On the Relationship Between Security and Privacy in the Context of Information Systems

Felix Thorwächter

19.06.2023, Bachelor's Thesis Final Presentation

Chair of Software Engineering for Business Information Systems (sebis)
Department of Computer Science
School of Computation, Information and Technology (CIT)
Technical University of Munich (TUM)
wwwmatthes.in.tum.de

Outline

Motivation

Approach

- Research Questions
- Methodology

Results

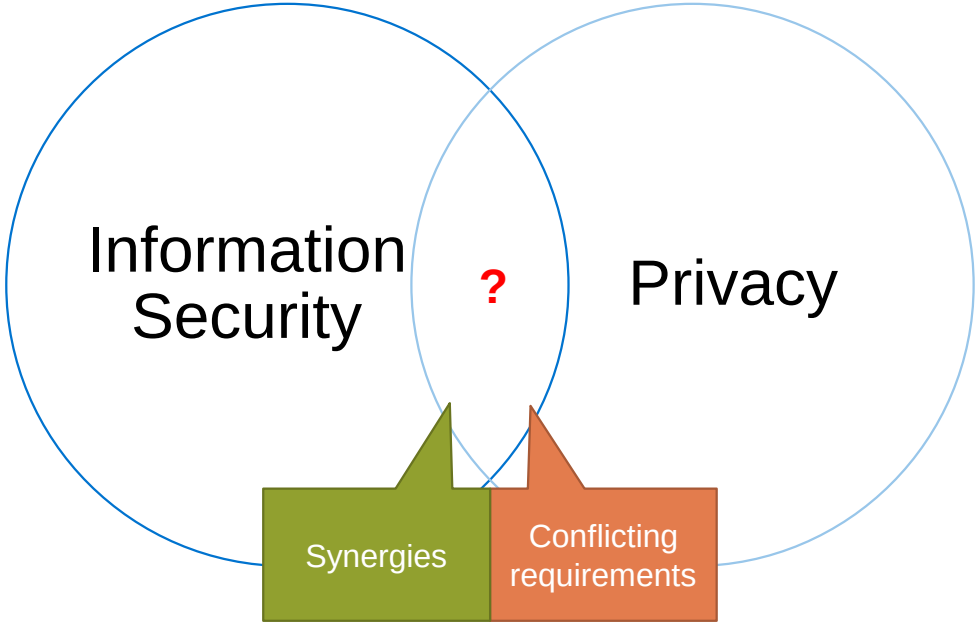
- Concept Map (RQ1 and RQ2)
- Evaluation of privacy impact of security measures (RQ2)
- Conflict Solving (RQ2 and RQ3)

Limitations and Future Work

Summary

Motivation

Problem: Unclear relationship between Information Security and Privacy in practice *



Possible consequences:

- Unclear responsibility
- Gaps in protection
- Unused synergies or inefficient processes

Examples for Synergies:

- Process for incident management
- Data protection from unauthorized access or disclosure

Examples for Conflicts:

- Data Retention vs Backup
- Data Minimization vs Monitoring

* This was confirmed during discussions with security experts, e.g., during the Feedback Workshop.

Outline

Motivation

Approach

- Research Questions
- Methodology

Results

- Concept Map (RQ1 and RQ2)
- Evaluation of privacy impact of security measures (RQ2)
- Conflict Solving (RQ2 and RQ3)

Limitations and Future Work

Summary

Research Questions

Theory → Best Practices → PETs as a possible solution

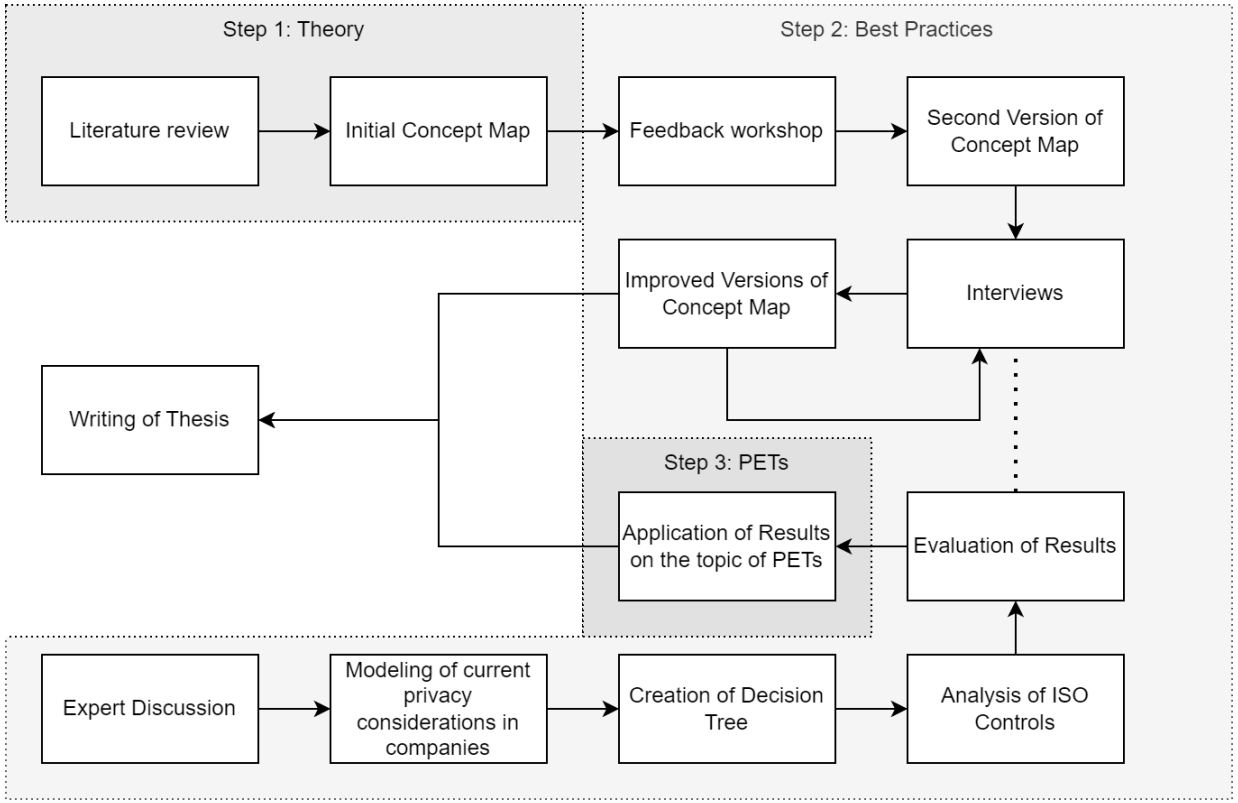
RQ 1:
What are the definitions of security and privacy, and how are these concepts related in **theory**?

RQ 2:
From the viewpoint of information security experts, how do the concepts of security and privacy overlap **in practice**, and what are possible conflicting requirements or synergies?

RQ 3:
To what extent can **PETs** fulfill information security requirements to replace information security measures in certain areas?

Methodology

Theory → Best Practices → PETs as a possible solution



Step 1 (Answer RQ 1):

- Literature review
- Creation of Concept Map

Step 2 (Validation of results from Step 1 and to answer RQ 2):

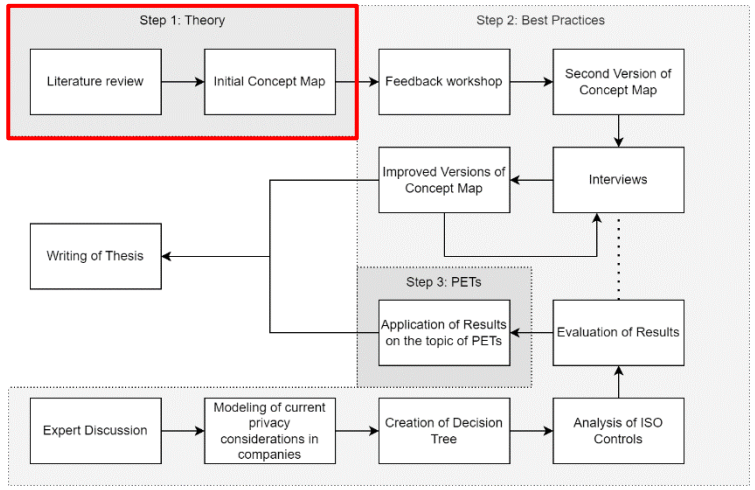
- Feedback Workshop
- Semi-Structured Interviews
- Improvement of Concept Map
- Development of 3-level decision tree
- Analysis of 92 ISO/IEC 27002 measures for their privacy implications

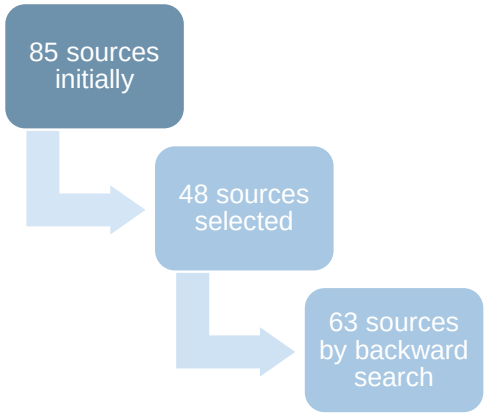
Step 3 (Answer RQ 3):

- Application of results to the topic of PETs

Methodology

Theory → Best Practices → PETs as a possible solution



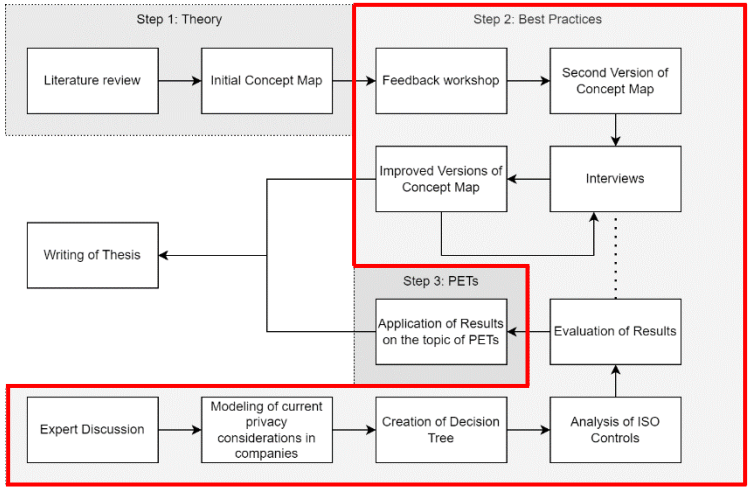


Step 1 (Answer RQ 1):

- Literature review:
  - Database:
    - Mainly IEEE Xplore (and Nautos)
    - Grey literature
  - Search strings as combinations of keywords:
    information security, security, privacy, information system, definition, standard, framework, regulation
  - Inclusion criteria:
    - German or English
    - Papers defining privacy
    - Papers addressing the intervened nature of security and privacy
    - Papers explaining the concepts in general
  - Exclusion criteria:
    - Papers describing implementations in detail
    - Papers outside the context of information systems in general
- Creation of Concept Map:
  - Visualizes results
  - Improved during Step 2 with multiple iterations

Methodology

Theory → Best Practices → PETs as a possible solution



Step 2 (Validation of Results from Step 1 + Answer RQ 2):

- Feedback Workshop:
  - 45 minutes
  - 10 participants
- Semi-Structured Interviews:
  - 6 participants
  - 107 years of combined working experience
  - ~ 5 hours and 10 minutes of interviews
- Analyze ISO/IEC 27002 controls for their privacy implications:
  - Discussion with I-1 to model current handling of PII
  - Creation of 3-level decision tree
  - Analysis of 92 controls

Participant	Role (* also ISO)	Brand Size (Employees)	Industry	(Main) Region
W-1	* Director Information Security	Large (> 500)	Build + Construct	USA
W-2	GRC Manager			
W-3	Corporate Information Security Officer	Holding of all other companies		
W-4	Security Architect			
W-5	* Team Lead Internal IT	Small (< 100))	Operate + Manage	Europe
W-6	* Team Lead Infrastructure and Security	Large (> 500)	Planning + Design	Europe
W-7	* Security Consultant	Small (< 100)	Digital Twin	Europe
W-8	* Global IT Security and Business Operations Manager	Large (> 500)	Planning + Design	Europe
W-9	Senior Corporate Security Engineer	Medium (100-500)	Planning + Design	USA
W-10	* Team Lead IT Network and Infrastructure	Medium (100-500)	Build + Construct	Europe

