IS4231 T3

Information Security Management

Tutorial 6

Presented by **T3G3**:
Ahmad Mudaafi' B Zainuddin (A0183370H)
Felix Halim (A0200664N)
Hubertus Adhy Pratama Setiawan (A0200816R)
Tan Yan An (A0199673H)

What will we discuss today?

01

Quiz Warm-up

LumiNUS Quiz

02

R&R in Data Governance

Various roles involved in Data Governance process

03

Challenge for Policy

Evaluation of NUS IT Security Policy against seven successful characteristics

04

InfoSec Governance Maturity Model

Model Introduction and Maturity Assessment against NUS Environment

01

Quiz Warm-up

Let’s Review the Quiz Questions

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.

V True

X False

According to NUS IT Security Poli should familiarize themselves with NUS IT Secu d all other relevant security standards and procedur case by case situations, ignorance will be accepte valid reason for noncompliance.

X False

Chapter 5

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.

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.

V True

X False

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 teaching is appropriately done, as the rank of School Dean is higher than faculty members' rank in the organization.

X False

Chapter 4

3.1.3 The rules used in the assignment of rights based on user roles must be explicit and rights assigned must be adequately segregated such that no single user has the ability to commit fraudulent or malicious activities. Access rights granted to each role should be documented and communicated to users and all relevant staff responsible for user access administration.

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

V True

X False

According to NUS IT Security Pol[illegible] control over the issue of access cards/keys to "secu[illegible]hall be in place.

V True

Chapter 6

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

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

V True

X False

According to NUS IT Sec ... non-critical data should be backed up daily and store ... secured off-site location.

X False

Chapter 8

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.

The **agreement between NUS and suppliers** may include which of the following requirements?

a. **Compliance** obligations
b. **S**ervice **l**evel **a**greement (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)

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

Chapter 3

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)

02

R&R in Data Governance

Various roles involved in Data Governance process

R&R in Data Governance

- **Data Owner**
- **Data Stewards**
- **Data Managers**
- **Data Custodian**
- **Data Users**
- **Data Governance Team**

- Individuals who has **access to data as part of assigned duties**
- **specialized in certain domains and data assets** with oversight responsibility for a subset of the organization's data in **tactical perspective**
- Team composed of **various roles who champions data governance**
- **technical professionals** and responsible for the storage, maintenance, and protection of sources of data
- responsible for the **implementation and oversight of the** organization's data management **goals, standards, practices, process, and technologies**
- **control the security and use of** a data

R&R in Data Governance

Data Owner

Individuals who **control the security and use of a particular set of information**, often involved in decision making.

- Approve **data glossaries and data definitions**
- Ensure **the accuracy of information**
- Oversee **activities related to data quality**

Data Stewards

Individuals who are **accountable for University Data and provide overall guidance** for the processing and use of University Data within their function and department.

- **Collection, use, maintenance, disposal, and protection** of University Data
- Ensure **necessary data procedures and guidelines are in place**
- Ensure that **areas of responsibility are defined and assigned**

Data Managers

Individuals who are **responsible for data management activities.**

- Handle **data sharing** with Data Users/ External Parties
- Provide **data requirement** to System Owners
- Develop **data procedures** and **guidelines**

R&R in Data Governance

Data Custodian

Individuals who are **responsible** for the **technical platform** hosting University Data including its **technology, design, modelling, technical maintenance and support**

- Responsible for **technical management** of the data
- Does **not access production data** without authorisation but may have **access to anonymised production data** for support purposes

Data Users

Individuals who has **access** to University **Data to do work** for NUS.

Consists of 2 categories: NUS and Non-NUS Staff

- Ensure that Non-NUS Staff are **bound to NDA**
- Ensure that Non-NUS Staff **uphold the principles of Data Management Policy**

Data Governance Team

Team composed of **various roles who champions data governance and drives awareness** and **transformation** within the organisation within the data governance plan.

03

Evaluation of NUS' IT Policy

Successful Policy Characteristics

Endorsed
Does/will the management support the policy?

Relevant
Inline with NUS' goals?

Realistic
Does the policy make sense?

Attainable
Can be implemented?

Adaptable
Can the policy be changed if needed?

Enforceable
Controls exists to support and enforce the policy

Inclusive
Policy scope includes all relevant parties

Possible Doubts/Challenges

Endorsed

Does/will the management support the policy?

C1 - 1.3.1
CTO can approve deviations

C1 - 3.3.2
NUS IT Steering Committee Chaired by Provost and Deputy Provost to provide **Strategic Direction**

Relevant

Inline with NUS' goals?

C8 - 5.1.2
Users are not allowed to develop or possess viruses or malicious software

Possible Doubts/Challenges

Realistic

Does the policy make sense?

C4 - 4.3.6
Deletion of accounts and **changing of role-based passwords**

C4 - 9.3.1
System admins must perform system monitoring activities as part of **daily work**

C6 - 5.1.3
All information on whiteboards or workboards must be erased after use.

Attainable

Policy scope includes all relevant parties

C8 - 6.2.7
Individuals are responsible for performing back-ups of critical files on their personal devices

Possible Doubts/Challenges

Inclusive

Policy scope includes all relevant parties

C1 - 1.3.2

- Audience is staff and students
- External parties that have dealings with NUS

Adaptable

Can the policy be changed if needed?

