ROLES & RESPONSIBILITY IN IMPLEMENTING MS ISO/IEC 27001:2007 ISMS

CONTENT

1) Objectives
2) Cabinet Decision on ISMS
3) Critical Services or Products and CNII Entities
4) Defining ISMS Scopes
5) Workshop Group Exercise
6) Reporting Progress
7) Instructions to CNII Entities
8) Some Common Questions

CONTENT

1) Objectives
2) Cabinet Decision on ISMS
3) Critical Services or Products and CNII Entities
4) Defining ISMS Scopes
5) Workshop Group Exercise
6) Reporting Progress
7) Instructions to CNII Entities
8) Some Common Questions

OBJECTIVES

1. Understanding Cabinet decision on ISMS

2. Implementation of Cabinet decision
   a) Roles & Responsibilities of Governing Agencies
   b) Identifying Critical Products and Services & CNII Entities
   c) Identifying ISMS's Scope
   d) Progress reporting requirements
   e) Instructions to CNII Entities

CONTENT

1) Objectives
2) Cabinet Decision on ISMS
3) Critical Services or Products and CNII Entities
4) Defining ISMS Scopes
5) Workshop Group Exercise
6) Reporting Progress
7) Instructions to CNII Entities
8) Some Common Questions

CABINET DECISION

1. Mesyuarat Jemaah Menteri pada 24 Februari 2010 telah memutuskan bahawa:

   a) Supaya dilaksanakan Pensijilan MS ISO/IEC 27001:2007 Pengurusan Sistem Keselamatan Maklumat (Information Security Management System-ISMS) untuk sektor-sektor Prasarana Maklumat Kritikal Negara (Critical National Information Infrastructure - CNII);

   b) Supaya pelaksanaan Pensijilan ISMS ini diselaraskan oleh kementerian-kementerian dan agensi-agensi regulatori yang bertanggungjawab terhadap sektor CNII Negara; dan

   c) Supaya organisasi-organisasi CNII mendapat Pensijilan ISMS dalam tempoh 3 tahun.

GOVERNING AGENCIES DEFINITION

1. Governing Agencies are:
   a) Regulatory Bodies (see *Regulatory Bodies*),
   b) *Central Agencies*,
   c) State Agencies and
   d) Ministries

   that have authority to direct CNIIs under their purview to comply to government directives and decisions.

2. Examples of these are:
   a) the Prime Minister's Department that oversees Petronas and
   b) the Ministry of Domestic Trade, Cooperatives and Consumerism that oversees Bank Rakyat.

3. The term Governing Agencies will be generally used instead of Regulatory Bodies which is specific to only one category of Governing Agencies.

GOVERNING AGENCIES RESPONSIBILITIES SUMMARY

1. Identify Critical Services or Products
2. Identify CNII Entities associated with the Critical Services or Products
3. Notify CNII Entities of Cabinet’s decision
4. Conduct briefing to CNII Entities on implementation of Cabinet decision
5. Collect ISMS Scope information from CNII Entities (within 2 months)
6. Collect information on ISMS implementation progress periodically
7. Report to NC3/NaCSAC on ISMS implementation progress
8. Respond to any queries from NC3/NaCSAC on ISMS implementation progress

CONTENT

1) Objectives
2) Cabinet Decision on ISMS
3) Critical Services or Products and CNII Entities
4) Defining ISMS Scopes
5) Workshop Group Exercise
6) Reporting Progress
7) Instructions to CNII Entities
8) Some Common Questions

NCSP FOCUS ON TEN SECTORS

1. National Defence & Security
2. Banking & Finance
3. Information & Communications
4. Energy
5. Transportation
6. Water
7. Health Services
8. Government
9. Emergency Services
10. Food & Agriculture

CRITICAL SERVICES AND PRODUCTS DEFINITION

1. Within the context of the NCSP, the Critical Services or Products are those that are delivered to the external organisation or the organisation's consumers and satisfy the critical services or products availability needs of the external organisation or consumers i.e. industry, public, the economy and the nation. This external organization or consumers may be other CNII entities.

2. However intra-services or products, i.e. services from one department that serves other departments in the same organisation e.g. Human Resources, Procurement and Finance, are NOT considered critical from the NCSP standpoint UNLESS those intra-services or products contribute to the immediate availability of the critical services or products delivered to the external organisation.

CRITICAL SERVICES OR PRODUCTS EXAMPLES

1. Example of services or products
   a) Internet Service – ISP
   b) Communication network services
   c) Electric power
   d) Banking services
   e) Securities services
   f) Water supply
   g) Air transportation
   h) Immigration services
   i) Customs services
   j) Defence & security services
   k) Health services
   l) Emergency services

CNII ENTITIES DEFINITION

1. **CNII:** Critical National Information Infrastructure (CNII) is defined as those assets (real and virtual), systems and functions that are vital to the nation that their incapacity or destruction would have a devastating impact on:

   a) **National economic strength** - Confidence that the nation's key growth area can successfully compete in the global market while maintaining favourable standards of living.

   b) **National image** - Projection of the national image towards enhancing stature and sphere of influence.

   c) **National defense and security** - Guarantee sovereignty and independence whilst maintaining internal security.

