Co-funded by the
European Union

NIPH
Norwegian Institute of Public Health

TSD

NTNU
HUNT forskningssenter

UNIVERSITAS BERGENSIS

SPUHiN

FAIR Secure Procurement and Use of Health data in Norway
Project number: 101128232

Deliverable number: D5.1
Deliverable title: Gap analysis report – SPE requirements

Date: February 2024

Disclaimer: "Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or Health and Digital Executive Agency. Neither the European Union nor the granting authority can be held responsible for them."

Contents

1. Background
2. Methodology
3. Requirements
4. Test plan
5. Gap analysis
6. Results
7. Next steps

Executive Summary

What has been done:

- We have suggested a defined set of requirements for Secure Processing Environments (SPE). The set of requirements builds on:
  - Article 50 in the proposed EHDS regulation
  - Compliance with an existing standard, complemented with EHDS-specific requirements as suggested in the TEHDAS D7.2 report*
  - Reviewing other outcomes from EHDS-related projects such as TEHDAS and the EHDS2 pilot
  - Results from threat modelling of existing analysis infrastructures
  - Review of existing relevant standards
- A gap-analysis for these requirements has been performed at the analysis infrastructures:
  - **TSD** (services for sensitive data)
  - **HUNT Cloud** (research infrastructure for researchers working with sensitive data)
  - **SAFE** (secure access to research data and e-infrastructure)

Outcome and next steps:

- There is a need to agree on minimum requirements for SPEs including harmonization of the level of control provided to data users. Especially related to:
  - That only the right people have access to the data
  - That only non-personal data is exported from the SPE (including assessment of risk related to the level of control for internet access)
- Final outcomes for minimum requirements and level of control will be formalised in national guidelines for SPE users and SPE providers.
- National process and mechanisms for verification of compliance will also be implemented.
- The following gaps will be prioritised to close at the analysis infrastructures in the project:
  - Improvement of the information security management system (ISMS) as preparation for a potential ISO27001 certification.
  - Adjustments to comply with the minimum requirements to be defined
  - Implementing eDelivery for machine-to-machine transport of data between data holder and SPE (part of WP7)

*TEHDAS' proposals for the implementation of EHDS technical infrastructure

1. Background

Introduction to the SPUHiN project

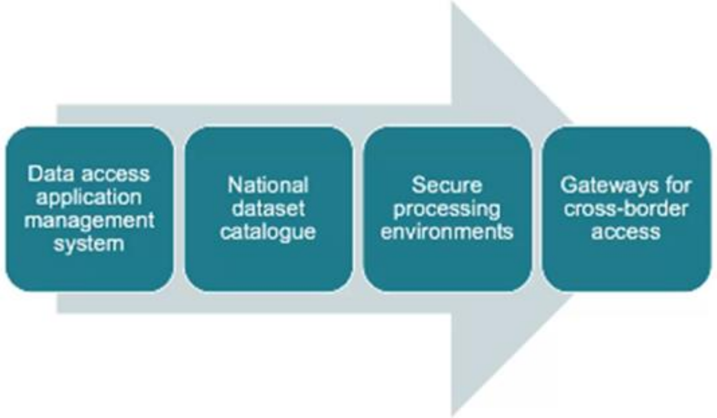
- The European Health Data Space (EHDS) proposes that Health Data Access Bodies (HDAB) are established in each EU/EEA country
- Health Data Service (HDS) in the Norwegian Institute of Public Health (NIPH) is established as the Norwegian HDAB
- Each HDAB is expected to implement a set of defined capabilities:
  - Data access application management system
  - National dataset catalogue
  - Secure processing environments
  - Gateways for cross-border access
- *See related illustration in the next page*

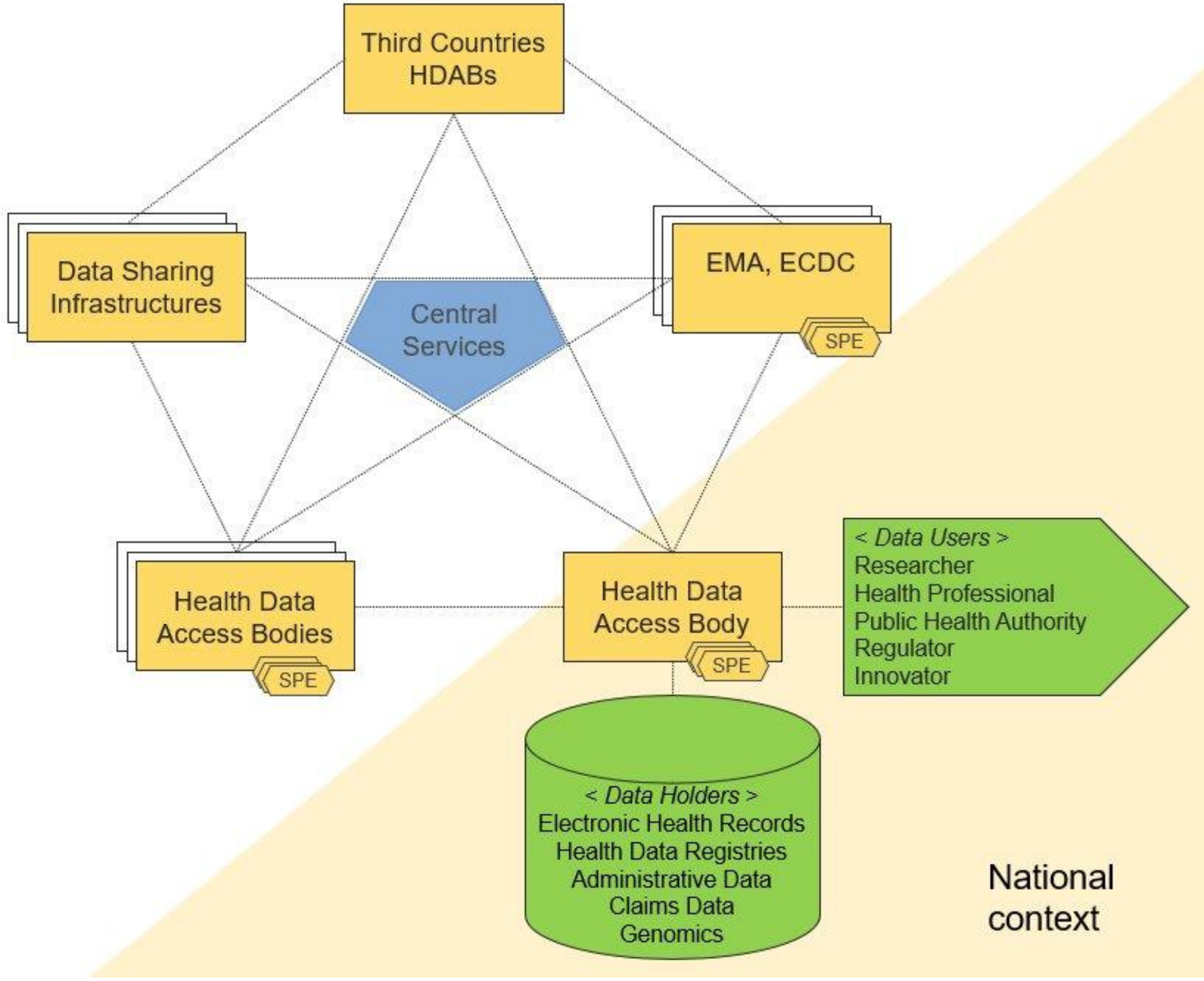
- The SPUHiN project has been granted funds via a Direct Grant from the EU4Health program to further develop the following capabilities:
  - Secure processing environments (SPE) – covered in WP5 and WP6
  - Gateway for cross-border access – covered in WP7 and WP8
  - National dataset catalogue – covered in WP9

