Joint Universities Computer Centre Limited
(“JUCC”)

Information Security Awareness Training- Session Two

Data Handling in University
Case Study- Information Security in University

Agenda

Case Study

- Background Information
- Frameworks
- Confidentiality-Integrity-Availability (CIA)
- Information Security Risk Management (ISRM)
- People-Process-Technology (PPT)
- Plan-Do-Check-Act (PDCA)
- Conclusion

Case Study

- A hypothetical scenario
- To understand how to apply the information security frameworks
- To illustrate how the frameworks help the evaluation and design of relevant controls
- Examples of controls to be implemented

The Hypothetical Scenario

- Current Situation: No centralised system
  - Research information handled by staff members individually
  - Information sharing is difficulty

Research Management System ("RMS")

- Proposed System Owner: Research Services Department
- System Users: Research Services administrators
  - Research Services/ departmental accountants
  - Researchers and faculty managers/ administrators
- User Interface: Web-based user interface

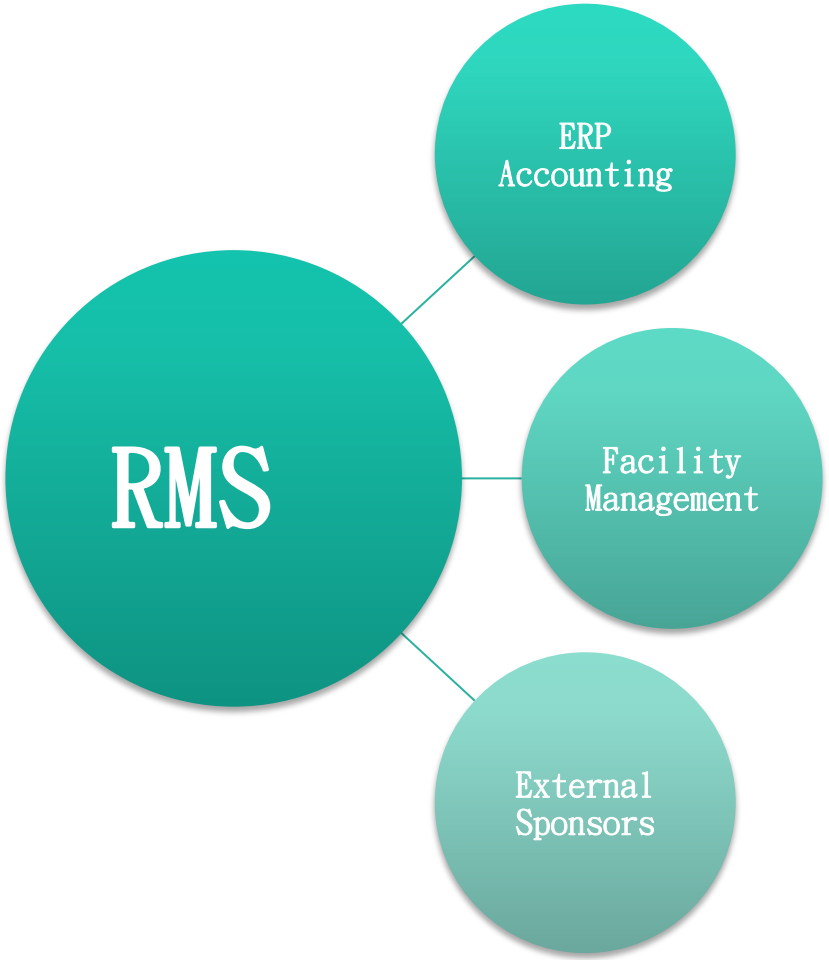
RMS

Proposed System Functions:

- Research Accounting
- Fund Management
- Researcher/ Staff Information
- Proposal Management
- Research Project Management
- Publication Management
- Resource Management (e.g. data, information, subscription, space…)
- Compliance Review
- Management Reporting

Proposed Interfaces:

- Accounting information with existing university ERP accounting system
- Research space information with existing facility management system
- Tailored interfaces for research data/ information with specific external sponsors