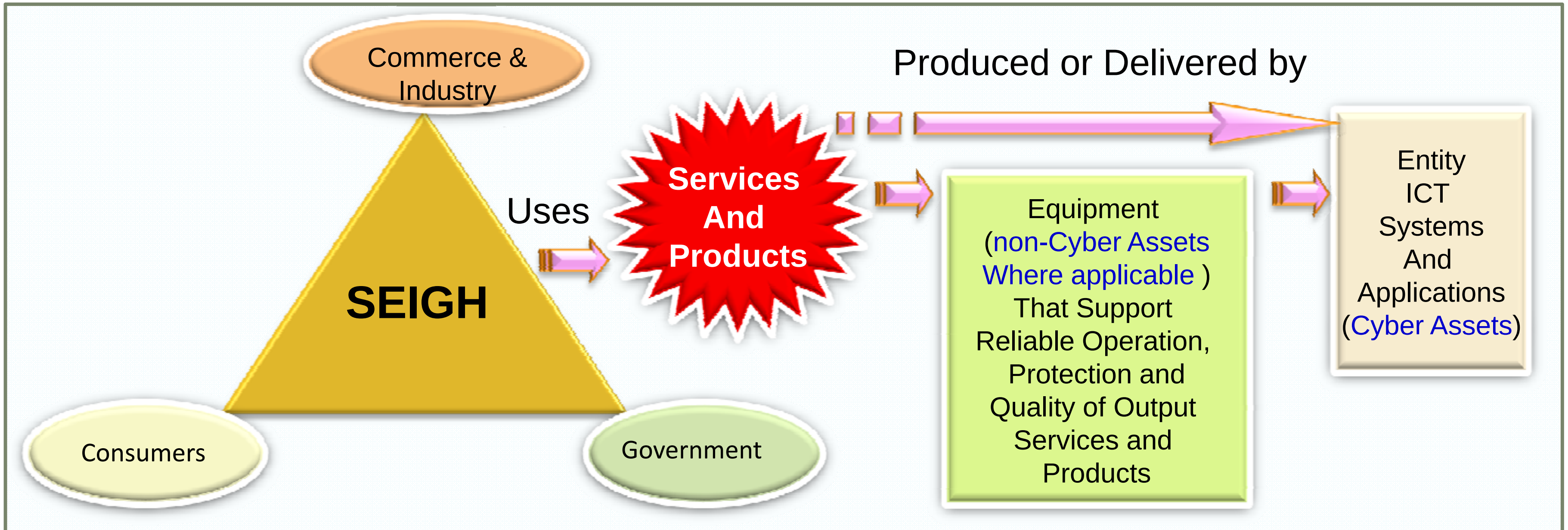
   d) **Government capability to function** - Maintain order to perform and deliver minimum essential public services.

   e) **Public health and safety** - Delivering and managing optimal health care to the citizen.

The CNII entities are those that depend on information assets or information systems for the delivery of their Critical Services or Products to the nation.

Source : National IT Council Portal - http://www.nitc.org.my/index.cfm?&menuid=60

TRACING CRITICAL SERVICES OR PRODUCTS TO CNII ENTITIES


Commerce & Industry
SEIGH
Consumers
Government
Uses
Services And Products
Produced or Delivered by
Equipment (non-Cyber Assets Where applicable) That Support Reliable Operation, Protection and Quality of Output Services and Products
Entity ICT Systems And Applications (Cyber Assets)

Steps 1 to 3 to trace from Critical Services and Products (that service the Nation and Economy) to the ICT Systems and Applications

