Tutorial 6
InfoSec Policies
&
Governance

Group 3:
Tan Jun Xue Keith
Muhammad Sholihin Bin Kamarudin
Yang Kai Ze

Background

Back in April 2017, a breach of the IT networks of NUS and NTU has been discovered. Intrusions into NTU's networks were detected when the university ran its regular checks on its systems on 19th April. NUS detected an unauthorized intrusion into its IT systems on 11th April, during cybersecurity assessments by external consultants who had been engaged to strengthen its cyber defense.

In each instance, NTU and NUS promptly alerted the Cyber Security Agency of Singapore (CSA) who has been assisting the affected universities to conduct forensic investigations to understand the nature and extent of these attacks. Based on investigations, both the attacks were the work of Advanced Persistent Threat (APT) actors. They are carefully planned and are not the work of casual hackers. The objective may be to steal information related to government or research. There is no evidence that information or data related to students was being targeted. However, as the universities' systems are separate from government IT systems, the extent of the APTs' activities appear to be limited. The daily operations of both universities, including critical IT systems such as student admissions and examinations databases, were not affected. Nonetheless, NUS and NTU have increased vigilance, and adopted additional security measures beyond those already in place.

After the incident, NUS continues to improve their information security policy and governance program.

Warm Up questions

1) According to NUS IT Security Policy, users should familiarize themselves with NUS IT Security Policy and all other relevant security standards and procedures. Though in case by case situations, ignorance will be accepted as a valid reason for noncompliance.

a. True

b. False

Warm Up questions

1) According to NUS IT Security Policy, users should familiarize themselves with NUS IT Security Policy and all other relevant security standards and procedures. Though in case by case situations, ignorance will be accepted as a valid reason for noncompliance.

a. True

b. False

Warm Up questions

Chapter 5 NUS IT Security Policy: Personnel Security

4.2.2 Users should familiarise themselves with NUS IT Security Policy and all other relevant security standards and procedures. Ignorance will not be accepted as a valid reason for non-compliance.

Warm Up questions

2) According to NUS IT Security Policy, it adopts need-to-know and least privilege access control principles. Therefore, by default, School Dean should have access to each faculty member's account on LumiNUS and evaluate whether the grading is appropriately done, as the rank of School Dean is higher than faculty members' rank in the organization.

a. True

b. False

Warm Up questions

2) According to NUS IT Security Policy, it adopts need-to-know and least privilege access control principles. Therefore, by default, School Dean should have access to each faculty member's account on LumiNUS and evaluate whether the grading is appropriately done, as the rank of School Dean is higher than faculty members' rank in the organization.

a. True

b. False

Warm Up questions

Chapter 4 NUS IT Security Policy: Access Control Security

2 Introduction

Allowing unnecessary access to NUS information system resources also invites unnecessary risk of confidentiality and integrity problems occurring due to accidental or intentional acts. Therefore, access to all information resources must be granted in a controlled manner driven by business requirements. The overall guideline is that access must only be granted based on need-to-have basis.

3.1.2 User access must be profiled using roles based upon job description, duties or function. The use of roles assists in the management of user access and provides consistency in the assignment of rights.

Warm Up questions

Job Description of Dean

They seek to meet the needs of students on campus and support social programs and activities.

Dean of Students will promote and inform students about admissions, health services and housing available on campus.

Contentious access control

Access to each faculty member's account on LumiNUS

Purpose:

Evaluate whether the grading is appropriately done

Warm Up questions

3) According to NUS IT Security Policy, dual control over the issue of access cards/keys to “secured areas” shall be in place.

a. True

b. False

Warm Up questions

3) According to NUS IT Security Policy, dual control over the issue of access cards/keys to “secured areas” shall be in place.

a. True

b. False

Warm Up questions

Chapter 6 NUS IT Security Policy: Physical and Environmental Security

3.5.3 Dual control over the inventory and issue of access cards/keys to 'secure areas' shall be in place.

Warm Up questions

4) According to NUS IT Security Policy, non-critical data should be backed up daily and stored in a secured off-site location.

a. True

b. False

Warm Up questions

4) According to NUS IT Security Policy, non-critical data should be backed up daily and stored in a secured off-site location.

a. True

b. False

Warm Up questions

Chapter 8 NUS IT Security Policy: Operations Management

6.2.5 Information systems data or functions are considered non-critical data if the unavailability of that information poses no disruption or minimal disruption of service to customers and vendors. Such information will be backed-up periodically and periodically moved to a secure off-site location.