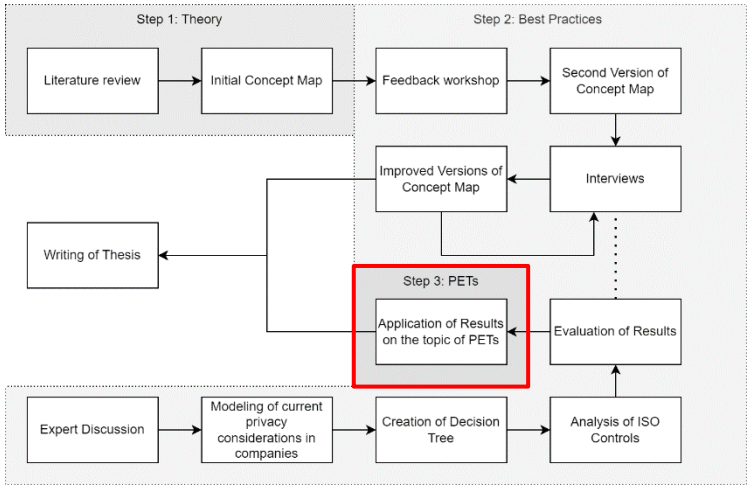
Workshop participants

Code	Role	Company Employees	Sector	(Main) Region	Work experience
I-1 / W3	Corporate Information Security Officer	5.000	AEC/O, Partly media and entertainment	USA and Europe	10-20 years
I-2 / W4	Security Architect				> 30 years
I-3	Security Manager				20-30 years
I-4 / W1	Info Security Director / ISO	500	AEC	USA	5-10 years
I-5	Data Protection Officer	5.000	Broadcasting	Germany	5-10 years
I-6	Project Owner and Lead Developer	> 50.000	Insurance and financial services	Europe	20-30 years

Interview participants

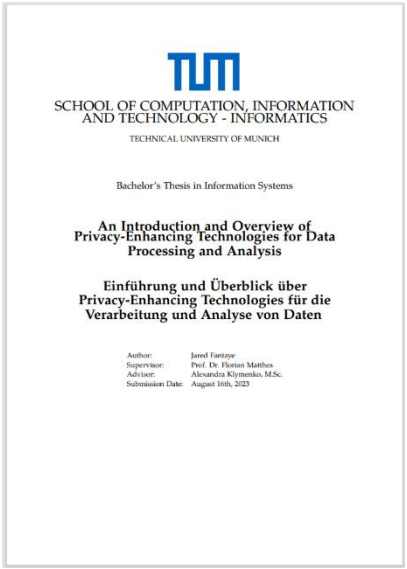
Methodology

Theory → Best Practices → PETs as a possible solution



Step 3 (Answer RQ 3):

- Application of results to the topic of PETs
  - Find solutions to discovered possible conflicts
  - Collect a list of PETs and find use cases for them within the ISO2700X framework



SCHOOL OF COMPUTATION, INFORMATION AND TECHNOLOGY - INFORMATICS

TECHNICAL UNIVERSITY OF MUNICH

Bachelor's Thesis in Information Systems

An Introduction and Overview of Privacy-Enhancing Technologies for Data Processing and Analysis

Einführung und Überblick über Privacy-Enhancing Technologies für die Verarbeitung und Analyse von Daten

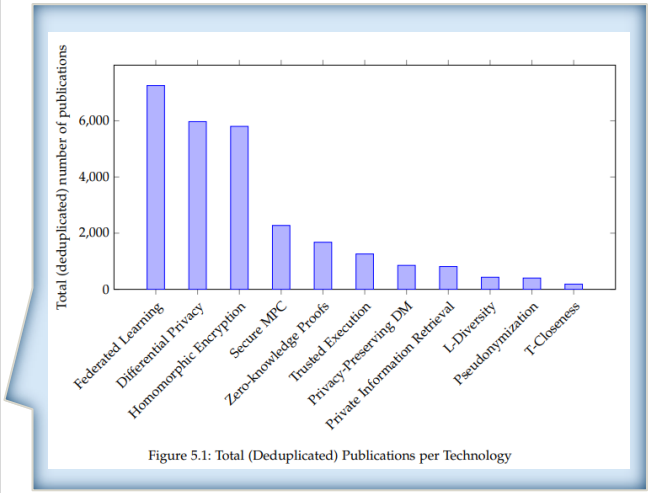


Figure 5.1: Total (Deduplicated) Publications per Technology

Outline

Motivation

Approach

- Research Questions
- Methodology

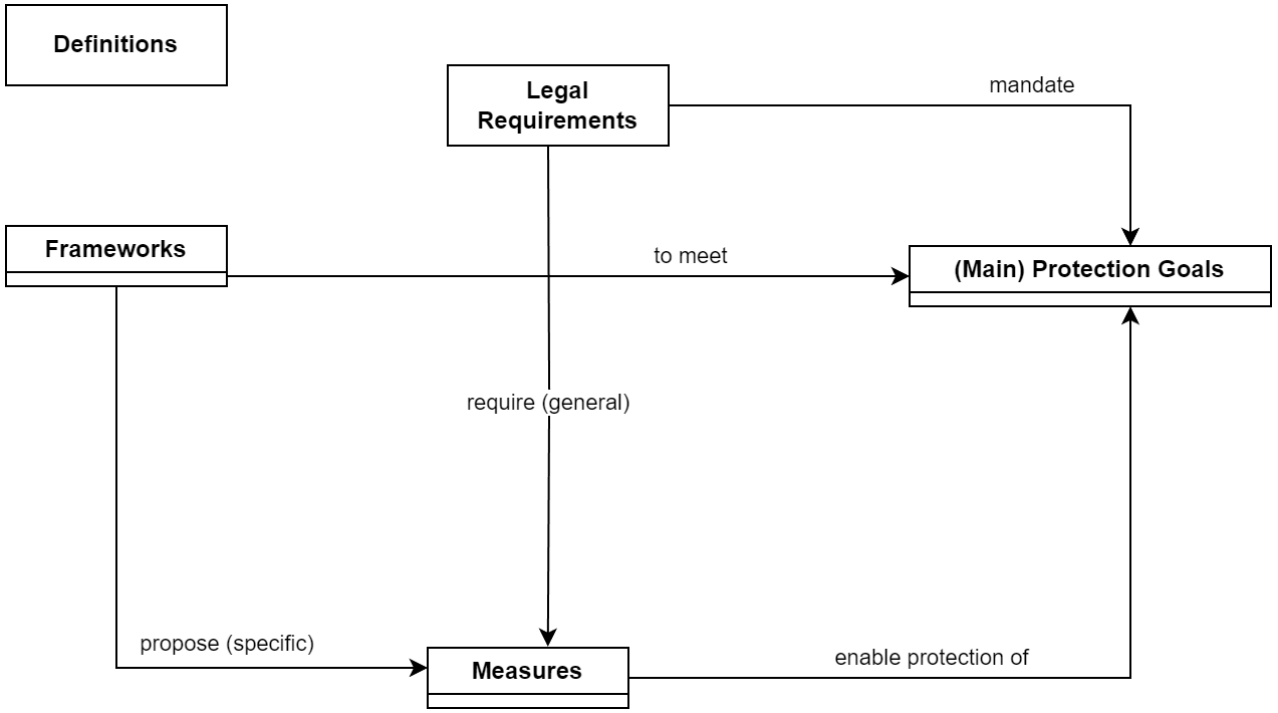
Results

- **Concept Map (RQ1 and RQ2)**
- Evaluation of privacy impact of security measures (RQ2)
- Conflict Solving (RQ2 and RQ3)