C1 - 1.3.1 | C3 - 3.5.4

CTO can approve deviations

C7 - 3.3.3

Emergency changes may be routed through relevant **Project or Network Manager** but must be documented and approved within 24 hours of the problem being resolved

Possible Doubts/Challenges

Enforceable

Controls exists to support and enforce the policy

C4 - 4.1.1, 5.1.1
No account sharing

C4 - 4.1.2, 4.3.2
Don't use privileged accounts for non-administrative/day-to-day purposes

C4 - 7.1.2
Log in with personal account before logging into administrative accounts of systems such as Unix

C4 - 5.1.3
Punishment for not protecting the confidentiality of his/her passwords

What characteristic do you think is the biggest challenge to the success of NUS' IT Policy?

Endorsed

Relevant

Enforceable

Attainable

Realistic

Inclusive

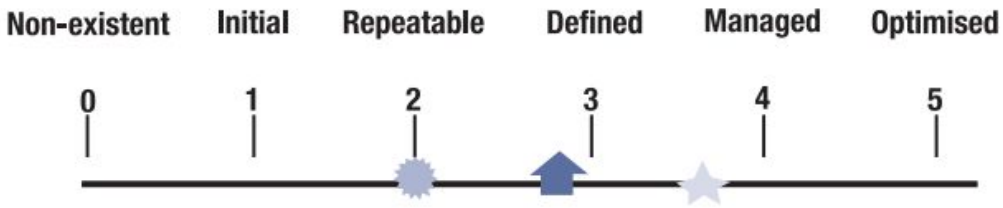
Adaptable

04

InfoSec Governance Maturity Model

A model to establish rankings for maturity within an organisation

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.

Information Security Risk Management

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Risk management has not been identified as relevant to acquiring IT solutions and delivering IT services **Risk assessment** for processes and business decisions **does not occur.**	The organisation **considers IT risks in an ad hoc manner**, without following defined processes or policies. **Informal assessments** of project risk take place **as determined by each project**.	An **approach** to risk assessment **exists**, but the **process is still immature** and developing	An organisation wide **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	Senior and IT management have **determined the levels of risk** that the organisation will **tolerate**. The assessment of risk is a **standard procedure** and **exceptions** to following the procedure **would be noticed** by IT management	Information security reporting provides **early warning of changing and emerging risk**, using **automated active monitoring** approaches for critical systems

Information Security Policies (Administration)

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Does not recognise need for InfoSec No recognisable system security administration process	**Recognises need** for InfoSec	**Emerging understanding** of importance of IT risks **Developing** security policies with **inadequate skills and tools**	**An information security plan exists**, driving risk analysis and security solutions.	Security policies and practices are **completed**, with **specific security baselines**	Information security requirements are **clearly defined, optimised** and included in a **verified security plan**

Organisation of information security

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Responsibilities and accountabilities are **not assigned** for ensuring security.	Information security breaches invoke finger-pointing responses if detected, because **responsibilities are unclear**.	Responsibilities and accountabilities for information security are **assigned to** an information security co-coordinator with **no management authority.**	Responsibilities for information security are **assigned**, but are **not consistently enforced.**	Responsibilities for information security are **clearly assigned, managed and enforced**	Risk management has developed to the stage that a **structured, organisation wide process** is **enforced, followed regularly and managed well**

System acquisition, development and maintenance

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Information Security is **not a part** of the organisation's processes	Information Security is **not a part** of the organisation's processes	Information Security is **not a part** of the organisation's processes	Information security **procedures are defined** and **fit** into a **structure for security policies** and procedures.	Information security **processes are coordinated** with the **overall organisation security** function	Security processes and technologies are **integrated organisation wide** Security functions are **integrated** with applications at the **design stage** and **end users are increasingly accountable** for managing security

Human Resource Security

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Employees are **not aware** of the risks and threats of the cyberspace.	Security awareness **depends** on the **individual, no formal training** from the organisation	Security awareness **fragmented** and limited.	A **standardized** and **formalized** security awareness **training**	A standardized and formalized security awareness training is well **managed** and **enforced** Security **certification** of staff is established User **identification, authentication** and **authorisation** are **standardised.**	A standardized and formalized security awareness training is well **managed** and **enforced** Security **certification** of staff is established User **identification, authentication** and **authorisation** are **standardised.**

Incident Response

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
No response process to information security breaches	Reactive incident response, with **no clear playbook** and **no person-in-charge**	Reactive incident response by **blindly adopting third-party offerings**.	An **information security plan exists**. A **proactive** approach to scan for vulnerability is done on an **ad-hoc basis**	An information security plan exists. Intrusion testing is a **standard** and **formalised** process.	The information security plan is supported by **automated** tools. Intrusion testing, root cause analysis, and threat intelligence are implemented.

Operations Security

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
No security monitoring and reporting measure is put in place	**No security monitoring and reporting** measure is put in place	Information security **information** is **generated**, but **not analysed**	Information security **information** is **generated**, but **not analysed** Information security **reporting** is **IT-focused**, rather than business-focused	**Cost-benefit analysis**, supporting the implementation of security measures. Information security reporting is linked to **business objectives.**	Information security reporting provides **early warning of changing and emerging risk,** using **automated** active monitoring approaches for critical systems.

Business Continuity Management

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Service continuity is **not considered** as needing management attention.	Responsibilities for continuous service are **informal, with limited authority.** Management is **becoming aware** of the risks related to and the need for continuous service	Responsibility for continuous service is assigned. The approaches to continuous service are **fragmented**. **Reporting** on system availability is **incomplete** and does not take business impact into account.	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**.	Responsibilities and standards for continuous service are **enforced**. **System redundancy** practices, including use of high-availability components, are **consistently deployed**	Continuous service plans and business continuity plans are **integrated**, **aligned** and routinely **maintained**. Buy-in for continuous service needs is secured from **vendors** and **major suppliers.**

So, what were your average ratings for NUS?

THANKS!

Feel free to share your opinion or queries 😀