Applying the concepts of IT Security Risk Management

S. Gabriel[1,2]

[1]Nikhef [2]EGI CSIRT

Sept. 2026

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

Some thoughts on Scope

Scope dimensions, the scope for a generic CSIRT has many dimensions, incomplete list:

- Organizational Scope
- Technical Scope
- Time Scope
- Decision Scope
- Third Party Scope
- Compliance Scope
- ...

Why is this relevant?

Scope definition is not a bureaucratic exercise, it is the decision that makes everything else possible or impossible. You cannot manage what you have not defined. Its the first process step in Strategy development, and IT Security Risk Management. (Step 0 being "Understanding the environment")
What for example follows from scope definition:

- Determines CSIRT operations.(Ex. what to monitor, what the security team responds to)
- Accountability and Ownership, who is responsible for what, Every asset, risk, function, and decision inside the scope needs an owner. (accordingly everything outside the scope needs a named owner, otherwise we will have gaps.
- Required for IT Security Risk Management, scope determines which risks are assessed, and which not.
- Resource Allocation can only be done when the *size of the Problem* is defined.
- KPI/KRIs need to cover a defined scope.

Key Performance Indicators

Key Performance Indicators (KPI)

- Performance against an objective, looks backwards, signals when performance deviates from target.
- A KPI measures whether something is being achieved now or was achieved in a period — it is a performance measurement, not a predictive signal.
- A KPI only functions as a performance measure if it has a defined target — a level that represents acceptable performance, and a level that represents underperformance.

Key Performance and Risk Indicators

Key Risk Indicators (KRI):

- A KRI signals that risk is increasing — it is predictive, not historical. It tells you something is trending in the wrong direction before the consequence arrives. (example AI and vulnerability management):
- A KRI is meaningless without a risk it is measuring. Every KRI must be traceable to a defined risk in the risk register.
- A KRI only functions as an early warning if it has defined thresholds — a level at which attention is required, and a level at which escalation or action is triggered.

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

Terminology, strategy/operation/tactic

Strategy, operation and tactics are terms in common language, sometimes used interchangeably, which is confusing, they are on different organisational levels, are on different timescales. Example:

Strategy: Win the Football World championship in 4y because it creates revenue (What to achieve, why. Timescale: Years)

↓

Operation: Get a competitive team together, intel about potential opponents (how do we organize to achieve the Objective. Timescale: Days, Months)

↓

Tactic: Loose against team X to avoid strong opponent Y in next round. (Timescale Hours, Days)

Terminology, Strategy

- Strategy — the "why" and "what we are going to do""
  - Long term (here 3-4 years). More abstract.
  - Answers: Scope, What risk posture does the Organisation accept? What's our target security maturity (monitored for example by external audits))! Which threats matter most to our business?)
  - Owned by Leadership. Informed by Organisation objectives, regulatory obligations, threat landscape trends[6].
  - Objectives need to have a measurable success.
  - Example would have been: Transition to tokens until date X.

[6] ENISA Threat Landscape

Terminology, Operation

Operation: How do we Organize to achieve it.

- Midterm (Months).
- Organize the team.
- Prepare to achieve defined objectives.
- Owned by Organisation CSIRT.[7]
- Example: Organisation CSIRT activity groups.

[7] Organisation CSIRT very much depends on how the organisation looks like. Fundamental difference in case you are the CSIRT for an Institute, Research center etc, or if you are a CSIRT for a federation

Terminology, Tactic

Tactics — the "how" and "what we do this day/this week"

- Short-to-medium term, concrete and executable.
- Owned by activity coordinators[8], translating Operation planning into deployable work.
- Adjusts frequently based on new threats, developments.
- Example: Patch CVE-2026-XXXX. (The decision, actual hands on like drafting, send out advisories.)