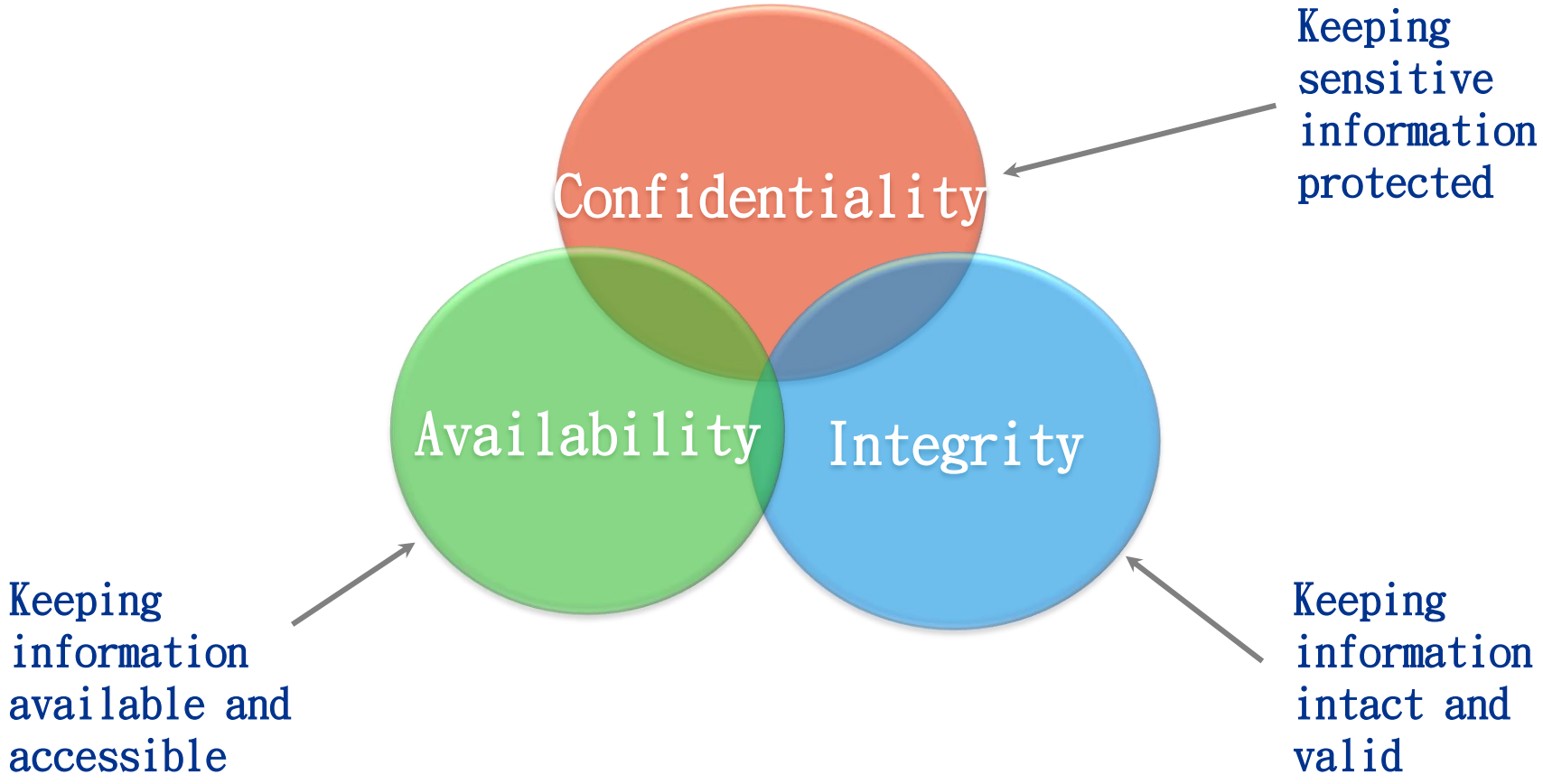


The Information Security Frameworks

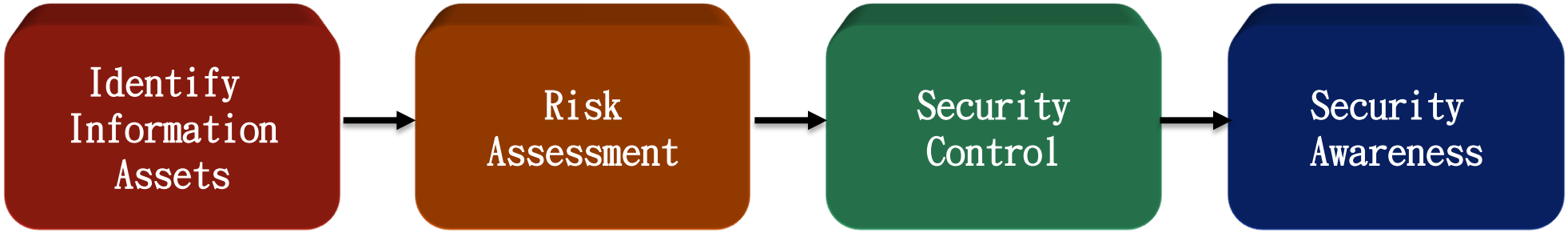
- Confidentiality, Integrity and Availability ("CIA")
- Information Security Risk Management (“ISRM”)
- People, Process and Technology ("PPT")
- Plan-Do-Check-Act (“PDCA”)

Frameworks are used as a starting point to facilitate security consideration when implementing new system/ process.