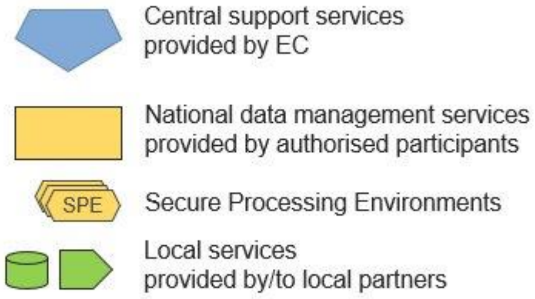
- Article 50 in the proposed EHDS regulation is specifically relevant for Secure Processing Environments
- The development of a Data access application management system is already part of the Norwegian HDAB activities, thus not as scope of the SPUHiN project

HDAB role and capabilities

Four Digital Business Capabilities to be deployed:


Data access application management system
National dataset catalogue
Secure processing environments
Gateways for cross-border access




Central support services provided by EC
National data management services provided by authorised participants
SPE
Secure Processing Environments
Local services provided by/to local partners

Source: European Health Data Space (europa.eu)

Gap analysis for SPE requirements

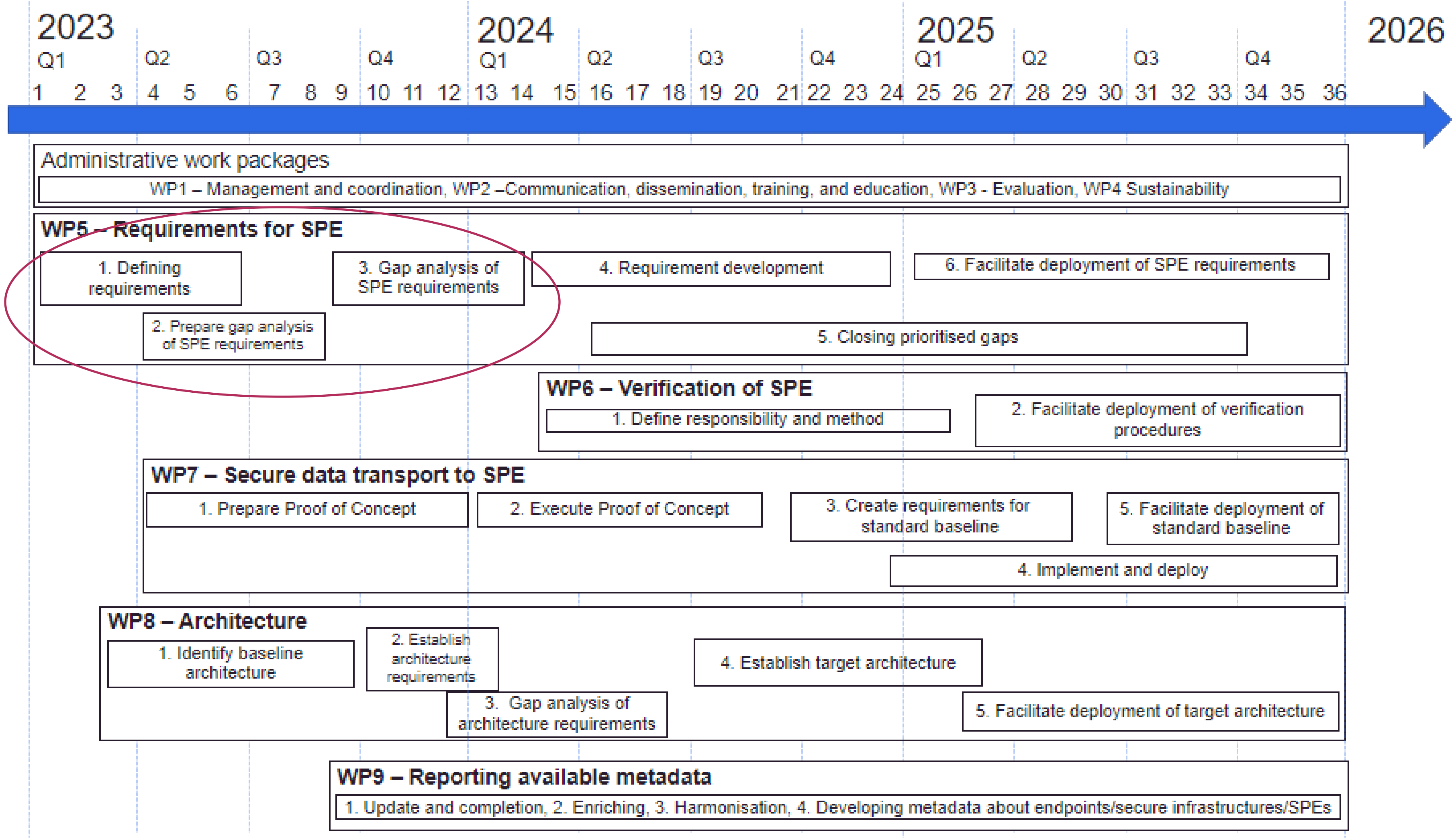
- This GAP analysis report concerns the initial SPUHiN project activities related to SPEs (WP5 and WP6).

Background to SPE development approach:

- The Ministry of Norwegian Health and Care Services has instructed the Norwegian HDAB to collaborate with the three main universities in Norway that already provide analysis infrastructures for processing health data for secondary purposes. These are:
  - **TSD** (services for sensitive data) at the University of Oslo (UiO)
  - **HUNT Cloud** (research infrastructure for researchers working with sensitive data) at the Norwegian University of Science and Technology (NTNU)
  - **SAFE** (secure access to research data and e-infrastructure) at the University of Bergen (UiB)
- The Norwegian legislation requires the HDAB to primarily permit health data to be processed in a ”closed, secure analysis infrastructure”, but no further guidance to this has yet been issued.

- For these main reasons, the work related to the SPE capability for the Norwegian HDAB focus primarily on:
  - Developing requirements (WP5) and verification procedures (WP6) for SPE
  - Support the existing analysis infrastructures in the project to comply with requirements (WP5)
- On an overall level, the first tasks of WP5 until the delivery of this report have consisted of:
  - Defining a set of requirements based on work performed in EU initiatives such as TEHDAS and HealthData@EU Pilot (T5.1)
  - Preparations to perform a gap analysis of the defined requirements (T5.2)
  - Performing a gap analysis and documenting the results, using an external party (T5.3)
- *The next page shows how T5.1, T5.2 and T5.3 relates to the full SPUHiN project plan.*

SPUHiN project plan



2023 Q1 1 2 3 Q2 4 5 6 Q3 7 8 9 Q4 10 11 12

2024 Q1 13 14 15 Q2 16 17 18 Q3 19 20 21 Q4 22 23 24

2025 Q1 25 26 27 Q2 28 29 30 Q3 31 32 33 Q4 34 35 36

2026

Administrative work packages

WP1 – Management and coordination, WP2 –Communication, dissemination, training, and education, WP3 - Evaluation, WP4 Sustainability

WP5 – Requirements for SPE

1. Defining requirements
2. Prepare gap analysis of SPE requirements
3. Gap analysis of SPE requirements
4. Requirement development
5. Closing prioritised gaps
6. Facilitate deployment of SPE requirements

WP6 – Verification of SPE

1. Define responsibility and method
2. Facilitate deployment of verification procedures

WP7 – Secure data transport to SPE

1. Prepare Proof of Concept
2. Execute Proof of Concept
3. Create requirements for standard baseline
4. Implement and deploy
5. Facilitate deployment of standard baseline

WP8 – Architecture

1. Identify baseline architecture
2. Establish architecture requirements
3. Gap analysis of architecture requirements
4. Establish target architecture
5. Facilitate deployment of target architecture

WP9 – Reporting available metadata

1. Update and completion, 2. Enriching, 3. Harmonisation, 4. Developing metadata about endpoints/secure infrastructures/SPEs

Gap-analysis objectives and outcomes

- Main objectives:
  - Gain experience in testing compliance with defined requirements to learn if both the requirements and test method are efficient and appropriate.
  - Learn more about the tested analysis infrastructures.
  - Gain experience in using an external party for performing gap analysis as learning towards the development of a potential certification process.

- Main outcomes:
  - An overall analysis of relevant standards.
  - Results from a threat modelling workshop.
  - An initial set of requirements for SPEs, including information security and functionality.
  - An initial test plan, to be used in a gap analysis.
  - Results from gap analysis performed at three analysis infrastructures in the project.
  - Learnings and recommendations for next steps.