6.2.6 Information systems data or functions are considered critical data if the unavailability of the information would completely interrupt the business from functioning (i.e., the process cannot be performed manually) and impact would be highly adverse. Such information must be backed-up daily and stored in a suitable off-site location. Consideration must be made as to whether incremental backups must occur between daily backups.

Warm Up questions

5) The agreement between NUS and suppliers may include which of the following requirements? (please select all the options that apply)

a. Compliance obligations

b. Service level agreement (e.g., availability, response time)

c. Right to monitor and review (e.g., privilege accounts, accesses, system performances, logs, configurations, transactions)

d. Right to audit (including sub-contractor)

Warm Up questions

5) The agreement between NUS and suppliers may include which of the following requirements? (please select all the options that apply)

a. Compliance obligations

b. Service level agreement (e.g., availability, response time)

c. Right to monitor and review (e.g., privilege accounts, accesses, system performances, logs, configurations, transactions)

d. Right to audit (including sub-contractor)

Warm Up questions

Chapter 3 NUS IT Security Policy: IT Security Management

3.6.4 Agreement with Supplier may include the following requirements:

(a) Compliance obligations

(i) Regulatory

(ii) Contractual

(b) Service level agreement (e.g. Availability, Response time)

(c) Logical/physical access management

(d) Right to monitor and review (e.g. privilege accounts, accesses, system performance, logs, configurations, transactions)

(e) Right to audit (including sub-contractor)

(f) Information classification

(g) Information processing (e.g. check for validity, accuracy, integrity, authenticity)

(h) Information handling (e.g. protection of information store, transfer and dispose),

(i) Backup, incidents, contingency and disaster recovery management

Discussion Questions

Discussion Question 1

1. Introduce the following roles and corresponding responsibilities.

1) Data Owner

2) Data Stewards

3) Data Managers

4) Data Custodian

5) Data Users

6) Data Governance Team

DATA OWNERS

Role : accountable for who has access to information assets within their functional areas.

NUS Context: University is the data owner of all data.

**University data does not belong to any individual or department*

DATA STEWARDS

Role: accountable for University Data within his/her functional area and ensures the accuracy, integrity, ethical conduct and use, availability and security of the data.

This includes:

(i) Defining the purpose and use of the data

(ii) Classifying the data

(iii) Creating, collecting and updating the data

(iv) Controlling access to the data

(v) Archiving or disposing the data

(vi) Ensuring the security of the data

NUS Context : Individual departments have stewardship responsibilities on behalf of the University. The department head undertakes the role of Data Steward for University Data within his/her functional area.

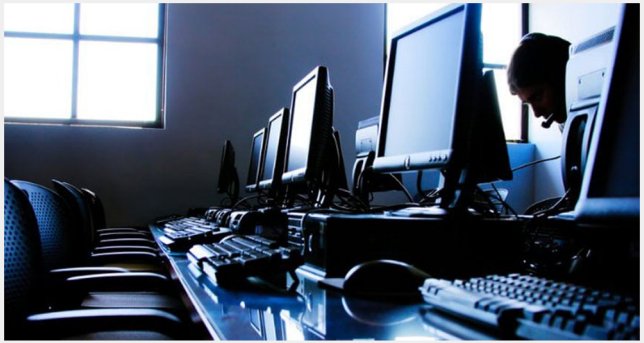
DATA MANAGER

Role: Has operational-level responsibility for data management activities and assists in day-to-day operational matters relating to University Data in his/her function and department.

NUS Context : NUS staff member (typically at the level of Manager and above or equivalent), appointed by the Data Steward, for data management

DATA CUSTODIAN

Role: responsible for the technical platform hosting University Data including its technology, design, modelling, technical maintenance and support



NUS Context :

NUS Staff (typically playing the role of an IT function)
who own the technical accountability for University Data
and are responsible for the technical management of the data

DATA USERS

Role in NUS Context :

A Data User is any person who has access to University Data to do work for NUS.