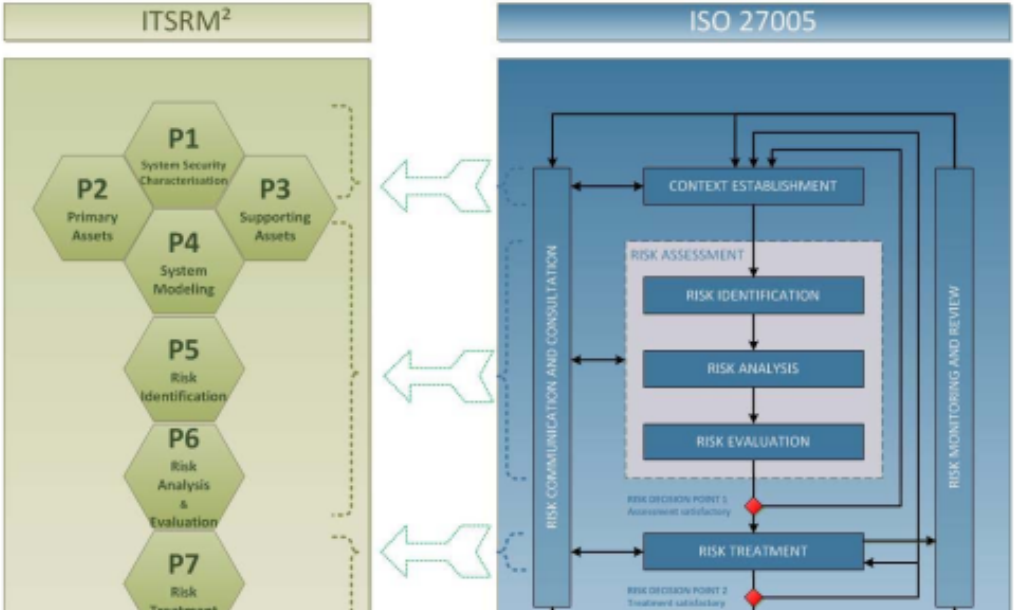
[8] more on that in the later presentations

Why this is relevant ...

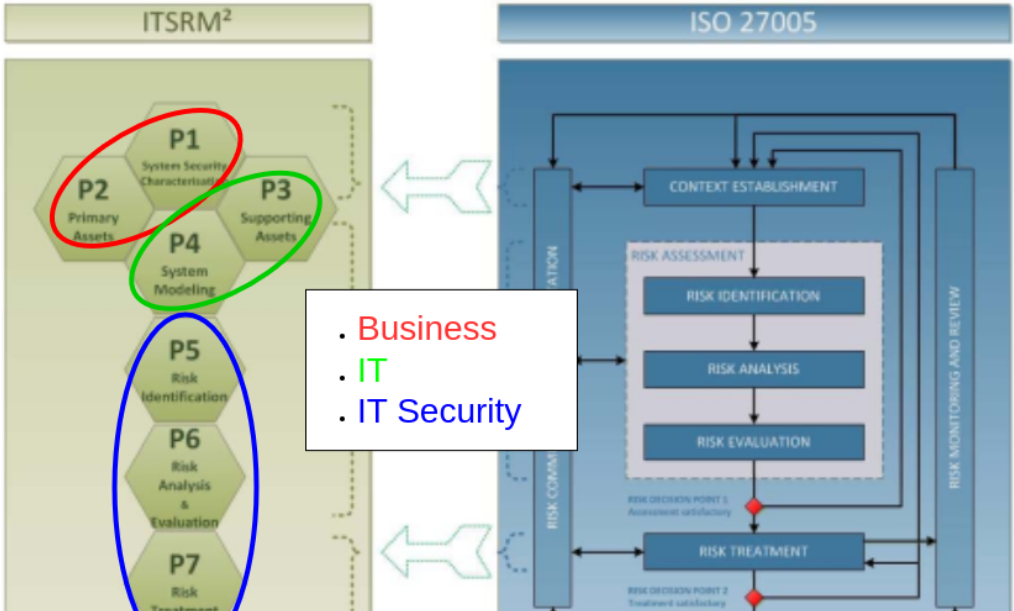
- A team that's all tactics, no strategy: tends to be reactive, ex: chasing the latest vulnerability/incident/vendor pitch without a coherent direction, leading to wasted spend and gaps nobody planned for.
- A team that's all strategy, no tactics: produces polished slide decks and risk registers (if you do IT Security Risk Management) that never actually reduce risk, because nothing concrete gets implemented.
- Good security programs deliberately trace every tactical action back to a strategic objective — if you can't explain why a specific control/project serves the strategy, it's worth questioning whether it should be prioritized at all.