2. Methodology

Overall goals for requirements

Standards based	Standards like ISO/IEC 27001 are already recognised and in broad use. Building on certification according to existing standards, can ease the process for both SPEs and auditors.
Meets the risk	Requirements need to be in line with the cyber security and privacy risk experienced related to SPEs.
In line with European requirements and initiatives	SPEs need to meet the requirements as described in EHDS, specifically Article 50. It is beneficial that Norwegian requirements are in line with those posed in other European countries.
Flexible, able to handle changes in technology and risk	The technology and risk landscape is constantly changing. This needs to be considered when selecting the requirements.

Preparing for requirement selection

To achieve the overall goals, we performed the following main activities prior to the selection of a set of requirements to use in the gap analysis:

- Review of existing relevant standards (page 13)
- Threat modelling for a general SPE infrastructure (page 14 – 18)
- Review of EHDS requirements and relevant outcome of related activities (page 19)

Review of standards

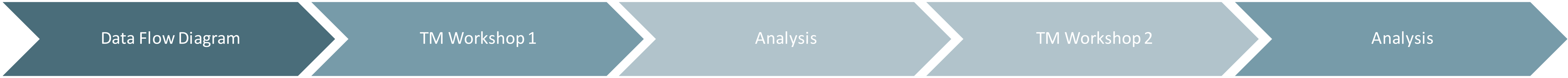
Standard / framework / etc.	Summary assessment
ISO/IEC 27001 and 27002	Internationally recognised standard for general information security. Certification process available and relatively widely used among IT service providers. Scope and risk level is however determined by each entity. Harmonisation in this area may be needed to ensure sufficient level of trust from use of this standard and certification scheme.
ENISA Cloud services cyber security certification scheme	The cloud security cyber security certification scheme concerns information security in an IT provider setting, but not all SPE providers can be considered as cloud services and the framework is relatively heavy. The development of cyber security certification schemes governed by ENISA would however be very interesting to consider if certification of SPE’s will be required. Perhaps development of a scheme for SPE / Trusted Research Environments (TRE) could be discussed.
Guideline on «State of the art» from Germany	Focusing on what technologies that are considered «state of the art» with focus on compliance with the German IT Security Act and GDPR. It is not intended as a check list or complete list of security measures to implement. It may however be a good tool in discussions on what type of technical implementation of security measures that is sufficient in the SPE setting. Especially since the state-of-the-art concept is used in 1b in the Article 50 of EHDS.
Building Trusted Research Environments – Principles and Best Practices («Five safes» report) from the UK	The general concepts for TRE and the five safes are also very relevant for EHDS, including the SPE concept. It may provide a good basis for discussion on requirements that are specifically important to safeguard for SPE’s. It is worth noting that it refers to ISO27001 when it comes to governance framework.
Data protection Code of Conduct for Cloud Service Providers	The Code of Conduct describe required concepts on a relatively general level and may be difficult to use directly to define requirements. As mentioned earlier not all SPE’s will be able to categorise as cloud service providers.
Finnish regulation 1/2022, including «Annex 1: Requirements for a Secure Operating Environment» and Katakri	There is a robust set up of regulation with detailed requirements both for the SPE providers, the accreditation and certification process. It does not however seem to be easily mapped to established standards. It would be very interesting to learn from the Finish experiences with both advantages and disadvantages with their set up.
French regulation	Limited review performed since the regulation is not available in English. Similar to the Finnish regulation it would be interesting to learn from the French experiences with their set up.
NIST Cyber Security Framework (CSF), NIST SP 800-53	The NIST framework is widely recognised and used internationally although it is American. The initial assessment is however that an international standard such as ISO may be more feasible to implement in a European setting.
The Norwegian «NSM grunnprinsipper» and «Normen»	We have mainly focused our assessment on standards that are used across Europe. These are however good examples of local implementation of good practice.

Threat modeling

«Threat modeling (TM) works to identify, communicate, and understand threats and mitigations within the context of protecting something of value." (OWASP)

Main steps performed:

- Description of the system (data flow diagram (DFD)) – what is it that we want to protect?
- Identification of potential threats to the system – what can go wrong?
- Identify mitigations – what can be done?



Data Flow Diagram

- Developed together with the analysis infrastructures HUNT Cloud, SAFE and TSD
- Individual meetings with TSD, SAFE and HUNT Cloud. Modeling of DFD by the Directorate of e-health in-between meetings
- Goal: high level general overview

TM Workshop 1

- Topic for discussion: What can go wrong?
- DFDs used as a basis for the discussions
- Participants from the Directorate of e-health and HUNT Cloud, SAFE and TSD

Analysis

- Goal: to identify the main findings from TM workshop 1, and identify areas where more discussion was needed
- Performed by the Directorate of e-health

TM Workshop 2

- Presented and discussed findings and open issues
- Participants from the Directorate of e-health and HUNT Cloud, SAFE and TSD

Analysis

- Documented the results from the threat modeling
- Performed by the Directorate of e-health

Focus of the discussion in the threat modelling workshops

- We made DFDs on, and discussed functionality related to, selected functionality areas.
- We used STRIDE as a mnemonic to have a more systematic approach to identifying threats

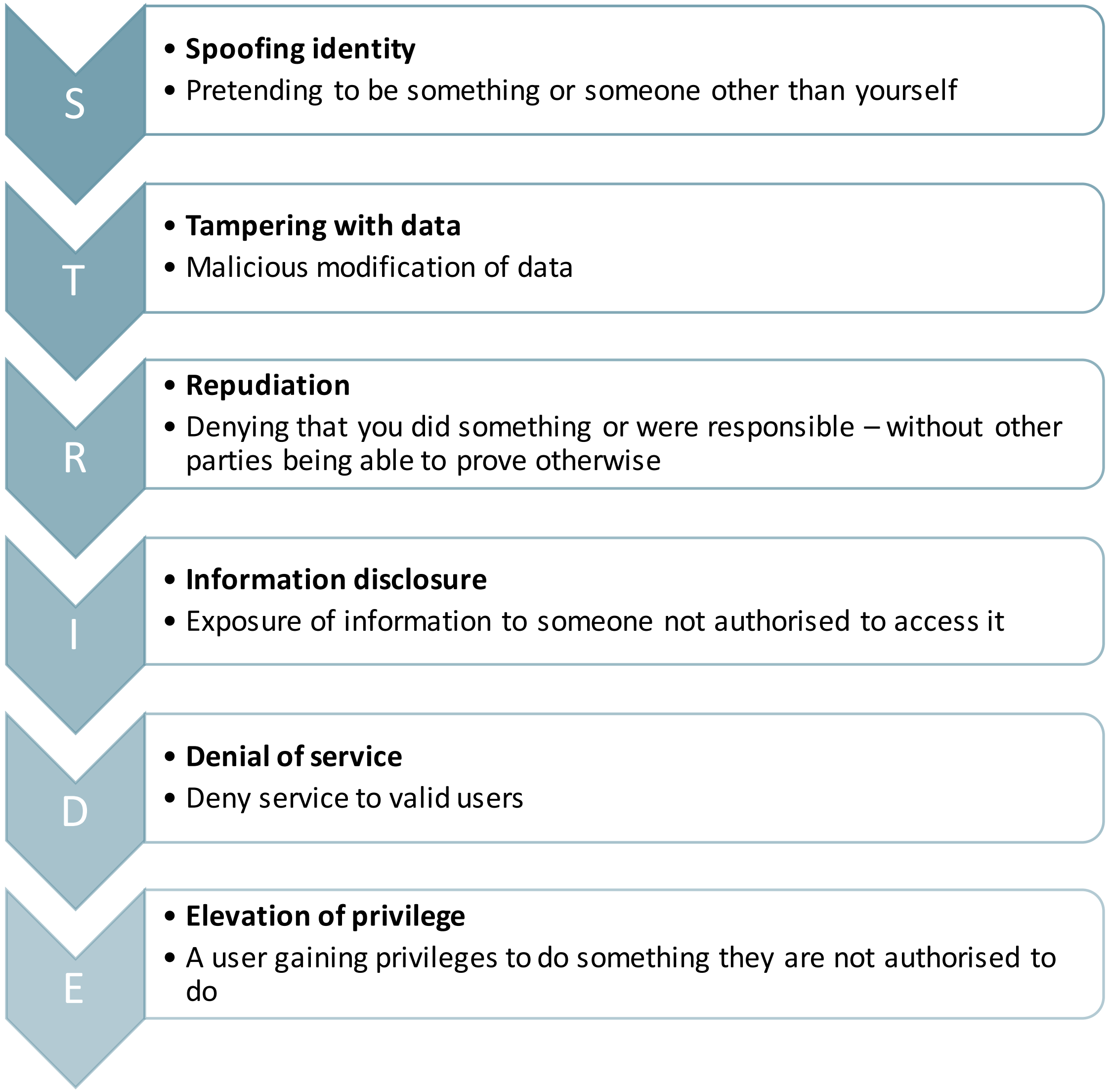
Functionality to:

Analyse data

Manage tools

Exchange data

Perform support functions, including operation



S
- **Spoofing identity**
- Pretending to be something or someone other than yourself

T
- **Tampering with data**
- Malicious modification of data

R
- **Repudiation**
- Denying that you did something or were responsible – without other parties being able to prove otherwise

I
- **Information disclosure**
- Exposure of information to someone not authorised to access it

D
- **Denial of service**
- Deny service to valid users

E
- **Elevation of privilege**
- A user gaining privileges to do something they are not authorised to do

Results of the threat modelling (1/3)

STRIDE

Spoofing

- Threat is addressed through access control and session management.
- Scientific project owner is responsible for who the projects request access rights for.
- Strong authentication requirements can be challenging in practice in case of foreign individuals.

Tampering

- Data traffic is mostly encrypted.
- Encryption at rest is challenging in practice (though can be done for parts of the solution). Risk is reduced by limiting both physical and internet access.
- Risk of malware addressed through Microsoft defender or similar solutions.

Repudiation

- Logging of actions on the infrastructure.
- Have chosen not to have logs on actions taken by researchers.
- Logs are protected – imported to a central database.
- Hard for SPEs to be both a service provider and the one auditing the use of the service. SPEs may however have a role in training researchers in their security responsibilities as users of an SPE.

Results of the threat modelling (2/3)

STRIDE

Information disclosure

- The biggest concern is human error – sending the wrong file, sending data to the wrong place, etc.
- Difficult to control that legitimate users do not take pictures of information on the screen, etc.
- Limited internet access reduces the risk.
- Risks related to data download was discussed. This is considered the responsibility of the researchers. Technical control is limited.
- (See also information on encryption under «Tampering»).

Denial of service

- As data is used for research purposes, unavailability for a limited amount of time is not critical – as compared to clinical use.
- Strong availability of import/export of data is not important – these services are only used for shorter amounts of time.
- Services for administration and operation may have stronger availability needs.
- Risk reduced through backups and limited internet access.

Elevation of privilege

- Strong technical controls limit the risk of getting access to other projects.
- Project manager can increase access privileges when this is needed.
- Vulnerability management, security patching.
- Privileged access secured through NDAs, personal accounts, open discussion of deviations, etc. Background checks could be an option but is challenging in practice.

Results of the threat modelling (3/3)

Main concern

- Large amount of personal information in the hands of unauthorised individuals

Main differences

- The extent to which users are allowed internet access, ability to download tools
- The extent to which user's self-service (access rights management, verify download of only non-personal data etc.)

Possible future developments

- APIs and micro services:
  - increasing need for authentication and token management.
  - APIs are more exposed and need to be secure, but risk of human error may be reduced.
  - in case of federated learning, this may bring new risks.
- eDelivery is coming, but the analysis infrastrucutures have not yet implemented.
- Some analysis infrastructures are considering a move towards «safety levels» with varying degrees of limitations on what researchers are allowed to do with the data.

Related EU requirements and activities

We have considered different input specifically relevant to EHDS, including:

- EHDS regulation, specifically requirements in article 50
- TEHDAS WP7 – Connecting the dots, specifically
  - Milestone 7.6 and Deliverable 7.2 – Active participation in working groups related to SPE. The milestone/deliverable include a lot of information and recommendations related to SPEs
  - Questionnaire to existing SPEs (available in the TEHDAS SharePoint)
- EHDS2 Pilot WP7 – Regulatory and legal compliance, specifically
  - Deliverable 7.2 – Relevant information on SPEs included in section on Data use
  - Questionnaire summary related to data provision and use
- Workshop ”Elements of Secure Processing Environments” organised by EOSC-Life and HealtyCloud (June 2023)
- BBMRI-ERIC Security and Privacy Architecture

Considerations

As basis for D7.2 from TEHDAS the participating countries were allowed to vote on different topics. The following outcomes have been especially relevant for our requirement selection:

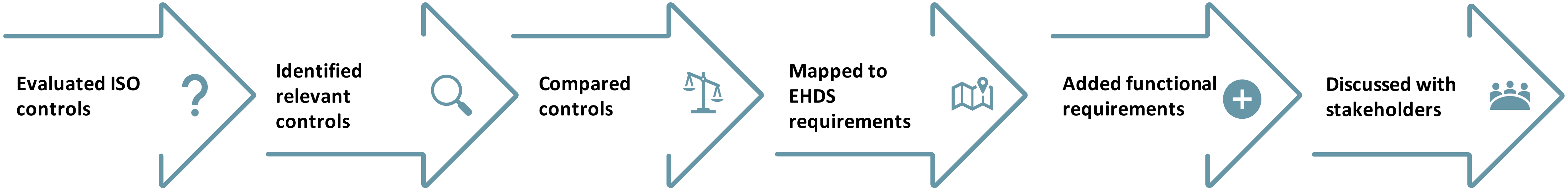
- Strong agreement on building on an existing standard and adding EHDS-specific requirements
- Strong agreement on verification of compliance through a certification process
- Agreement on EU harmonisation for requirements on extraction of data
- Agreement on EU level minimum functional SPE capabilities

Based on our initial standards review:

- ISO27001 with the support of ISO27002 stands strongest among existing standards to use as a basis
- Detailed requirements on security quickly means «heavy» standards that will require a lot of resources both to maintain and to implement

3. Requirements

What we did



Evaluated ISO controls

Identified relevant controls

Compared controls

Mapped to EHDS requirements

Added functional requirements

Discussed with stakeholders

01

Evaluated all ISO/IEC 27002 controls (Low/Medium/High)

- Is this control of particular relevance to SPEs (as compared to other types of IT-systems)?
- Is this control directly important to fulfil requirements in EHDS article 50?
- Is this control of particular relevance to the risk highlighted in the threat modeling workshops?

02

Identified the most relevant ISO/IEC 27002 controls (and groups of controls)

03

Compared the identified controls to what is proposed by other initiatives

- Are the same controls covered there?
- Something missing in our controls?

04

Revised suggestion – mapped the identified controls to EHDS article 50 requirements

05

Added functional requirements

06

Discussed the suggested controls with stakeholders, and revised as needed

Evaluation of security controls

- This is an example of the documentation from our evaluation of the ISO 27002 controls relevance

No.	Control	Specific needs for SPEs	H/M/L*	EHDS article 50	H/M/L	Threat modeling	H/M/L
5.15	Access control	Access control is central to offering an SPE. Responsibility for access control divided between SPE and project. Access control also for privileged users. Needs may not be very different from other services that use sensitive data.	M	a) b) e) ++	H	A lot of emphasis on and discussion on access control. Considered important.	H

- The most relevant controls were then grouped in different requirement categories that we compared with the outcome from other EHDS relevant initiatives. Some adjustments were made in selected categories.
- This was then used as a basis for a suggested set of security related requirements.

