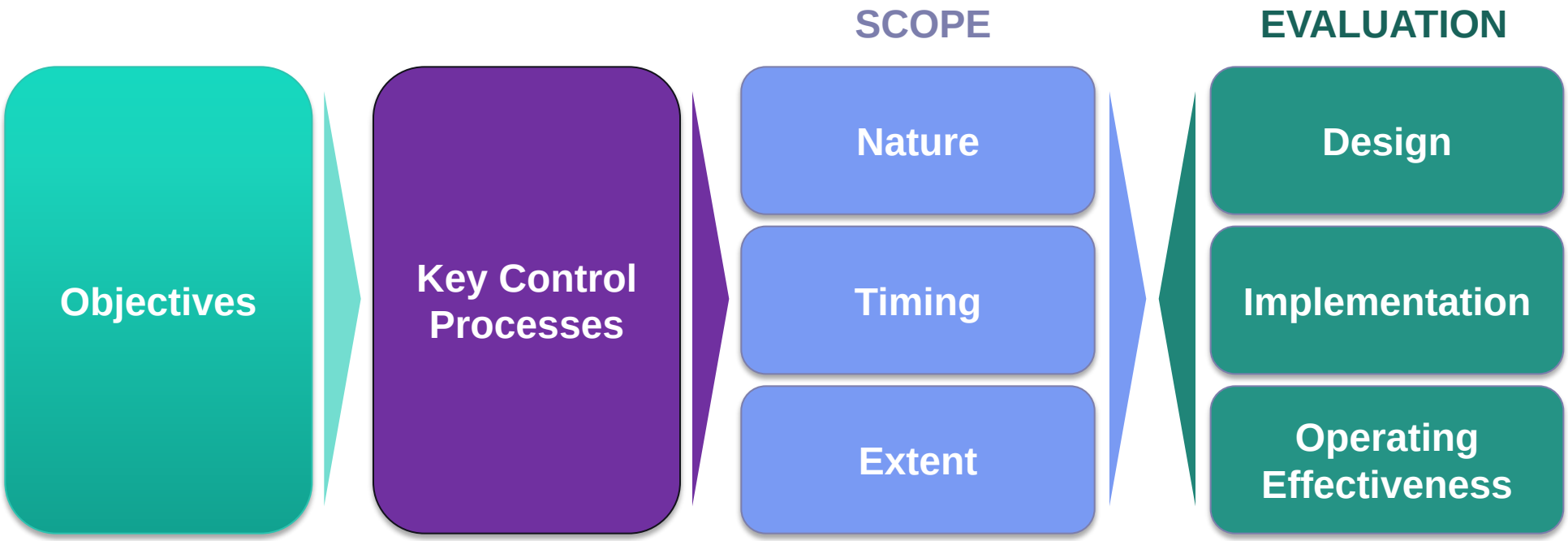


End User Responsibilities

- Understand the environment and security requirements
- Familiarise oneself with EUC policy and legal and contractual obligations
- Create a mapping between the organisation objectives/ requirements and own roles under each EUC programs

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

Observe physical security against computing devices.

Inspection of documentation and sign-off of significant program changes

Timing

- Regular
- Perpetual

Annual control evaluation exercise

Perpetual evaluation on rotation basis

Scoping

Extent

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

Inspect sample program change request forms

Full review of end user computer access activity log

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
Finance	Head of Department	Payroll records are backed up monthly	Monthly	Inspect the sign-off by Head of Finance Department 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 supervisor for significant matters
- Produce documentation/ working paper (if required)
  - For future reference
  - As evidence of review
- Evaluation of findings
  - Evaluate residual risks
  - Assign risk rating [**H** / **M** / **L**]
  - Provide insights for future improvements

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
- ...

Follow Up

- Identify deficiencies, vulnerabilities and improvement opportunities
- Agree upon the follow-up action with stakeholders
- Decide an actionable target completion date for each follow-up action
- Develop a detailed action plan
- Re-evaluate the control effectiveness subsequent to improvement

Reporting

Regular reporting

- Archive self assessment records periodically (e.g.: monthly, quarterly, bi-annually, annually, etc.)
- Example: quarterly list program changes approved, monthly update on patch level upgrade

Incident Reporting

- Report when unusual activity is found
- Follow incident reporting procedures strictly

Control Self Assessment

- Self assessment allow control owners to evaluate whether the control processes are:
  - Effective at end user level; and
  - Aligned with the university's IT security requirements
- The assessment process is carried out by end user for their responsible EUC program