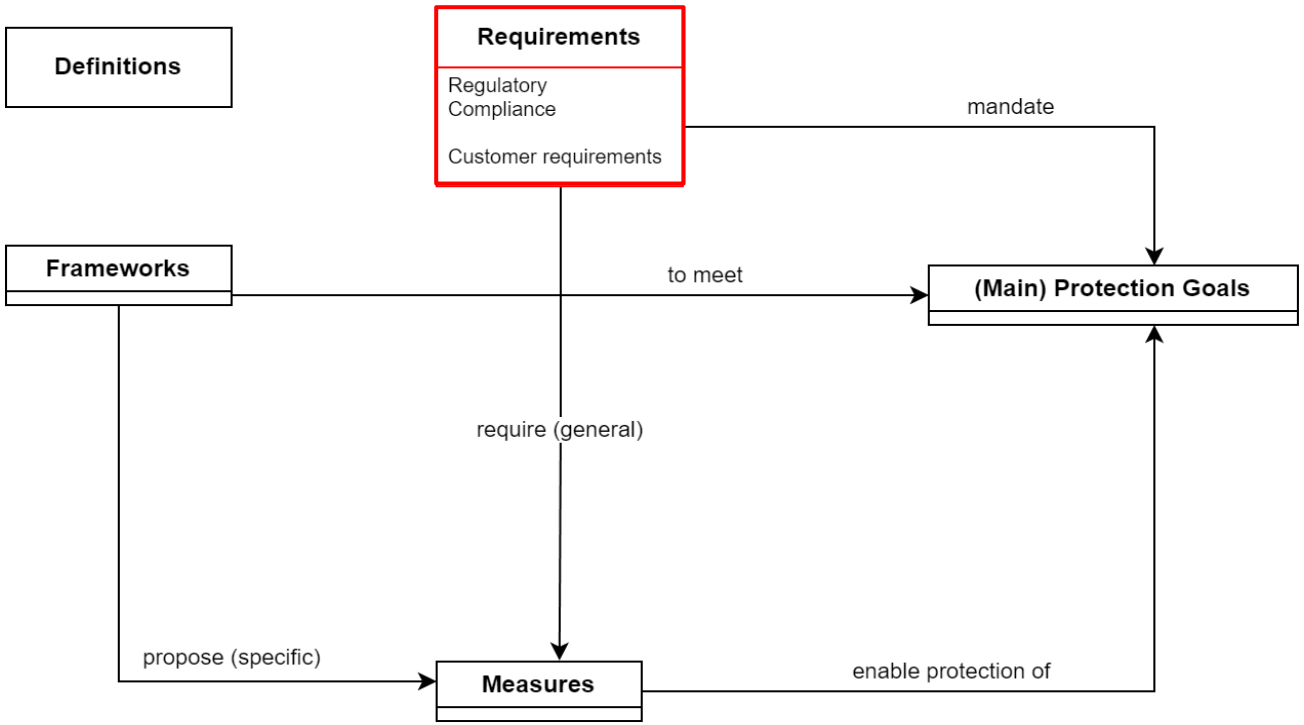
Limitations and Future Work

Summary

Concept Map – Evolution of the Overview

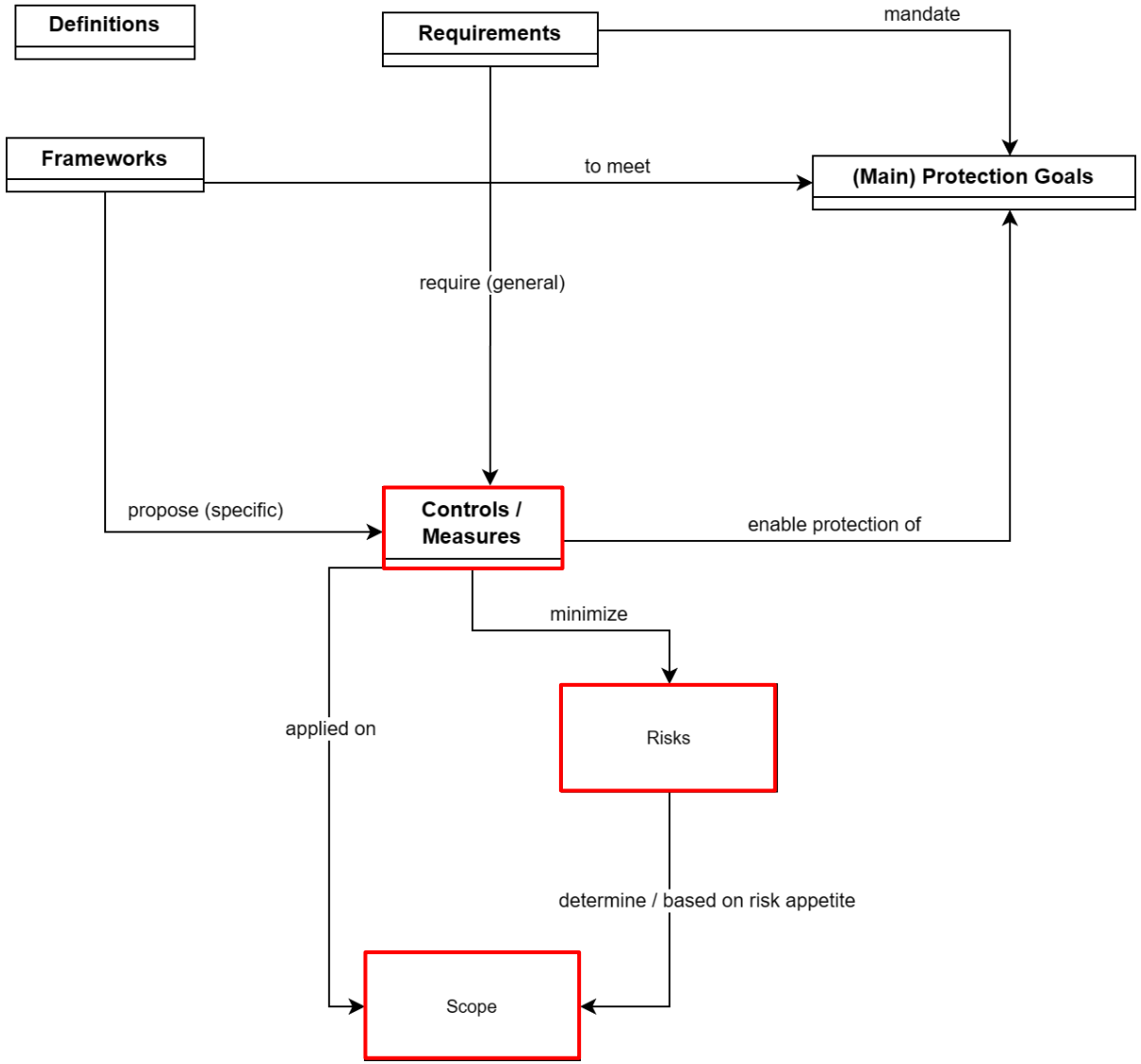


Concept Map – Evolution of the Overview



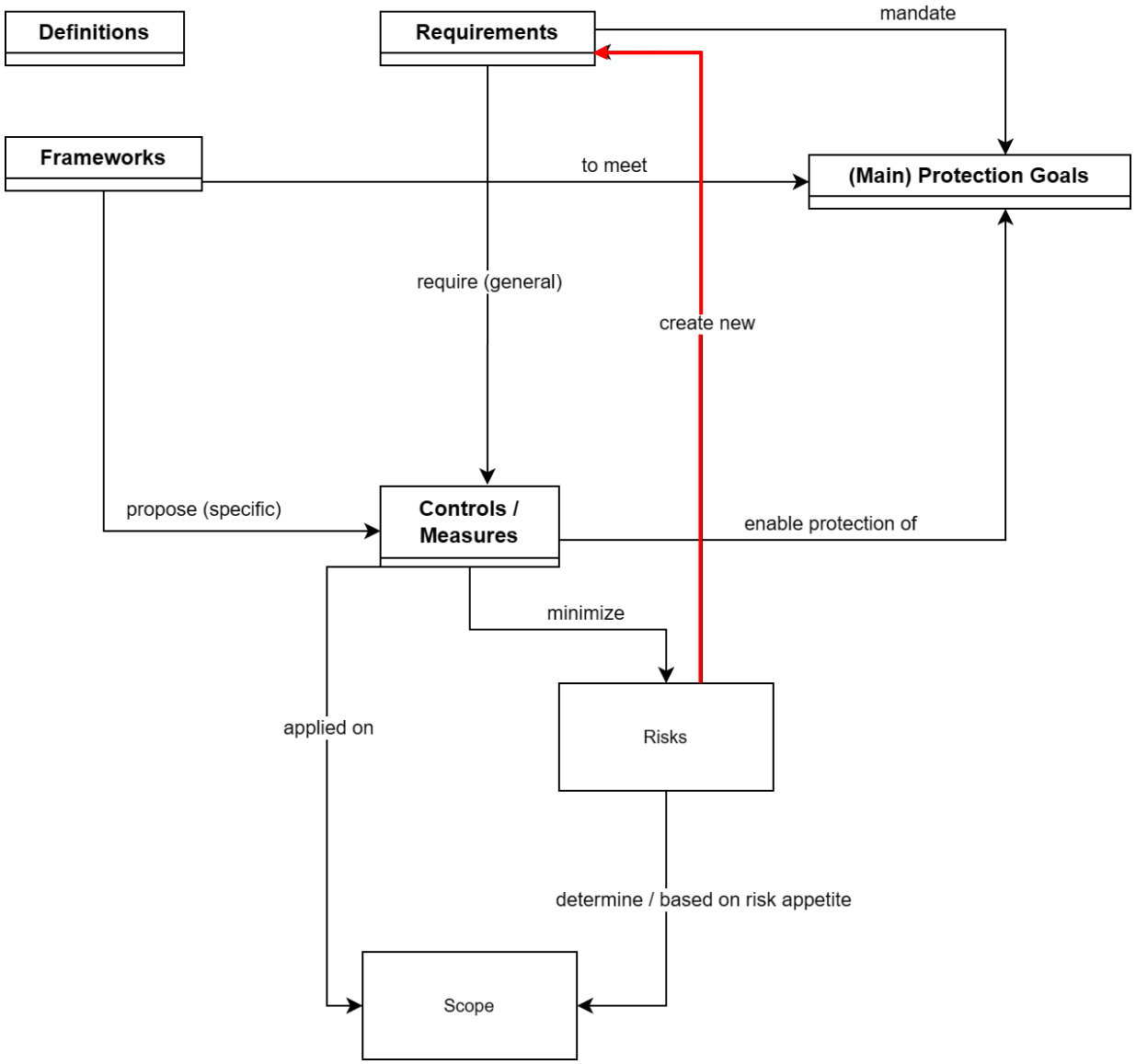
Concept Map – Evolution of the Overview

Theory → Best Practices → PETs as a possible solution

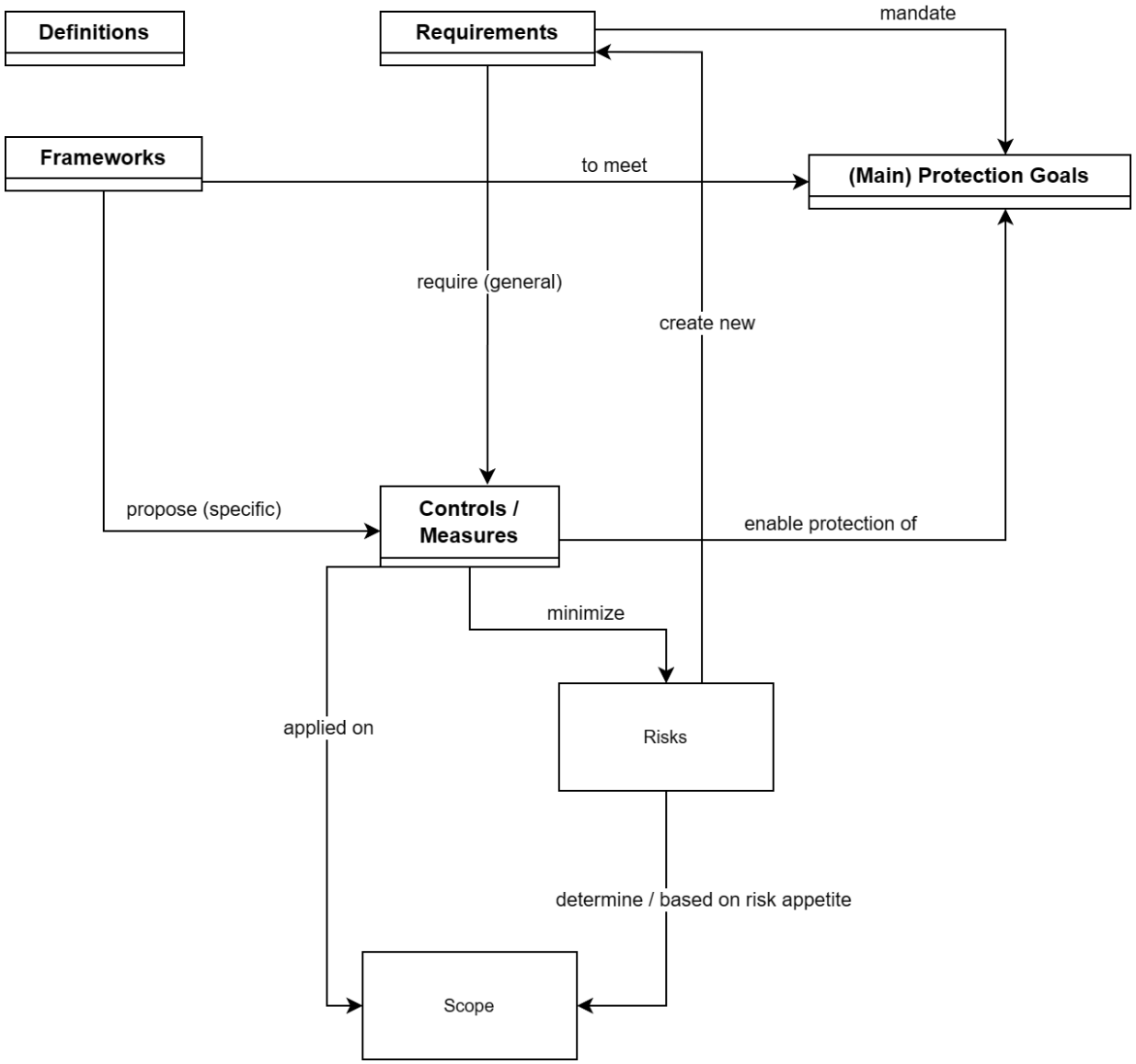


Concept Map – Evolution of the Overview

Theory → Best Practices → PETs as a possible solution



Concept Map - Overview



Concept Map – Live Demo

Live Demo: https://s.icepanel.io/KWS6whIVxy4b0J/T7ft

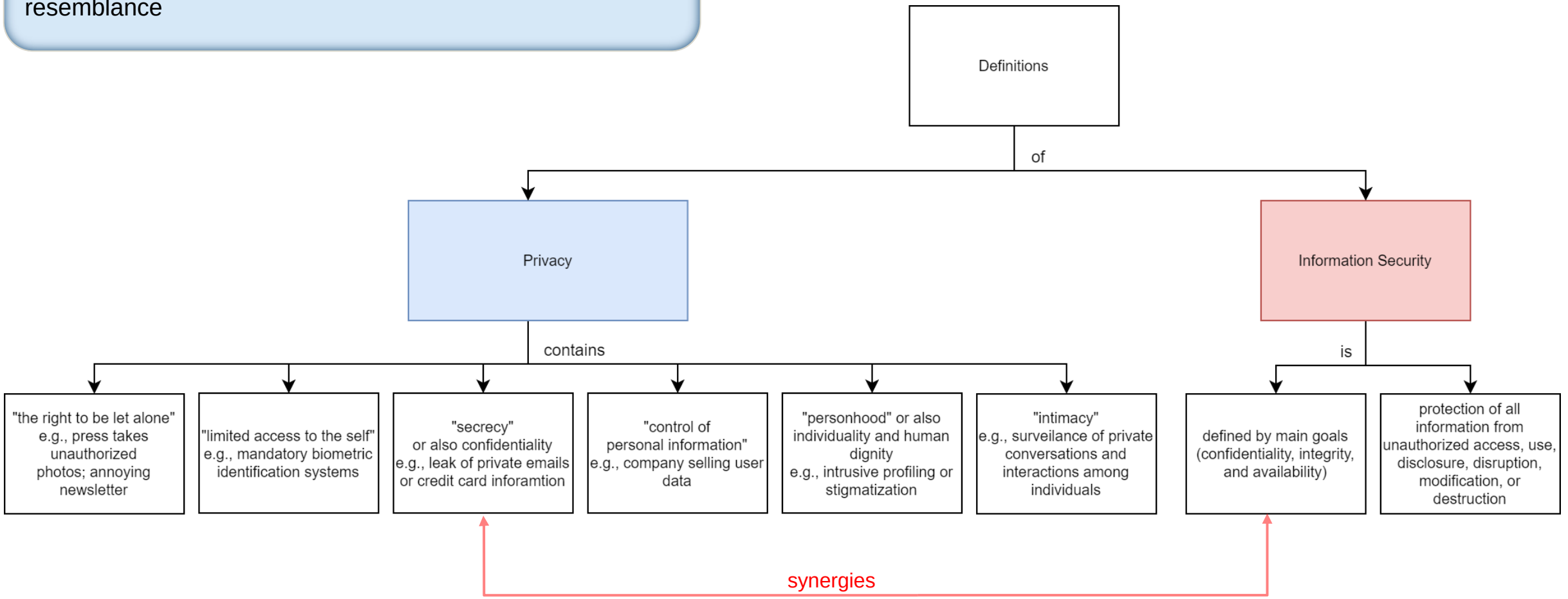
Concept Map - Definitions

Theory → Best Practices → PETs as a possible solution

Colour key:

Blue	Privacy
Red	Security
Green	Both

Key finding #1:
Privacy is hard to define; better described by overlapping *similarities* following Wittgenstein's description of family resemblance



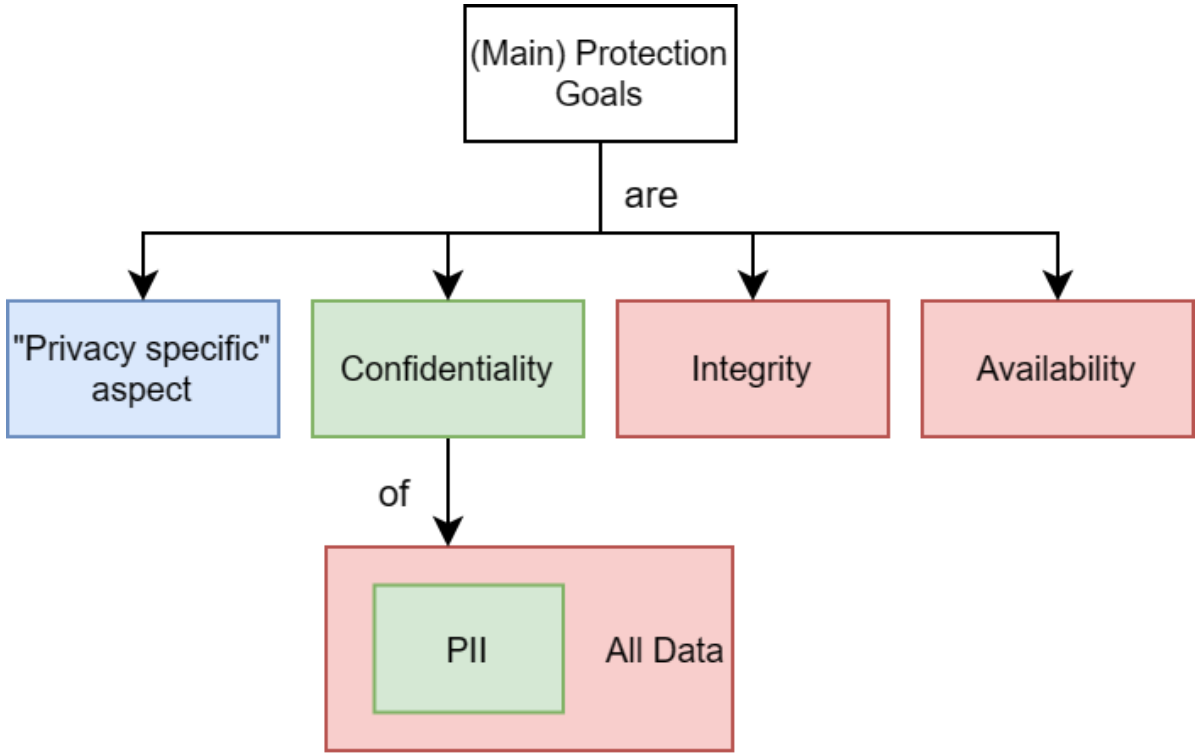
* Privacy definition according to classification from Daniel J. Solove, Conceptualizing Privacy, 90 Cal. L. Rev. 1087 (2002).