The IT Security Risk Management Methodology (ITSRM^2)

ITSRM^2 and ISO 27005

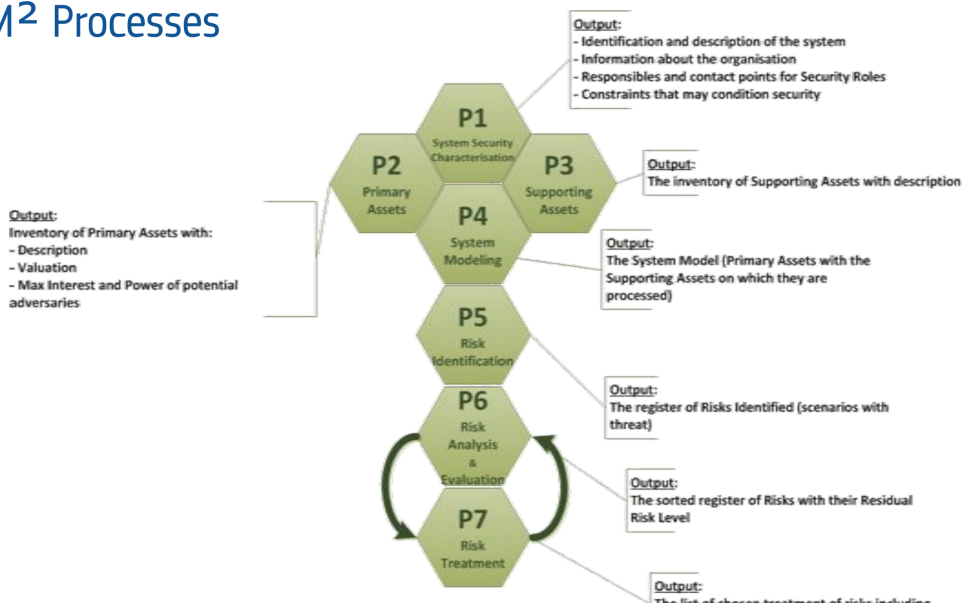


ITSRM^2 and ISO 27005



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:

1. System Overview
    1.1 Key Security Roles (Table, Head of Department (Accountable), System Owner (Responsible), Data Owner, System Security Officer, Security Risk Manager)

[9] 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)

[9] 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)

[9] 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[9] (GDPR, AUP, Security Baseline, Central logging, etc) along with Mandatory Security Measures.

[9] 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[9] (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.)

[9] 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[9] (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,

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

Accountable/Responsible

- Responsible: The person or team that does the work and carries out the task (possibly multiple people, can be delegated).
- Accountable: The person who owns the outcome, makes the final decision, and is answerable for whether the task is completed correctly (single person, can not be delegated).

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System[10];

[10] This is the overall System, which may consist of many (sub) Systems, each having a System Owner

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System[10];
- System Owner (SO): individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and decommissioning of a Communication and Information System (CIS) ;

[10] This is the overall System, which may consist of many (sub) Systems, each having a System Owner

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System[10];
- 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;

[10] This is the overall System, which may consist of many (sub) Systems, each having a System Owner

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System[10];
- 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

[10] This is the overall System, which may consist of many (sub) Systems, each having a System Owner

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System[10];
- 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;

[10] This is the overall System, which may consist of many (sub) Systems, each having a System Owner

ITSRM: Governance, depends on the organisation

- Head of Department (HoD): Accountable, owning the risks of the Target System[10];
- 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.

[10] This is the overall System, which may consist of many (sub) Systems, each having a System Owner

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[12]	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[13]	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

[11] here DO and DPC is one role

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

[13] 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

Coffee and discussion

what the Primary Assets can be

(You are the SRM)

Primary asset 1 — Taxonomic dataset

Why it is a primary asset

The accumulated body of taxonomic knowledge — species names, classifications, synonyms, and naming history — built since the Linnaean foundation. It has intrinsic value independent of any supporting system. It is **irreplaceable**: no alternative source exists globally. Loss of integrity would invalidate decades of published biological research worldwide.