Self Assessment

- **Potential problems**
  - End users may be slack in conducting self-assessment as they may top operational convenience over IT security compliance
  - The assessor may easily overlooked the adequacy of controls in place
  - If each EUC program control is assessed by their respective control owner, a large number assessors will be involved, causing the evaluation process management reporting and follow-up to be difficult

- **Facilitated Self Assessment**
  - Internal Audit unit of the university (or third-party services 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

Compliance Review

- What are the **policies and standards** applicable?
- What are **required** according to the policies and standards?
- What is the level of compliance?
    - Sufficient **documentation**?
    - Proper **sign-off**?
    - Adequate **review**?
    - Timely **follow up**?
    - Document **retention**?

Review of Access Control

Determine whether access to the workgroup network and system resources is granted to users appropriately

Common types of users

- **Administrator** – who has the least restrictions on access to any resource or system component
- **Normal user** – who can only access the data and programs associated directly with their own work and who cannot install or remove programs or modify system settings
- **Guest** – who can only access resources that are available to the public or visitors to the organisation

Assessment of Access Control over Shared Infrastructure

In cases of shared machines are used:

•Checking regularly the last **access and modification** date to determine if files are edited by other unauthorised users
•Observe whether co-workers share **password**
•Review the **access rights** of folders to determine if unnecessary access rights are granted
•Review the storage used for the shared machines to determine if **critical files** are placed under inappropriate storage area

Review of Monitoring Control

- **Verification of status of system and software updates**
  Ensure anti-virus and end-point protection software are installed and activated

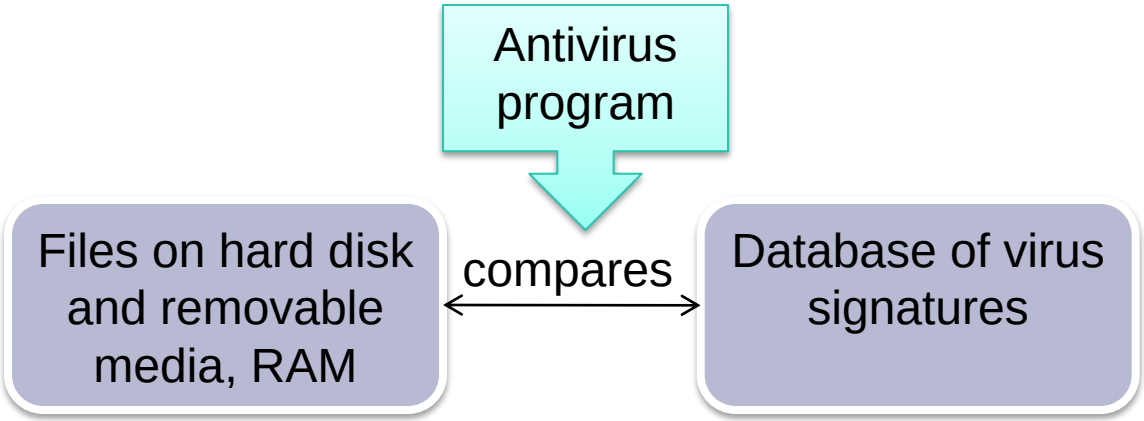
- **Verification of system integrity**
  Perform regular system file scan to ensure that files have not been modified

Review of Patch Level

- **Obtain a list of patches** available from IT department or vendors regularly
- **Verify patch update** using security scanning tool (eg: Secunia Personal Security Inspector (PSI) – it automatically scans the PC and alerts the user whenever programs and plug-ins installed require updating)
- Determine if automated patch updates **aligns with the organisation's patch management policies**
- Be certain that applications and operating systems are **up-to-date** with approved patches

Review of anti-virus signature update

- A virus signature is a binary pattern coded for a particular virus
- Generic detection is less likely to be effective against completely new viruses and more effective at detecting new members of an already known virus
- The need to update anti-virous signature is a recurring activity



Review of anti-virus signature update

Areas for review:

- **Monitor vendors' websites** for signature updates regularly
- **Update** the anti-virus software **regularly**
- Enable **auto signature update feature**
- Ensure the existence of **prompt notification** upon new updates or outdated signatures
- **Verify if** detected **malware is** properly **quarantined**

Summary

- Good management of EUC allows universities to maximise the benefits of EUC.
- Universities are encouraged to establish a standardised set of EUC policy for delivering output of consistent quality.

Q&A

?

Copyright Statement