NUS Staff

(i) NUS Faculty and Staff

(ii) Part-time Teaching Staff

(iii) Contingent (casual/temporary) Staff

Non-NUS Staff

(iv) NUS and Non-NUS Student assistants, interns, helpers or volunteers (in departments, NUSSU, clubs and societies, halls and residences)

(v) Volunteers

(vi) Contractors, vendors, temporary workers

(vii) Any others who do work for the University

DATA USERS

Who is considered a data user?

2.4 A Data User is any person who has access to University Data to do work for NUS. Data Users include all NUS Staff and Non-NUS Staff. They do not include External Parties who do not do any work for NUS. Data Users have shared responsibility to ensure the appropriate use, integrity, classification and protection, of University Data. Although they have access to the data, they may only share with or disclose to others based on proper authorisation. When in doubt, they take guidance from respective Data Stewards in the handling of University Data.

2.5 The DMP applies to all Data Users who have access to University Data. Data Users include:

NUS Staff

(i) NUS Faculty and Staff
(ii) Part-time Teaching Staff
(iii) Contingent (casual/temporary) Staff

Non-NUS Staff

(iv) NUS and Non-NUS Student assistants, interns, helpers or volunteers (e.g. in departments, NUSSU, clubs and societies, halls and residences)
(v) Volunteers
(vi) Contractors, vendors, temporary workers
(vii) Any others who do work for the University

2.6 Data Users do not include those who are "customers" of the University (e.g. applicants and students in general) as they typically only access their own data for their own purposes. As such, the DMP does not apply to them.

DATA USERS

Roles of a data user

5.4 Data Users are expected to follow these instructions on use of University Data:

(i) Data Users who access University Data must only do so for the purpose of conducting University-related business or matters within their scope of work and duties. In the case of data received from External Parties in the course of work, such data must only be used for the purpose agreed with the External Parties and Data Users must comply with the NDA or equivalent terms and conditions agreed.

(ii) Data Users must abide by applicable laws and University statutes, regulations and policies with respect to the use of University Data. In particular, Data Users may not use, copy, publish, store or transmit University Data in violation of copyright laws.

(iii) Data Users must respect the confidentiality of individuals, whose Personal Data they are authorised to access, and abide by the PDPA.

(iv) The University forbids the access or use of University Data by Data Users for personal gain or profit, or to satisfy personal curiosity.

(v) Data Users must comply with all applicable protection, disclosure and control procedures for University Data to which they have been granted the right to view, copy, download or otherwise access or use.

DATA GOVERNANCE TEAM

Role in NUS Context: is a management working committee that

- Develops the enterprise data strategy including policies, standards and processes for the appropriate management of University Data.
- Determine key data sets to facilitate a single source of truth for Data Sharing.

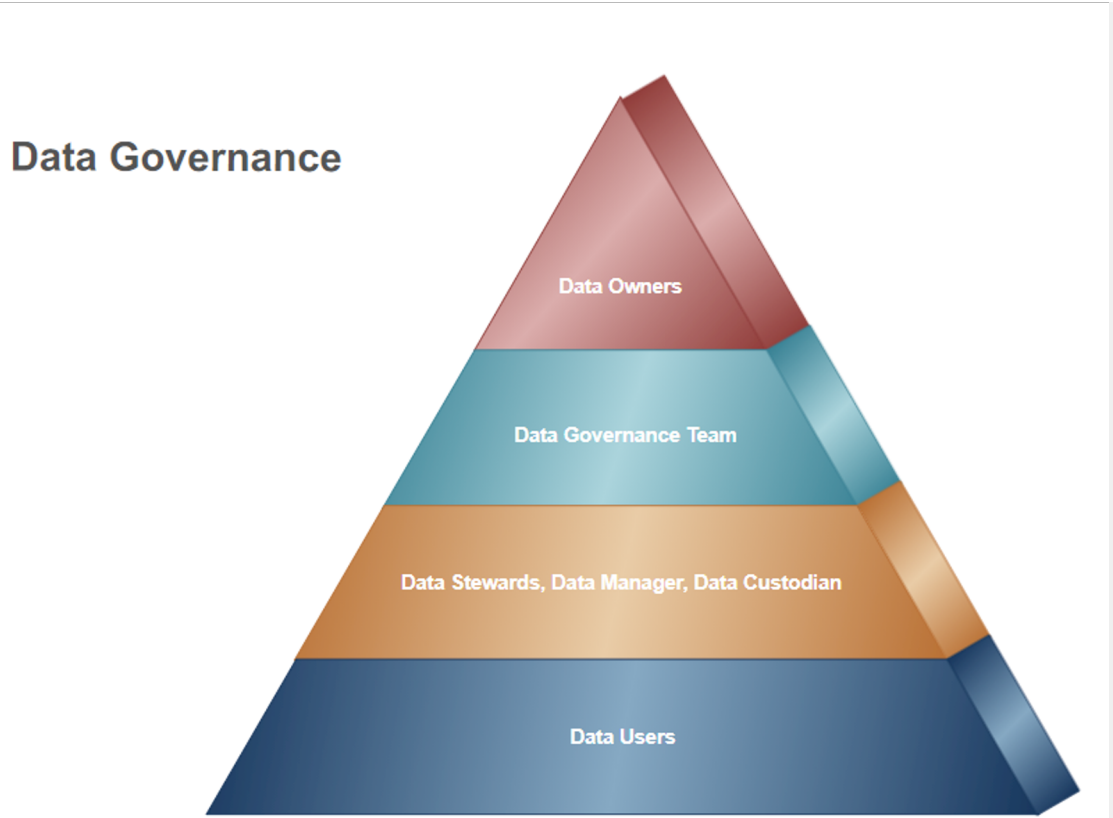
Examples include Student data (under Registrar's Office) and Staff data (under Office of Human Resources)