Step 1 : Identify Critical Services and Products

Step 2 : Trace Delivery
2a : Direct
2b : Indirect

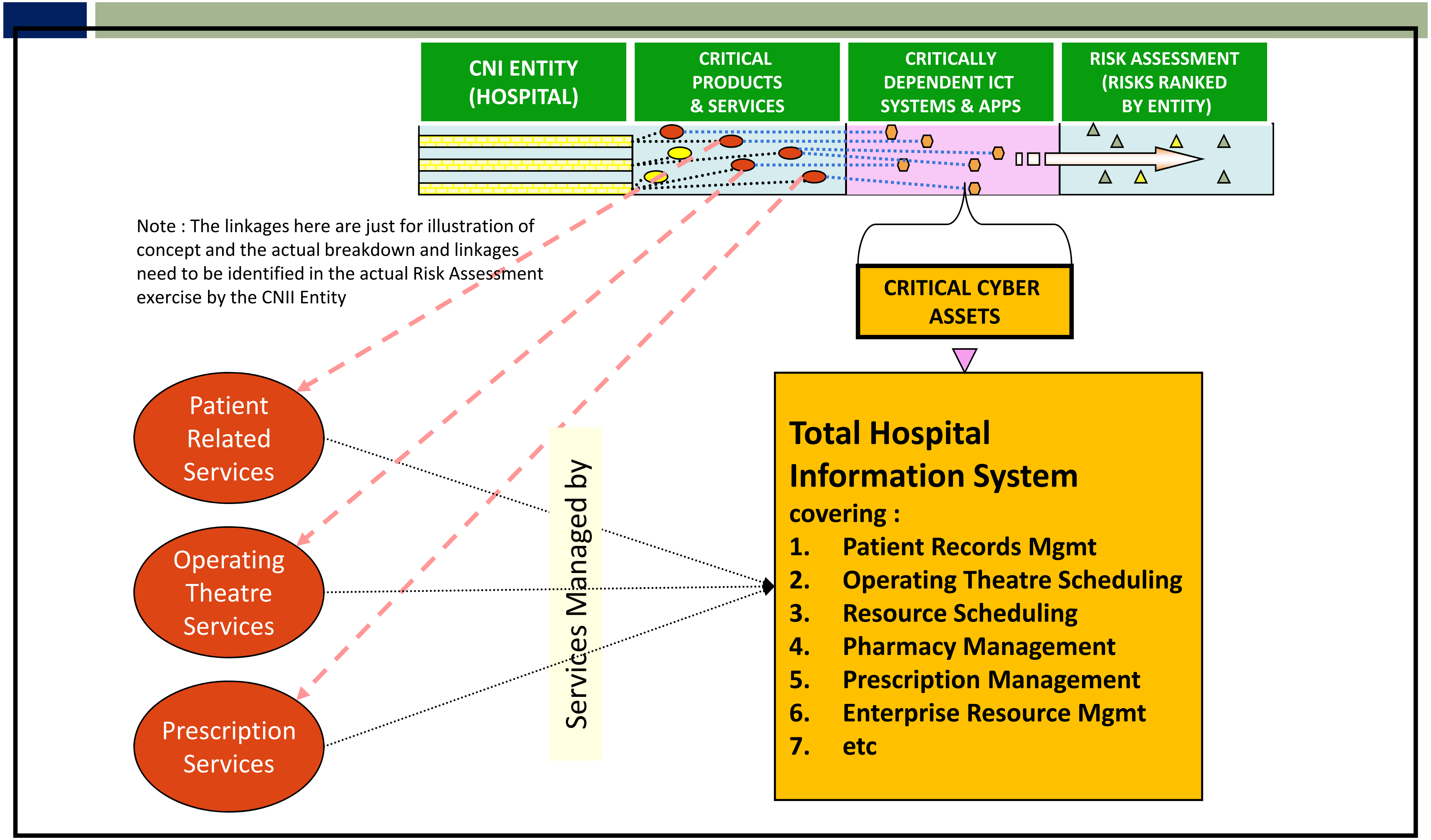
Step 3 : Identify Entity and Critical Information Assets and Information Systems

TYPES OF ENTITIES

1. Type 1 : Entities that use cyber assets to deliver critical products and services directly (e.g. hospital, banks, securities)

2. Type 2 : Entities that use cyber assets through non-cyber assets to deliver critical products and services (e.g. power generation, power transmission)

EXAMPLE OF TYPE 1 ENTITIES USING HOSPITAL SERVICES AS EXAMPLE



CNI ENTITY (HOSPITAL)

CRITICAL PRODUCTS & SERVICES

CRITICALLY DEPENDENT ICT SYSTEMS & APPS

RISK ASSESSMENT (RISKS RANKED BY ENTITY)

Note : The linkages here are just for illustration of concept and the actual breakdown and linkages need to be identified in the actual Risk Assessment exercise by the CNII Entity