Concept Map – Protection Goals

Colour key:

Blue	Privacy
Red	Security
Green	Both

Key finding #2:
Overlap in the Confidentiality aspect with a difference in the scope:
Security protects all data; privacy focuses on PII
→Privacy is a subsection of security in this area
→But there are aspects to privacy that go beyond security

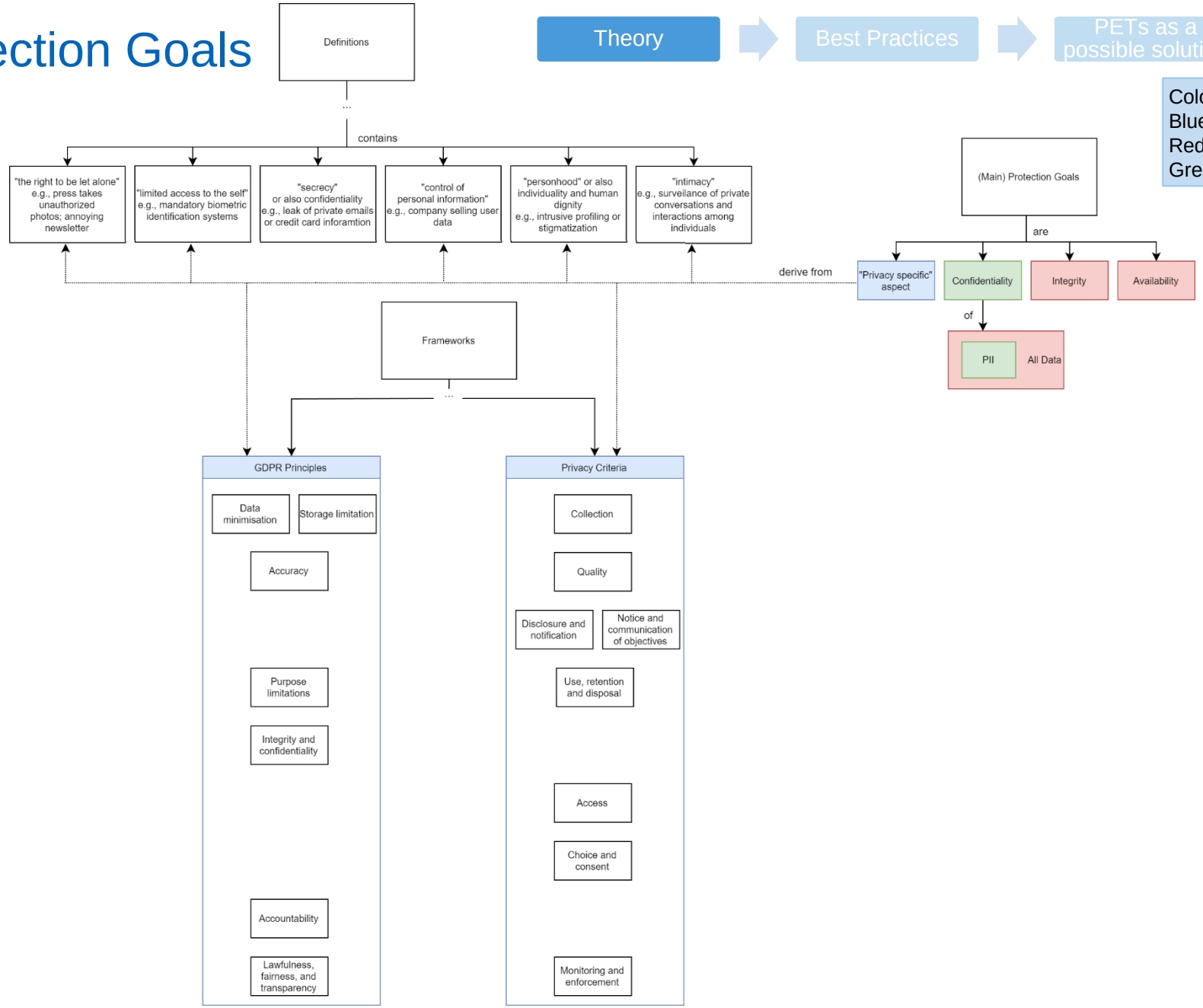


Concept Map – Protection Goals

Theory → Best Practices → PETs as a possible solution

Colour key:

Blue	Privacy
Red	Security
Green	Both



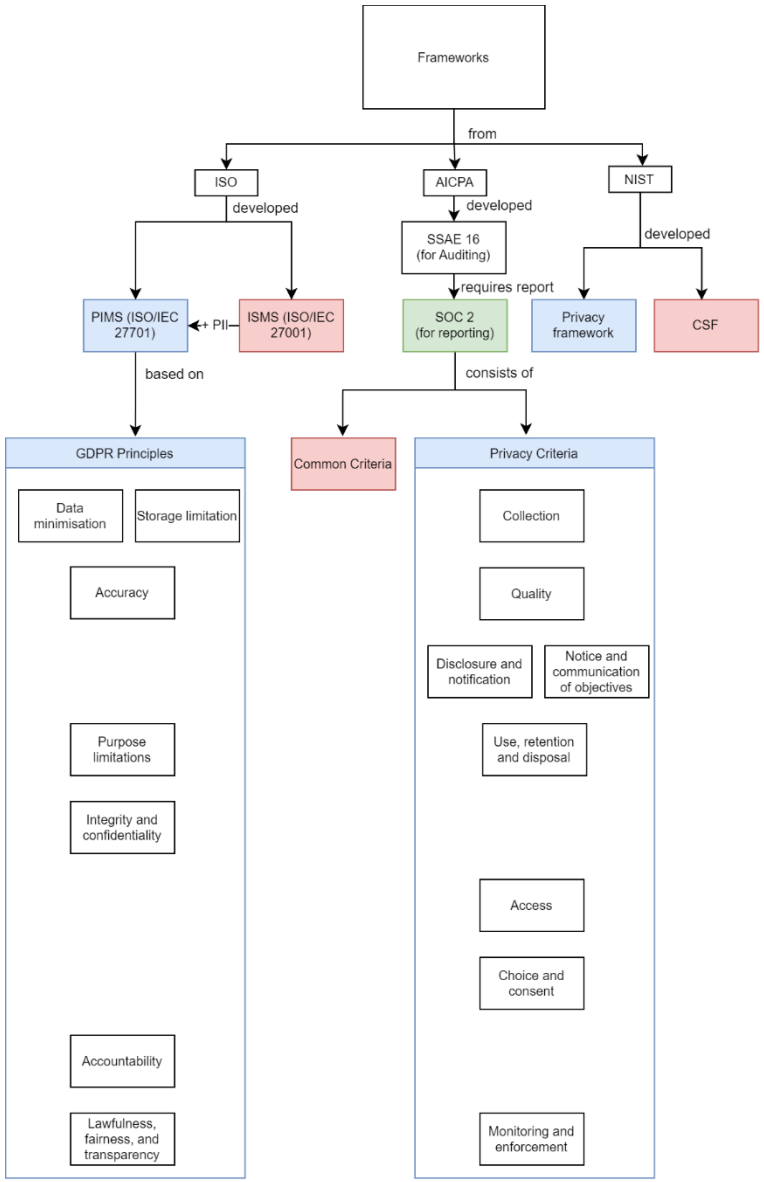
 * Similar privacy principles on the same level because of overlaps between frameworks. As this was an additional finding, it is only a draft; more research is needed.

Concept Map – Frameworks

Theory → Best Practices → PETs as a possible solution

Colour key:

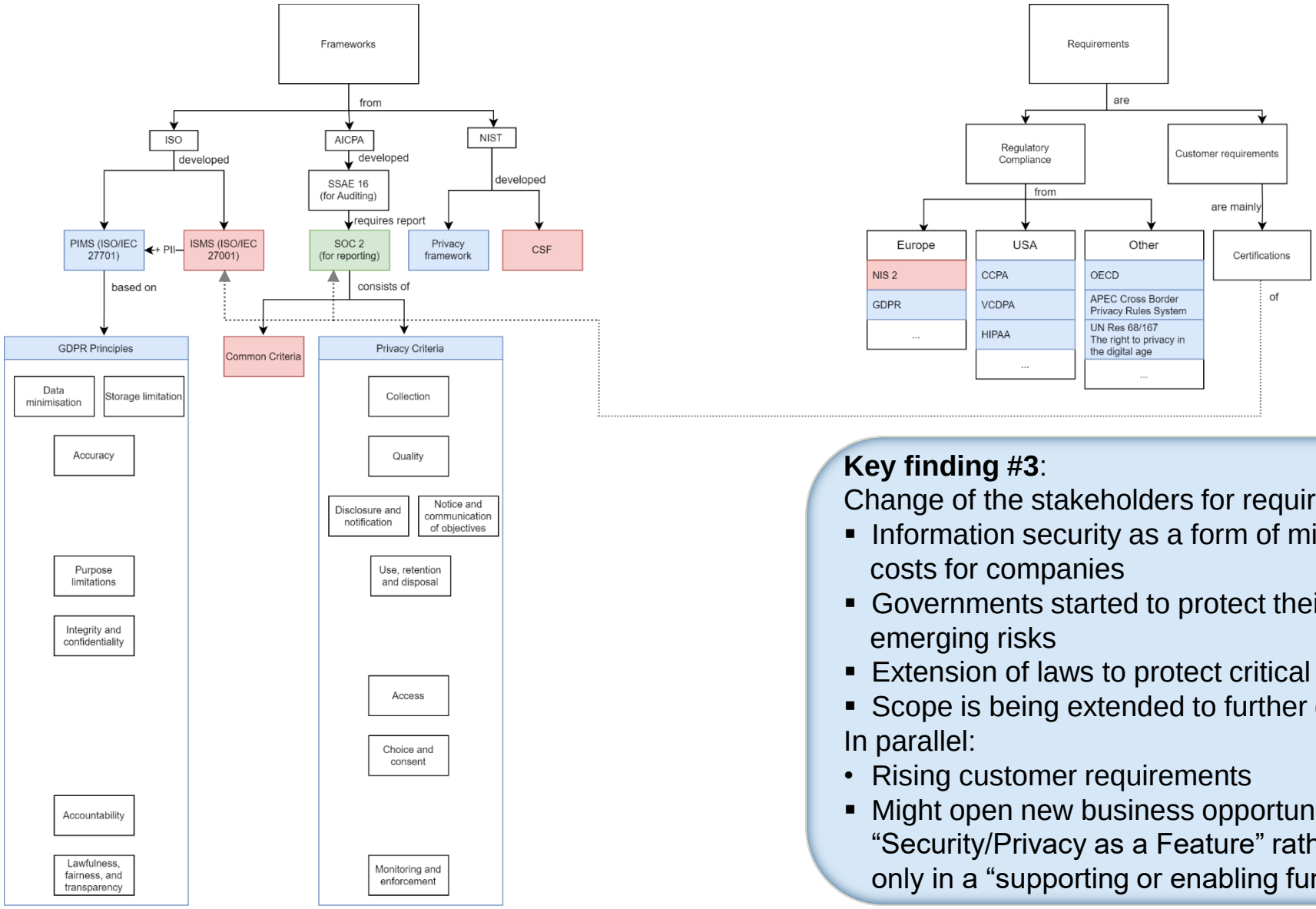
Blue	Privacy
Red	Security
Green	Both



Concept Map – Frameworks and Requirements

Colour key:

Blue	Privacy
Red	Security
Green	Both



Key finding #3:
Change of the stakeholders for requirements

- Information security as a form of minimizing opportunity costs for companies
- Governments started to protect their institutions due to emerging risks
- Extension of laws to protect critical infrastructure
- Scope is being extended to further companies