DATA GOVERNANCE TEAM

Who are they specifically?

Data Type	Policy	Contact
Administrative Data	This DMP	NUS IT DMP Team at dmp@nus.edu.sg
Research Data	Research Data Management Policy RDMP Guidelines	Office of the Deputy President (Research and Technology) at rcio@nus.edu.sg
Personal Data	NUS Personal Data Protection Policy NUS PDPA Compliance Guidelines	Data Protection Officer (DPO) at dpo@nus.edu.sg
Teaching and Instructional Materials	-	Office of the Senior Deputy President and Provost

DATA GOVERNANCE STRUCTURE



Discussion Question 2

Using the seven successful policy characteristics to evaluate NUS IT Security Policy, which characteristic causes the most doubt/challenge for this policy's success?

Quick Recap : 7 successful policy characteristics

1. Endorsed
   The policy has the *support of management*.
2. Relevant
   The policy is *applicable and supports the goals* of the organization.
3. Realistic
   The policy makes *sense*.
4. Attainable
   The policy can be *successfully implemented*.

Question for the class!

Based on the NUS IT Security Policy, which chapter and section of of the policy shows that the it is **endorsed?**

Chapter 3 NUS IT Security Policy: IT Security Management

3 Information Security Organisation

3.1 NUS IT Steering Committee

3.1.1 NUS IT Steering Committee is chaired by Provost and Deputy President and comprises of members from key departments. This committee provides high level support and commitment for NUS information security initiatives.

Quick Recap : 7 successful policy characteristics

5. Adaptable
   The policy can *accommodate changes*.
6. Enforceable
   There are *existing controls* that can be used to support and enforce the policy.
7. Inclusive
   The policy scope *includes all relevant parties*.

Question for the class!

Based on the NUS IT Security Policy, which chapter and section of of the policy shows that the it is **adaptable?**

Chapter 1 NUS IT Security Policy

3 Information Security

3.1 Deviations from IT Security Policy

3.1.1 Deviations from the IT Security Policy may be necessary based on operational, technical and/or cost considerations.

When a need arises that dictates that an exception to the Policy is in the best interests of NUS:

- A deviation approval request should be submitted to Chief Information Technology Officer (CITO), NUS IT;
- The request must include justifications based on a risk assessment process so that management is aware of the risks to NUS. The justifications should include the following information:
  - Security measure that has to be deviated from;
  - Reasons for the deviation;
  - Alternative security measures that have been implemented;
  - Potential impact to NUS should a breach in security occur; and
  - The period for which this deviation is required for.

Question!

What **type of Information Security Policies** does the "NUS IT Security Policy" fall under ?

A. None of the Below
B. Systems-specific policies (SysSPs)
C. Enterprise information security program policy (EISP)
D. Issue-specific information security policies (ISSP)

Question!