*H: High, M: Medium, L: Low

Functional requirements

- As the instructions from the Ministry of Norwegian Health and Care was to collaborate with the three main universities in Norway that already provide analysis infrastructures for processing health data for secondary purposes, the scope of the current functional requirements are based on these analysis infrastructure's user groups. There are other types of types of analysis infrastructures relevant for secondary usage of sensitive health data, with a broader set of user groups than those currently covered.
- An early observation was that discussions on functional requirements quickly can turn in to a discussion on the definition of an SPE. Early on we also determined that we should focus on functional requirements that need to be present with all SPEs. There is however a need to describe additional functionality with different SPEs, but these will not be considered minimum requirements. The work to be done in task "T9.4 Developing metadata about endpoints/secure infrastructures/SPEs", may be a relevant manner to describe and publish information on such additional functionality.
- We noted that where security requirements are tightly connected to risk, functional requirements are tightly connected to user needs and may vary more between different SPE providers on a detailed level.
- We identified functional requirements mainly through workshops with representatives from the analysis infrastructures TSD, SAFE and HUNT Cloud and project members that represent the user perspective.
- We noted that several of the defined security requirements also can be considered functional requirements, such as mechanisms for access control, importing data, controlling exported data, backup and archiving.

Requirements (1/3)

Primarily security related requirements

No	Requirement description	Priority
R1	The SPE provider operates an information security management system (ISMS) according to ISO/IEC 27001. The scope of the ISMS covers the SPE provider's organisational units, locations and processes for providing the SPE infrastructure.	High
R2	The SPE provider has policies and systems for digital access control (including identification, authentication and authorisation) on a security level that is in line with the level of risk. Risk related to privileged access control is managed.	High
R3	Possible processes for import of health data (both digital and manual processes) are identified and sufficiently secured in line with the level of risk. The communication channels within any distributed SPE infrastructures are set up in a secure manner.	Medium
R4	Services for extracting data from the SPE only allow for extract of non-personal health data.	High
R5	Where cryptography is used, the key length, strength of encryption algorithms and key management is in line with the risk level, also considering how long the cryptographic protection needs to last.	Medium

Requirements (2/3)

Primarily security related requirements

No	Requirement description	Priority
R6	The SPE provider performs logging and monitoring on a level that makes the SPE provider capable to discover the most important types of unwanted events that has been identified in risk assessments.	Medium
R7	The SPE provider continuously backup digital assets and the backups are protected against unauthorised access.	Medium
R8	Health data is sufficiently secure during storage and storage equipment is protected during its whole lifetime (including decommissioning).	Medium
R9	The SPE provider is prepared to manage information security incidents.	Medium
R10	The SPE provider has a documented security architecture that meets the identified needs of SPEs, including of segregation between SPEs within the SPE infrastructure. Both physical and digital security is a part of this architecture.	High
R11	The SPE provider has a documented and established good practice for secure operations of the SPE infrastructure.	Medium

Requirements (3/3)

Purely functional requirements

No	Requirement description
R12	The SPE provider has documented standard analysis capabilities or tools that are available to the user. The SPE provider has processes for secure import of new or updated tools based on user needs. The SPE provider has processes for license management.
R13	The SPE provider has documented and established good practice for support, maintenance and development for the SPE services.
R14	The SPE provider has documented and established services for archiving or secure integration with archiving systems.
R15	The SPE provider has documented and established secure services for persons and/or systems to interact with the data and tools for analysis.

4. Test plan

Creating a test plan

- The main approach for specifying test activities has been to leverage on an ISO27001 certification, and in addition verify that the scope and risk level is appropriate for an SPE.
- As only one of the analysis infrastructures in the project is currently ISO27001 certified we also developed an alternative test plan.
- With this approach we were allowed to evaluate the benefit of leveraging on an existing certification.
- Regardless of certification, the requirements with high priority were more extensively tested than the others.
- With the authority we currently have, we will not be able to test compliance related to the responsibility of the data users. We can however test the mechanisms that the analysis infrastructures provide to the data users to be able to comply with their responsibilities (e.g. access management and controlling data export). The requirement descriptions were updated accordingly.
- All selected requirements are relatively high level with few details on HOW they are to be implemented.
- In summary, the requirements and test plan is aiming to be standards based, risk based and technology independent.

Assessment of the approach

Standards based, risk based and technology independent requirements

- Pros:
  - More flexible and easier to maintain – does not need to be updated for every change in threats and technical solutions
  - Reduced risk of misplaced controls, where SPEs end up being too compliance driven
  - Emphasis on the most important controls
  - Not a new framework for SPEs – reuse of work that SPEs normally need do anyway (ISO 27001)
  - Easier to audit as can use the ISO 27001 certificate
  - Tightly connected to article 50 – strong motivation for the controls, support in fulfilling article 50 requirements

- Cons:
  - Risk based and technology independent controls are more difficult to evaluate than more specific controls – thus the current approach puts high requirements on the evaluator
  - Risk that different evaluators may end up with different evaluations → less trust
  - High requirements for competence and maturity of SPE providers

Mitigating activities

Suggestions on how the ”cons” may be dealt with

- Clear guidelines on expectations for SPEs on implementing requirements, including detailed examples
- Clear guidelines on how to audit and definition or examples of accept criteria
- Roles and responsibilities within and across organisations need to be specified
- Similar training for auditors coordinated between EU countries
- Discussion of this theme in a Community of Practice to exchange experiences between EU countries
- Central oversight function to identify and evaluate differences between the practice in different EU countries

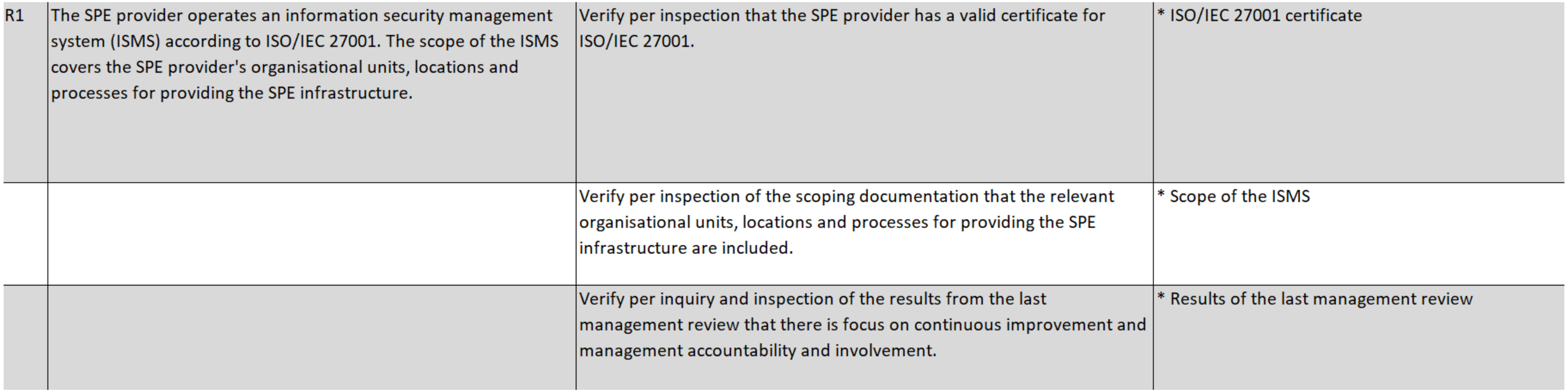
Test plan - summary

The next 4 slides are meant to depict the difference between testing of the following:

- ISO certified vs non-certified SPEs
  - The test plan and type of requested information is different
  - Testing for ISO certified entities rely heavily on the ISO certificate and the status of controls in the Statement of Applicability (SoA) document
  - More documents are requested for inspection for non-certified SPEs
- High vs medium priority requirements
  - The high priority requirements include inspection and observation to a higher degree
  - High priority requirements look into more details of how the mechanisms related to the requirement are set up
  - Medium priority requirements require mainly inquiry, especially for ISO certified entities

Example test plan (1/4)

