Applying the concepts of IT Security Risk Management

S. Gabriel[1,2]

[1]Nikhef [2]EGI CSIRT

April 2025

What is this lecture about . . .

Enabled learning objectives:

- Understand the concept of a particular IT Security Risk management approach.
- Understand the terminology.
- Be able to apply a IT Security Risk Management Methodology to a (simple) example.

What is IT Security Risk Management?

Risk Management in

- Definition *risk management: coordinated activities to direct and control an organization with regard to risk,*
- Definition *Risk: The effect of uncertainty on objectives(ISO-27005) . . .*
  - *Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.*
- Definition *Threat:* Potential cause of an unwanted incident, which may result in harm to a system or organization. (ISO/IEC 27000:2018) (threat actor, threat event: action or occurance that exploits a vulnerability, these are collected in different catalogues used in risk scenarios.)

Why IT Security Risk Management? ... Motivation for IT OpSec people

- Dealing with IT Security Risk Management is a challenge.
- Doing Operational Security for some time leaves a nagging feeling: *... are we looking at the right spot? Is the approach to IT Sec complete/enough? and some more*.
- $\rightarrow$ a continuous process to check this would be helpful (involving the relevant stakeholders and going beyond IT security incident debriefing, RCA).
- (less good, still) ... it may be forced on you (compliance, reaching an organisational maturity level, NIS2, etc).

Some Challenges in Risk Management

Which Risk Management Method to use?

- Many different Risk Management Methods[1][2]
- Common elements
  - Define Scope/Context
  - Governance
  - Risk Assessment/Treatment

[1] https://www.enisa.europa.eu/sites/default/files/publications/0.7.2-T2-Risk_Management_standards.pdf

[2] https://www.enisa.europa.eu/publications/interoperable-eu-risk-management-toolbox

Risk Management Framework, Methodology, Tool

- Framework: ex. ISO-27005, NIST 800, OCTAVE
- Methodology: Ex. ITSRM[2]
- Tool: Ex GOVSEC.RM, MONARC, Spreadsheet; required to get "values" for Risk Scenarios, Impact analysis, Asset Valuation, contains functions[3] to calculate Risk Parameters, mapping descriptive outcomes to numerical values.

[3] simple functions like products, sums of parameters

Language

- Who is the recipient of the Risk Study?
- "Interpreter Challenge", Languages:
  - "Business terms", mostly financial, ROI, maybe also (MTPD, RTO, RPO)[4]
  - "IT lingo" (Network segmentation/Protocols/Ports/Bandwidth, Firewall rules),
  - "IT-Sec lingo" (Confidentiality, Integrity, Availability; Threats; Vulnerabilities; Security Measures.
  - Terminology across Frameworks not consistent

[4] Maximum Tolerable Period of Disruption, Recovery Time Objective, Recovery Point Objective are key metrics in disaster recovery (DR) and business continuity planning (BCP).

The Task for the Workshop

The Task

Apply ITSRM[2] to the system: University of Harderwijk Herbal Research Infrastructure, produce an IT Security Plan[5].
(The above stated business aspects of Context/Scope/Governance are provided :-))

[5] A strategic document containing a plan of actions designed to improve the security and resilience of infrastructures and services including measures to protect the confidentiality, integrity, and availability of information and systems

The IT Security Risk Management Methodology ($ITSRM^2$)

