ISM Exercise 1/2 – NI4OS VMs

- You are a service provider that has been on-boarded to the NI4OS pre-production environment.
- You are offering different types of VMs to the EOSC customers
- A customer can choose a VM flavor using the following parameters
  - OS (Ubuntu LTS, CentOS, FreeBSD, Kali Linux)
  - CPU cores (2 – 8)
  - RAM size (16 GB – 64 GB)
  - Disk size (512 GB – 2 TB)
  - Network (private / public / both)

ISM Exercise 2/2 – NI4OS VMs service provider

- Identify the most important information assets and related risks of the NI4OS VMs service provider!

  – Which assets are how critical for the operation of the services?
  – What are the potential vulnerabilities, threats and resulting security risks?

- Define reasonable information security policies and controls to address the identified risks!

FitSM

Standards for lightweight
IT service management

Service Planning & Delivery

Advanced training in service planning and delivery according to FitSM

Version 2.5

This work has been funded by the European Commission.

FitSM Standards for lightweight IT service management

Information security management (ISM)

Objective

To manage information security effectively through all activities performed to deliver and manage services, so that the confidentiality, integrity and accessibility of relevant information assets are preserved

ISM: Important terms & concepts

Definition following FitSM-0:

Information security:

Preservation of *confidentiality*, *integrity* and *accessibility* of information

- Key information security aspects:
  - **Confidentiality**
  - **Integrity**
  - **Accessibility** of information

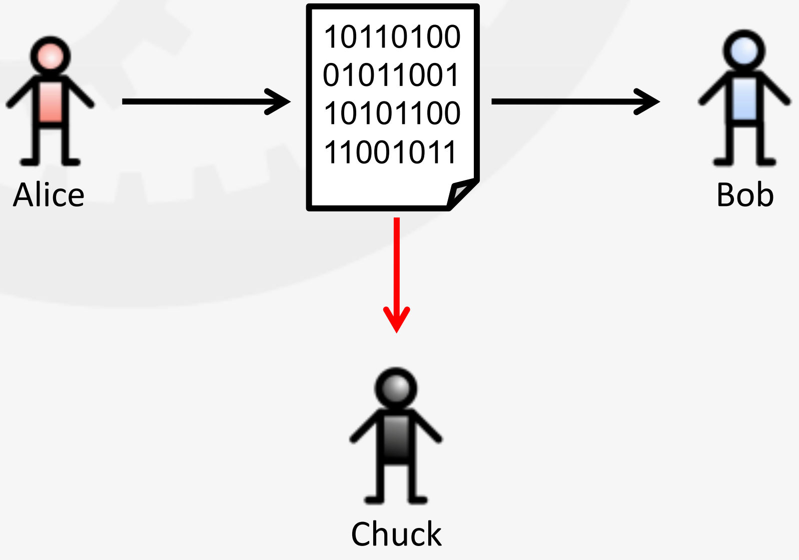
Definition following FitSM-0:

Information security control:

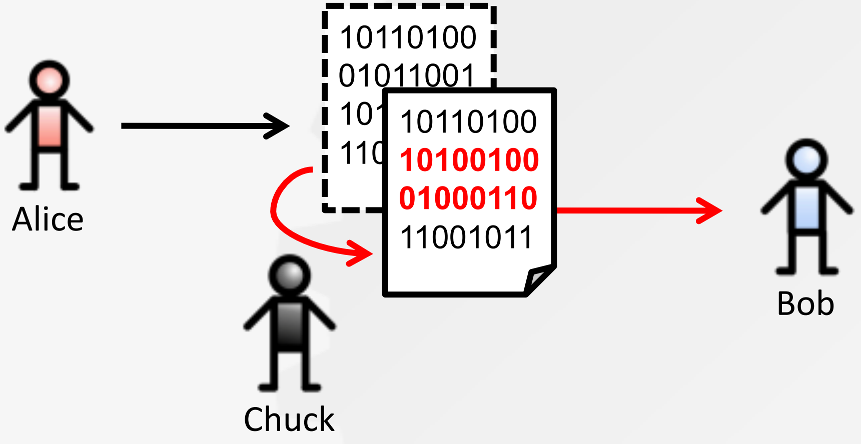
A means of controlling or managing one or more *risks* to *information security*

ISM: Confidentiality and integrity

Confidentiality: To protect information from unauthorized disclosure



Integrity: To protect information from modifications, additions, deletions, rearrangement, duplication or re-recording



ISM: Important terms & concepts

Definition following FitSM-0:

Information security event:

An occurrence or previously unknown situation indicating a possible breach of *information security*

Note: An occurrence or situation is considered a potential breach of information security if it may lead to a negative impact on the confidentiality, integrity and / or accessibility of one or more information assets.