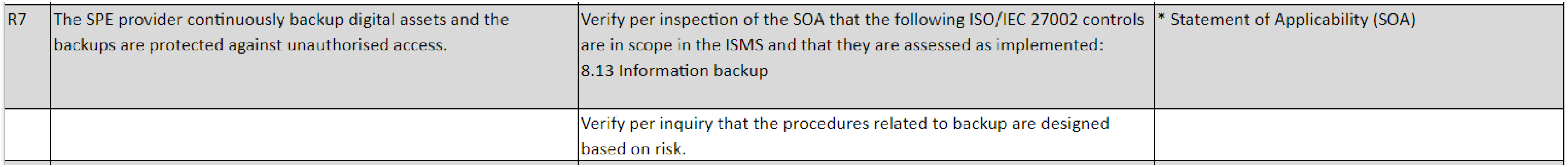
High priority requirement, certified entity



R1	The SPE provider operates an information security management system (ISMS) according to ISO/IEC 27001. The scope of the ISMS covers the SPE provider's organisational units, locations and processes for providing the SPE infrastructure.	Verify per inspection that the SPE provider has a valid certificate for ISO/IEC 27001.	* ISO/IEC 27001 certificate
		Verify per inspection of the scoping documentation that the relevant organisational units, locations and processes for providing the SPE infrastructure are included.	* Scope of the ISMS
		Verify per inquiry and inspection of the results from the last management review that there is focus on continuous improvement and management accountability and involvement.	* Results of the last management review

Example test plan (2/4)

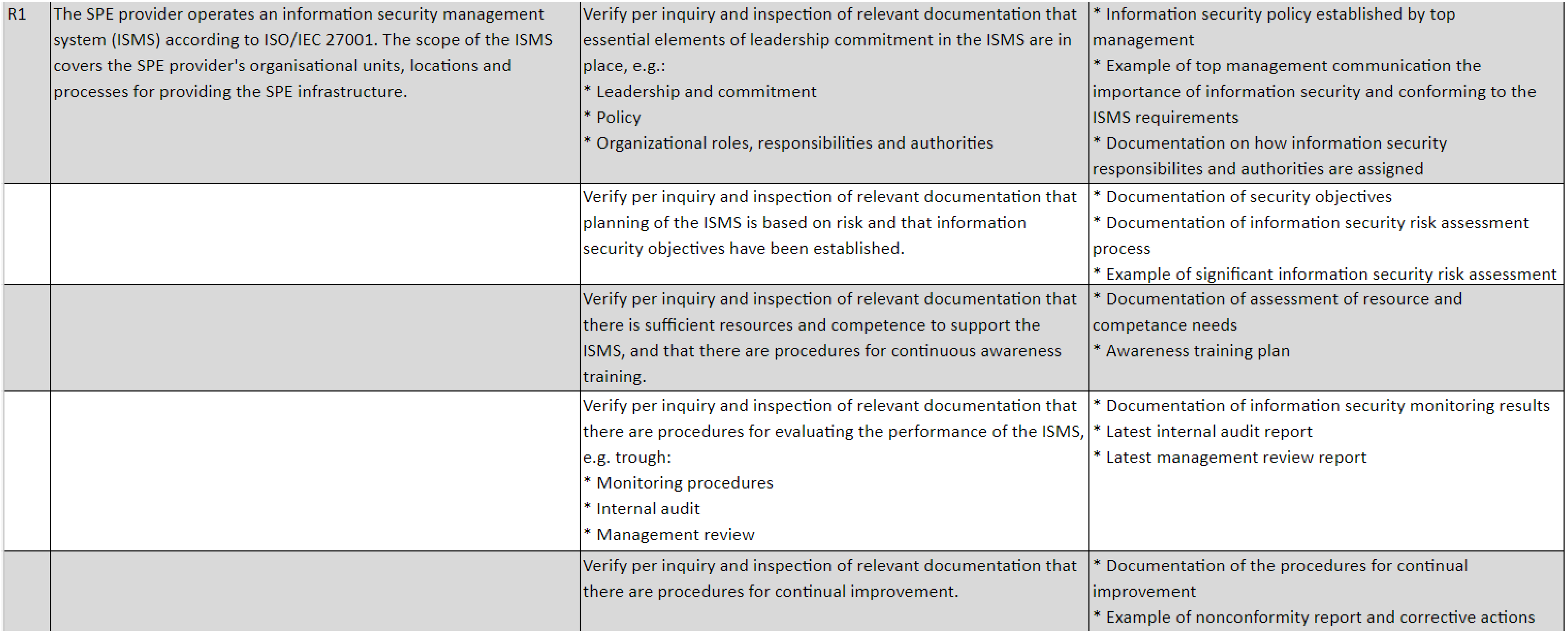
Medium priority requirement, certified entity



R7	The SPE provider continuously backup digital assets and the backups are protected against unauthorised access.	Verify per inspection of the SOA that the following ISO/IEC 27002 controls are in scope in the ISMS and that they are assessed as implemented: 8.13 Information backup	* Statement of Applicability (SOA)
		Verify per inquiry that the procedures related to backup are designed based on risk.	

Example test plan (3/4)

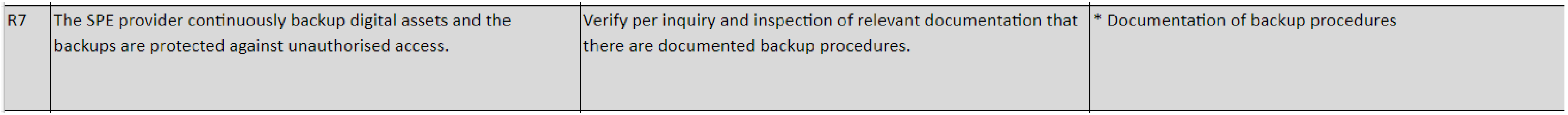
High priority requirement, non-certified entity



R1	The SPE provider operates an information security management system (ISMS) according to ISO/IEC 27001. The scope of the ISMS covers the SPE provider's organisational units, locations and processes for providing the SPE infrastructure.	Verify per inquiry and inspection of relevant documentation that essential elements of leadership commitment in the ISMS are in place, e.g.: * Leadership and commitment * Policy * Organizational roles, responsibilities and authorities	* Information security policy established by top management * Example of top management communication the importance of information security and conforming to the ISMS requirements * Documentation on how information security responsibilites and authorities are assigned
		Verify per inquiry and inspection of relevant documentation that planning of the ISMS is based on risk and that information security objectives have been established.	* Documentation of security objectives * Documentation of information security risk assessment process * Example of significant information security risk assessment
		Verify per inquiry and inspection of relevant documentation that there is sufficient resources and competence to support the ISMS, and that there are procedures for continuous awareness training.	* Documentation of assessment of resource and competance needs * Awareness training plan
		Verify per inquiry and inspection of relevant documentation that there are procedures for evaluating the performance of the ISMS, e.g. trough: * Monitoring procedures * Internal audit * Management review	* Documentation of information security monitoring results * Latest internal audit report * Latest management review report
		Verify per inquiry and inspection of relevant documentation that there are procedures for continual improvement.	* Documentation of the procedures for continual improvement * Example of nonconformity report and corrective actions

Example test plan (4/4)

Medium priority requirement, non-certified entity



R7	The SPE provider continuously backup digital assets and the backups are protected against unauthorised access.	Verify per inquiry and inspection of relevant documentation that there are documented backup procedures.	* Documentation of backup procedures

5. Gap analysis

Preparation for gap analysis

- To ensure a successful gap analysis there were several preparatory steps to take. These include:

What to test	Requirement selection and development of test plan are described in the previous two chapters. Representatives from TSD, SAFE and HUNT Cloud were involved in the whole process of selecting requirements and developing the test plan. The draft document was also discussed with a group in the Institute of Public Health and Directorate of health, including some further representatives from information security, data holders and data users.
Who to test	TSD, HUNT Cloud and SAFE were all willing to participate as test subjects in this gap analysis. The main contact persons for each analysis infrastructure were responsible to invite the correct people to the test session.
Who to perform test	An existing frame agreement was used to make a formal request for proposals for the activity of performing this gap analysis. A consultant from EY was selected for the task. The Directorate of e-health selected to generally participate with minimum three resources from WP5/6 in all test sessions to seize this learning opportunity.
When to test	We started the detailed planning of testing a couple of months prior to expected start-up. Due to a heavy load on the test subject resources, we ended up with performing all test sessions in December. We recommended to send documentation prior to the test session. A detailed (but flexible) agenda was sent out ahead and it was based on the requirements to make efficient use of resources that may not need to be present for the whole session.

