Joint Universities Computer Centre Limited (“JUCC”)

Information Security Awareness Training - Session Four

End User Security, IS Control Evaluation & Self- Assessment

End User Computing Security

Agenda

- End User Computing Fundamental
- End User Computing Security
  - Access Control
  - Program Change and Development Maintenance
  - Backup and Restoration
  - Continuous Monitoring
  - Physical Security
  - Other Security Controls

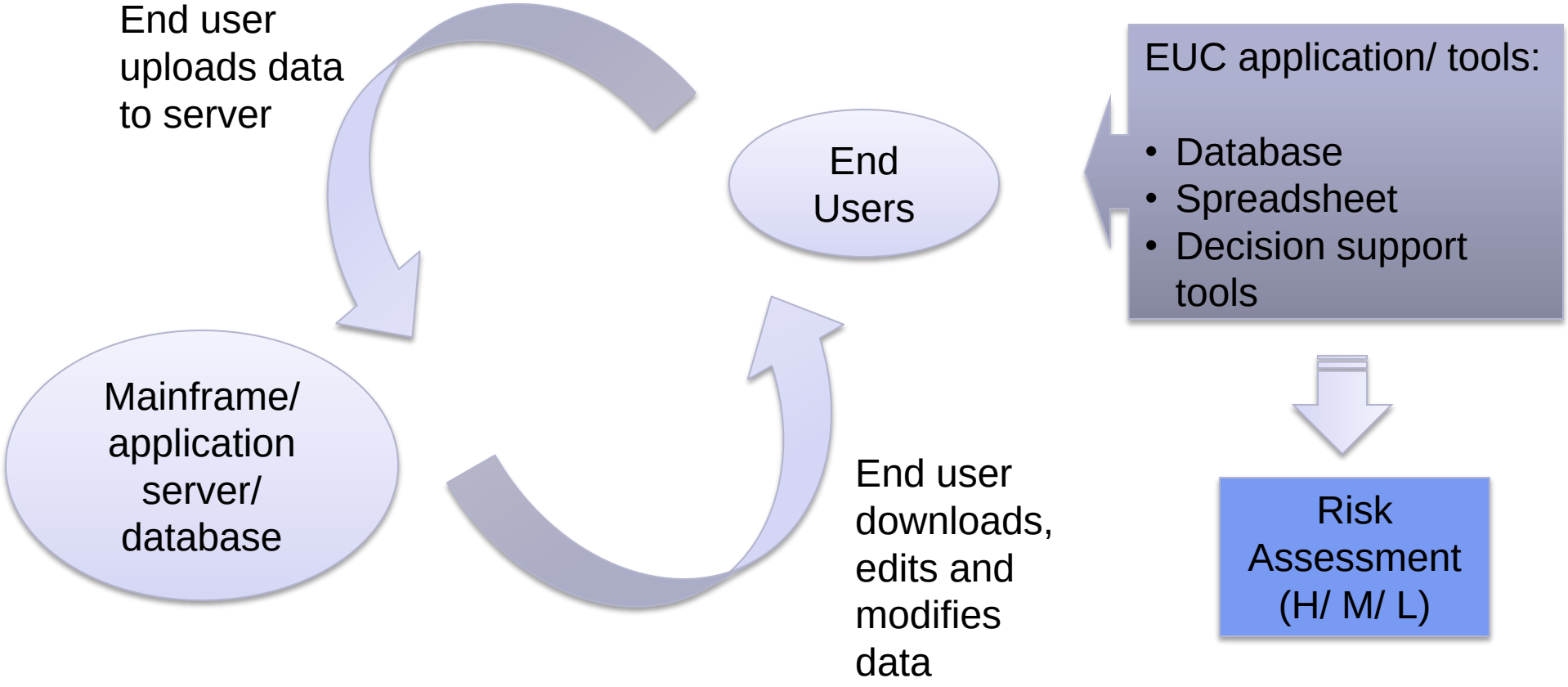
End User Computing (EUC)

Systems in which end users with non-programming knowledge can design, create and maintain working applications