Definition following FitSM-0:

Information security incident:

Single *information security event* or a series of information security events with a significant probability of having a negative impact on the delivery of *services* to *customers*, and therefore on the *customers*' business operations

ISM: Requirements according to FitSM-1

PR6 Information Security Management (ISM)

REQUIREMENTS

- PR6.1 Information security policies shall be defined.
- PR6.2 Physical, technical and organizational information security controls shall be implemented to reduce the probability and impact of identified information security risks.
- PR6.3 Information security policies and controls shall be reviewed at planned intervals.
- PR6.4 Information security events and incidents shall be given an appropriate priority and managed accordingly.
- PR6.5 Access control, including provisioning of access rights, for information-processing systems and services shall be carried out in a consistent manner.

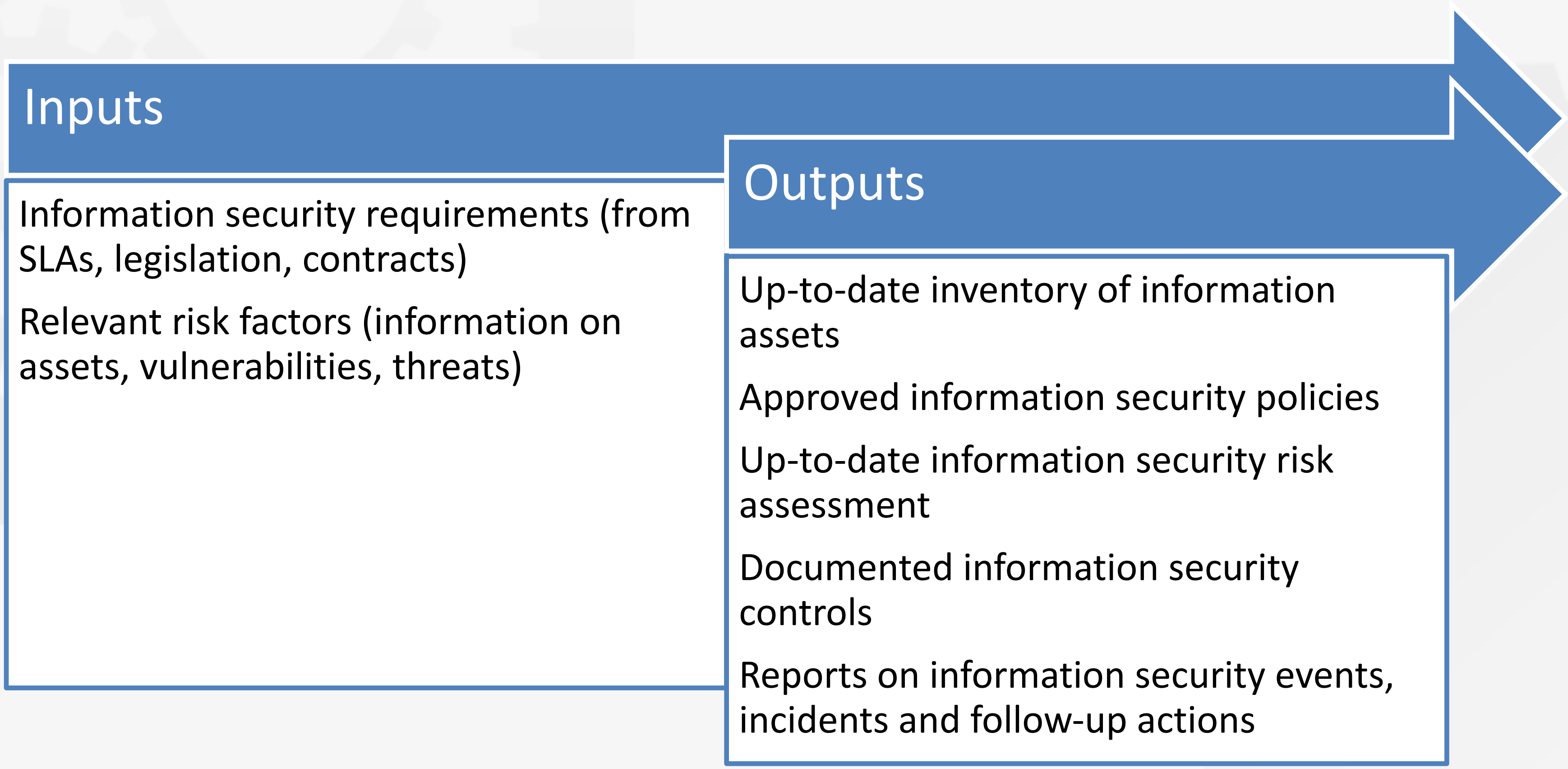
ISM: Initial process setup

Initial activities	Typical results
Define a scheme to classify information assets according to their sensitivity / criticality	Information classification scheme
Define a way to document an inventory of (information) assets	Initial (empty) asset inventory
Identify, describe and classify the most important information assets	Asset inventory filled with initial data on information assets
Identify the most important links between configuration items (CIs) such as information-processing systems / facilities and the information assets identified before	Asset inventory filled with information assets linked to CIs

ISM: Initial process setup

Initial activities	Typical results
Define a method / scheme to identify and assess information security risks	Risk assessment method and scheme
Perform an initial risk assessment, based on the identified assets, and focused on the most significant information security risks	Risk assessment report
Define clear information security policies as a basis for effective information security governance	Various information security policies
Define a way to document information security controls and to monitor their status and progress of implementation	Initial (empty) repository of information security controls
Identify and document the most important technical, physical and organisational information security controls in place	Documented information security controls

ISM: Inputs & outputs



Inputs

Information security requirements (from SLAs, legislation, contracts)

Relevant risk factors (information on assets, vulnerabilities, threats)