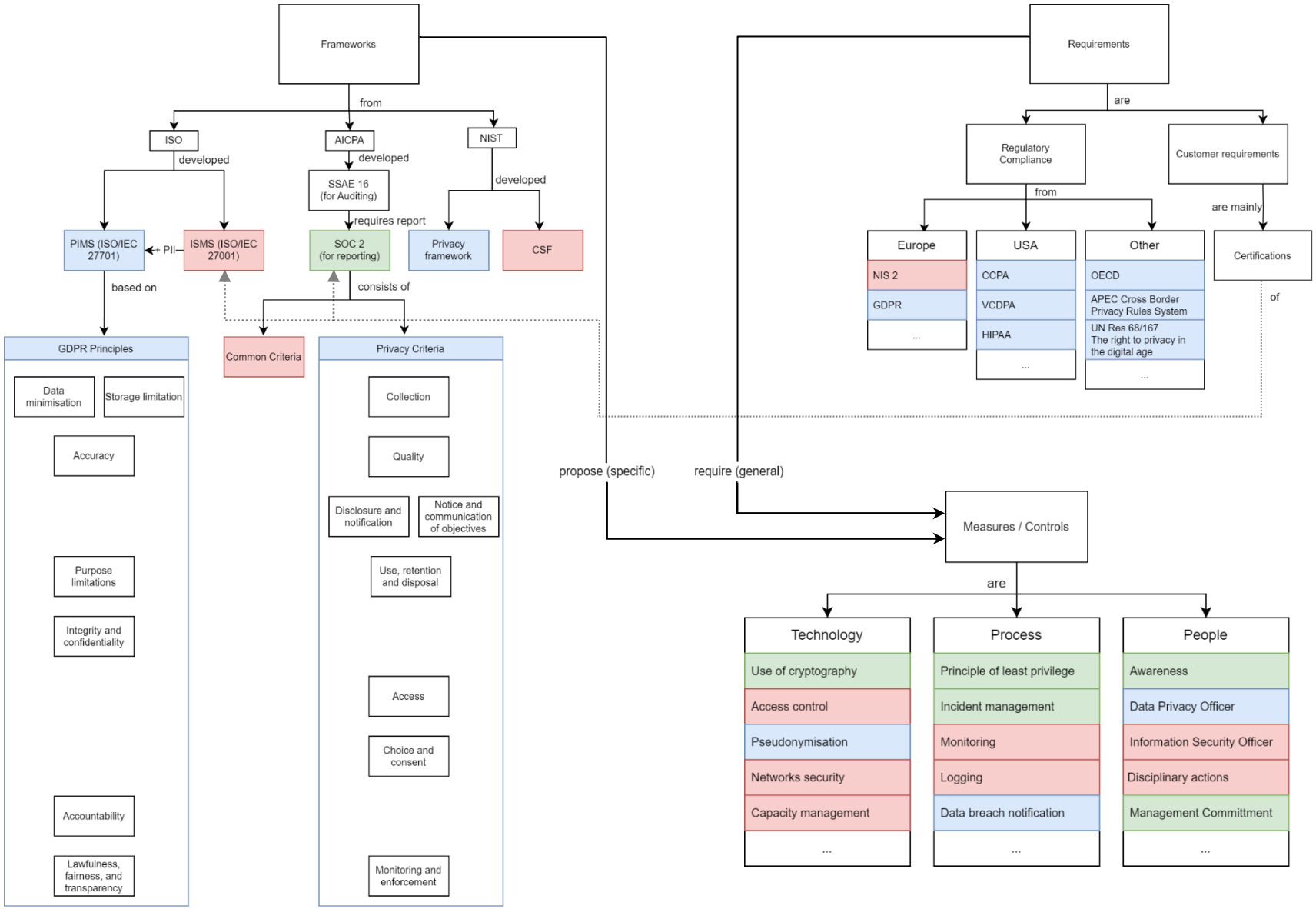
In parallel:

- Rising customer requirements
- Might open new business opportunities by, e.g., “Security/Privacy as a Feature” rather than them staying only in a “supporting or enabling function” [I-1]

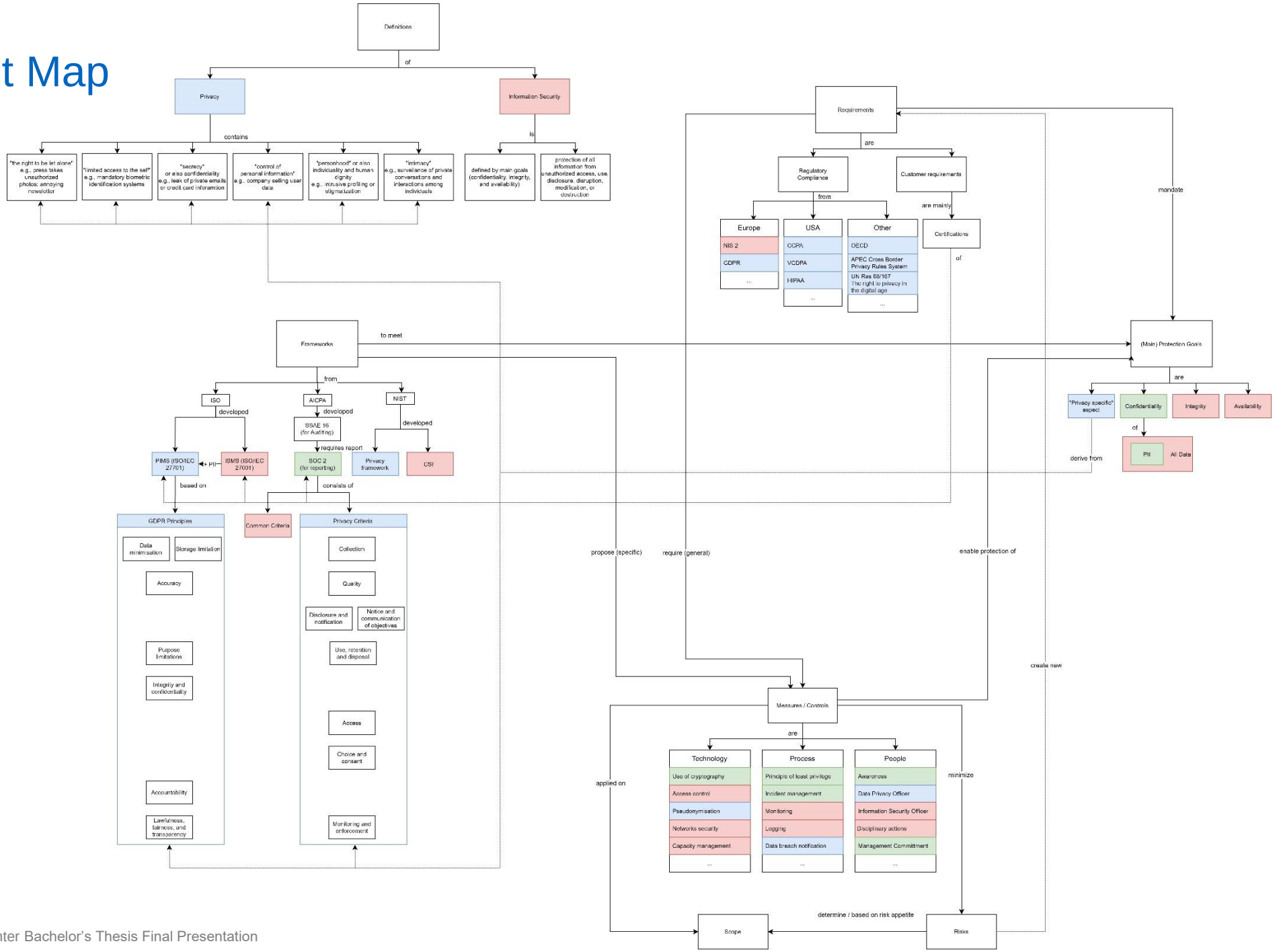
Concept Map – Frameworks and Requirements and Measures / Controls

Colour key:

Blue	Privacy
Red	Security
Green	Both



Concept Map



Colour key:

Blue	Privacy
Red	Security
Green	Both

Outline

Motivation

Approach

- Research Questions
- Methodology

Results

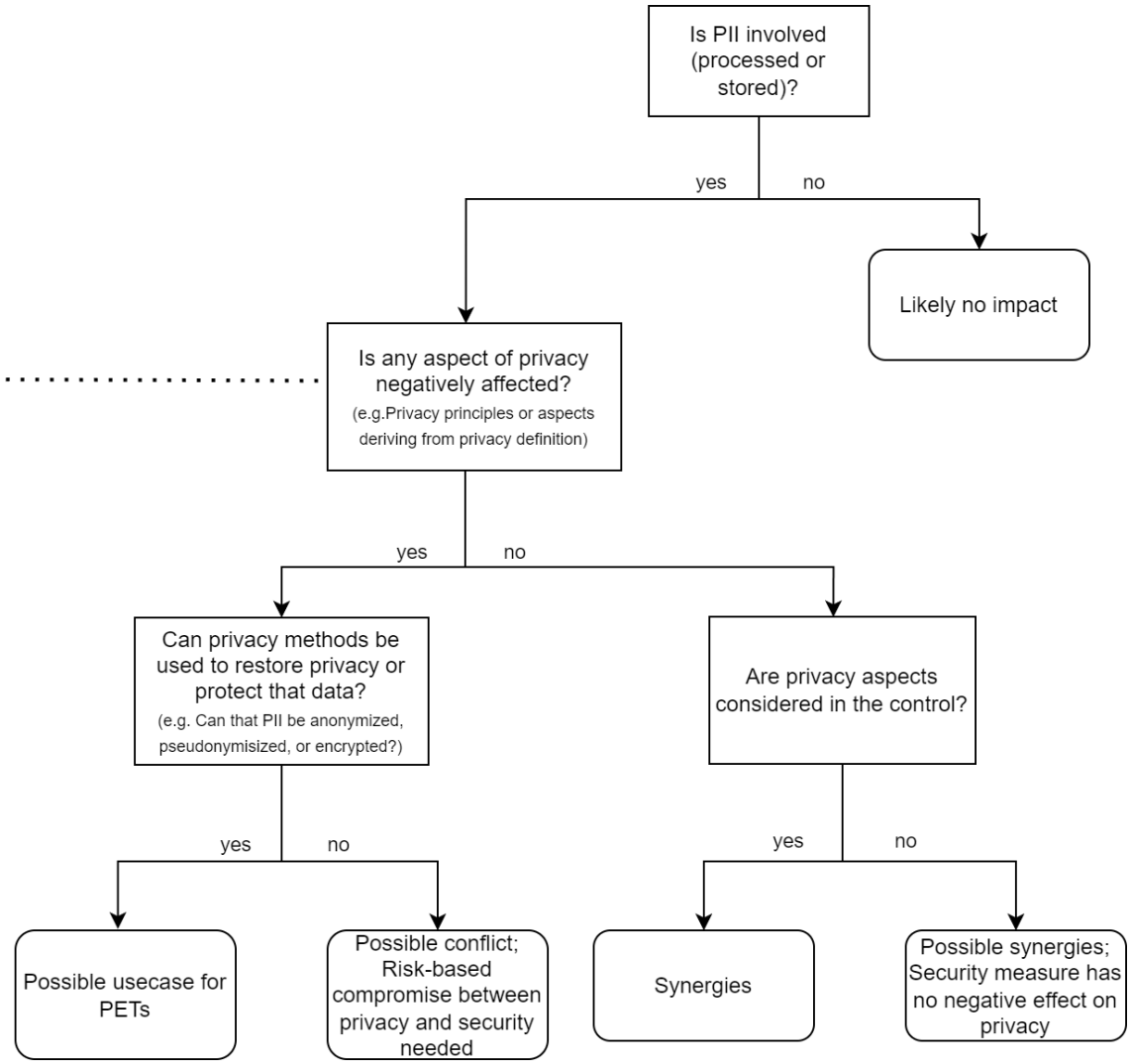
- Concept Map (RQ1 and RQ2)
- **Evaluation of privacy impact of security measures (RQ2)**
- Conflict Solving (RQ2 and RQ3)

Limitations and Future Work

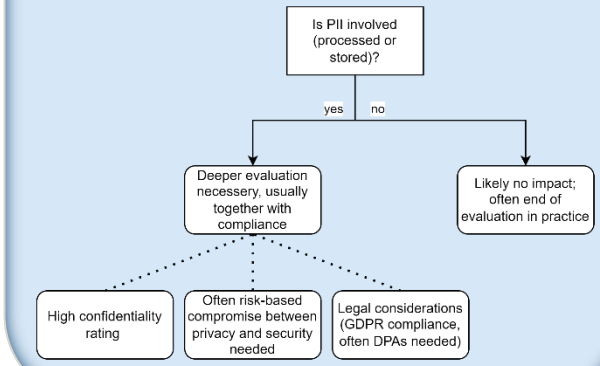
Summary

Decision Tree for Impact Evaluation

Privacy specific aspects
Privacy principles directly deriving from privacy definition (Right to be let alone, Limited Access to the Self, Secrecy, Control Over Personal Information, Personhood, and Intimacy)
Data minimilization: Is only PII collected or stored that is necessary for the purpouse? Is no further PII (in particular metadata) created?
Lawfullness: Is there a legal basis for processing PII?
Fairness and Transperency: Is the processing of PII limited to the purposes that have been disclosed?
Purpouse limitations: Is only PII collected or stored that is necessary for the purpouse?
Accuracy: Is the accuracy of PII ensured?
Storage limitation: Is PII only retained for the necessary duration ?
Accountability: Are measures and records in place to prove PII is handled in a responsible way?