Security requirements (CIA)

Confidentiality	**Public.** Dataset must be freely accessible — restriction destroys value.
Integrity	**Critical.** Manipulation has irreversible global scientific consequences. Dominant requirement.
Availability	**Critical.** Global research community depends on continuous access.

Integrity dominates: subtle data manipulation is worse than unavailability — bad taxonomy actively harms science.

Primary asset 2 — Taxonomic naming and classification process

Why it is a primary asset

The authoritative process by which plant species are named, classified, and indexed. It is the **core mission** of the HRI and exists independently of any supporting technology. The process — not the database — is what the global biology community defers to. If the process is destroyed, no server can recreate it. It also provides unique non-reassigned naming, without which biological research cannot function.

Security requirements (CIA)

Confidentiality	**Low.** Process outputs are public by design.
Integrity	**Critical.** Process must produce correct, consistent, authoritative results. Non-repudiation required.
Availability	**Critical.** Process must be executable without unreasonable interruption. Key-person risk is significant.

Key-person dependency: institutional knowledge exists partly in the minds of experienced taxonomists. Loss of staff is an availability risk with no technical mitigation.

Primary asset 3 — Species identification and indexing service

Why it is a primary asset

The operational process through which the taxonomic dataset is made accessible globally — queries, submissions, validation, and publication. It enables community contribution and citizen science, including household garden ecological composition queries. Availability has direct **societal impact** consequences, which determine continued funding. Unavailability of the service threatens BBC2 programming continuity and therefore the university's funding justification.

Security requirements (CIA)

Confidentiality — **Public.** Service is public-facing by design.

Integrity — **Critical.** Results must be accurate and unmanipulated. Users must trust the authoritative source.

Availability — **Critical.** Global real-time dependency. Downtime has direct funding consequences.

Availability is the dominant operational concern here. DDoS protection and geographic redundancy are priority controls. BBC2 dependency makes downtime politically visible.

Primary asset 4 — Community contribution process

Why it is a primary asset

The process through which the globally distributed user community — researchers, institutions, and citizens — submits new species observations and corrections to the authoritative record. Without community contribution the dataset becomes **static and degraded** over time. Community trust is itself an asset: a security incident that exposes contributor data or manipulates submissions could cause permanent community disengagement — degrading the database in a way no technical recovery can reverse.

Security requirements (CIA)

Confidentiality	**Medium.** Contributor identities and unpublished observations may be sensitive.
Integrity	**High.** Contributions must be validated before entering the authoritative record.
Availability	**High.** Contributors must be able to submit without unreasonable friction.

Community trust is an invisible but critical asset. Breach of contributor confidentiality or manipulation of submissions could permanently destroy this asset — no backup restores lost community trust.

Primary asset 5 — Naming authority and governance records

Why it is a primary asset

The institutional basis for the HRI's authority — its founding history, governance decisions, naming dispute resolutions, and the documented legitimacy that gives its classifications global acceptance. The HRI's value derives not just from its data but from its **recognised authority**. Without documented governance, any organisation could build a species database — it is the authority that makes the HRI's database definitive. The Linnaean heritage is what makes the authority globally accepted.

Security requirements (CIA)

Confidentiality	**Medium.** Some governance deliberations and dispute resolutions may be sensitive.
Integrity	**High.** Governance records must not be altered. Non-repudiation is essential.
Availability	**Medium.** Not needed continuously — essential when the HRI's authority is challenged.

Authority is socially constructed — it exists because the global community accepts it. Manipulation of governance records could undermine the HRI's claim to be the authoritative naming source.

Primary asset summary — CIA valuation

Primary asset	Type	C	I	A	Dominant requirement
PA1 · Taxonomic dataset	Information	Public	Critical	Critical	Integrity
PA2 · Naming & classification process	Business process	Low	Critical	Critical	Integrity + availability
PA3 · Species identification service	Business process	Public	Critical	Critical	Availability + integrity
PA4 · Community contribution process	Business process	Medium	High	High	Integrity + community trust
PA5 · Naming authority & governance	Information	Medium	High	Medium	Integrity

Key finding: The HRI asset profile is dominated by integrity across all primary assets. Confidentiality is largely irrelevant — the dataset must be public to have value. The IT Security Plan must prioritise tamper detection, write access controls, audit logging, and integrity verification above all other controls.