Outputs

Up-to-date inventory of information assets

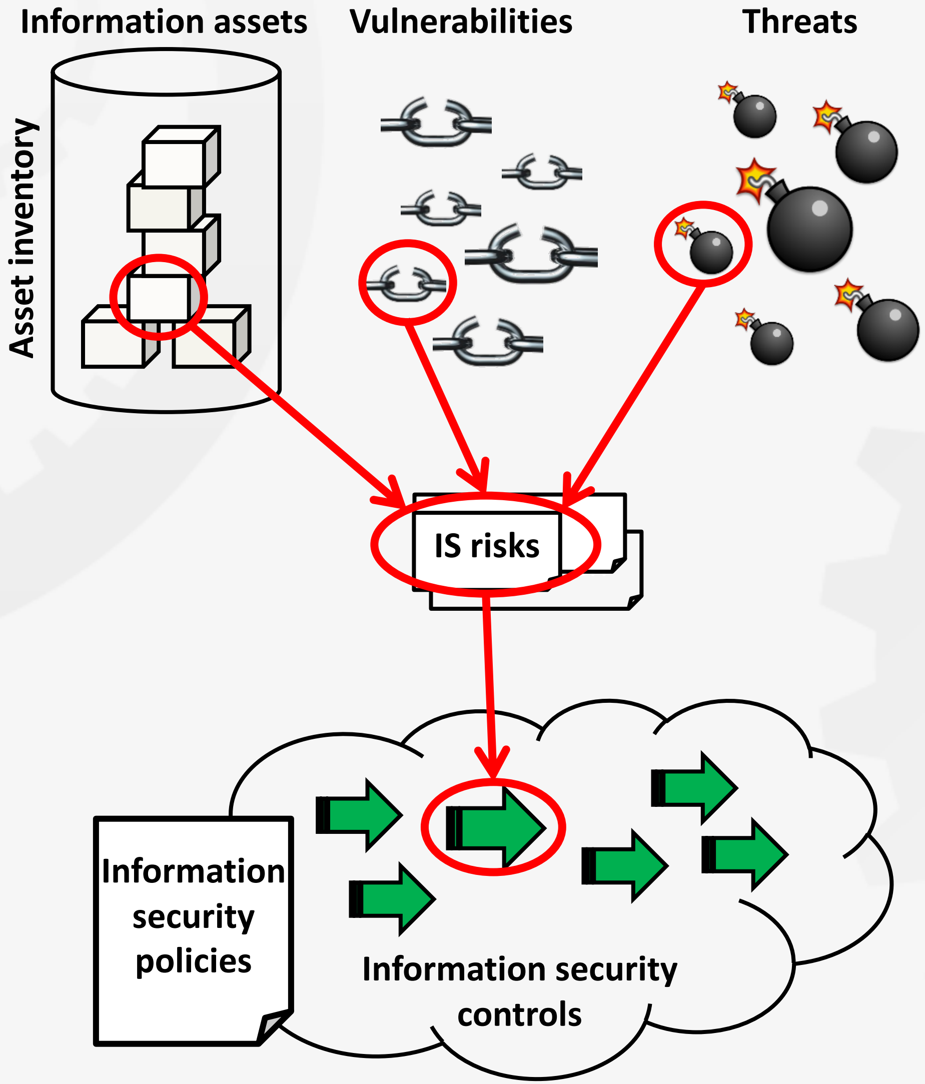
Approved information security policies

Up-to-date information security risk assessment

Documented information security controls

Reports on information security events, incidents and follow-up actions

ISM: Inputs & outputs



ISM: Ongoing process activities

- Manage (information) assets:
  - Add an information asset to the asset inventory
  - Update the description or classification of an information asset in the asset inventory
  - Remove an information asset from the asset inventory
- Manage information security risks:
  - Identify and assess a new or changed information security risk
  - Review or repeat the information security risk assessment (in regular intervals)

ISM: Ongoing process activities

- Maintain information security policies:
  - Create, approve and communicate a new information security policy
  - Update an existing information security policy
  - Retire an existing information security policy
- Plan and implement information security controls:
  - Specify a new information security control
  - Update the specification of an existing information security control
  - Retire an existing information security control

ISM: Ongoing process activities

- Manage information security events and incidents:
  - Monitor, record and classify information security events
  - Identify and handle an information security incident
  - Define and monitor follow-up actions after an information security incident
- Perform access control
  - Process requests for access rights
  - Provide access rights
  - Modify or revoke access rights
  - Review access rights (in regular intervals)

ISM: Roles

Role	Tasks	Ca. number of persons performing this role
Process owner ISM	*Generic tasks of a process owner applied in the context of ISM*	1 in total
Process manager ISM (Information security manager / officer)	*Generic tasks of a process manager, plus:* • Act as the primary contact of the service provider for all information security-related issues • Monitor the status and progress of all activities connected to the process of information security management, in particular the maintenance of the asset inventory, information security risk assessment and handling of information security events and incidents • Ensure that information security incidents are detected and classified as such as quickly as possible, and handled in an effective way to minimise harm caused by them • Ensure that all security-related documentation is maintained ad up-to-date	1 in total