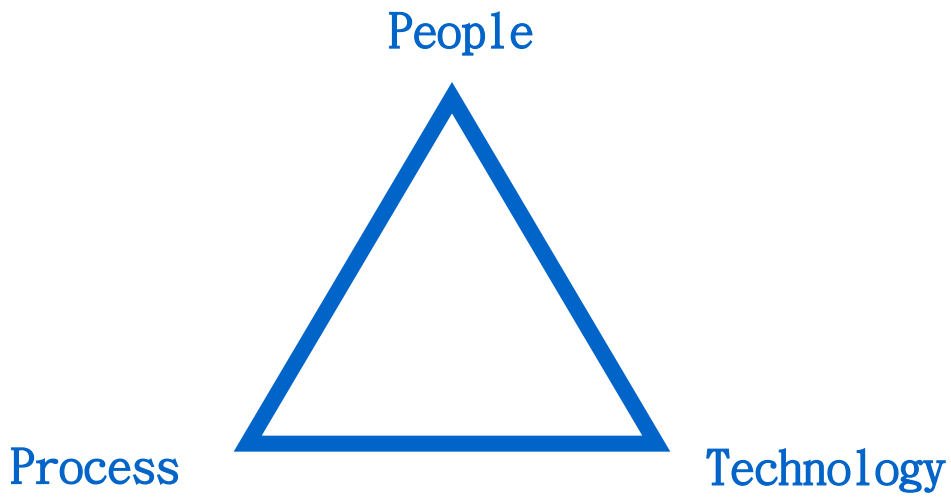
The CIA Concept



Frameworks- ISRM



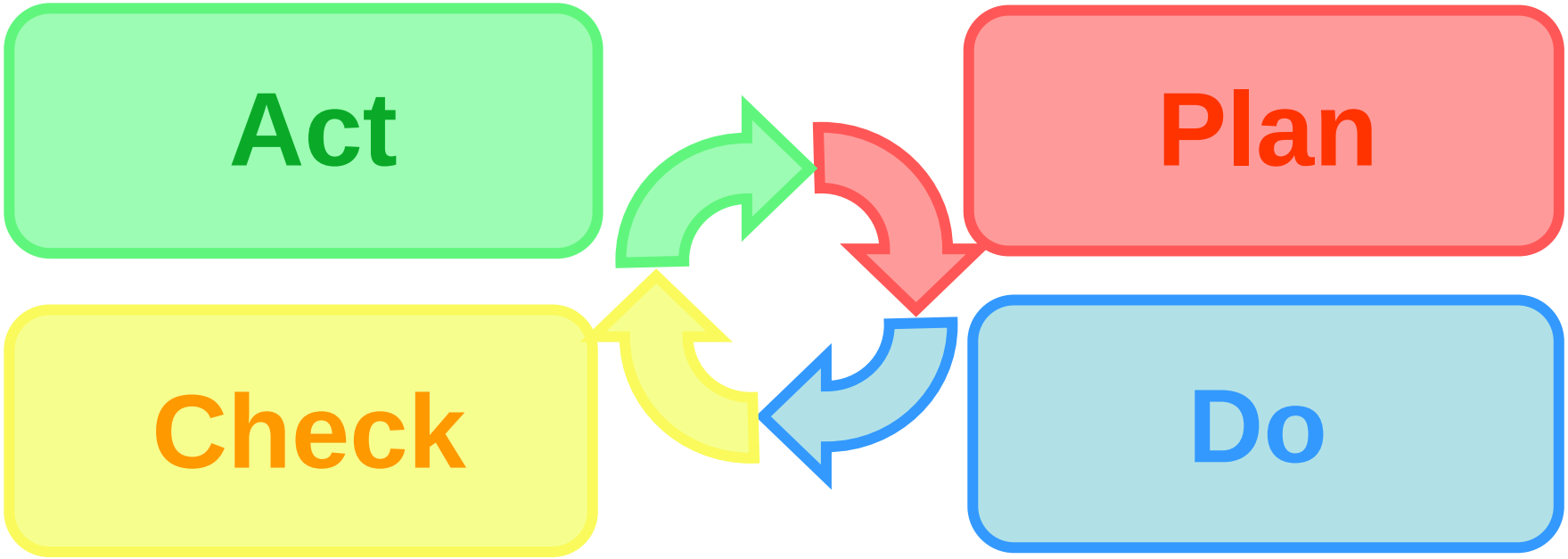
Frameworks- PPT



- *Information security is not only related to computer systems.*
- *People are always the weakest link.*
- *A complete framework is required to manage information security.*