Main participants

Requirement development and gap analysis

Organisation (in 2023)	Core team
Directorate of e-health	Klara Lundgren Anne Heidi Skogholt Inger Anne Tøndel Tonje Stegavik Olav Astad Kristiansen
Norwegian Institute of Public Health	Elisabeth Hagen
Directorate of health	Tricia Larose
EY (consultant)	Birgitte Fjærestad

Organisation	Contributors
TSD	Gard Thomassen Leon Charl du Toit Haneef Awan Frode Strømsvåg
HUNT Cloud	Oddgeir Lingaas Holmen Tom-Erik Røberg Qussay Ghazeia
SAFE	Christine Stansberg Haakon Fannemel Breivik Tore Linde Askil Laastad Jarl Magnar Hansen Kristoffer Baldysz Erling Langøigjelten

Reflections from the test sessions

- We planned for 2-3 days of testing for each test subject but used approximately 2 days.
- It was positive that all test subjects had the necessary staff in place to answer questions related to the requirements.
- It was especially helpful that all had included at least one participant with experience from work with controls and audit.
- It was very positive that several of the test subjects saw this session as a learning opportunity, which potentially will be helpful in the work going forward.
- It was relatively busy to perform three different gap analysis in three weeks time since it left little room for preparation and follow-up directly in conjunction with each test session.

- Since this was a gap analysis in a «pilot» setting, we did not require to obtain and retain all the documentation we examined.
- In a «real» setting more time may need to be used for ensuring a sufficient level of documentation.
- Some of the requested documentation was sent ahead. In a «real» setting it may be beneficial if this is planned to be sent earlier to allow for sufficient review ahead of the test session.
- Notes from the test session was summarised and provided to the test subjects for fact checking and detailed feedback. These notes have been used as a basis for the test summary in the next chapter.
- A couple of working weeks after the test sessions we had a summary meeting with each test subject to discuss the main findings and allow for fact checking.

6. Results

Summary of results

- As there are not yet any formal minimum requirements for SPEs, the results from the gap analysis focus on how the analysis infrastructures in the project have implemented the tested requirements.
- In this report, we have decided to highlight the following five areas related to the gap analysis:
    - Information security management system
    - Access management
    - Data export
    - Data import
    - Functional requirements
- These are all areas that stand out as relevant to SPEs and are also related to mechanisms for the project owner to maintain their responsibilities as a data user.
- The following pages sum up the main characteristics in each area for the test subjects. The characteristics are comparable between the test subjects through numbering within each area.
- An overall observation is that all the analysis infrastructures have high focus on both functionality and security. At the same time, the chosen set up differs between them. This information provides for a very good basis for the work ahead.

Summary HUNT Cloud

Area	Summary Results
Information security management system	a) ISO 27001 (Information security), ISO 9001 (Quality) and ISO 27701 (Privacy) Certified. b) Clear connection and anchoring with the management of NTNU. c) Choice and design of controls could be more connected to risk. Responsibilities for the projects and its users could be more clearly described.
Access Management	a) Access is set up by HUNT Cloud, based on written authorisation through a form filled by the project owner. b) Active users may review access. The project owner is not always an active user. c) Access logs are available upon request. d) Users are allowed access after project owner's approval, and the project owner is responsible for authentication. e) Granulated access on file-level in a project is not available. f) All users must sign a user agreement.
Data Export	a) Secure export function (Kista) available. b) Project owner must approve set-up with Kista's and specify who can perform export. c) Some alerts for monitoring export, but few mechanisms for the project owner to review data export. d) No copies of the exported data retained.
Data Import	a) Secure import function (Kista) . b) Machine to machine transfer available. Not generally set up between register to analysis infrastructure.
Functional requirements	a) Provide a basis set of analysis tools and have procedure for adding more tools if requested. b) Allow for internet access mainly with the purpose of being able to use tools that require internet connection. c) License management is based on "Bring-your-own-license"

Summary TSD

Area	Summary Results
Information security management system	a) Not ISO 27001 certified but is a part of the ISMS by UiO. b) Missing some documented connection between UiO ISMS and TSD's security work. c) Some routines missing formalization and/or documentation.
Access Management	a) Self-service portal for access management. b) Access review is available for project owner in the self-service portal. c) Some access logs are available to the project owner in the self-service portal. d) Norwegian users are authenticated by BankID. Foreign users are allowed access after project owner approval. The project owner is responsible to perform authentication using passport verification. e) It is possible to granulate access on file-level in a project. f) All users must sign a user agreement.
Data Export	a) Secure export function available. b) Export of data is only accessible for users that have been given access to this by the project owner. c) Export of data is logged and available for project owner in the self-service portal. d) Copy of the exported file is not retained.
Data Import	a) Secure import function through the self-service portal. Available to import by using a link if the data owner does not have access to the SPE. b) Machine to machine transfer available. Not generally set up between register to analysis infrastructure.
Functional requirements	a) Provide a basis set of analysis tools and have procedure for adding more tools if requested. b) Internet connection not allowed. Provide mirrored versions of tools that requires internet connection. c) TSD provides license for UiO-users. For other users, license management is based on "Bring-your-own-license“.

Summary SAFE

Area	Summary Results
Information security management system	a) Not ISO 27001 certified but is a part of the ISMS by UiB. b) Missing the connection between UiB ISMS and SAFE's security work. c) Several routines missing formalization and/or documentation.
Access Management	a) Access is set up by SAFE, based on an access document in excel administered by the project owner. b) The project owner has the possibility to review access by running a script, and manually through the access document. c) Access logs are available upon request. d) Norwegian users require a UiB account, authenticated using MinID. Foreign users are allowed access after project owner approval. The project owner is responsible to perform authentication using at least one type of identification number. e) It is possible to granulate access on file-level in a project. f) All users must have an UiB account, where they sign the ICT-rules, security information and privacy statement for UiB.
Data Export	a) Secure export function available by using a personalised export-folder. b) Project owner controls who has access to export. File is encrypted and must be opened with a password only available to the user. c) Project owner has access to export logs. d) A copy of the exported file is retained. The project owner can request that export needs to be approved before it is exported.
Data Import	a) Secure import function by using a personalised import-folder. b) Machine to machine transfer is available. Not generally set up between register to analysis infrastructure.
Functional requirements	a) Provide a basis set of analysis tools and have procedure for adding more tools if requested. b) Internet connection not allowed. Provide mirrored versions of tools that requires internet connection. c) UiB provides some license for all UiB-accounts and SAFE distributes licenses to all fixed analysis tools, Outside of this license management is based on "Bring-your-own-license"

User need and responsibilities

- All analysis infrastructures in the project operate with a trust model where the data user institutions and projects are responsible for handling the data according to laws and regulations.
- The projects have a responsibility for ensuring sufficient information security, maintaining and controlling access management, controlling data export and ensuring secure data import. It is also important for the projects to have access to necessary tools in a secure manner.
- As illustrated in the previous summary pages, the providers of analytics infrastructures in the project offer different levels of mechanism to help the projects fulfil their needs and maintain their responsibilities.
- The learnings from the gap analysis about the current set up at each analysis infrastructure in the project will be very valuable input in the next steps of the project that will include:
  - Agreeing on minimum requirements
  - Developing national guidelines
  - Closing prioritised gaps at the analysis infrastructures in the project

7. Next steps

Harmonisation of minimum requirements

Based on learnings from the gap analysis, the following needs to be clarified as a basis for all ongoing work:

- Minimum requirements for mechanisms the data users need to comply with their responsibilities related to:
  - That only the right people have access to the data
  - That only non-personal data is exported from the SPE (including assessment of risk related to the level of control for internet access)
- Harmonisation of different levels of control in SPEs (data safety levels?), their associated minimum requirements and which data that can be processed on each level

It is important with sufficient involvement of relevant stakeholders in this work, especially representatives from data users on different levels.