What **type of Information Security Policies** does the "NUS IT Security Policy" fall under ?

A. None of the Below
B. Systems-specific policies (SysSPs)
C. Enterprise information security program policy (EISP)
D. Issue-specific information security policies (ISSP)

Discussion Question 2

Using the seven successful policy characteristics to evaluate NUS IT Security Policy, which characteristic causes the most doubt/challenge for this policy's success?

Discussion! Pen your thoughts!

Discussion Question 2

Attainable

4.4 Review of user access rights

4.4.1 All special or privileged access to systems (such as administrative or supervisor accounts at the application or system level) must be reviewed every twelve (12) months or when major changes are made to the IT systems.

4.4.2 The review of user access rights should be conducted every twelve (12) months to revoke rights that are no longer required by users.

4.4.3 User access rights for all NUS applications must be onboarded and managed by the central Identity and Access Management (IAM) System.

Discussion Question 3

What is Information Security Governance Maturity Model

1. **To establish rankings for maturity within an organization**
2. **Help people assess the current effectiveness of the organization and supports figuring out what capabilities they need to acquire next in order to improve their performance**

Discussion Question 3

What it is used for:

1. **Self-assessment against the scales, deciding where the organization is**
2. **Using the results of the self-assessment to set targets for future development, based on where the organization wants to be on the scale, which is not necessarily at the top level**
3. **Planning projects to reach the targets, based on an analysis of the gaps between those targets and the present status**

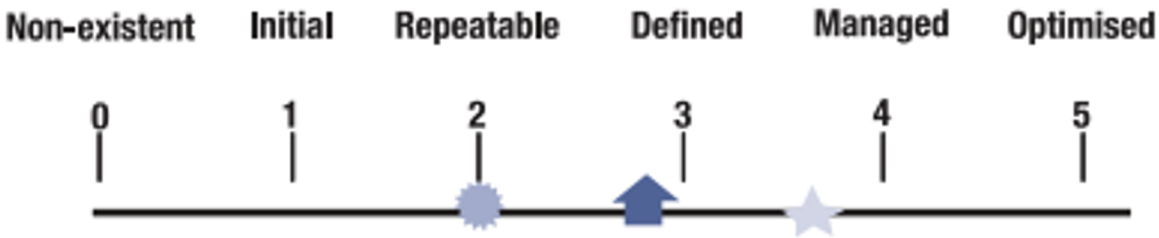
Discussion Question 3

Applied as a method for:

4. **Prioritising project work based on project classification and an analysis of its beneficial impact against its cost**

Discussion Question 3

Figure 3—Maturity Model Dashboard



LEGEND FOR SYMBOLS USED

- Enterprise current status
- Industry average
- Enterprise target

LEGEND FOR RANKINGS USED

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

Discussion Question 3

How to use a Maturity Model

1. Assess yourself
    a. Determine your current level of maturity
2. Determine how far you want to go in maturity
    a. Does not have to be the highest level
3. Identify gaps
    a. Set goals and plans in place to get to the next level
    b. Should not skip multiple levels (eg. level 1-4)

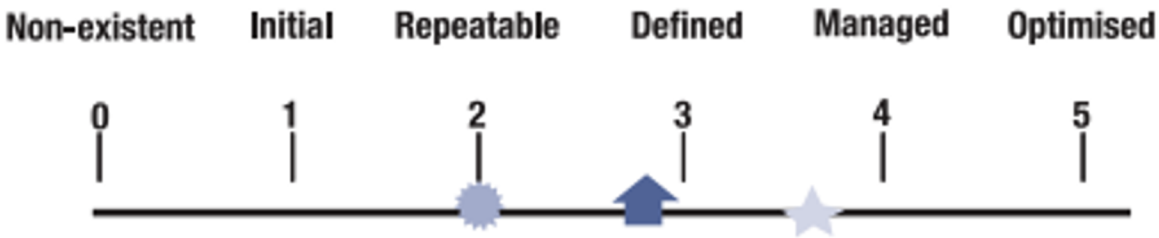
Discussion Question 3

Maturity Level Description

1. **Risk assessment**
2. **System security administration process**
3. **Service continuity**

Discussion Question 3

Figure 3—Maturity Model Dashboard



LEGEND FOR SYMBOLS USED

- Enterprise current status
- Industry average
- Enterprise target

LEGEND FOR RANKINGS USED

0—Management processes are not applied at all.
1—Processes are *ad hoc* and disorganised.
2—Processes follow a regular pattern.
3—Processes are documented and communicated.
4—Processes are monitored and measured.
5—Good practices are followed and automated.