Common End User System Tools

Text and multimedia handling tools	Word processing, web-publishing, presentation software
Data handling tools	Spreadsheet, database
Communication tools	E-mail, messenger
Knowledge management	Data mining, information retrieval

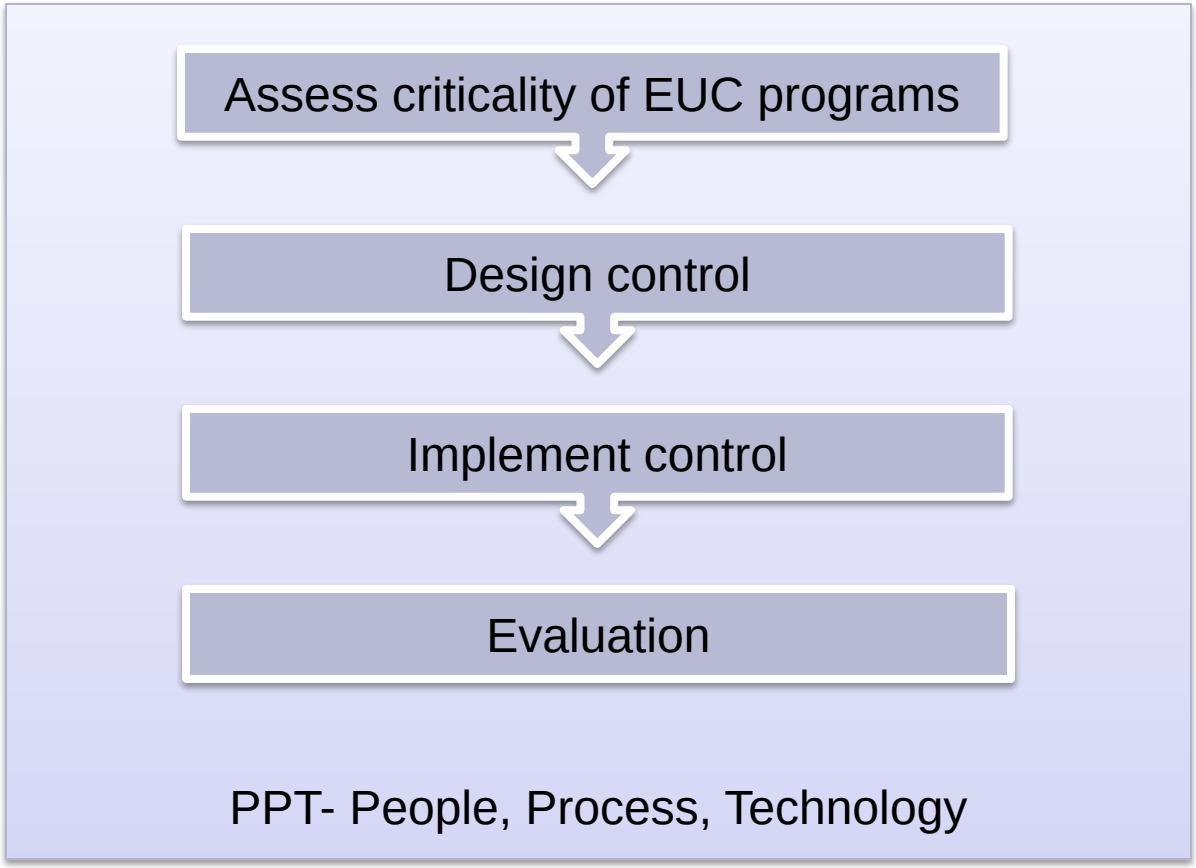
End User Computing (EUC)



Problems with End User Computing

- Development errors
- Data entry errors
- Lack of backup
- Lack of standardisation
- Lower level of security
- Insufficient training for end user
- Blurred line between business and personal use