ISM: Roles

Role	Tasks	Ca. number of persons performing this role
Information security risk manager	• Ensure that the asset inventory is complete and up-to-date • Ensure that the asset owners maintain the descriptions and classifications of the assets under their ownership and provide other information relevant for identifying and assessing information security risks • Perform a solid risk assessment periodically, based on available information on assets to be protected, as well as up-to-date information on vulnerabilities and threats • Update the risk assessment, whenever necessary – in particular, if a significant risk factor has changed • Together with other experts, identify, plan, implement and document information security controls to treat risks	1 in total

ISM: Roles

Role	Tasks	Ca. number of persons performing this role
Asset owner	• Maintain and review the description and classification of a specific (information) asset in the asset inventory • Act as a primary contact point for the asset under his/her ownership • Support the identification and analysis of information security risks connected to the asset under his/her ownership by providing information / input to the risk assessment	1 per (information) asset
Information security control owner	• Maintain and review the specification / documentation of a specific information security control • Act as a primary contact point and expert for the control under his/her ownership	1 per security control

ISM: Critical success factors & KPIs

Critical success factors	Key performance indicators (KPIs)
An up-to-date asset inventory is available and reviewed regularly.	• Number of assets identified and described in the asset inventory
Information security risks are identified and assessed.	• Number of risks identified
Technical, physical and organisational / administrative measures (controls) to mitigate information security risks are effectively implemented and continually reviewed and improved.	• Number of security controls planned / implemented • Costs of implementing and maintaining security controls vs. loss / damage avoided
Information security incidents are avoided effectively.	• Number of potential information security incidents that have been avoided through effective countermeasures
If an information security incident occurred, it is identified as such and handled in an effective way.	• Number of information security events identified • Number of information security incidents