CRITICAL CYBER ASSETS

Patient Related Services

Operating Theatre Services

Prescription Services

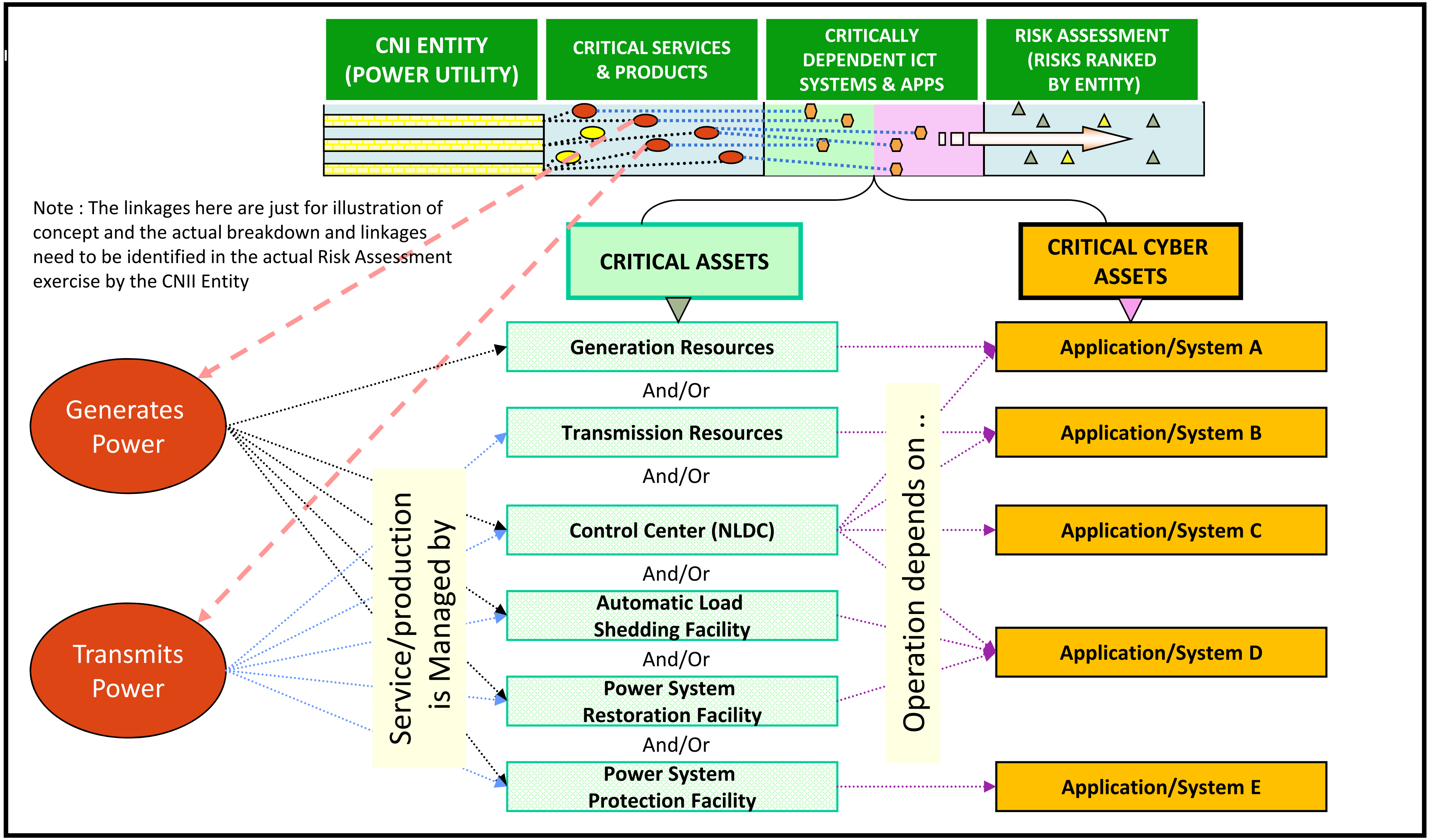
Services Managed by

Total Hospital Information System

covering :

1. **Patient Records Mgmt**
2. **Operating Theatre Scheduling**
3. **Resource Scheduling**
4. **Pharmacy Management**
5. **Prescription Management**
6. **Enterprise Resource Mgmt**
7. **etc**

EXAMPLE OF TYPE 1 ENTITIES USING POWER GENERATION AND TRANSMISSION AS EXAMPLE



Note : The linkages here are just for illustration of concept and the actual breakdown and linkages need to be identified in the actual Risk Assessment exercise by the CNII Entity

CONTENT

1) Objectives
2) Cabinet Decision on ISMS
3) Critical Services or Products and CNII Entities
4) Defining ISMS Scopes
5) Workshop Group Exercise
6) Reporting Progress
7) Instructions to CNII Entities
8) Some Common Questions

DEFINING SCOPES OF ISMS

1. Similar to Quality Management System (QMS), a Scope needs to be defined for ISMS implementation and certification

   a) Defines the boundary

   b) Clarity of Management control and oversight

   c) Enables more manageable and focused implementation

   d) Enables priority of implementation, where necessary

DEFINING SCOPES OF ISMS (CONTD)

2. Scope for ISMS implementation to meet NCSP and Cabinet directive context:
    a) Must address the delivery of critical services or products
    b) Must mention the actual critical services or products delivered

3. Risk Assessment in ISMS Plan phase must address:
    a) Impact of unavailability of critical services or products to the nation, national economy, industry
    b) Risk of non-compliance to Cabinet decision

DEFINING SCOPES OF ISMS (CONTD)

4. Example Scopes - Refer to handout (ISMS Implementation Scope Statements)

5. Possible Scope texts,
   a) “The ISMS covers the information assets and information systems that manage and deliver the ISP services.”
   b) “The ISMS covers the information assets and information systems that manage, control and delivery of electric power to the national power grid.”