Plan-Do-Check-Act (PDCA)

A model adopted by ISO27001

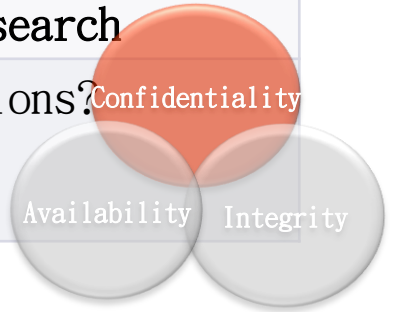


Applying the Frameworks

Confidentiality

- What objects (data/ information/ process) should not be disclosed to unauthorised subjects?

Accounting information	Should research assistant have access to accounting information? **NO**
Funding information	Should researchers and departmental managers have access to all funding information? **NO** Will it be on an as-needed basis? **YES**
Research information/ Proposal/ Project Management	Should Research Services department have access to research results and data in-progress? **NO- but they should have access to the status of research**
Publications	Who should have access to the publications? **Defined by the research team according to requirements**



Confidentiality

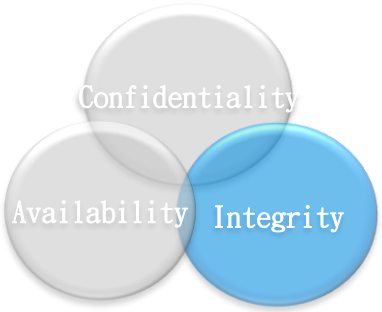
- What objects (data/ information/ process) should not be disclosed to unauthorised subjects?

Resource Management	Who should have access? **The Research Service Coordinators** **Research team, as-needed (by roles or project)**
Compliance Review	Who should have access? **Research team and appointed investigators**
Other public information?	Publicly published research (publication) only
System Administration	Who should have the administrator privileged? **Dedicated Research Services Manager only**
System Database	Who should have direct database access? **Vendor/ Dedicated Database Administrator with proper segregation of duties and approval**

Integrity

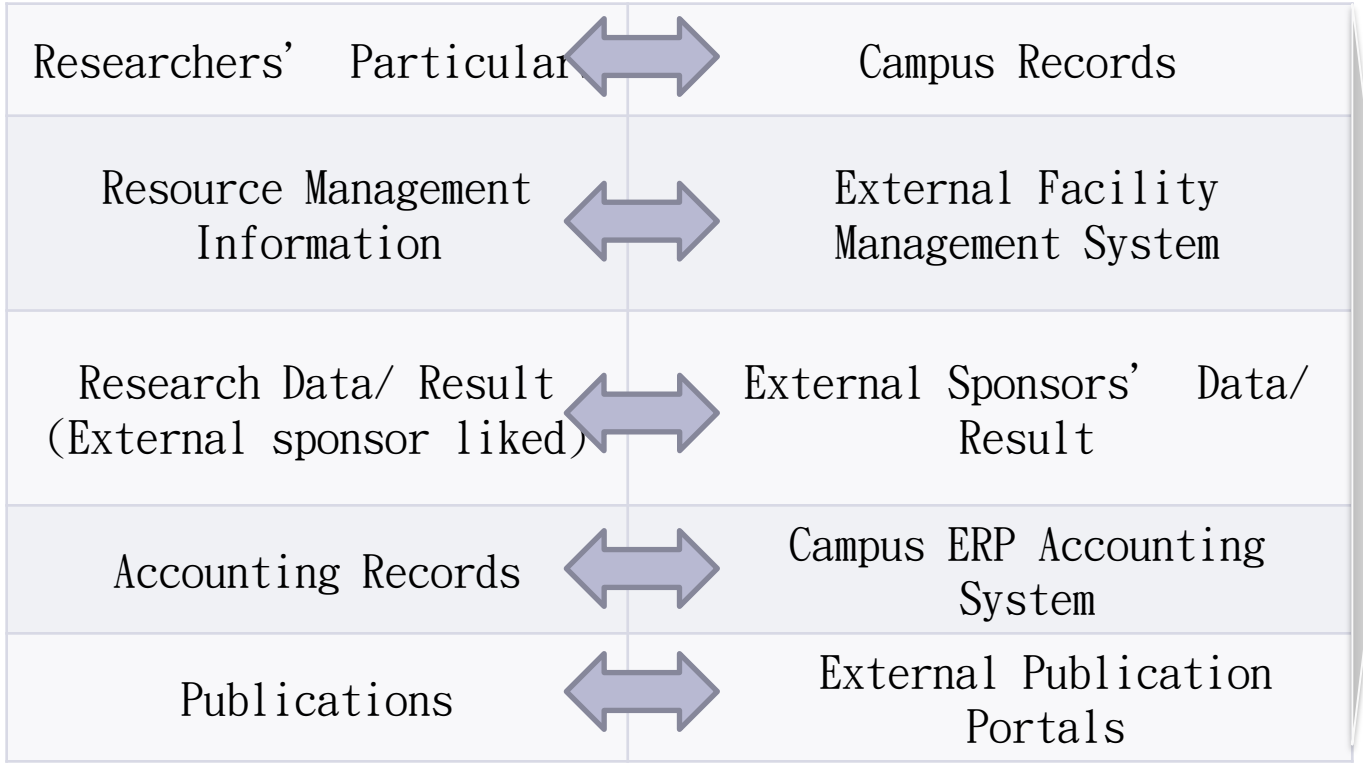
- Objects retain their veracity and are only intentionally modified by authorised subjects.