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[14] = 1; Negligible damage to image and reputation

[14] 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)[15] [16] [17]
- (Residual) Risk $RR = R * (1MF(SM1)) * ... * (1MF(SMn))$ [18]

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

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

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

[18] 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[19] ("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

[19] 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:

2. IT Security Risk Assessment Results
   2.1 Risk Assessment Approach (Defined in P1)

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

Table of contents:

2. IT Security Risk Assessment Results
   - 2.1 Risk Assessment Approach (Defined in P1)
   - 2.2 Primary Assets (Defined in P2)

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

Table of contents:

2. IT Security Risk Assessment Results
   - 2.1 Risk Assessment Approach (Defined in P1)
   - 2.2 Primary Assets (Defined in P2)
   - 2.3 Asset Valuation Conclusions (Calculated with the RM tool defined in P1)

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

Table of contents:

2. IT Security Risk Assessment Results
   - 2.1 Risk Assessment Approach (Defined in P1)
   - 2.2 Primary Assets (Defined in P2)
   - 2.3 Asset Valuation Conclusions (Calculated with the RM tool defined in P1)
   - 2.4 Secondary Assets (from IT–Support, including which PA is supported)

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[20] 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[21] Identifier

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

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

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

Required input: System Model from P4, Threat Catalogue[22], 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)[23]
- (Residual) Risk $RR = R * (1 MF(SM1)) * ... * (1 MF(SMn))$ [24]

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

[22] ITSRM^2 detailed catalogues, Annex C4

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

[24] MF: Mitigation Factor per Security Measure

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

Table of contents:

2. IT Security Risk Assessment Results
   2.5 Risk Identification and Analysis Conclusions

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

Table of contents:

2. IT Security Risk Assessment Results
   - 2.5 Risk Identification and Analysis Conclusions
   - 2.6 Deviations from Default Values (In case parameters set in the RM tool are changed)

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
  - ...

SA section re-done

Supporting Assets — HRI; System Modelling

Supporting assets are identified across the five official ITSRM² categories and mapped to the five HRI primary assets. Organisational elements (policies, procedures) are **security controls** — not supporting assets — and appear in Phase 5 (Risk Treatment), not this register.

ITSRM² SA categories

- HW Hardware
- SW Software
- NW Network
- PE Personnel
- PH Physical

Primary assets

- PA1 Taxonomic dataset
- PA2 Naming process
- PA3 ID service
- PA4 Community contribution
- PA5 Governance records

● Supports ● Critical/shared ○ N/A

Supporting assets — HW Hardware

Supporting asset	PA1	PA2	PA3	PA4	PA5	Inherited CIA requirement
Database servers — primary	●	○	●	○	○	I:Max · A:Max — shared PA1+PA3
Database servers — replica/DR	●	○	●	○	○	A:Max — geographic redundancy
Storage arrays — primary	●	○	○	○	○	I:Max · A:Max
Storage arrays — backup	●	○	○	○	●	I:Max · A:Max (PA1) · I:Max (PA5)
Tape / offline backup media	●	○	○	○	○	I:Max — ransomware-proof backup
Hardware Security Module (HSM)	●	○	○	●	●	I:Max (PA1,PA5) · C:Max (PA4)
Web and application servers	○	○	●	●	○	I:Max · A:Max (PA3) · I:Max · A:Sig (PA4)
Load balancers	○	○	●	○	○	A:Max — traffic distribution
DDoS mitigation appliances	○	○	●	○	○	A:Max — volumetric attack protection
CDN edge nodes	○	○	●	○	○	A:Max — geographic distribution
API gateway hardware	○	○	●	○	○	I:Max · A:Max
Taxonomist workstations	○	●	○	○	○	A:Max — naming process execution
Research computing servers	○	●	○	○	○	A:Max — classification analysis
Contribution portal servers	○	○	○	●	○	I:Max · A:Sig
Contributor data storage	○	○	○	●	○	C:Max · I:Max — personal data
Document management servers	○	●	○	○	●	I:Max (PA2+PA5) · A:Sig (PA5)

Highest-priority hardware SA: Database servers (primary) carry PA1 (I:Max · A:Max) and PA3 (I:Max · A:Max) simultaneously. Their failure is a dual-Maximum availability and integrity event. Geographic redundancy and DR failover are mandatory controls.