Discussion Question 3

Based on your reading of NUS information security related policies and your daily observation on InfoSec management on campus, assess NUS information security governance management, which maturity level does NUS meet?

Discussion Question 3

Our group thinks:

Somewhere between 3 and 4. Closer to 3

Discussion Question 3

Why?

3 Defined Process

- An organisationwide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training.
- Security awareness exists and is promoted by management. Security awareness briefings have been standardised and formalised. Information security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for information security are assigned, but are not consistently enforced. An information security plan exists, driving risk analysis and security solutions. Information security reporting is IT-focused, rather than business-focused. *Ad hoc* intrusion testing is performed.
- Management communicates consistently the need for continuous service. High-availability components and system redundancy are being applied piecemeal. An inventory of critical systems and components is rigorously maintained.

4 Managed and Measurable

- The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management. It is likely that IT risk management is a defined management function with senior-level responsibility. Senior management and IT management have determined the levels of risk that the organisation will tolerate and have standard measures for risk/return ratios.
- Responsibilities for information security are clearly assigned, managed and enforced. Information security risk and impact analysis is consistently performed. Security policies and practices are completed, with specific security baselines. Security awareness briefings are mandatory. User identification, authentication and authorisation are standardised. Security certification of staff is established. Intrusion testing is a standard and formalised process, leading to improvements. Cost-benefit analysis, supporting the implementation of security measures, is increasingly being utilised. Information security processes are co-ordinated with the overall organisation security function. Information security reporting is linked to business objectives.
- Responsibilities and standards for continuous service are enforced. System redundancy practices, including use of high-availability components, are consistently deployed.

Discussion Question 3

Why?

3 Defined Process

- An organisationwide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training.

4 Managed and Measurable

- The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management. It is likely that IT risk management is a defined management function with senior-level responsibility. Senior management and IT management have determined the levels of risk that the organisation will tolerate and have standard measures for risk/return ratios.

Chapter 2 NUS IT Security Policy: Risk Analysis for Information Systems

1 Purpose and scope

The objective of risk assessment is to gain a sound understanding of the security risks associated with an information system and to determine which controls should be put in place to reduce the level of risk or to lessen the impact of a security breach.

2 Introduction

Risk assessment is an essential part of an effective approach to IT systems security. Risk assessment is performed by business owners and provides a practical mechanism for understanding the magnitude of security exposures, and assists in the evaluation and selection of appropriate controls.

3 Performing Risk Analysis

3.1 Conduct of risk analysis

3.1.1 For high impact projects, risk analysis should be performed at the initiation stage of the systems development project so that the required controls can be incorporated to the design of the system and the business processes. Risk analysis should also be performed after the system is in operation and whenever significant new developments are initiated.

3.2 Risk Analysis Process

3.2.1 A business impact analysis should be performed to assess the impact if a security breach were to occur.

Security breaches involving data or IT services, can be in the form of:
- A loss of confidentiality;
- A loss of integrity; or
- A loss of availability.

Business impact can include, but is not limited to:
- Disruptions to NUS operations;
- Legal liabilities
- Direct or indirect financial losses;
- Damage to the University's reputation and good standing; and
- Infringement of privacy issues.

3.2.2 A threat and vulnerability assessment should be performed to identify all possible risks originating from human, environmental or technical causes. Examples of threats include:
- Intentional acts – theft, fraud, information modification, hacking;
- Accidental acts – errors and omissions, information deletion/destruction, negligence;
- Natural catastrophes – fire, water damage, lightning; and
- Technical threats – bugs, viruses and malicious codes, equipment failure.

Discussion Question 3

Why?