6. Scope can be very elaborate to define the boundary or the boundary and details can be further elaborated in ISMS implementation documents

UNIQUE EXCEPTIONS GOVERNING AGENCIES THAT ARE ALSO CNII ENTITIES

- Governing Agencies That Are Also CNII Entities

1. Governing Agencies that are also CNII Entities are to report their progress on ISMS implementation together with CNII Entities under their purview e.g.

   a) Bank Negara Malaysia

   b) Department of Civil Aviation

CROSS REPORTING OVERLAPS RESOLUTION
– The Possible Issues

1. Some CNII Entities belong or are responsible to comply to more than one Governing Authority e.g.

   a) Bank Rakyat is under Ministry of Domestic Trade, Cooperatives and Consumerism, but must comply to BNM Guidelines. Question is which GA should enforce ISMS and/or report progress; Ministry of Domestic Trade or BNM?

   b) Customs Department is under Ministry of Finance. Which GA should enforce ISMS and/or report progress; Ministry of Finance or MAMPU?

   c) JPJ is under Ministry of Transport. Which GA should enforce ISMS and/or report progress; Ministry of Transport or MAMPU?

   d) Immigration Department is under Ministry of Home Affairs. Which GA should enforce ISMS and/or report progress; Ministry of Home Affairs or MAMPU?

DISCUSSION BREAK

CONTENT

1) Objectives
2) Cabinet Decision on ISMS
3) Critical Services or Products and CNII Entities
4) Defining ISMS Scopes
5) Workshop Group Exercise
6) Reporting Progress
7) Instructions to CNII Entities
8) Some Common Questions

WORKSHOP PROCESS

1. Participants break out into groups.

2. Groups to discuss and enter their responses in the forms provided
   a) ISMS Implementation Scope Statements – Lampiran A
   b) Critical Services/Products and Entities Matrix – Lampiran B

3. Present results – one spokesperson per group

WORKSHOP EXERCISES
- Workshop Exercises and Deliverables

1. Identify and critical services and/or products to the nation from Entities under your purview. Be prepared to explain your list.

2. Formulate the Scope of ISMS covering the critical services and/or products.
   a) There can be more than one Scope for ISMS implementation and certification in one Entity

   b) Demarcate the Scopes based on your best knowledge of the CNII Entities' operations or organisational demarcation e.g. Possible separate scopes for:
      i. TNB Generation and TNB Transmission
      ii. Retail Banking and International Banking
      iii. Each of Petronas' Gas Processing Plant (GPP1 to GPP3)
      iv. ISP and Communications Switching/Transmission services
      v. Port Container Management and Shipping Operations
      vi. Flight dispatching operations and flight support services

WORKSHOP EXERCISES

- Workshop Exercises and Deliverables **(CONTD)**

3. List the CNII Entities and Sub-entities delivering the critical services and/or products and the draft Scopes for ISMS implementation and certification
   a) Note that the list and draft Scopes are as the Governing Agencies view them. Final responsibility to draft the scope lies with the CNII Entity and Sub-Entities
   b) Do not spend time fine tuning the wording. Capture the essence of the Scopes that depict the ISMS implementation to address delivery of critical services or products

4. Present your results in workshop

CONTENT

1) Objectives
2) Cabinet Decision on ISMS
3) Critical Services or Products and CNII Entities
4) Defining ISMS Scopes
5) Workshop Group Exercise
6) Reporting Progress
7) Instructions to CNII Entities
8) Some Common Questions

REPORTING PROGRESS OF ISMS IMPLEMENTATION IN CNII ENTITIES

- Governing Agency Reporting Preparedness

1. Governing Agency to ensure they are able to explain (if required):

    a) The inclusion (classification) or exclusion of an entity or organisation, as a CNII entity,

    b) The Critical Services or Products delivered by the entities,

    c) The rationale for the logical grouping or boundary of ISMS scopes of the entities, especially if more than one ISMS is being implemented in a particular entity,

    d) The entities' stage of progress in implementing ISMS and be ISMS certified, and reasons for deviations, if any.