ITSRM^2 and ISO 27005

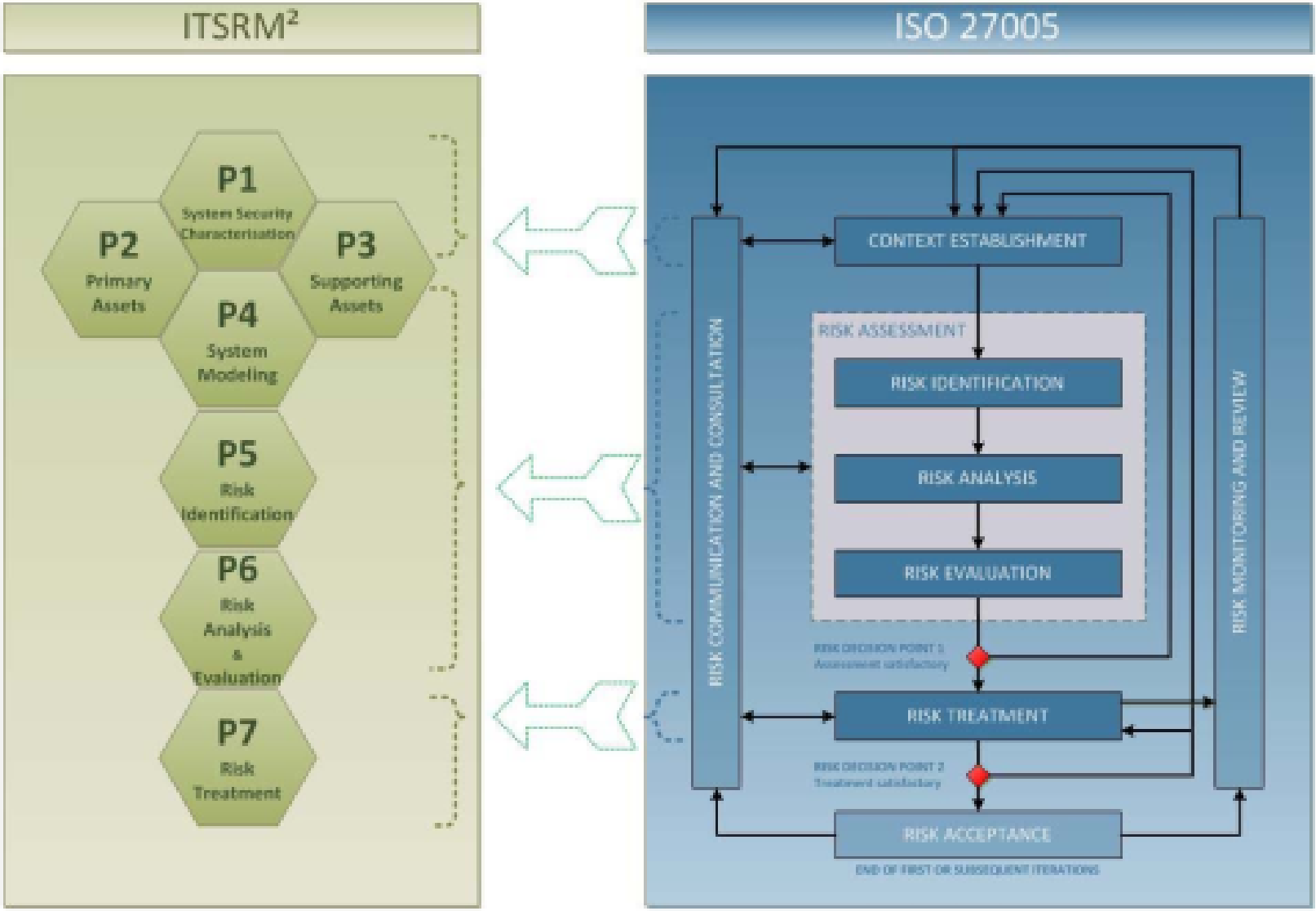


Figure 1-1: Mapping between ISO 27005 and ITSRM Methodology processes

ITSRM^2 and ISO 27005

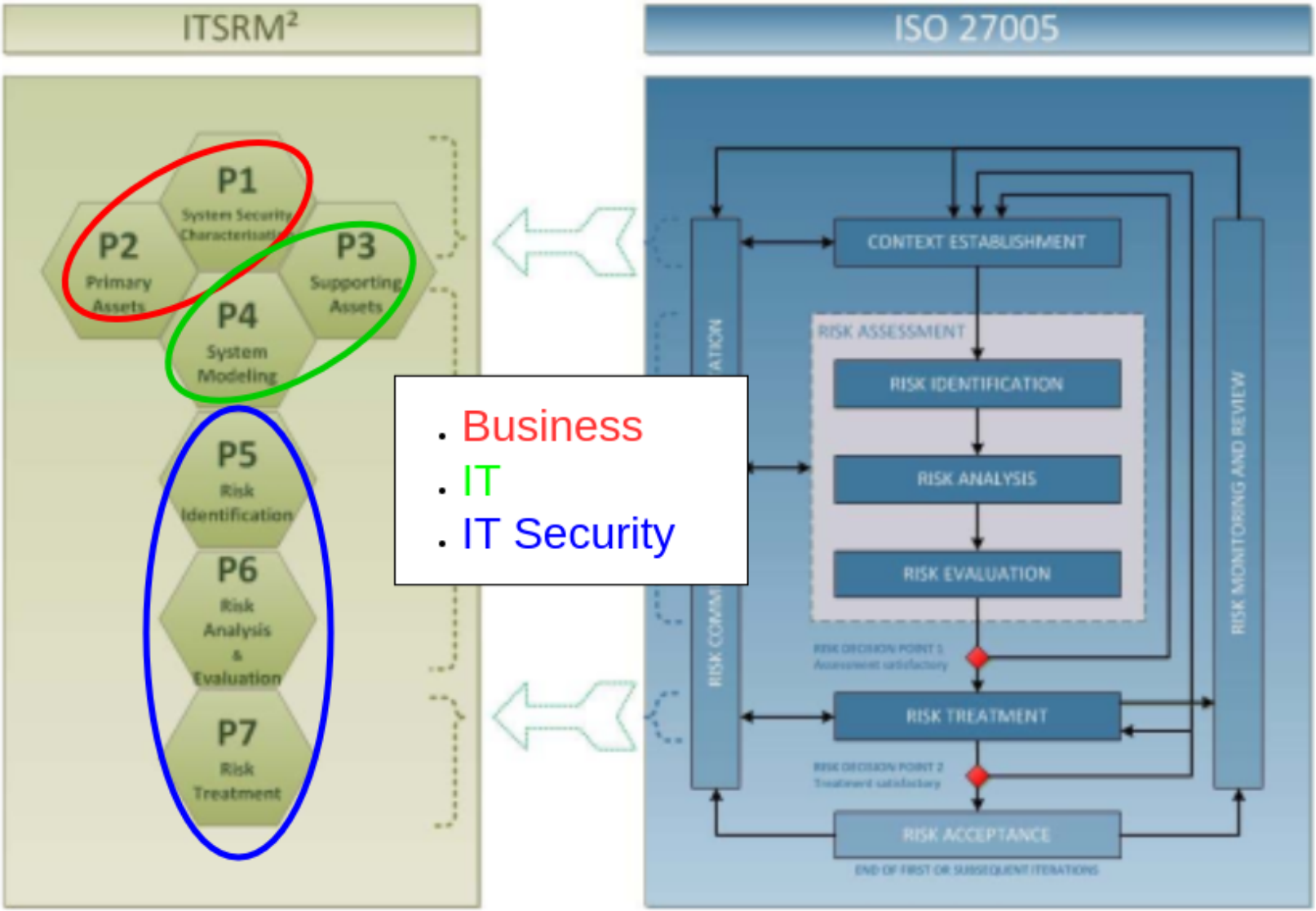
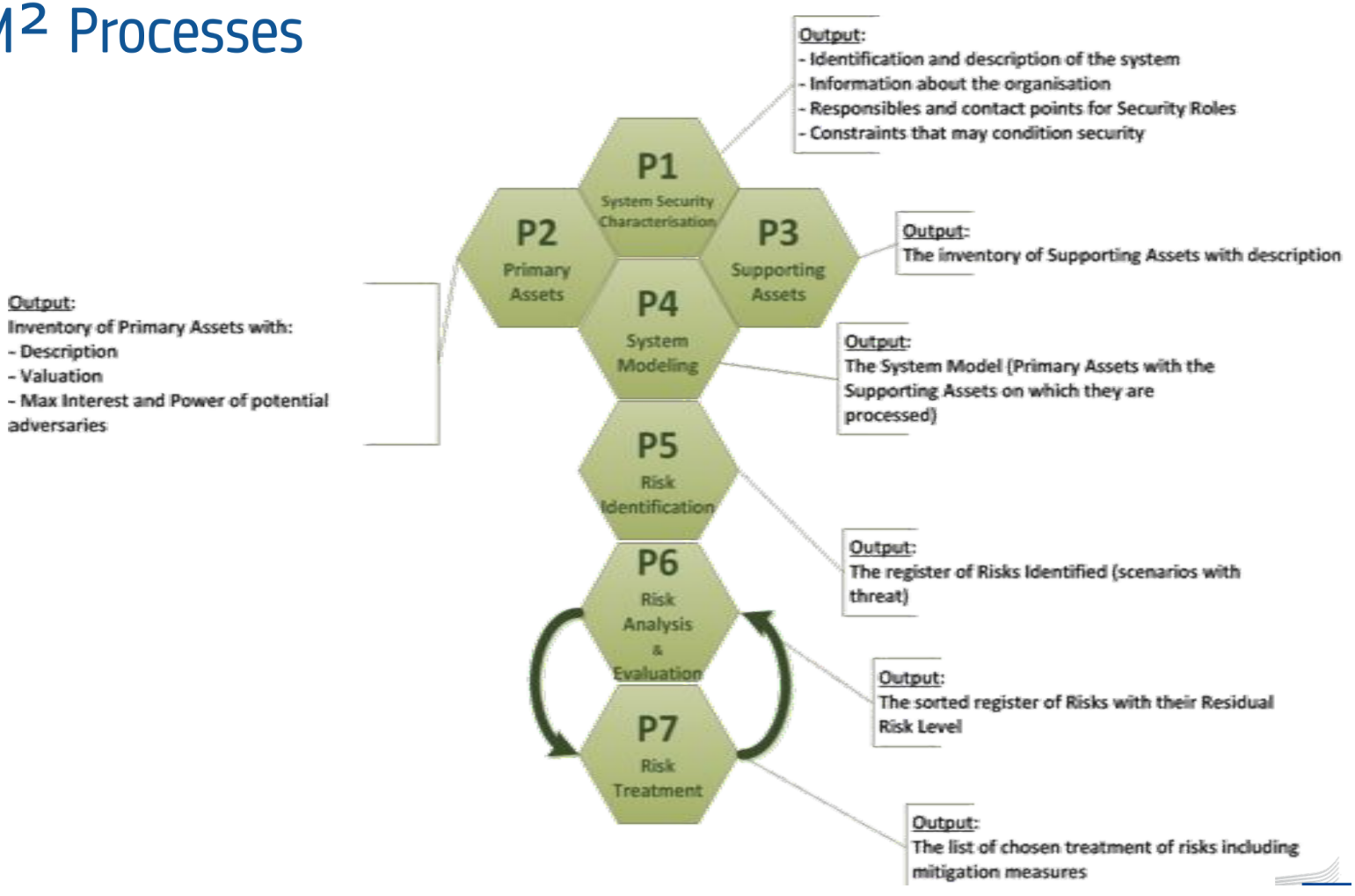