3 Defined Process

- An organisationwide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training.
- Security awareness exists and is promoted by management. Security awareness briefings have been standardised and formalised. Information security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for information security are assigned, but are not consistently enforced. An information security plan exists, driving risk analysis and security solutions. Information security reporting is IT-focused, rather than business-focused. *Ad hoc* intrusion testing is performed.
- Management communicates consistently the need for continuous service. High-availability components and system redundancy are being applied piecemeal. An inventory of critical systems and components is rigorously maintained.

4 Managed and Measurable

- The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management. It is likely that IT risk management is a defined management function with senior-level responsibility. Senior management and IT management have determined the levels of risk that the organisation will tolerate and have standard measures for risk/return ratios.
- Responsibilities for information security are clearly assigned, managed and enforced. Information security risk and impact analysis is consistently performed. Security policies and practices are completed, with specific security baselines. Security awareness briefings are mandatory. User identification, authentication and authorisation are standardised. Security certification of staff is established. Intrusion testing is a standard and formalised process, leading to improvements. Cost-benefit analysis, supporting the implementation of security measures, is increasingly being utilised. Information security processes are co-ordinated with the overall organisation security function. Information security reporting is linked to business objectives.
- Responsibilities and standards for continuous service are enforced. System redundancy practices, including use of high-availability components, are consistently deployed.

Discussion Question 3

Security awareness exists and is promoted by management. Security awareness briefings have been standardised and formalised. Information security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for information security are assigned, but are not consistently enforced. An information security plan exists, driving risk analysis and security solutions. Information security reporting is IT-focused, rather than business-focused. *Ad hoc* intrusion testing is performed.

3.2 Risk Analysis Process

3.2.1 A business impact analysis should be performed to assess the impact if a security breach were to occur.

Responsibilities for information security are clearly assigned, managed and enforced. Information security risk and impact analysis is consistently performed. Security policies and practices are completed, with specific security baselines. Security awareness briefings are mandatory. User identification, authentication and authorisation are standardised. Security certification of staff is established. Intrusion testing is a standard and formalised process, leading to improvements. Cost-benefit analysis, supporting the implementation of security measures, is increasingly being utilised. Information security processes are co-ordinated with the overall organisation security function. Information security reporting is linked to business objectives.

Discussion Question 3

Responsibilities for information security are clearly assigned, managed and enforced. Information security risk and impact analysis is consistently performed. Security policies and practices are completed, with specific security baselines. Security awareness briefings are mandatory. User identification, authentication and authorisation are standardised. Security certification of staff is established. Intrusion testing is a standard and formalised process, leading to improvements. Cost-benefit analysis, supporting the implementation of security measures, is increasingly being utilised. Information security processes are co-ordinated with the overall organisation security function. Information security reporting is linked to business objectives.

4.2 Security training and awareness

4.2.1 All new staff and students should have access to copies of all relevant IT Security Policy, security standards, procedures and security

awareness materials appropriate for their position and role in NUS. The material is made available via the University intranet.

4.2.2 Users should familiarise themselves with NUS IT Security Policy and all other relevant security standards and procedures. Ignorance will not be accepted as a valid reason for non-compliance.

4.2.3 It is the responsibility of NUS IT Security Group to promote constant security awareness to all users.

4.2.4 Security advisories should be posted to ensure that all users who may be affected have access to these documents. Several options are available for posting security advisories; including, e-mail and/or MOTD. Security advisories should include warnings on specific risks including issues such as viruses, social engineering, technical vulnerabilities and NUS-specific risks and countermeasures.

4 Terminology

The terminology used in this Policy to convey the level of compliance to the requirements set out is as follows: Must, Shall, or Mandatory: The item mentioned is an absolute requirement and compliance is mandatory. Should: The item mentioned indicates recommended activities.

Discussion Question 3

Responsibilities for information security are clearly assigned, managed and enforced. Information security risk and impact analysis is consistently performed. Security policies and practices are completed, with specific security baselines. Security awareness briefings are mandatory. User identification, authentication and authorisation are standardised. Security certification of staff is established. Intrusion testing is a standard and formalised process, leading to improvements. Cost-benefit analysis, supporting the implementation of security measures, is increasingly being utilised. Information security processes are co-ordinated with the overall organisation security function. Information security reporting is linked to business objectives.

3.3 Personnel screening

3.3.1 The Office of Human Resources or the department should perform a background check of all staff before the staff joins NUS. This may include character references, education verification, credit check (if applicable) and independent identity check. If the employee is being hired via a third party or recruitment agency, proper screening checks must be verified by that agency as well as Office of Human Resources.