Prioritised gaps

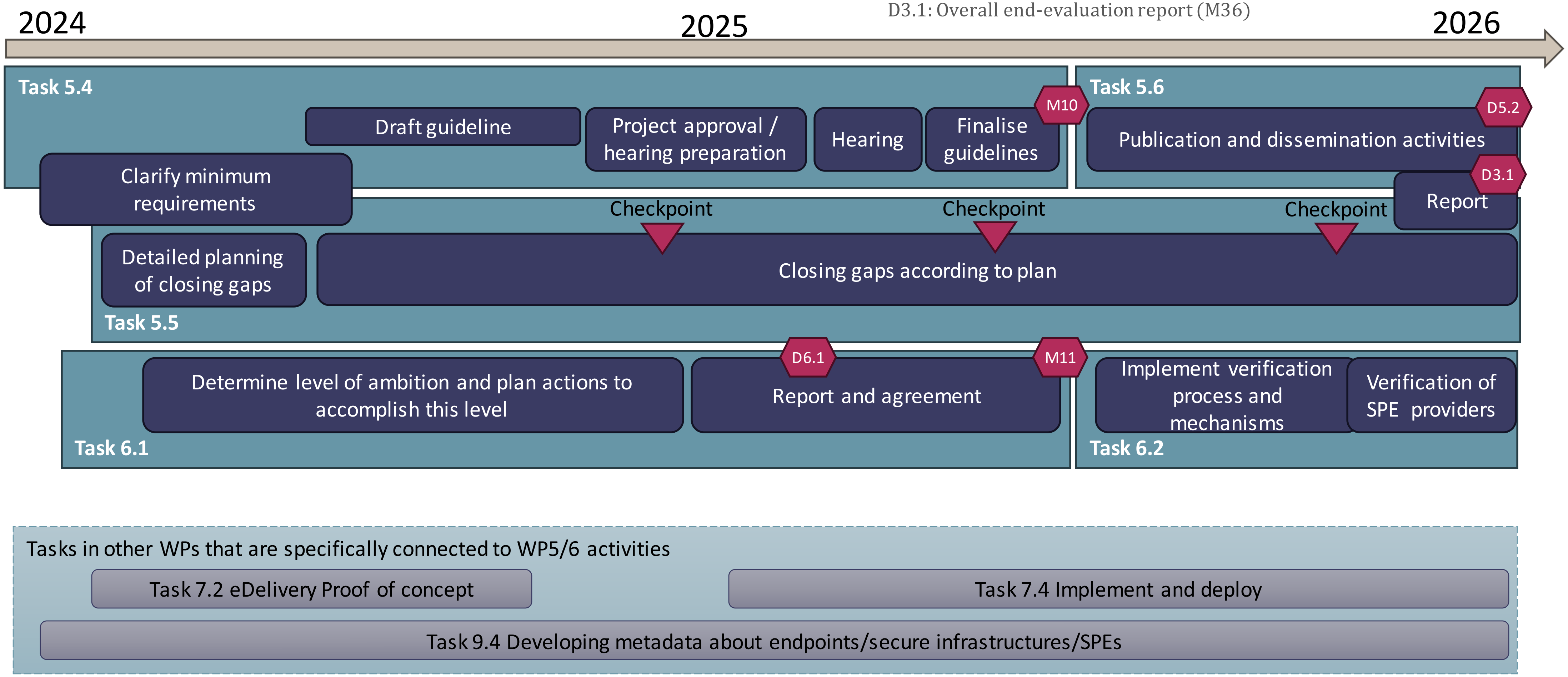
On an overall level, these are the gaps that should be prioritised in task T5.5 Closing prioritised gaps:

- Improvement of the information security management system (ISMS) as preparation for a potential ISO 27001 certification.
- Adjustments to comply with the minimum requirements to be defined with establishment of different «data safety levels».
- Implementing eDelivery for machine to machine transport of data between data holder and SPE (part of WP7).

Overall time line - WP5 and WP6

Preliminary

M10: Agreed on secure processing environment requirements (M24)
D5.2: Published national recommendations for SPEs (M36)
M11: Agreed on verification procedures to be used in Norway (M26)
D6.1: Report on Norwegian verification procedures for SPE requirements M25)
D3.1: Overall end-evaluation report (M36)



2024
2025
2026

Task 5.4
Draft guideline
Project approval / hearing preparation
Hearing
Finalise guidelines
M10
Clarify minimum requirements

Task 5.6
D5.2
Publication and dissemination activities
D3.1
Report

Checkpoint
Checkpoint
Checkpoint
Detailed planning of closing gaps
Closing gaps according to plan
Task 5.5

D6.1
M11
Determine level of ambition and plan actions to accomplish this level
Report and agreement
Task 6.1
Implement verification process and mechanisms
Verification of SPE providers
Task 6.2

Tasks in other WPs that are specifically connected to WP5/6 activities
Task 7.2 eDelivery Proof of concept
Task 7.4 Implement and deploy
Task 9.4 Developing metadata about endpoints/secure infrastructures/SPEs

Overall timeline – WP5 and WP6

Preliminary

WP5 (task 5.4 and 5.6)

2024:

- Q1-Q2: Workshops with relevant stakeholders, e.g. related to minimum requirements for control of access and export + data safety levels
- Q3: Draft guidelines for SPE users and SPE providers sent to internal hearing in the organisations involved in the project, and maybe other selected stakeholders
- Q4: Approval of draft to hearing in project management group, project board, HDIR/NIPH management. Also consider involvement of the health data infrastructure board, the health data advisory board and the health data reference group

2025:

- Q1: Public hearing for official national guideline
- Q2: Work with hearing responses and finalise guideline
- Q3-Q4: Publish guideline and perform dissemination activities
- Q4: Report for summary of work and status

WP5 (task 5.5)

- 2024 Q1-Q2: Same workshops as for 5.4/5.6
- 2024 Q1-Q2: Detailed planning of activities to close prioritised gaps for each analysis infrastructure in the project
- 2024 Q2- 2025 Q4: Follow up according to defined check-points for planned activities
- 2025 Q4: Report for summary of work and status

WP6 (task 6.1 and 6.2)

2024:

- Determine level of ambition for the period and plan actions to accomplish this level (self-assessment?)

2025:

- Q1-Q2: Report and agreement of verification procedures
- Q3: Implementation of verification process and mechanism, including dissemination
- Q4: Verification of SPE providers

Success criteria

- For the gap analysis
  - Close collaboration with analysis infrastructures and data holders
  - Active involvement in relevant EHDS projects on EU level
  - Concrete and hands-on activities
  - Minimum viable product (MVP) approach and continuous improvement
  - Project team continuity

- For next steps
  - *Continuing with the same success criteria as for the gap analysis*
  - Closer involvement of data user representatives
  - Dialogue with other potential SPE providers
  - Close collaboration between the new Directorate of Health and the Institute of Public Health
  - Closer collaboration between work packages in the project

Appendix

Glossary and abbreviations

Phrase/Abbreviation	Description
SPE	Secure Processing Environment as specified in the EHDS regulation, article 50.
TRE	Trusted Research Environment. Term that is used for environments with similar use as an SPE but more generally for all type research.
Analysis infrastructure	Term used in this report for providers of secure services to process health data for secondary use. Research infrastructure is a similar term that is also used elsewhere. When an analysis infrastructure complies with the minimum requirements of an SPE they can be referred to as an SPE.
EHDS	European Health Data Space
TEHDAS	The European Health Data Space project
HDAB	Health Data Access Bodies
SPUHiN	Abbreviation of the project FAIR Secure Procurement and Use of Health data in Norway, co-funded by the EU4Health program
ISMS	Information Security Management System
Project owner	The person responsible for the project that is using an analysis infrastructure. They are also data responsible according to GDPR. This role is in practice referred to as project responsible, principal investigator etc. but in this report we have decided to use project owner to describe this role.
Review access	Possibility to check who has access at this moment
Access log	Possibility to see who has logged on and when
Machine to machine transfer	Possibility to transfer data without users having to do a manual operation