Figure 1-1: Mapping between ISO 27005 and ITSRM Methodology processes

ITSRM^2 and ISO 27005

ITSRM^2 Processes



The Process Steps, input required, output to be produced

ITSRM^2 System Security Characterization, Primary Assets Identification (P1)

To be produced output:

- Identification and description of the System
- Information about the organisation
- Responsibilities and Contact Points for Security Roles, usually represented in Responsible, Accountable, Supporting, Consulted and Informed. RASCI table.
- Constraints that may condition security Compliance with policies, standards; ex: Access control, GDPR, Central Syslog, Vulnerability Management

Task: IT Security Plan, required input from Business

Table of contents:

[6] First set of Security Measures may come from compliance requirements

Task: IT Security Plan, required input from Business

Table of contents:

[6] First set of Security Measures may come from compliance requirements

Task: IT Security Plan, required input from Business

Table of contents:

[6] First set of Security Measures may come from compliance requirements

Task: IT Security Plan, required input from Business

Table of contents:

[6] First set of Security Measures may come from compliance requirements

Task: IT Security Plan, required input from Business

Table of contents:

1. System Overview
   - 1.1 Key Security Roles (Table, Head of Department (Accountable, System Owner (Responsible), Data Owner, System Security Officer, Security Risk Manager)
   - 1.2 User Population and priority (ex. Students, IT-Personal (Admins), Employees (FD etc), External collaborators)
   - 1.3 System Description/System high-level architecture (Organisation/Departments etc)
   - 1.4 Constraints and Compliance[6] (GDPR, AUP, Security Baseline, Central logging, etc) along with Mandatory Security Measures.
   - 1.5 Risk Acceptance Criteria (Risks calculated for scenarios are automatically accepted below the defined threshold.)

[6] First set of Security Measures may come from compliance requirements

Task: IT Security Plan, required input from Business

Table of contents:

1. System Overview
   - 1.1 Key Security Roles (Table, Head of Department (Accountable, System Owner (Responsible), Data Owner, System Security Officer, Security Risk Manager)
   - 1.2 User Population and priority (ex. Students, IT-Personal (Admins), Employees (FD etc), External collaborators)
   - 1.3 System Description/System high-level architecture (Organisation/Departments etc)
   - 1.4 Constraints and Compliance[6] (GDPR, AUP, Security Baseline, Central logging, etc) along with Mandatory Security Measures.
   - 1.5 Risk Acceptance Criteria (Risks calculated for scenarios are automatically accepted below the defined threshold.)
   - 1.6 Primary Assets, Functions, Data, "Business Goals and Processes" and their valuation (Business Impact Analysis (BIA) in Confidentiality, Integrity, Availability,

[6] First set of Security Measures may come from compliance requirements

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System;

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System;
- System Owner (SO): individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and decommissioning of a Communication and Information System (CIS) ;

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System;
- System Owner (SO): individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and decommissioning of a Communication and Information System (CIS) ;
- Data Owner (DO): individual responsible for ensuring the protection and use of a specific Data Set handled by a CIS;

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System;
- System Owner (SO): individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and decommissioning of a Communication and Information System (CIS) ;
- Data Owner (DO): individual responsible for ensuring the protection and use of a specific Data Set handled by a CIS;
- System Security Officer (SSO): Advises the System Owner, System Manager and Project Manager on the IT security approach, takes an active role as IT security expert to define IT security requirements and assists in the architecture, design, implementation and verification activities of IT security

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System;
- System Owner (SO): individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and decommissioning of a Communication and Information System (CIS) ;
- Data Owner (DO): individual responsible for ensuring the protection and use of a specific Data Set handled by a CIS;
- System Security Officer (SSO): Advises the System Owner, System Manager and Project Manager on the IT security approach, takes an active role as IT security expert to define IT security requirements and assists in the architecture, design, implementation and verification activities of IT security
- IT Staff: IT-related personnel in charge of development and/or operation of the CIS;

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System;
- System Owner (SO): individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and decommissioning of a Communication and Information System (CIS) ;
- Data Owner (DO): individual responsible for ensuring the protection and use of a specific Data Set handled by a CIS;
- System Security Officer (SSO): Advises the System Owner, System Manager and Project Manager on the IT security approach, takes an active role as IT security expert to define IT security requirements and assists in the architecture, design, implementation and verification activities of IT security
- IT Staff: IT-related personnel in charge of development and/or operation of the CIS;
- Security Risk Manager (SRM): the person performing the Risk Management.