4 User access management

4.1 Account and password management

4.1.1 Each system user-ID must be unique and associated with only one user to whom it has been assigned.

4.1.2 Common privileged accounts should only be used by authorized personnel for administrative purposes only. For users with similar duties, group or role based access controls should be used to assign permissions and accesses to individual accounts.

4.1.3 Account administrators must consistently use NUS approved user-ID naming standards.

4.1.4 Where technically feasible, systems and applications should be configured to only accept passwords that are of a minimum of eight (8) characters in length and be comprised of letters, numbers, and/or special characters.

4.1.5 Initial issued passwords must not be easily associated with NUS or the user (i.e. NRIC number, employee number, address, numerical equivalent of name, etc.) and should have a minimum length of eight (8) characters.

4.1.6 Where technically feasible, systems and applications must use password history techniques to maintain a history of used passwords. This feature will prevent users from reusing passwords when they change their passwords. The history file must contain, at the least, the last six (6) user passwords and store them in encrypted form.

4.2 Authentication schemes

4.2.1 Access to NUS classified information resources should, at minimum, require a user to supply a unique user-ID and a secret password for authentication.

4.2.2 A strong authentication mechanism should be implemented for sensitive systems. This includes the use of LDAP and RADIUS, etc.

4.2.3 Authentication methods may require one or more of the following: something you have e.g., a token-based card, something that you know e.g., as a password, and something you are e.g., a thumbprint.

Advanced authentication schemes such as two-factor authentication, is recommended to be deployed for accesses to NUS critical or sensitive information resources. In such a case, users must possess two of the three requirements for authentication.

Discussion Question 3

Security awareness exists and is promoted by management. Security awareness briefings have been standardised and formalised. Information security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for information security are assigned, but are not consistently enforced. An information security plan exists, driving risk analysis and security solutions. Information security reporting is IT-focused, rather than business-focused. *Ad hoc* intrusion testing is performed.

Responsibilities for information security are clearly assigned, managed and enforced. Information security risk and impact analysis is consistently performed. Security policies and practices are completed, with specific security baselines. Security awareness briefings are mandatory. User identification, authentication and authorisation are standardised. Security certification of staff is established. Intrusion testing is a standard and formalised process, leading to improvements. Cost-benefit analysis, supporting the implementation of security measures, is increasingly being utilised. Information security processes are co-ordinated with the overall organisation security function. Information security reporting is linked to business objectives.

3.2.3 All systems shall be owned by the respective business/operating units and not by the IT Department.

Discussion Question 3

Why?

3 Defined Process

- An organisationwide risk management policy defines when and how to conduct risk assessments. Risk assessment follows a defined process that is documented and available to all staff through training.
- Security awareness exists and is promoted by management. Security awareness briefings have been standardised and formalised. Information security procedures are defined and fit into a structure for security policies and procedures. Responsibilities for information security are assigned, but are not consistently enforced. An information security plan exists, driving risk analysis and security solutions. Information security reporting is IT-focused, rather than business-focused. *Ad hoc* intrusion testing is performed.
- Management communicates consistently the need for continuous service. High-availability components and system redundancy are being applied piecemeal. An inventory of critical systems and components is rigorously maintained.

4 Managed and Measurable

- The assessment of risk is a standard procedure and exceptions to following the procedure would be noticed by IT management. It is likely that IT risk management is a defined management function with senior-level responsibility. Senior management and IT management have determined the levels of risk that the organisation will tolerate and have standard measures for risk/return ratios.
- Responsibilities for information security are clearly assigned, managed and enforced. Information security risk and impact analysis is consistently performed. Security policies and practices are completed, with specific security baselines. Security awareness briefings are mandatory. User identification, authentication and authorisation are standardised. Security certification of staff is established. Intrusion testing is a standard and formalised process, leading to improvements. Cost-benefit analysis, supporting the implementation of security measures, is increasingly being utilised. Information security processes are co-ordinated with the overall organisation security function. Information security reporting is linked to business objectives.
- Responsibilities and standards for continuous service are enforced. System redundancy practices, including use of high-availability components, are consistently deployed.

Q&A

Thank you!

Any questions for us?