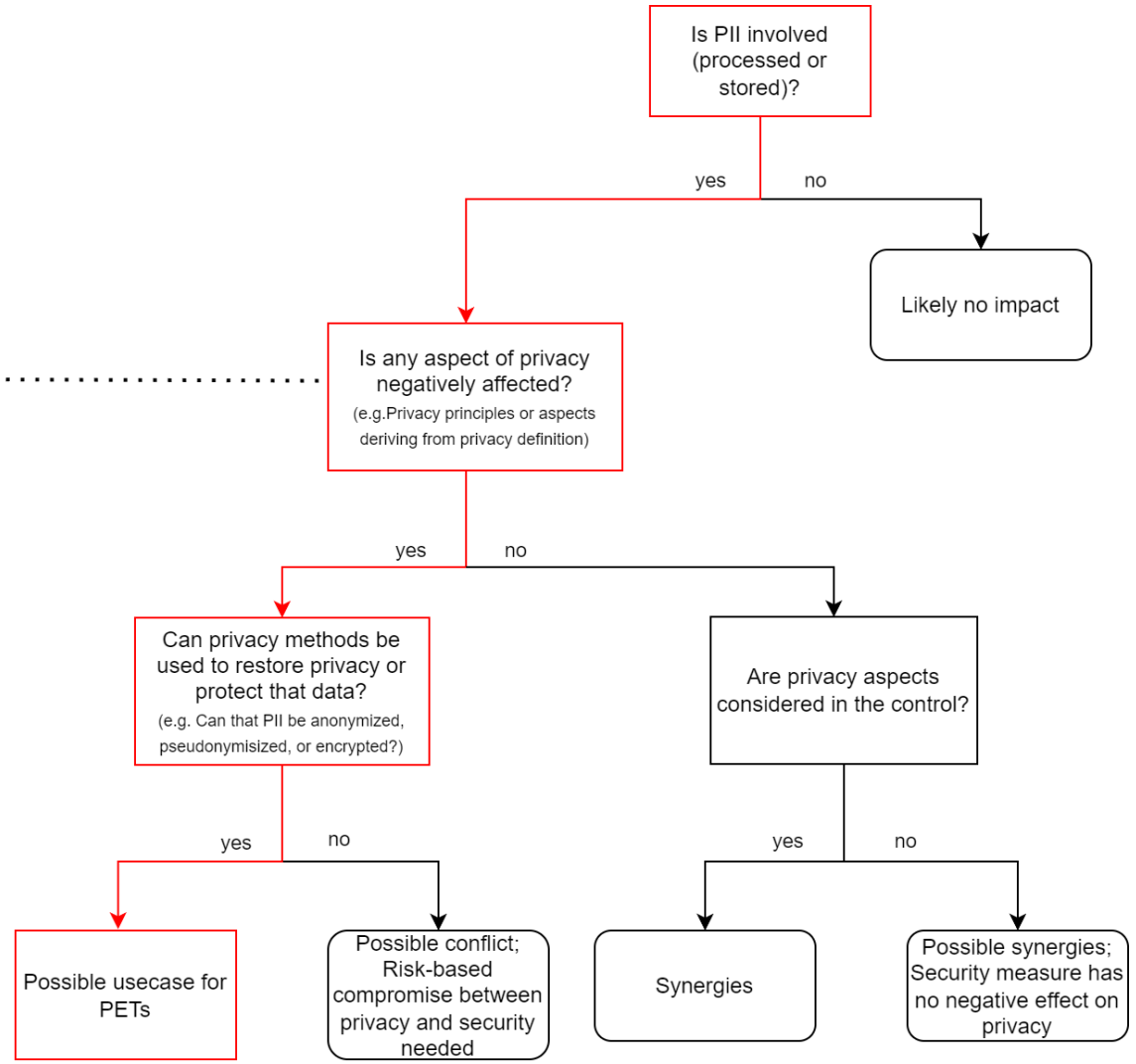
From Kick-Off: How does information security deal with PII in practice?



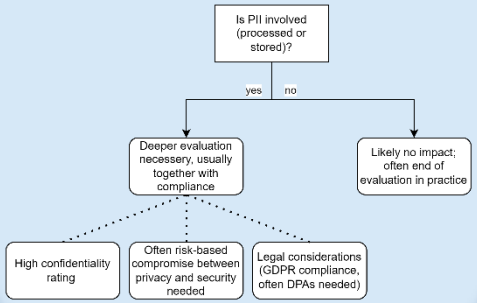
Examples:
Access control (5.15) → Possible use case for PETs
Logging (8.15) → Possible use case for PETs
Disciplinary actions (6.4) → Possible conflict
Use of cryptography (8.24) → Synergies

Decision Tree for Impact Evaluation

Privacy specific aspects
Privacy principles directly deriving from privacy definition (Right to be let alone, Limited Access to the Self, Secrecy, Control Over Personal Information, Personhood, and Intimacy)
Data minimilization: Is only PII collected or stored that is necessary for the purpouse? Is no further PII (in particular metadata) created?
Lawfullness: Is there a legal basis for processing PII?
Fairness and Transperency: Is the processing of PII limited to the purposes that have been disclosed?
Purpouse limitations: Is only PII collected or stored that is necessary for the purpouse?
Accuracy: Is the accuracy of PII ensured?
Storage limitation: Is PII only retained for the necessary duration ?
Accountability: Are measures and records in place to prove PII is handled in a responsible way?

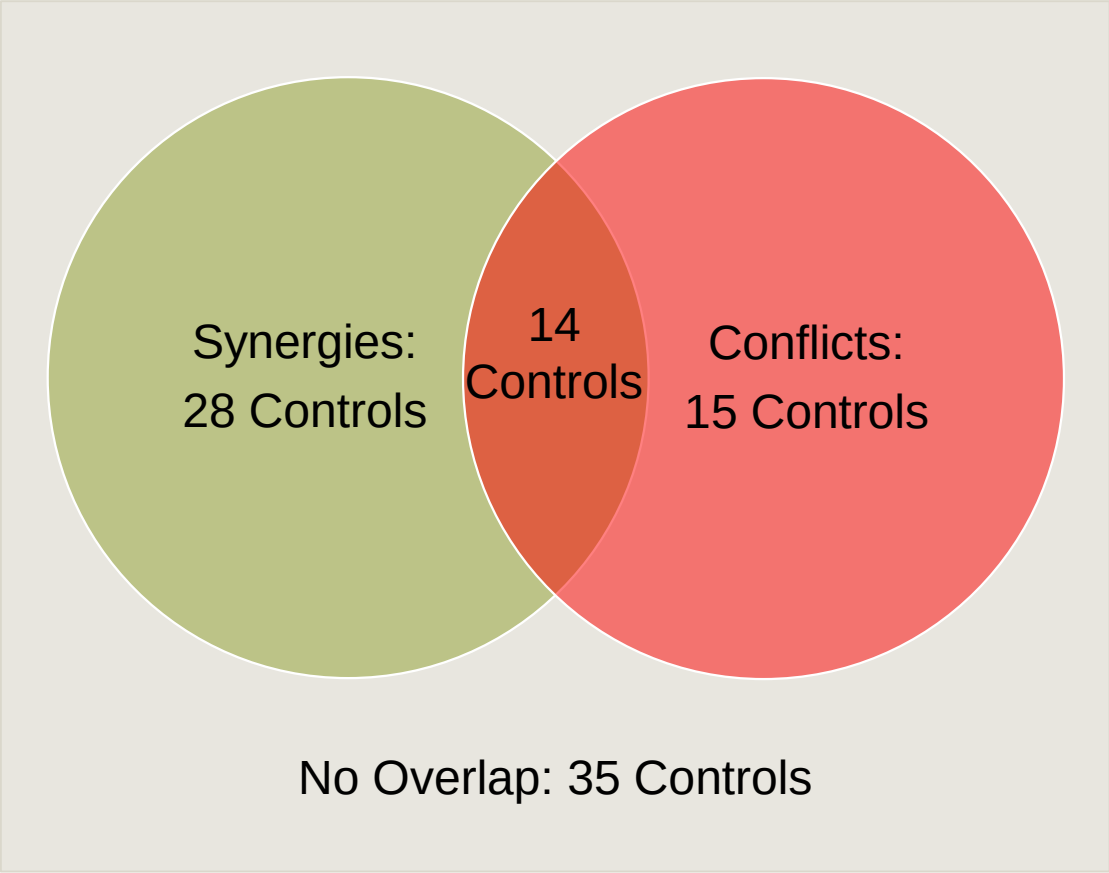


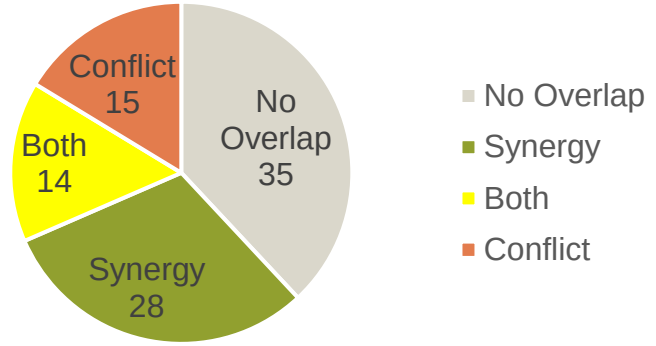
Kick-off: How does information security deal with PII in practice?



Examples:
Access control (5.15) → Possible use case for PETs
Logging (8.15) → Possible use case for PETs
Disciplinary actions (6.4) → Possible conflict
Use of cryptography (8.24) → Synergies

Results of the Impact Evaluation:





Key finding #4:
Some controls contain synergies as well as conflicts. E.g., to some extent, the *Accountability* and *Data Minimization* privacy principles conflict, which results in multiple controls having overlap with both

Results of the Impact Evaluation:

Theory → Best Practices → PETs as a possible solution

Synergies

Already:

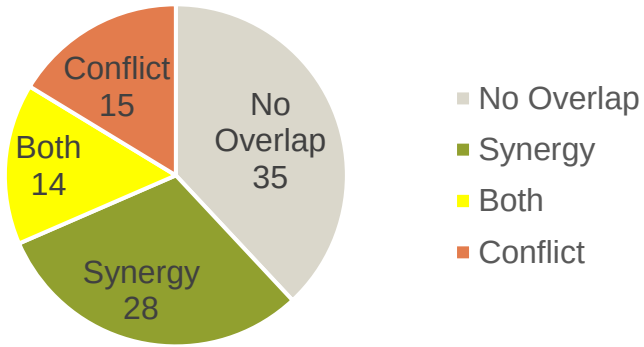
- Segregation of duties (5.3)
- Contact with authorities (5.5)
- Contact with special interest groups (5.6)
- Acceptable use of information and other associated assets (5.10)
- Labelling of information (5.13)
- Access rights (5.18)
- Addressing information security within supplier agreements (5.20)
- Information security for use of cloud services (5.23)
- Intellectual property rights (5.32)
- Privacy and protection of PII (5.34)
- Confidentiality or non-disclosure agreements (6.6)
- Remote working (6.7)
- Clear desk and clear screen (7.7)
- Storage media (7.10)
- Secure disposal or re-use of equipment (7.14)
- Information deletion (8.10)
- Data masking (8.11)
- Data leakage prevention (8.12)
- Use of cryptography (8.24)
- Application security requirements (8.26)
- Secure system architecture and engineering principles (8.27)
- Separation of development, test and production environments (8.31)
- Test information (8.33)

Possible:

- Information security in project management (5.8)
- Classification of information (5.12)
- Information security in supplier relationships (5.19)
- Managing information security in the ICT supply chain (5.21)
- Terms and conditions of employment (6.2)

Synergies and Conflicts

- Information transfer (5.14)
- Access control (5.15)
- Identity management (5.16)
- Authentication information (5.17)
- Information security incident management planning and preparation (5.24)
- Response to information security incidents (5.26)
- Legal, statutory, regulatory and contractual requirements (5.31)
- Protection of records (5.33)
- User endpoint devices (8.1)
- Privileged access rights (8.2)
- Information access restriction (8.3)
- Access to source code (8.4)
- Secure authentication (8.5)
- Logging (8.15)



Conflicts

- Inventory of information and other associated assets (5.9)
- Return of assets (5.11)
- Collection of evidence (5.28)
- Screening (6.1)
- Information security awareness, education and training (6.3)
- Disciplinary process (6.4)
- Physical entry (7.2)
- Physical security monitoring (7.4)
- Security of assets off-premises (7.9)
- Capacity management (8.6)
- Protection against malware (8.7)
- Information backup (8.13)
- Monitoring activities (8.16)
- Networks security (8.20)
- Security of network services (8.21)
- Web filtering (8.23)

Key finding #5:
There are already many overlaps and synergies between security and privacy.

- Synergies mainly in areas where confidentiality/secrecy is prioritized.
- Security frameworks started to include privacy controls like *Data masking* (8.11) or *Privacy and protection of PII* (5.34).