Responsibilities

Who is responsible for what? RASCI table

RASCI Value	Description
(R) Responsible	Has the obligation to act and take decisions to achieve required outcomes. Does the work. Others can be asked to assist in a supporting role.
(RD) Responsible	Responsible by delegation
(A) Accountable	An accountable role is answerable for actions, decisions and performance. Ultimately answerable for the correct and thorough completion of the work. There is just one accountable person.
(S) Support	People that actively support the work developed by the responsible roles.
(C) Consulted	Roles used to complete, complement or validate the information resulting from each process.
(I) Informed	Those informed (kept up-to-date) of the results obtained from the execution of the methodology.

Putting things together

Putting the definition of roles and the responsibilities together ...

	SO	DO	SSO	SRM	IT Staff	HoD
System Sec Characterization						
System Description[8]	R	C	S	R(D)	-	A
Id'fy Sec. Roles	R	C	S	R(D)	-	A
Org. Description	R	-	S	R(D)	-	A
Id'fy Main Constraints[9]	R	-	S	R(D)	-	A
Id'fy Main Sec Measures	R	-	S	R(D)	-	A
Primary Assets (PA)						
PA Identification	R	S	C	R(D)	S	A
Asset Validation	R	S	C	R(D)	-	A
PA Valuation	R	S	C	R(D)	-	A

[7] here DO and DPC is one role

[8] Name, Purpose/Functions, Information handled, user population, high level architecture

[9] In the categories Organisational and Risk Treatment

IT Security Plan, Key Security Roles, table

Security Role	Name	Contact
Head of Department (HoD) Ex.	Director of Institute	Accountable
System Owner(SO)	Eve	dirteam@univ.sw
Data Owner(DO)	Alice	dpo@univ.sw
System Security Officer (SSO)	Bob	it-so@univ.sw
Security Risk Manager (SRM)	Charles	charles@univ.sw

Depending on the size of the organisation, more roles may be defined, like LISO, Data Protection Coordinator ...

Task: IT Security Plan, summary of what we have now

- We have a high-level description of the system (purpose, goals, primary processes and functions . . .)
- We know who is responsible for what.
- We now the different user groups accessing our system(s)
- We have a list of documents we need to be compliant with.
- Open question: What are the Primary Assets? How to get them from the info we have so far in *University of Harderwijk Herbal Research Infrastructure IT Security Plan*

Primary and Secondary (Supporting) Assets

Definitions

Definitions Primary Assets(PAs); Secondary Assets(SAs)(in ITSRM^2):

- PA: For the application of this methodology this will be referred to as Data (a set of information which serves a specific business process or activity of the organisation) and Functions (The processing of information comprises all functions of a CIS with regard to Data Sets, including creation, modification, display, storage, transmission, deletion and archiving of information. Processing of information can be provided by a CIS as a set of functionalities to users and as IT services to other CIS).
- SA: Asset used or involved in the processing of the Data and Functions provided by the Target System. Hardware, software, personnel, locations and services are the main supporting assets that build an IT System. Supporting Assets are also known as Secondary Assets or IT Assets.

Data and Function Primary Assets

Data PA Examples:

- Legal texts, Intellectual property related docs
- Personal information
- Research (meta) Data

The support of the data does not matter here, only the information itself

Function PA Examples:

- Provisioning operations
- Service Management
- User Management
- Publishing information

The equipment carrying out the function does not matter here, only the function itself

PA/SA Concept

Concept:

- Hierarchical organization of assets.
- Primary Assets(PAs) are under control of Business
- Secondary Assets(SAs) support one or more PAs.
- SAs are in general under control of IT.

Task 1 PAs for University Harderwijk

Get Primary Assets for University Harderwijk

- Read:University of Harderwijk Herbal Research Infrastructure IT Security Plan
  - 1. Executive Summary
  - 2.3. System Description
  - 2.4. System high-level architecture
- Discuss/Identify PAs

Business Impact Analysis (BIA)

What is BIA in ITSRM^2

Asset Valuation:
The objective of this task is to determine the Primary Asset value from a Business and a Data Protection perspective. This objective can be achieved through one of the following methods.