	Integrity Requirement
Accounting	**High**
Funding	**High**
Researcher Particulars	Medium
Proposal	Medium
Project Management	Low
Resources Management	Low
Compliance	Medium
Management Reports	**High**



Integrity

- Data consistency with external or internal systems



Consider:

- System Interface
- Real-time synchronisation & heart-beat
- Automated reconciliation (e.g. day-end)
- Manual reconciliation reports
- Streamlined administration process (e.g. staff particulars)

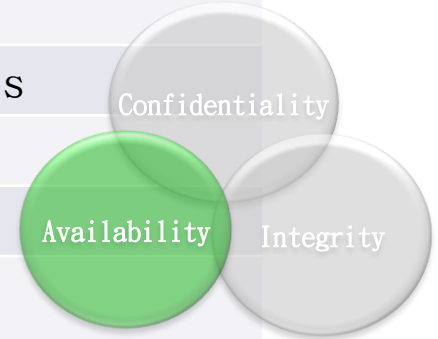
Availability

- Authorised subject … ted access to objects

Project Management Information
- Pending Tasks
- Research Results
- Project Timeline
- Status Tracking
- Team collaboration …

Critical for research progress

Data		
Accounting		…t for
Funding		
Researcher Particulars	Low	Campus records/ peer information
Project Management	**High**	**N/A**
Publication	Low	Other publishing portals
Resource Management	Medium	N/A
Compliance	Medium	N/A
Management Reports	Medium	Printed management reports



Identifying Information Asset

- Objects retain their veracity and are only intentionally modified by authorised subjects.

Modules	Information Asset
Accounting	• Historical financial data (project and campus-wide research function) • Costing data and calculation • Budget • Salary- [Sensitive]
Funding	• Current sources of fund (Gift/ Trust/ Government) • Potential sources of fund- [Sensitive] • Fund related contractual requirements (compliance) • Fund status and utilisation

Identify Information Assets

Identifying Information Asset

Modules	Information Asset

Researcher Information	• Personal data of research teams- [Private]
	  • Contacting information
	  • Academic background
	  • Assessment and appraisal

Research Project Management	• Project Management
	  • Project timeline
	  • Project tracking
	  • Financial data
	• Research Data- [Confidential]
	  • Research work-in-progress (WIP)
	  • Data and statistics (e.g. medical information of research subject)
	  • Research results
	  • Business confidential information (e.g. unpatented WIP)

Identify Information Assets

Identifying Information Asset

Modules	Information Asset
Publication Management	• Public and restricted publications
Resource Management	• Centralised subscription database • Shared research information and statistic • Space utilisation
Compliance Review	• Contractual/ regulatory requirements- [Sensitive] • Project compliance status
Management Reporting	• Consolidated financial performance and position • Project and staff performance assessment • Overall research project status tracking • Available in both electronic and printe copies

Identifying Information Asset

- The process (examples)

Step 1: The data	Step 2: System and media	Step 3: Organisation Objective	Step 4: Criticality
Research Data/ Results	**Storage**: Database, file server **In-transit**: Interface with external sponsors **View**: Access by research team **Backup**: Backup tapes	Fulfil contractual requirements (e.g. confidentiality of data) Observe regulation (e.g. privacy of research subjects)	In case of breach: -Withdrawal of fund -Loss of competitiveness -Litigation -Damage to reputation
Researchers' Particular	**Storage**: Database **View**: Access by administrator and research team **Backup**: Backup tapes	Observe regulatory requirements (Personal Data (Privacy) Ordinance)	- Litigation in case of breach