Outline

Motivation

Approach

- Research Questions
- Methodology

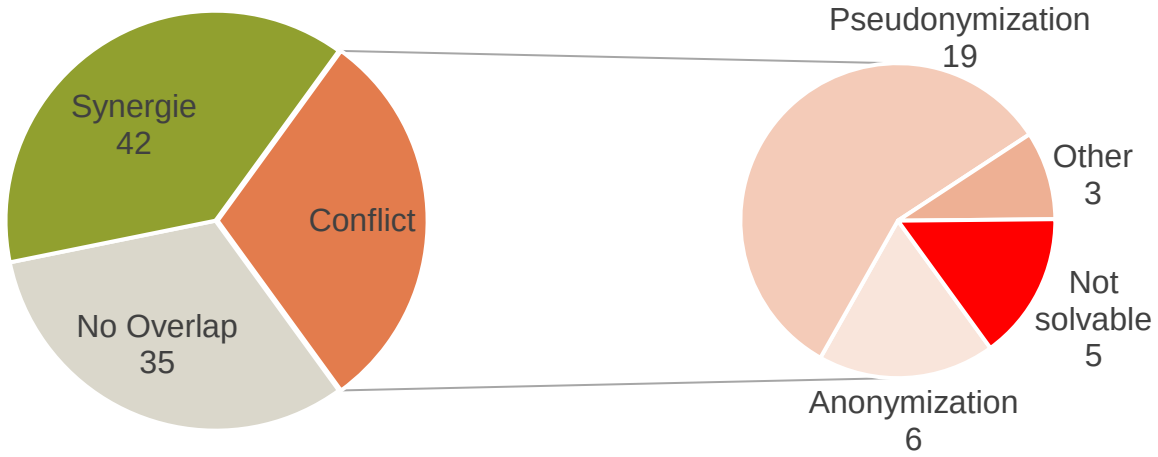
Results

- Concept Map (RQ1 and RQ2)
- Evaluation of privacy impact of security measures (RQ2)
- **Conflict Solving (RQ2 and RQ3)**

Limitations and Future Work

Summary

Conflict Solving



Key finding #5:
- Most conflicts are solvable, the majority by applying two methods from PETs.
- Those were already added to the ISO (security) framework. (*Data masking in* 8.11)

(Partly) solvable:
- **Anonymization**, if data is collected and analyzed mainly for improving availability, e.g., Capacity Management (8.6).
- **Pseudonymization**, if data needs to be traced back to individuals in cases of identified breaches
- **Other** cases where privacy could be (partly) restored:
  - Return of assets (5.11): Disable permanent GPS tracking of assets
  - Authentication information (5.17): Have biometric authentication as optional
  - Screening (6.1): Separate screening process into two steps: First step (data collection) to remove PII, which could validate *personhood*. That way, negative effects are prevented in second step (data evaluation)

Not solvable
- Information transfer (5.14): "*Identification of information owners, risk owners, security officers, and information custodians*".
- Legal, statutory, regulatory and contractual requirements (5.31): Cryptography often restricted, e.g., "*telecommunications service providers must be able to decode any telecommunications which are protected through technical measures*" on government orders.
- Protection of records (5.33) and Information backup (8.13): Right to access, to correction, and to erasure (data retention) are limited.
- Disciplinary process (6.4): Names of perpetrators needed, e.g., for legal actions or to assign awareness measures

Possible use cases for PETs

List of PETs: *

- Federated Learning
- Differential Privacy
- Homomorphic Encryption
- Secure Multi-Party Computation (SMPC)
- Zero-Knowledge Proofs
- Trusted execution environments
- Privacy-Preserving Data Mining
- Private Information Retrieval
- L-Diversity
- Pseudonymization
- Anonymization
- T-Closeness
- Synthetic data

PETs with possible use cases:

Zero-Knowledge Proofs
Verify documents during Screening (6.1) (e.g., degrees, review of criminal records, …) or in the context of supplier relationship (5.19) (e.g., certifications)

Trusted execution environments
Analog to principles in controls for production environment (8.31), segregation of networks (8.22), or separation of physical security parameters (7.1)

Pseudonymization
In 19 discussed cases

Anonymization
In 6 discussed cases

Synthetic data
Create test information (8.33)

* List according to Fantayes Bachelor's Thesis *("An Introduction and Overview of Privacy-Enhancing Technologies for Data Processing and Analysis")* and the Information Conmmissioner's Offices "*PETs guidance*"

Can PETs replace security measures?

Background:
Privacy, and therefore also PETs, mainly focus on the confidentiality of PII. In some cases, this protection also increases integrity.
Therefore, the included question is: *Can PETs replace security measures if they are not only applied to PII but also to further data?*

In general:

No, security is still necessary.
"*Because we have not only confidentiality but also integrity and availability. And we also have confidential data that is separate from personal data*." [I-1]
E.g., "We *could still break [a] system by running a DDoS attack. [...] That would not infringe privacy.*" [I-2]

In specific applications:

No, if the measure also has availability aspects. Then, a PET is unlikely to ensure that.

Yes, if the use case for which the PET is designed overlaps with the protection need of a security measure. Mainly in cases where confidentiality or integrity are prioritized.

Instead of replacing the security measure, certain PETs and privacy measures are more likely to be integrated as further protection on top. This is already the case, e.g., *Pseudonymization* integrated as part of the *Data masking* control (8.11).

Outline

Motivation

Approach

- Research Questions
- Methodology

Results

- Concept Map (RQ1 and RQ2)
- Evaluation of privacy impact of security measures (RQ2)
- Conflict Solving (RQ2 and RQ3)

Limitations and Future Work

Summary

Limitations and Future Work

- **Researcher bias** due to the high impact of manual paper selection, e.g., the literature review
- **Limited generalizability** due to sampling bias and size of Interviewee pool (was improved due to very experienced interview partners and additional feedback workshop)
- **Scope** of the thesis was to create a general overview, but often, details are important
- **Approach** “From the viewpoint of information security experts”
→ Mapping starting from the privacy side might reveal further important aspects
- **One security framework** (ISO 2700X) was analyzed
→ Deeper dive into other frameworks, e.g., Special Publication 800-53 from NIST could reveal different relationships
- **Different versions** between ISO/IEC 27001 (& 27002) and ISO/IEC 27701.
→ ISO/IEC 27001 could be integrated into the analysis once it’s released in 2024
- **Finding use cases** for PETs was one small part of the thesis and, therefore, only very briefly done
→ Further investigations necessary
- Interviewees criticized **current implementations of privacy** (e.g., usability of cookies, understandability of juristically texts, …)
→ Finding solutions to those problems is necessary

Outline

Motivation

Approach

- Research Questions
- Methodology

Results

- Concept Map (RQ1 and RQ2)
- Evaluation of privacy impact of security measures (RQ2)
- Conflict Solving (RQ2 and RQ3)

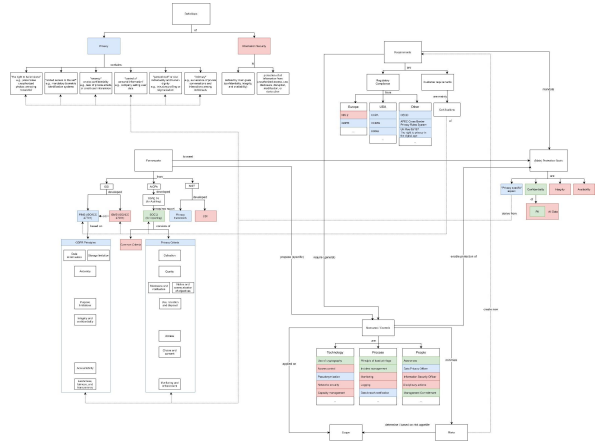
Limitations and Future Work

Summary

Summary

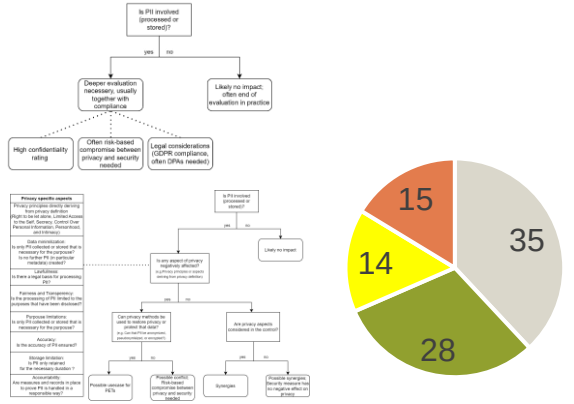
RQ1: What are the definitions of security and privacy, and how are these concepts related in theory?

- **Security** can be defined by three (main) protection goals: *Confidentiality, Integrity, and Availability.*
- **Privacy** can be described by overlapping *similarities*: *The Right to Be Let Alone, Limited Access to the Self, Secrecy, Control Over Personal Information, Personhood, and Intimacy.*
- Privacy is a subcategory of Security in the *Confidentiality* Overlap, as it covers only PII.
- But: Privacy is also exceeding Security with "*Privacy-Specific*" aspects, which derive from *privacy principles* and the *similarities.*
- Other relationships in the *Concept Map.*



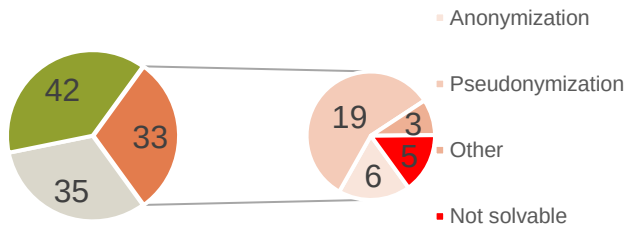
RQ2: From the viewpoint of information security experts, how do the concepts of security and privacy overlap in practice, and what are possible conflicting requirements or synergies?

- Findings are also represented in *Concept Map.*
- Security has a "*supporting or enabling function for privacy.*" [I-1] in the context of confidentiality.
- There are *conflicting requirements*, which makes *"[b]alancing the need for security measures with preserving privacy [...] a delicate task*". [I-2]
- Process to investigate *conflicting requirements* was developed (decision tree) based on current privacy impact evaluation process.
- ISO/IEC 27002 controls were analyzed.



RQ3: To what extent can PETs fulfill information security requirements to replace information security measures in certain areas?

- PETs are designed for very specific use cases. If that use case matches with security requirements, they could replace them.
- It is more likely that the security measure adopts the PETs rather than be replaced by them.
- Most identified *conflicts* could be resolved by applying *pseudonymization* and *anonymization* techniques
- Other use cases of PETs were identified for: *Zero-Knowledge Proofs, Trusted execution environments, Pseudonymization, and Synthetic data.*



Felix Thorwächter
Bachelor's Student Information Systems

Technical University of Munich (TUM)
TUM School of CIT
Department of Computer Science (CS)
Chair of Software Engineering for Business Information Systems (sebis)

Boltzmannstraße 3
85748 Garching bei München

+49.89.289.17132
matthes@in.tum.de
wwwmatthes.in.tum.de

Backup

Thank you for your attention and the feedback!

Detailed Outline

Introduction
- Motivation

Approach
- Research Questions
- Methodology

Results
- Concept Map (RQ1 and RQ2)
  - General Concept Map
  - Dimensions in detail
  - Evolution of the Concept Map } live-demo
- Evaluation of privacy impact of security measures (RQ2)
  - Decision Tree for Impact Evaluation
  - Results of the Impact Evaluation: Overlaps, Conflicts
- Conflict Solving
  - Conflict Solving
  - Possible use cases for PETs (RQ3)

Limitations and Future Work

Summary

Motivation

Case: Introduction of security measure led to privacy discussion

Problem: Conflicting requirements Data Minimization vs Monitoring
Zero Trust as security gain vs. the fear of privacy loss due to collection of employee PII (Personally Identifiable Information)

Solution: Application of privacy principles to turn security measure into kind of PET (Privacy Enhancing Technology)
Anonymize the collected PII, deeper investigation only when necessary (e.g., security incidents)

Picture from https://www.zscaler.de/

Methodology

Theory → Best Practices → PETs as a possible solution

RQ 1: Literature review
→ Create concept map
→ Understand definitions of security and privacy and their relationship in theory

RQ 2: Analyze ISO/IEC 27001 measures for their privacy implications
→ Create decision tree for analysis and evaluaion
→ Identify areas with overlaps, and whether their requirements are conflicting or have synergies

RQs 1 & 2: Semi-Structured Interviews and Workshop
→ Validate results
→ Get insights into the views of information security experts on the topic of privacy

RQ 3: Apply the results to the topic of PETs
→ Find possible use cases for PETs
→ Define (security) requirements for PETs

Interview Questionnaire

Chair of Software Engineering for Business Information Systems
Department of Computer Science
School of Computation, Information and Technology
Technical University of Munich

Disclaimer

Before we start the interview, I would like to mention that this interview will be recorded for subsequent transcription. The transcription itself and any findings within will be utilized for research purposes and for the eventual publication in a thesis and/or research paper. Any personally identifiable information will be anonymized, and the final results will be shared in the end. Could you please confirm your consent to these terms?

Questionnaire

Background

1. What is your **position and role**?
2. How many **years of experience** in this field and in the company do you have?

Definitions

3. How would you **define security?**
4. How would you **define privacy**?

General Relationship between Privacy and Security

5. How do you view the **general relationship** between security and privacy?
    - What are the **main differences and overlaps** between security and privacy?
    - Are they **conflicting or complementary**?
    - Can you think of examples where they have **conflicts**?
    - Can you think of examples where they have **synergies**?
6. Does this **overview of the concept map** represent the relationship as you view it?
7. Does this **concept map** show the most important aspects of the relationship?

Privacy/Security in Practice

8. What role does privacy/security play in your **work**?
    - Do you think privacy/security will become a **bigger concern**?
9. How do you **collaborate** with other departments regarding privacy/security topics?
    - Do you think the **responsibilities** of privacy/security topics will shift to other departments? (If yes, where?)
10. What are the **biggest challenges** or threats to privacy/security that you are confronted with in your work?