EUC Controls Framework

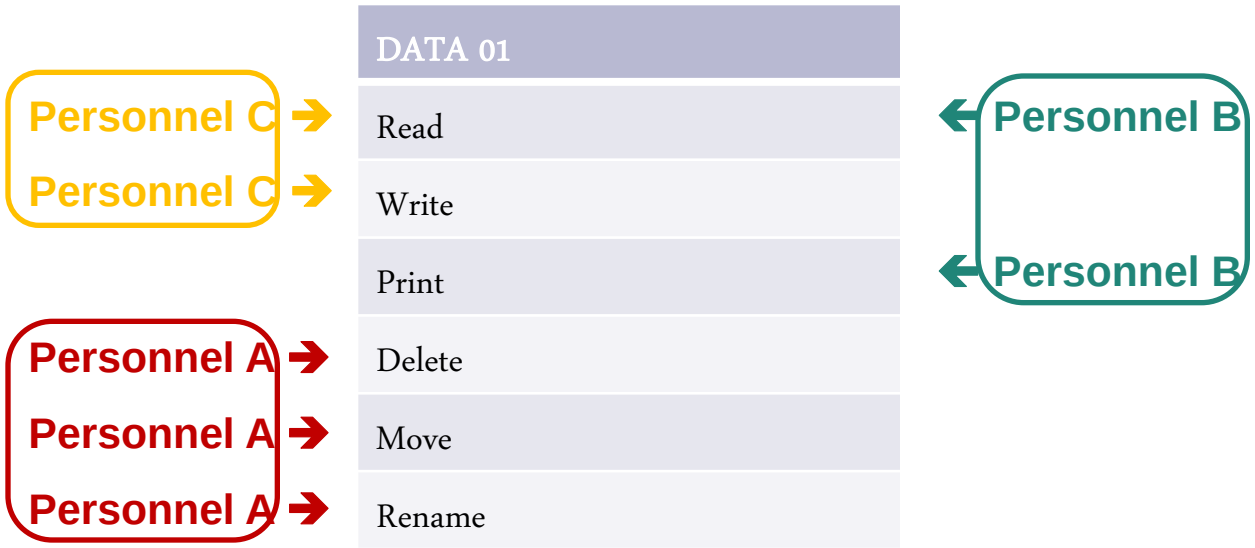


Suggested Controls

- Enable login passwords
- Enable screen saver and screen lock
- Apply zip encryption to double protect compressed files
- Log all significant administrative activities
- Verify the identity of user who request remote access from your computer

Suggested Controls

- Least privilege and role-based access control



Objectives

An effective system of change control can minimize the company's risk of using programs that:

- Originates from an unauthorised source
- Includes extraneous code
- May cause changes to output data and result in system errors

Suggested Controls

- Compare program test result against implemented changes to ensure no unauthorised changes were made
- Document significant changes
- Test changes to EUC programs

Two approaches to handling data backup and restoration

- **Centralised**

  Perform backup, restoration and problem management for EUC programs centrally by IT department

- **Decentralised**

  Execute the operations controls in a distributed way

Suggested controls

- Elicit automatic restoration processes
- Implement regular backup
- Off-site backup of critical files in a secured location

Continuous Monitoring

Continuous Monitoring involves **periodic review** or **internal audit** on the relevant controls over EUC programs:

- To **assess the effectiveness** of EUC management
- To **detect any deficiencies** (e.g. deviation from established control requirement, missing control area, etc.)

Monitoring Activities

•Perform annual policies and procedures reviews and updates
•Perform quarterly system configuration and software reviews and updates
•Perform monthly vulnerability scanning of relevant systems

Physical Security

- Log off or shut down computer when leaving desks
- Secure portable devices with cable lock in the office and while traveling
- Secure the casing of the workstations
- Configure computer BIOS to prevent intruders from booting the computer with USB flash drive or FireWire hard disk
- Use of bios password and the password should be only kept by authorised IT administrator
- Remove floppy and CD/DVD drivers and disable USB and FireWire ports if not in use

Other Security Controls

- Maintain an updated EUC process register
- Perform manual reconciliation/verification on EUC program output
- Perform regular system health check and virus scan
- Ensure only work-related activities are performed on university’s computer

Summary

- End-user computing security should be effectively supported and planned
- A solid set of management metrics and standards should form an essential part in end-user computing

Q&A

?

Copyright Statement