Identify Information Assets

Risk Assessment

Risk Assessment- Assignment of value for potential harm/ loss

Quantitative	Qualitative
$ $ $ $ $ Annualised Loss Expectancy (ALE) Annualised Rate of Occurrence (ARO) Single Loss Expectancy (SLE) Asset Valuation (AV) Exposure Factor (EF) $ $ $ $ $ SLE = AV x EF ALE = SLE x ARO	5 4 3 2 1

Risk Assessment

Risk Assessment- Example

Asset	Asset Valuation	Vulnerabilities & Threats	Impact	Occurrence	ALE
Research Data	-Withdrawal of fund - Loss of competitive advantage - Litigation - Damage to reputation =$1,000,000	**Vulnerabilities:** Unencrypted data transfer with external sponsors **Threats:** Interception of data in-transit	Leakage of confidential research data	ARO = 0.2 / Year	EF = 30% = AV x EF x ARO = $1,000,000 x 30% x 0.2 **= $60,000**
	5	3	4	2	Avg. = **3.5**

Quantitative
- How much to pay for countermeasure?

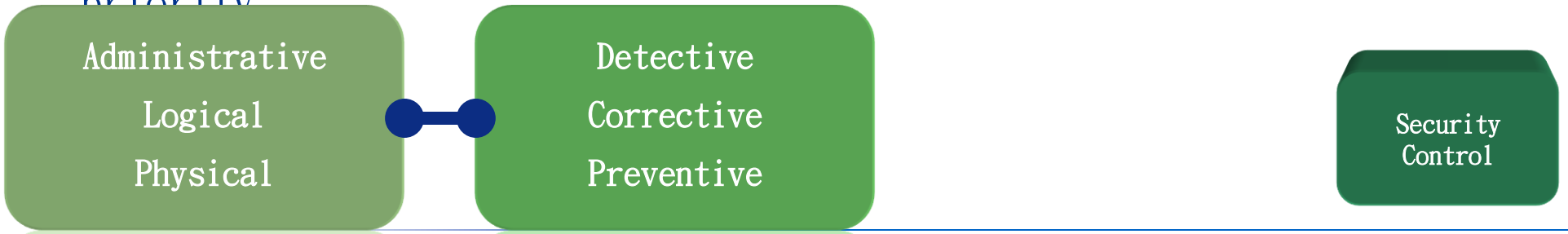
Qualitative
- How to prioritise for resource allocation?

Risk Assessment

Security Control

Research Data:

- Quantitative- ALE = $60,000
  - If control can be implemented with an averaged annual cost below $60,000 to prevent/ detect/ correct the occurrence of leakage of research data, such control can be considered
- Qualitative- ALE= 3.5
  - With limited fund in implementing controls to protect the RMS, funds should be allocated to identified assets of higher averaged priority



Security Control

Research Data Protection- *Considering Control Implementation*

- Implementing a network-based data leakage prevention system with an annual **total cost of $300,000** may **not be justified** solely in preventing the loss of research data leakage (due to low expected occurrence of such event).
- Implementing data encryption for all external interfaces with research data transfer is expected to mitigate over 80% of the exposure to research data leakage. The implementation involves an **annual cost of $10,000**. This control **may be considered** in mitigating the risk of research data leakage.
- Implementing a more granular access control mechanism is estimated to cost **$8,000** per annum averaged. This control may also be considered together with the data encryption control.

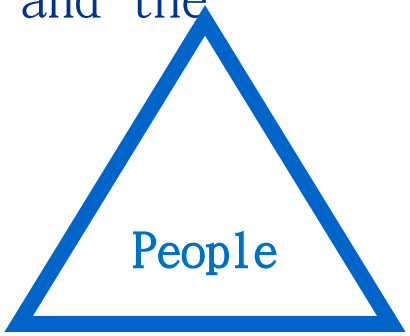
Security Awareness

Assuming the a granular access control to research data is to be implemented-

- Security awareness to both the research team and Research Services administrators should be conducted to cover:
  - Importance of research data
  - Importance of the access control implemented
  - How to design an effective access control according to the project nature
  - Importance of regular access right maintenance and review

People

- Required expertise to manage the RMS- Technical and management competence.
- Additional personnel required for the implementation and operation of RMS
  - Factored in during the budget preparation
- Consider users acceptance of the system. Consider rolling out the RMS in phases to build acceptance and to smooth migration
- Management awareness of the potential difficulties, risk and the importance of management support
- Regular communication to all relevant parties



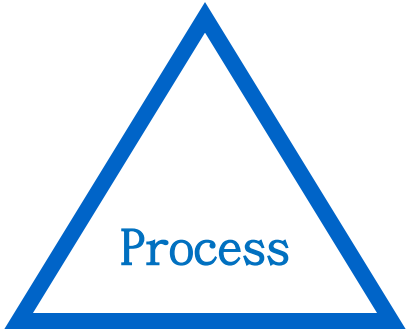
If PEOPLE are not ready for the new system, should we consider postponing the implementation?