SOME REPORTING TOOLS PROVIDED

1. Two spreadsheets workbooks
   a) CNII Entities to record progress and submit response to Governing Agencies

   b) Governing Agencies to consolidate responses from CNII Entities and report to NC3 and NaCSAC

2. Refer to Excel workbooks provided. Lampiran D.

CONTENT

1) Objectives
2) Cabinet Decision on ISMS
3) Critical Services or Products and CNII Entities
4) Defining ISMS Scopes
5) Workshop Group Exercise
6) Reporting Progress
7) Instructions to CNII Entities
8) Some Common Questions

INSTRUCTIONS TO CNII ENTITIES

- Instructions to CNII Entities and Briefing to CNII Entities

1. Refer to letter template and customise. Lampiran F

2. Schedule workshop for CNII Entities (if required)

3. Follow up for CNII Entities to submit Scope of ISMS implementation and certification within 2 months, preferably earlier.

GOVERNING AGENCIES RESPONSIBILITIES SUMMARY

1. Identify Critical Services or Products
2. Identify CNII Entities associated with the Critical Services or Products
3. Notify CNII Entities of Cabinet’s decision
4. Conduct briefing to CNII Entities on implementation of Cabinet decision
5. Collect ISMS Scope information from CNII Entities (within 2 months)
6. Collect information on ISMS implementation progress periodically
7. Report to NC3/NaCSAC on ISMS implementation progress
8. Respond to any queries from NC3/NaCSAC on ISMS implementation progress

CONTENT

1) Objectives
2) Cabinet Decision on ISMS
3) Critical Services or Products and CNII Entities
4) Defining ISMS Scopes
5) Workshop Group Exercise
6) Reporting Progress
7) Instructions to CNII Entities
8) Some Common Questions

SOME COMMON QUESTIONS

1. Is my organisation a CNII entity?
2. What is the difference between Adopting, Complying and Certified ISMS?
3. What scope of the organisation’s ISMS implementation needs to be reported to the NC3 and NaCSAC?
4. What sorts of disruptions to services are considered critical?
5. How do organisations report the compliance to the ISMS implementation decision?
6. Will the Government fund the costs for ISMS implementation?

END OF WORKSHOP
GENERAL DISCUSSION,
SUGGESTIONS,
Q&A

38 THANK YOU

Lampiran A: ISMS Implementation Scope Statement

Lampiran B: Critical Services/Products and Entities Matrix

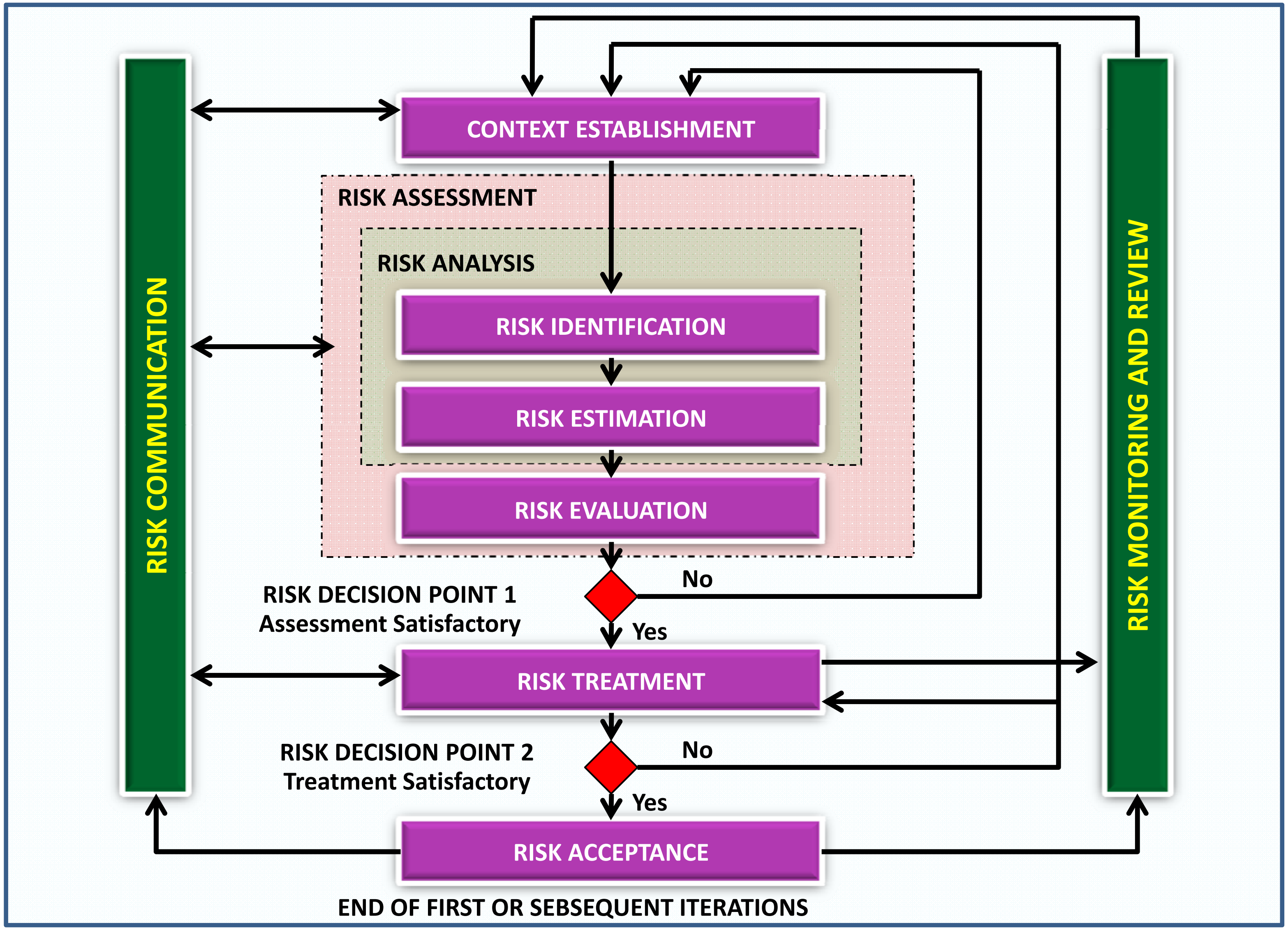
Lampiran C: ISMS Scope Notification Form