- Re-use of previous valuation
- Estimation based on Impact scale (Business or Data Protection (Annex B.1.)
- By hypothesis, ex for PA containers, when it is not knwn in advance which Data will be processed and which Functions will be executed by the Target System (generic services like file server, a document management system, a Database)
- By formal Impact Assessment

Formal Impact Assessment

The Impact Assessment (IA) is a technique to estimate the Primary Asset values based on the potential consequences for the organisation in case of a loss of the confidentiality, integrity and/or availability of the identified Primary Assets.

- PA Value, estimated as maximum impact of loss in CIA
- Impact Scenario is a combination of: PA, Sec. Dimension (CIA), impact type (Financial Loss, Reputational Damage, Operational Disruption, Data Loss, . . .)

Formal Impact Assessment cont'd

- Build and describe impact scenarios, Impact Scenario starts when there is a loss of Confidentiality, Integrity and/or Availability (due to any possible problem); it ends with an Impact that can be assessed.
  - look at the PA, describe a scenario which would result in the loss of each Security Dimension (CIA) (how specifically is not of interest now)
  - Identify Consequences per Security Dimension (CIA)
  - Consequences in Availability (outage of a PA) depends on the duration of the outage. Ex. Few seconds, minutes $\rightarrow$ Neglible, Low; When Maximum Tolerable Period of Disruption (MTPD) is reached, Consequences are max.

Impact Scenario, Per PA, per Dimension

Mainly connect defined tabular values

- Starts with a loss of C,I,A, ends with an Impact that can be assessed. (Business perspective, negative impact)
- Impact Type (Annex B.1.A Functions; Annex B.1.B Data); Financial Loss in %age of budget; Infringement of Laws; Disruption of Service; etc
- Per Type, Effect (Imapct level: 0, no impact, 10 loss of more then 100% of budget; Legal consequences affecting the Organisation; 50% delay in service delivery, service availability)
- Results in a numerical Asset value per Dimension..
- Final Asset value is the highest number among the different scenarios

Interest Scenario, Per PA, per Dimension

Mainly connect defined tabular values

- Starts with a loss of C,I,A, ends with a possible benefit for the Potential Adversary that can be used to assess its interest to attack the Primary Asset. (Adversary perspective, what she/he gains performing an attack)
- $Attractiveness = Power + Interest$ (of the adversary)
- Power (Annex C.2): depends on adversary type (Nation States (5), Cybercriminals(4) . . . Script Kiddies(1). Also Insiders (3-5)
- Interest (Annex B.2): High(5), Medium(3), Low(1)

Task2 Provide Asset Value and Asset Attractiveness for PAs identified

Mainly connect defined tabular values (Also check the intentional and unintentional failures)

Example PA Data management:

PA description: Provide dataspace to participants to store data and provide means to control access to the data (also Publishing). Provide means also to delete data. Provide research collaboration tools.

Impact Scenarios per Dimension (C,I,A), Confidentiality

Description: This function is build with open-source components, there is no Confidentiality issue in the function.

- Impact Type: Reputation damage (in lack of a useful type available in the catalogue
- Consequence[10] = 1; Negligible damage to image and reputation

[10] Catalogue value

Impact Scenarios per Dimension (C,I,A), Integrity

Description: compromise of the integrity of the data management function would render one of the most visible services of the Harderwijk Univ.e as partly (services and data) for the users.

- Imapact Type: Damage organisation image and reputation
- Consequence = 3; Consequential, limited to local/specific public

Impact Scenarios per Dimension (C,I,A), Availability

Description: compromise of the integrity of the data management function would render one of the most visible services of the Harderwijk Univ.e as partly (services and data) for the users.