Process

- Vendor selection criteria
- Security policies
- Security audit requirements
- System hardening baseline
- Third-party service support
- Change management cycle
- Patch management process
- User awareness program
- Incident management
- User administration

Consider:

- **Availability** of such processes
- **Applicability** of such processes over the new RMS
- Requirement of **additional** process to cater for the implementation of RMS
- User **awareness** of the processes

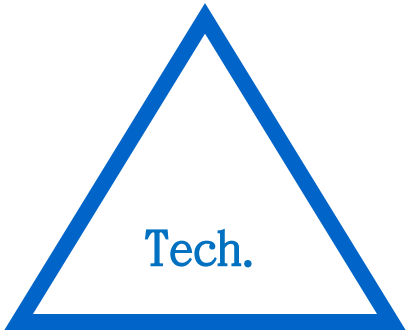


Technology

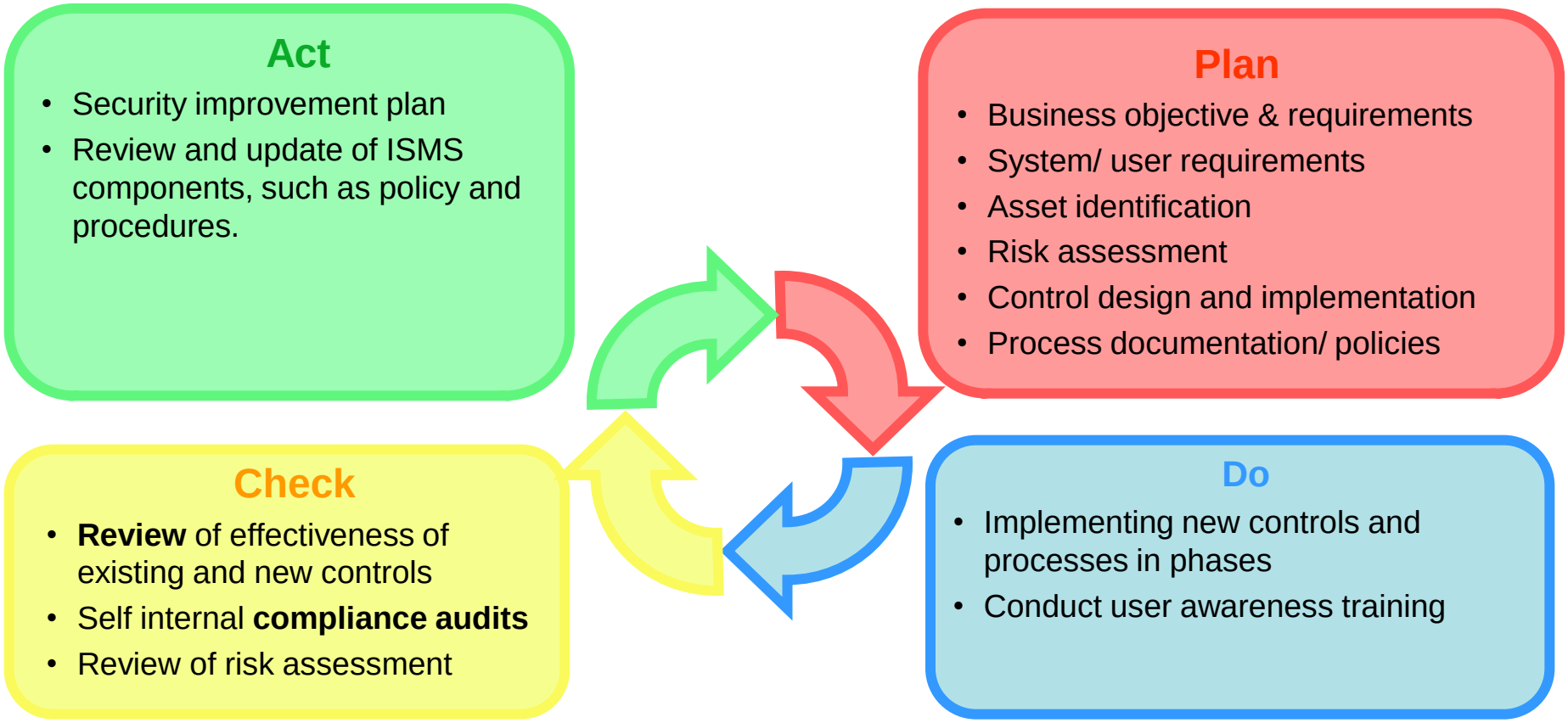
- Network access controls (e.g. firewall, IPS, logs…)
- User access controls (e.g. login mechanism- SSO)
- Anti-virus on end-user (Research Services & departmental) machines
- Physical access control to servers and network equipments