Lampiran D: Respondents

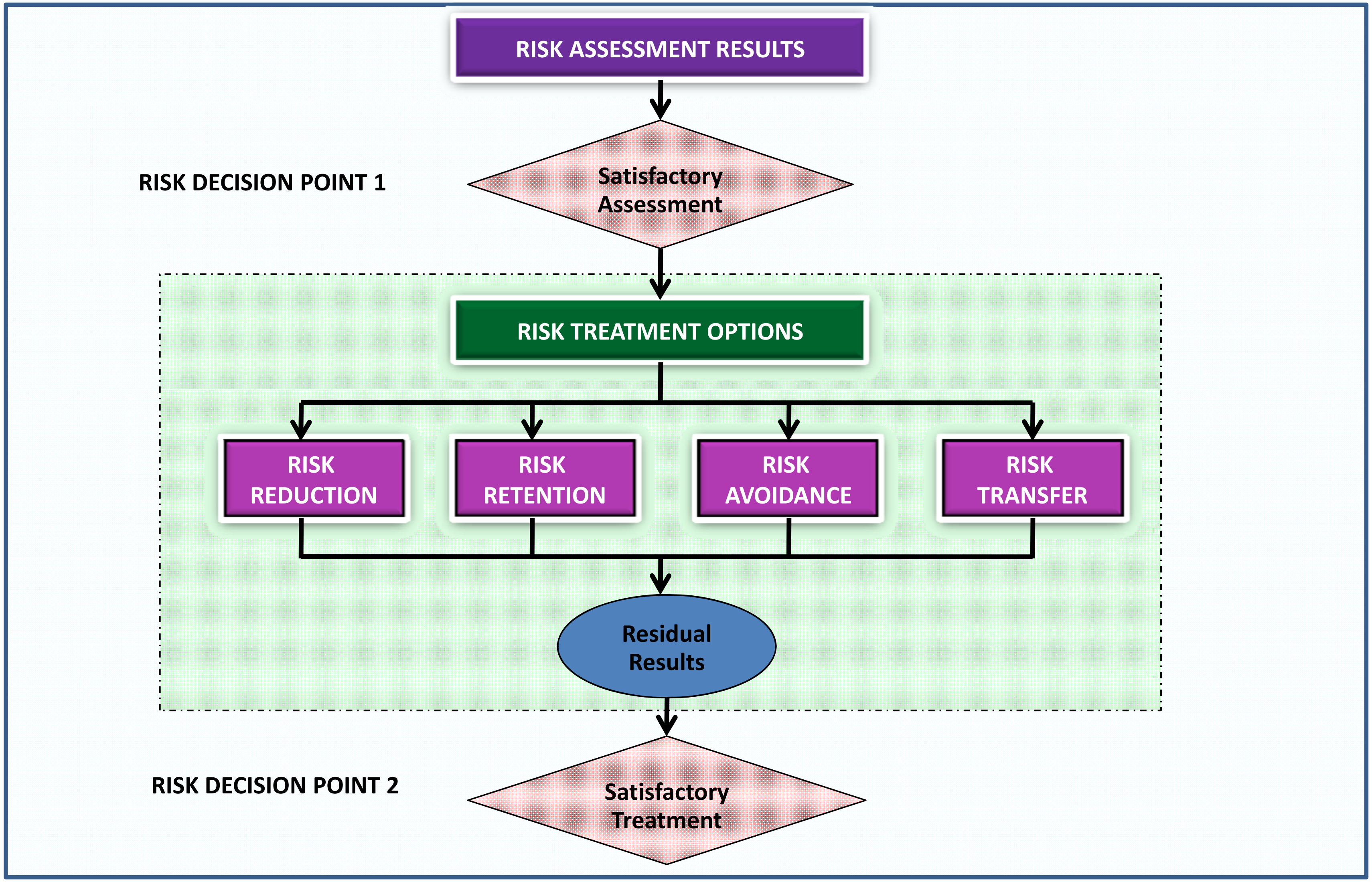
Lampiran E: Scope of ISMS – Examples From Other
Organisation Certified