Supporting assets — SW Software

Supporting asset	PA1	PA2	PA3	PA4	PA5	Inherited CIA requirement
Database Management System	●	○	●	○	○	I:Max · A:Max — core dataset storage
Backup and recovery software	●	○	○	○	●	I:Max · A:Max (PA1) · I:Max (PA5)
Integrity verification software	●	○	●	○	●	I:Max across PA1, PA3, PA5
IAM / access control software	●	○	●	●	●	I:Max (PA1) · C:Max (PA4) · I:Max (PA5) 4 PAs
Audit logging software	●	○	●	●	●	I:Max (PA1) · C:Max (PA4) · I:Max (PA5) 4 PAs
Anomaly detection software	●	○	●	○	○	I:Max — detects manipulation patterns
Database replication software	●	○	●	○	○	A:Max — replica synchronisation
Web application software	○	○	●	●	○	I:Max · A:Max (PA3) · I:Max (PA4)
Web application firewall (WAF)	○	○	●	○	○	I:Max — injection and manipulation
DDoS protection software	○	○	●	○	○	A:Max — cloud-based scrubbing
API management software	○	○	●	○	○	I:Max · A:Max
Monitoring and alerting software	○	○	●	●	○	A:Max (PA3) · C:Max (PA4)
Taxonomic decision support sw	○	●	○	○	○	I:Max · A:Max — naming analysis
Digital signature software	○	●	○	○	●	I:Max — non-repudiation
Knowledge management system	○	●	○	○	○	I:Max · A:Max — institutional knowledge
Submission validation software	○	○	○	●	○	I:Max — pre-database entry validation
Encryption software	○	○	○	●	○	C:Max — contributor personal data
Data loss prevention (DLP)	○	○	○	●	○	C:Max — exfiltration prevention
GDPR consent management	○	○	○	●	○	C:Max — Art.7 legal compliance
Document management system	○	●	○	○	●	I:Max · A:Sig (PA5)
Version control system	○	○	○	○	●	I:Max — governance record history

Supporting Assets, Software

IAM and audit logging are the most critical software SAs — each spans 4 primary assets. Compromise of either simultaneously undermines write-access control (I:Max, PA1) and personal data protection (C:Max, PA4) and governance record integrity (I:Max, PA5).

Supporting assets — NW Network

Supporting asset	PA1	PA2	PA3	PA4	PA5	Inherited CIA requirement
Internal network — DB segment	●	○	●	○	○	I:Max · A:Max
Network segmentation/firewall	●	○	●	●	○	I:Max (PA1) · C:Max (PA4) — shared
Out-of-band management network	●	○	●	○	○	I:Max — admin without production exposure
Internal network — research	○	●	○	○	○	A:Max — taxonomist connectivity
Secure communication channel	○	●	○	○	●	I:Max · C:Lim (PA2) · C:Sig (PA5)
Internet connectivity — primary	○	○	●	●	○	A:Max (PA3) · A:Sig (PA4)
Internet connectivity — backup	○	○	●	○	○	A:Max — redundant uplink
DNS infrastructure	○	○	●	○	○	A:Max · I:Max — critical single SA
BGP routing infrastructure	○	○	●	○	○	A:Max — global reachability
TLS certificate infrastructure	○	○	●	●	○	I:Max (PA3) · C:Max (PA4)
Network segmentation — contrib.	○	○	○	●	○	C:Max — isolates personal data
Intrusion detection system	○	○	●	●	○	I:Max (PA3) · C:Max (PA4)
Restricted internal network	○	○	○	○	●	C:Sig · I:Max — governance access
VPN — secure remote access	○	○	○	○	●	C:Sig · I:Max — authorised remote

DNS is a critical single-point SA for PA3. Its failure or hijacking makes the species identification service globally unreachable or misdirected — full A:Max impact from one infrastructure component. DNS requires independent availability and integrity controls.

Network segmentation spans PA1 and PA4 simultaneously. It prevents lateral movement from the public-facing service (PA3) to the database (PA1) and isolates contributor personal data (PA4). Its compromise is a multi-PA integrity and confidentiality event.