Specific technical considerations- to help *people* follow *process*

- System configured password configuration requirements (password length, complexity & expiry)
- Restricted access to RMS by pre-configured IP address
- Input validation



PDCA


Act
• Security improvement plan
• Review and update of ISMS components, such as policy and procedures.
Plan
• Business objective & requirements
• System/ user requirements
• Asset identification
• Risk assessment
• Control design and implementation
• Process documentation/ policies
Check
• **Review** of effectiveness of existing and new controls
• Self internal **compliance audits**
• Review of risk assessment
Do
• Implementing new controls and processes in phases
• Conduct user awareness training

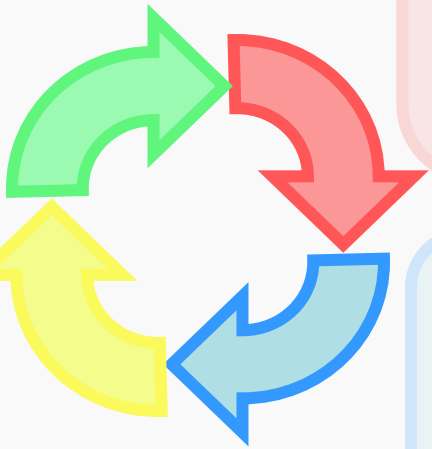
PDCA

Act

- Security improvement plan
- Review and update of ISMS components, such as policy and procedures.

Check

- **Review** of effectiveness of existing and new controls
- Self internal **compliance audits**
- Review of risk assessment



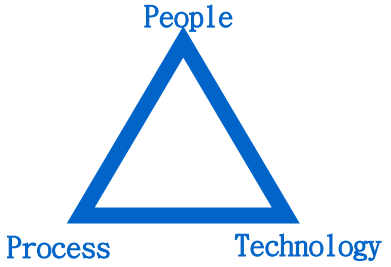
CHECK & ACT

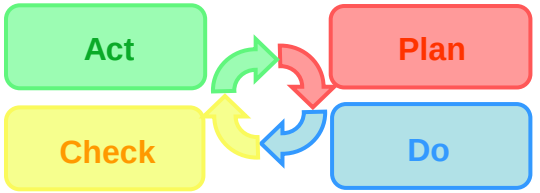
On-going Review and Update

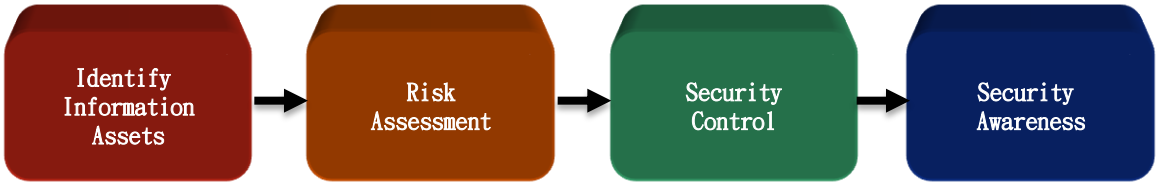
Conclusion

The information security frameworks facilitate the management process in considering the handling of data and implementation of system/ process.

- Identifying asset
- Determining security requirement
- Risk assessment
- Control evaluation
- Control implementation
- Process monitoring and update







Conclusion

Suggested Controls:	Detective	Corrective	Preventive
Administrative	• Rotation of administrator duties • Management review of access controls • Review of IPS, firewall and web application logs • Data reconciliation (between RMS, ERP and facility management systems	• Business continuity plan • Disaster recovery plan	• Separation of duties • Technical training for responsible IT personnel • Communicated security policy • User account administration
Logical	• Network Intrusion Detection System especially for externally exposed hosts (external interface) • System logs • System integrity check	• Network Intrusion Prevention System • Anti-virus software	• Granular access control to personal data and research information • Data encryption for external interfaces • Web-based authentication • Anti-virus software
Physical	Data Centre/ Research Office • Camera & alarms • Security guards • Regular asset count	• Emergency power supply	• Physical access control (e.g. swipe cards, biometric locks) to computer facilities • Environment controls • Regular offsite backup of data

?

Copyright Statement