Lampiran F: Letter Template

Risk Management Process - From ISO 27005



Risk Treatment Activity - From ISO 27005



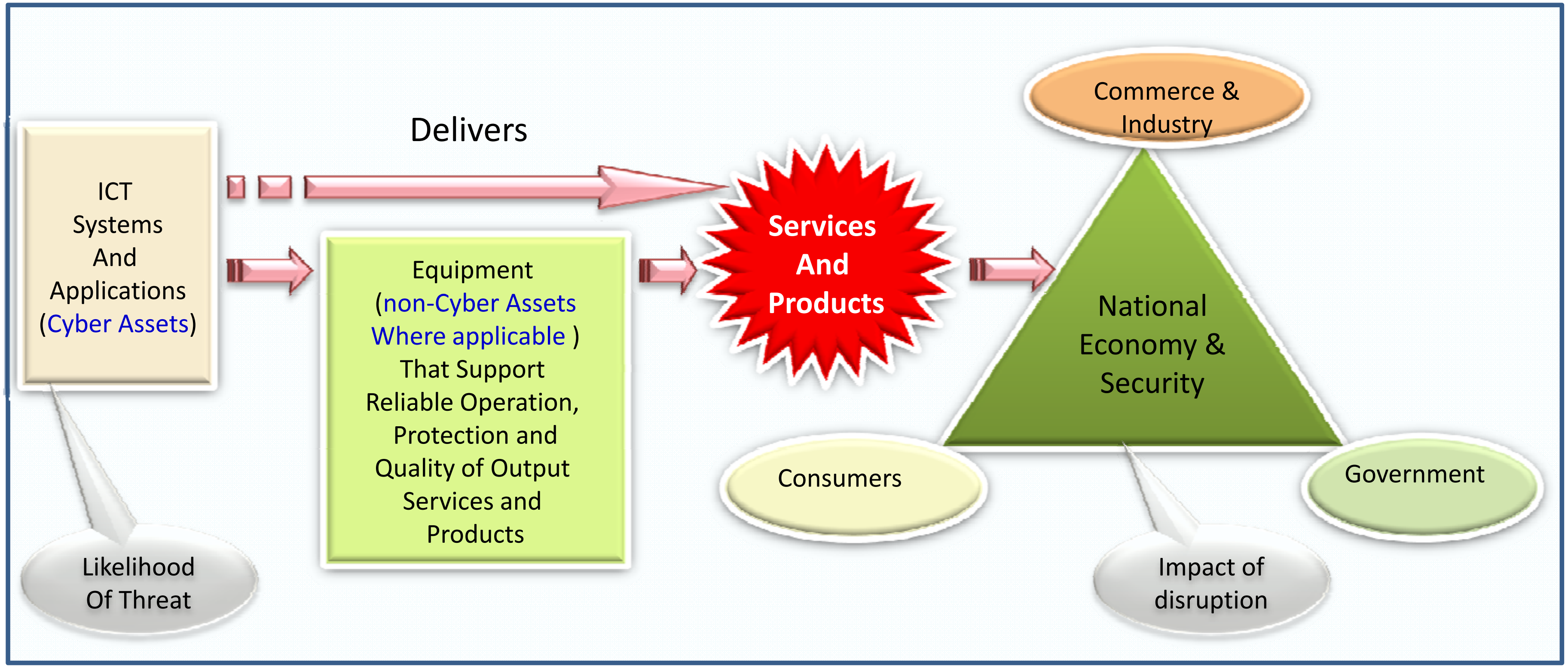
Risk Assessment – Risk Focus

Risk Assessment in NCSP context must look at the

likelihood of threats exploiting vulnerabilities to **Cyber Assets**

disrupting/compromising delivery of **Products and Services** and the

consequence or impact of the disruption/compromises of the **Products and Services to the Nation**, Commerce, Industry, Government, Consumers and other beneficiaries


ICT Systems And Applications (Cyber Assets)
Delivers
Equipment (non-Cyber Assets Where applicable) That Support Reliable Operation, Protection and Quality of Output Services and Products
Services And Products
Commerce & Industry
National Economy & Security
Consumers
Government
Likelihood Of Threat
Impact of disruption