Supporting assets — PE Personnel

Supporting asset	PA1	PA2	PA3	PA4	PA5	Inherited requirement / risk
Senior taxonomists	●	●	○	○	●	A:Max (PA2) — **irreplaceable key-person risk**
Junior taxonomists and curators	○	●	○	●	○	A:Max (PA2 succession) · I:Max (PA4)
Naming dispute resolution authority	○	●	○	○	●	I:Max — decision attribution and authority
Database administrators	●	○	●	○	○	I:Max · A:Max — shared critical role
Security administrators	●	○	●	●	●	I:Max (PA1) · C:Max (PA4) · I:Max (PA5)
Backup and recovery operators	●	○	○	○	●	I:Max · A:Max (PA1) · I:Max (PA5)
System administrators	○	○	●	●	○	A:Max (PA3) · A:Sig (PA4)
Security operations staff	●	○	●	●	○	I:Max (PA1+PA3) · C:Max (PA4)
Network engineers	○	○	●	○	○	A:Max — DDoS and connectivity response
On-call incident response team	●	○	●	●	○	A:Max (PA3 RTO=1h) · C:Max (PA4)
Community managers	○	○	○	●	○	C:Max · A:Sig — contributor trust
Data Protection Officer (DPO)	○	○	○	●	○	C:Max — **GDPR Art.37 legally required**
Process governance officer	○	●	○	○	●	I:Max — process and record integrity
Governance officers	○	○	○	○	●	I:Max · C:Sig
Legal counsel	○	○	○	●	●	C:Max (PA4) · C:Sig (PA5)
Institutional archivist	○	●	○	○	●	I:Max — Linnaean heritage records

Senior taxonomists carry an irreversible key-person risk. PA2 (naming process) has no technical substitute. Loss of all senior taxonomists is an A:Max event from which no backup or failover system can recover. Succession planning and knowledge documentation are mandatory security controls.

DPO is a legally mandated supporting asset. Under GDPR Article 37, appointment of a Data Protection Officer is mandatory where personal data is processed at scale. The DPO must be named in the IT Security Plan and have a defined role in the breach notification procedure (GDPR Art.33 — 72 hours).

Supporting assets — PH Physical

Supporting asset	PA1	PA2	PA3	PA4	PA5	Inherited CIA requirement
Primary data centre	●	○	●	●	○	I:Max · A:Max (PA1+PA3) — single point of failure
DR / secondary data centre	●	○	●	○	○	A:Max — failover for PA1 and PA3
Offline backup facility	●	○	○	○	○	I:Max — air-gapped ransomware protection
Research offices and labs	○	●	○	○	○	A:Max — physical workspace for naming process
Herbarium and specimen collection	○	●	○	○	○	I:Max · A:Max — **irreplaceable physical asset**
CDN provider facilities	○	○	●	○	○	A:Max — geographic edge nodes
EU-resident data centre	○	○	○	●	○	C:Max — **GDPR data residency obligation**
Secure document archive room	○	○	○	○	●	I:Max · C:Sig — governance record storage
UPS and power infrastructure	●	●	●	●	○	A:Max (PA1+PA3) · A:Max (PA2) · A:Sig (PA4)
Cooling and HVAC systems	●	○	●	○	○	A:Max — server infrastructure availability
Fire suppression systems	●	●	●	○	●	I:Max · A:Max — physical destruction prevention
Flood protection measures	●	●	○	○	●	I:Max — data centre and archive protection
Physical access control systems	●	●	●	●	●	I:Max · C:Max (PA4) — all PAs benefit
Environmental monitoring	○	●	○	○	○	I:Max — herbarium temperature and humidity

The herbarium is a unique and irreplaceable physical SA. Species naming decisions reference physical specimens from the Linnaean collection. Loss through fire, flood, or theft impairs PA2 (naming process) with no digital substitute. Environmental monitoring, fire suppression, and humidity control are security controls of equal priority to database backup.

Primary data centre is the highest-risk physical SA. It carries PA1 (I:Max · A:Max), PA3 (I:Max · A:Max), and PA4 (C:Max) simultaneously. Its physical loss is a multi-Maximum event. The DR data centre must be geographically separated and capable of assuming full PA1 and PA3 operations within defined RTOs.