- Imapct Type: Degradation of the Universities Service in %age of expected time (SLA).
- Consequence = 6; It would take 1 working day to recover the service from back up, and to re-process the data send during this period. (50% of MTPD(2 days))
- Consequence = 6

- (Inherent) Risk $R = Likelyhood * Consequence$
  - Consequence: Asset Value (P2)
  - Likelyhood: Frequency (accidental) or $(EASINESS + POWER + INTEREST)/3$ (intentional)[11] [12] [13]
- (Residual) Risk $RR = R * (1–MF(SM1)) * ... * (1–MF(SMn))$ [14]

[11] Easiness: easy/100/every day; extremely difficult/0.01/once in a century, ITSRM^2, Annex B3

[12] Power, Annex C.2: Catalogue of potential adversary types, 1-5

[13] Interest: Annex B.2: Interest level scale: 1,3,5

[14] MF: Mitigation Factor per Security Measure

Input from IT to the ITSP, Secondary Assets (P3) and their relation to Primary Assets (P4)

ITSRM^2 Supporting/Secondary Assets (P3)

To be produced output: Supporting Asset (SA) inventory.

- SA Identifier, Name
- Type[15] ("Hierarchical" description), ex. Software $\rightarrow$ (Middleware, Firmware, End User Application) $\rightarrow$ (Web/DB/ server, OS, Network stack, Hypervisor)
- Description (which PA it supports, relation to other SAs)
- SA Owner/Responsible for the SA

[15] See Annex C3 ITSRM^2 doc, other top level types are: Hardware, Personnel, Service, (Physical) Location

Task3 Propose Secondary Assets supporting the PAs of Harderwijk Univ.

You are now in the role of IT, you are asked which tools, services etc. are required to achieve the Business goals.

Primary Assets:

- Usermanagement (Function, consists of open source software)
- Service Provisioning (Function, Services to be defined)
- Taxonomy data (Data)

Provide a System Model (Matrix) showing which SAs support which PA

Task: IT Security Plan, required input, Support from IT

Table of contents:

Task: IT Security Plan, required input, Support from IT

Table of contents:

Task: IT Security Plan, required input, Support from IT

Table of contents:

Task: IT Security Plan, required input, Support from IT

Table of contents:

Risk Identification and analysis, Risk Register

The objective of the risk identification is to identify risks that will be analysed, evaluated and treated in next processes. Risk scenario is a Combination of:

- Identifier for the Risk Scenario,
- a Primary Asset Identifier
- a Security Dimension (C,I,A),
- a Threat[16] that can harm this Security Dimension for this Primary Asset, and
- the Supporting Asset Identifier on which the Primary Asset is located and where the Threat materialises.
- Threat[17] Identifier

[16] Threat-Based IT Security Management focuses on identifying, analyzing, and mitigating threats to an organization's IT infrastructure.

[17] Note the different categories *accidental, intentional* threats

Risk Identification and analysis, how to do it ...

Required input: System Model from P4, Threat Catalogue[18], Security Measures from compliance analysis in P1.

- (Inherent) Risk $R = Likelyhood * Consequence$
  - Consequence: Asset Value (P2)
  - Likelyhood: Frequency (accidental) or $(EASINESS + POWER + INTEREST)/3$ (intentional)[19]
- (Residual) Risk $RR = R * (1–MF(SM1)) * ... * (1–MF(SMn))$ [20]

All this is coded in the Risk Management Tool ...

---

[18] ITSRM^2 detailed catalogues, Annex C4

[19] Easiness: easy/100/every day; extremely difficult/0.01/once in a century, ITSRM^2, Annex B3

[20] MF: Mitigation Factor per Security Measure

Task: IT Security Plan, required input, Support from IT-Sec

Table of contents:

Task: IT Security Plan, required input, Support from IT-Sec

Table of contents:

Finally

- The Risk assessment report will help the Operational Security team to prioritize the available resources to:
  - Security Monitoring (ex. access control)
  - System audits, log processing, alerting
  - Back-up Strategy
  - ...