SA × PA dependency matrix — shared and critical assets

Cat.	Supporting asset	PA1	PA2	PA3	PA4	PA5	PAs	Priority
SW	IAM / access control software	●	○	●	●	●	4	Critical — I:Max+C:Max × 4 PAs
SW	Audit logging software	●	○	●	●	●	4	Critical — integrity evidence × 4 PAs
PE	Security administrators	●	○	●	●	●	4	Critical — I:Max+C:Max × 4 PAs
HW	Database servers — primary	●	○	●	○	○	2	Critical — I+A:Max dual-PA
PH	Primary data centre	●	○	●	●	○	3	Critical — single point of failure × 3
NW	Network segmentation/firewall	●	○	●	●	○	3	High — I:Max+C:Max cross-contamination
SW	Backup and recovery software	●	○	○	○	●	2	High — I+A:Max recovery capability
SW	Integrity verification software	●	○	●	○	●	3	High — I:Max × 3 PAs
PE	Security operations staff	●	○	●	●	○	3	High — monitoring × 3 PAs
PE	On-call incident response team	●	○	●	●	○	3	High — RTO compliance × 3 PAs
PH	UPS and power infrastructure	●	●	●	●	○	4	High — A:Max × 4 PAs
PH	Physical access control systems	●	●	●	●	●	5	High — all PAs benefit
SW	DBMS	●	○	●	○	○	2	Medium — I+A:Max core software
NW	DNS infrastructure	○	○	●	○	○	1	Medium — critical single-point SA
SW	Digital signature software	○	●	○	○	●	2	Medium — I:Max non-repudiation × 2
PE	Senior taxonomists	●	●	○	○	●	3	Unique — no technical substitute
PH	Herbarium and specimens	○	●	○	○	○	1	Unique — irreplaceable physical asset
PE	Data Protection Officer	○	○	○	●	○	1	Legal — GDPR Art.37 mandatory
PH	EU-resident data centre	○	○	○	●	○	1	Legal — GDPR data residency

■ Critical — 3+ PAs or Maximum CIA across multiple PAs ■ High — 2–3 PAs or Maximum CIA ■ Medium — 1–2 PAs ■ Unique — no technical or procedural substitute

Supporting assets — key findings and control priorities

Key findings

1. IAM and audit logging are the most critical SAs.
Both span 4 PAs across HW, SW, NW, PE, and PH. Their compromise simultaneously undermines write-access control (PA1 I:Max) and personal data protection (PA4 C:Max) and governance evidence (PA5 I:Max).

2. The primary data centre is a single point of failure.
Carries PA1 (I+A:Max), PA3 (I+A:Max), and PA4 (C:Max) simultaneously. Physical loss is a multi-Maximum event requiring geographically separated DR.

3. Senior taxonomists are irreplaceable.
The only SA with no technical substitute. Loss is an A:Max event for PA2 from which no system recovers. Succession planning is a mandatory security control.

4. The herbarium is a unique physical SA.
Physical specimen collection supporting PA2 — irreplaceable. Environmental controls and fire suppression are security controls of equal priority to the database backup programme.

5. Two SAs are legally mandated.
DPO (GDPR Art.37) and EU-resident data centre (GDPR data residency) are not optional architectural choices — they are legal compliance requirements for PA4.

Control priorities derived from SA analysis

1. Harden IAM and audit logging across all five PA boundaries. Immutable logs, least-privilege write access, MFA for all privileged accounts — highest priority across all SA categories.
2. Geographically separate DR data centre capable of assuming PA1 and PA3 operations within RTO (1h for PA3, 4h for PA1).
3. DNS protection — DNSSEC, redundant resolvers, registry lock — treating DNS as a critical single SA for PA3.
4. Succession plan and knowledge documentation programme for senior taxonomists — mandatory security control for PA2.
5. Physical security and environmental controls for the herbarium — fire suppression, humidity monitoring, access control independent of IT systems.
6. GDPR compliance for PA4 — DPO appointment, EU data centre, encryption, breach notification within 72h.
7. Network segmentation rigorously enforced between the public-facing service (PA3), the database (PA1), and contributor personal data storage (PA4).