ISO Measures

11. What do you think of the **approach**?
12. What would you change/evaluate **differently**?
13. How did you deal with those **conflicts**?
    - Which **situations** did you experience where prioritizing security measures might compromise privacy, or vice versa?
    - What are the considerations to find the right **balance** between privacy and security measures?

PETs (Privacy Enhancing Technologies)

14. Are you familiar with PETs?
15. Do you use PETs? (If yes, which?)
16. Do you think PETs could replace the need for some security measures in some areas? (e.g., privacy by design)

Looking Forward

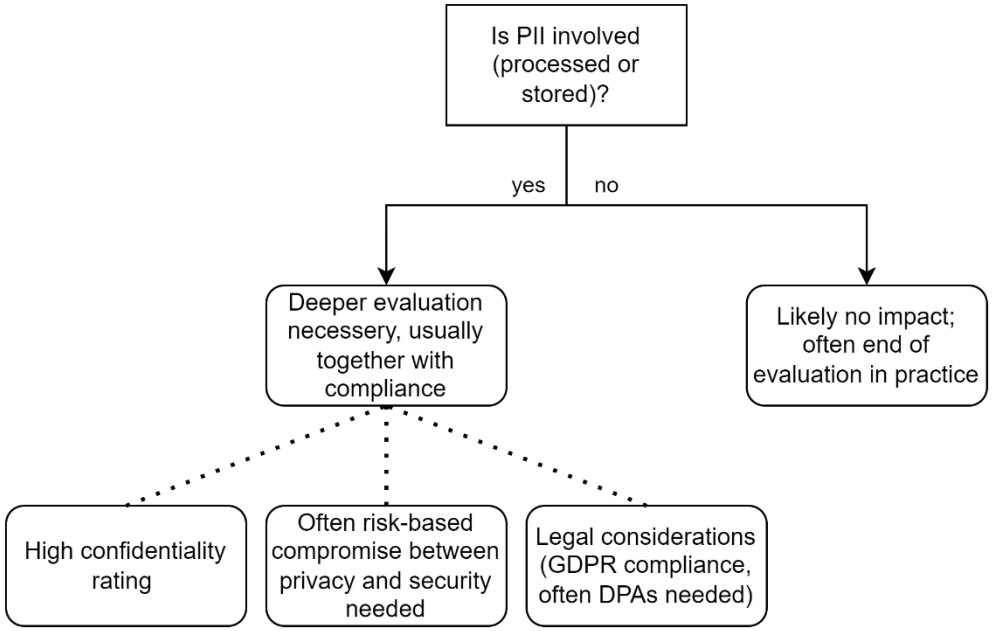
17. Is there anything else you would like to **add** regarding privacy and security?
    - Do you have any **additional insights** you would like to share?
    - Is there any aspect of this topic we may have **missed**?
18. Can you **refer** anyone who would also be able to contribute to this discussion?

Draft of Decision Tree for Impact Evaluation

Problem: How does information security deal with PII in practice?

Method: Discussion with security expert (#3)

Solution:



Insight 6: PII leads to high confidentiality rating

Insight 7: Privacy is currently mainly a compliance topic

ISO/IEC 27002 Analysis

Control ID	Control Name	Is PII involved? (If yes, which)	Is any privacy principle breached? (If yes, which, if no: are there synergies?)	Category	Is the conflict solvable? (If yes, how)
5.1	Policies for information security	No			
5.2	Information security roles and responsibilities	No			
5.3	Segregation of duties	No	No: Indirect synergies as foundations to role-based access and least privilege principles (5.15)	Indirect synergies	
5.4	Management responsibilities	No			
5.5	Contact with authorities	No	No: Indirect synergies as privacy breaches also need to be reported and process could be synchronized	Indirect synergies	
5.6	Contact with special interest groups	No	No: Indirect synergies analog to 5.5	Indirect synergies	
5.7	Threat intelligence	No			
5.8	Information security in project management	Yes, all kind of data within projects	No: Synergies possible by combining security assessment and privacy assessment in project management, including information determination and classification (5.12)	Synergies possible	
5.9	Inventory of information and other associated assets	Yes, names	Yes: Data Minimization (names of information- and asset owners)	Possible conflict	Yes, pseudonymize metadata
5.10	Acceptable use of information and other associated assets	Yes, all kind of data	No: Synergies with Purpose Limitation and Accountability	Synergies	
5.11	Return of assets	Yes, names and metadata	Yes: Data Minimization (names who possess assets and location tracking of assets)	Possible conflict	Yes, pseudonymize metadata,
5.11					Partly: Change tracking from permanently to necessary
5.12	Classification of information	Yes, all kind of data	No: Synergies possible by including privacy category in information classification	Synergies possible	
5.13	Labelling of information	Yes, all kind of data	No: Synergies dependent if intellectual property falls under definition of personal data	Synergies	
5.14	Information transfer	Yes, all kind of data	No: Synergies with Secrecy and DPAs	Synergies	
5.14			Yes: Data Minimization (contacts related to transfer including information owners, risk owners, security officers and information custodians)	Possible conflict	No
5.15	Access control	Yes, all kind of data	Yes: Data minimization (Logging)	Possible conflict	Yes, pseudonymize metadata
5.15			No: Synergies by enforcing need-to-know / need-to-use principle and least-privilege principles, as assurance for purpose limitation and data minimization, and Secrecy	Synergies	
5.16	Identity management	Yes, names	Yes: Data Minimization (names)	Possible conflict	Yes, pseudonymize names
5.16			No: Synergies with Accountability, Transparency, and Secrecy	Synergies	

ISO/IEC 27002 Analysis

Control ID	Control Name	Is PII involved? (If yes, which)	Is any privacy principle breached? (If yes, which, if no: are there synergies?)	Category	Is the conflict solvable? (If yes, how)
5.17	Authentication information	Yes, biometric data	Yes, Limited Access to the Self (only if biometric authentication is mandatory)	Possible conflict	Yes, leave alternatives to biometric authentication
5.17			No: Synergies with Secrecy	Synergies	
5.18	Access rights		No: Synergies with Transparency and Secrecy	Synergies	
5.19	Information security in supplier relationships	Yes, all kind of data	No: Synergies possible by also considering privacy of suppliers	Synergies possible	
5.20	Addressing information security within supplier agreements	Yes, all kind of data	No: Synergies by also considering privacy in supplier agreements (e.g., DPAs)	Synergies	
5.21	Managing information security in the ICT supply chain	Yes, all kind of data	No: Synergies possible by also considering privacy of supply chain	Synergies possible	
5.22	Monitoring, review and change management of supplier services	Yes, all kind of data	No specific overlap.		
5.23	Information security for use of cloud services	Yes, all kind of data	No: Synergies, as PII protection should be considered	Synergies	
5.24	Information security incident management planning and preparation	Yes, all kind of data	Yes: Data Minimization (Monitoring, Detection, Analyzing, Evidence collection, Root cause analysis)	Possible conflict	Yes, pseudonymize metadata
5.24			No: Synergies with Transparency (logging of incident management activities)	Synergies	
5.25	Assessment and decision on information security events	No			
5.26	Response to information security incidents	Yes, all kind of data	Yes: Data Minimization (Evidence collection, Forensic analysis, Root cause analysis)	Possible conflict	Partly, pseudonymize metadata, but no, if necessary in legal case
5.26			No: Synergies with Transparency (Logging of incident response activities)	Synergies	
5.27	Learning from information security incidents	No			
5.28	Collection of evidence	Yes, all kind of data	Yes: Data Minimization (Evidence collection, Forensic analysis, Root cause analysis), Data Retention (data stored for legal cases)	Possible conflict	Partly, pseudonymize metadata, but no, if necessary in legal case

ISO/IEC 27002 Analysis

Control ID	Control Name	Is PII involved? (If yes, which)	Is any privacy principle breached? (If yes, which, if no: are there synergies?)	Category	Is the conflict solvable? (If yes, how)
5.29	Information security during disruption	No			
5.30	ICT readiness for business continuity	No			
5.31	Legal, statutory, regulatory and contractual requirements	Yes, all kind of data	Yes: Cryptography (Legal requirements restrict usage)	Possible conflict	No
5.31			No: Synergies possible by including privacy laws	Synergies possible	
5.32	Intellectual property rights	Yes, intellectual property	No: Synergies dependent if intellectual property falls under definition of personal data	Synergies	
5.33	Protection of records	Yes, all kind of data	Yes: not control itself, by but keeping records (that include PII)	Possible conflict	No
5.33			No: Synergies, as records should be kept secret and encryption is recommended (8.24)	Synergies	
5.34	Privacy and protection of PII	Yes, PII	No: Synergies due to PII protection for compliance with regulations, recommendation of privacy officer, Accountability	Synergies	
5.35	Independent review of information security	No			
5.36	Compliance with policies, rules and standards for information security	No			
5.37	Documented operating procedures	No			
6.1	Screening	Yes, PII	Yes: Data Minimization (Collection of employee data, but with consideration of privacy regulation), Personhood (too extensive screening, prejustices)	Possible conflict	Partly, involves usecases for Zero-Knowledge-Proofs
6.2	Terms and conditions of employment		No: Synergies possible by including privacy principles	Synergies possible	
6.3	Information security awareness, education and training	Yes, names and metadata	Yes: Data Minimization (names)	Possible conflict	Partly, pseudonymize metadata
6.4	Disciplinary process	Yes, names	Partly: Control demands protection of name of perpetrators,	Possible conflict	No
6.5	Responsibilities after termination or change of employment	No			

ISO/IEC 27002 Analysis

Control ID	Control Name	Is PII involved? (If yes, which)	Is any privacy principle breached? (If yes, which, if no: are there synergies?)	Category	Is the conflict solvable? (If yes, how)
6.6	Confidentiality or non-disclosure agreements	Yes	No: Synergies (Secrecy)	Synergies	
6.7	Remote working	Yes	No: Synergies (Secrecy)	Synergies	
6.8	Information security event reporting	No			
7.1	Physical security perimeters	No			
7.2	Physical entry	Yes, names and biometric data	Yes: Data Minimization (physical logbook of all access), Limited Access to the Self (biometric authentication, inspection and examination of personal belongings)	Possible conflict	Manual: No, Digital: Yes, pseudonymize metadata, leave alternatives to biometric authentication
7.3	Securing offices, rooms and facilities	No			
7.4	Physical security monitoring	Yes, recordings	Yes: Data Minimization (surveillance in accordance to data protection laws)	Possible conflict	Partly, anonymize metadata / automatically blur faces
7.5	Protecting against physical and environmental threats	No			
7.6	Working in secure areas	No			
7.7	Clear desk and clear screen	Yes, all kind of data	No: Synergies (Secrecy)	Synergies	
7.8	Equipment siting and protection	No			
7.9	Security of assets off-premises	Yes, names and metadata	Yes: Data Minimization (names by logging of custody, location tracking of devices)	Possible conflict	Yes, pseudonymize metadata
7.10	Storage media	Yes, all kind of data	No: Synergies (Secrecy, by promoting cryptographic techniques)	Synergies	
7.11	Supporting utilities	No			
7.12	Cabling security	No			
7.13	Equipment maintenance	No			
7.14	Secure disposal or re-use of equipment	Yes, all kind of data	No: Synergies (Secrecy, Cryptography)	Synergies	

ISO/IEC 27002 Analysis

Control ID	Control Name	Is PII involved? (If yes, which)	Is any privacy principle breached? (If yes, which, if no: are there synergies?)	Category	Is the conflict solvable? (If yes, how)
8.1	User endpoint devices	Yes, metadata	Yes: Data Minimization (end user behaviour analytics 8.16)	Possible conflict	Yes, anonymize metadata
8.1			No: usage of privacy screen filters, consider PII protection laws in the BYOD context	Synergies	
8.2	Privileged access rights	Yes, names and metadata	No: Accountability	Synergies	
8.2			Yes: Data Minimization (record of all privileges allocated,	Possible conflict	Yes, pseudonymize metadata
8.3	Information access restriction	Yes, metadata	No: Synergies with accountability (no anonymous access)	Synergies	
8.3			Yes: Data Minimization (monitor the use of the information, no anonymous access	Possible conflict	Yes, anonymize metadata
8.4	Access to source code	Yes, metadata	No: Accountability (log accesses and of all changes to source code)	Synergies	
8.4			Yes: Data Minimization (log accesses and of all changes to source code)	Possible conflict	Yes, pseudonymize metadata
8.5	Secure authentication	Yes, metadata and biometric data	No: Accountability	Synergies	
8.5			Yes: Data Minimization (logging unsuccessful and successful attempts), Limited Access to the Self (biometric authentication)	Possible conflict	Yes, pseudonymize metadata, leave alternatives to biometric authentication
8.6	Capacity management	Yes, metadata	Yes: Data Minimization (Monitoring)	Possible conflict	Yes, anonymize metadata
8.7	Protection against malware	Yes, metadata	Yes: Data Minimization (Scanning of all incoming traffic, as well as webpages)	Possible conflict	Yes, pseudonymize metadata
8.8	Management of technical vulnerabilities	No			
8.9	Configuration management	No			
8.10	Information deletion	Yes, all kind of data	No: Synergies with data retention and secrecy	Synergies	

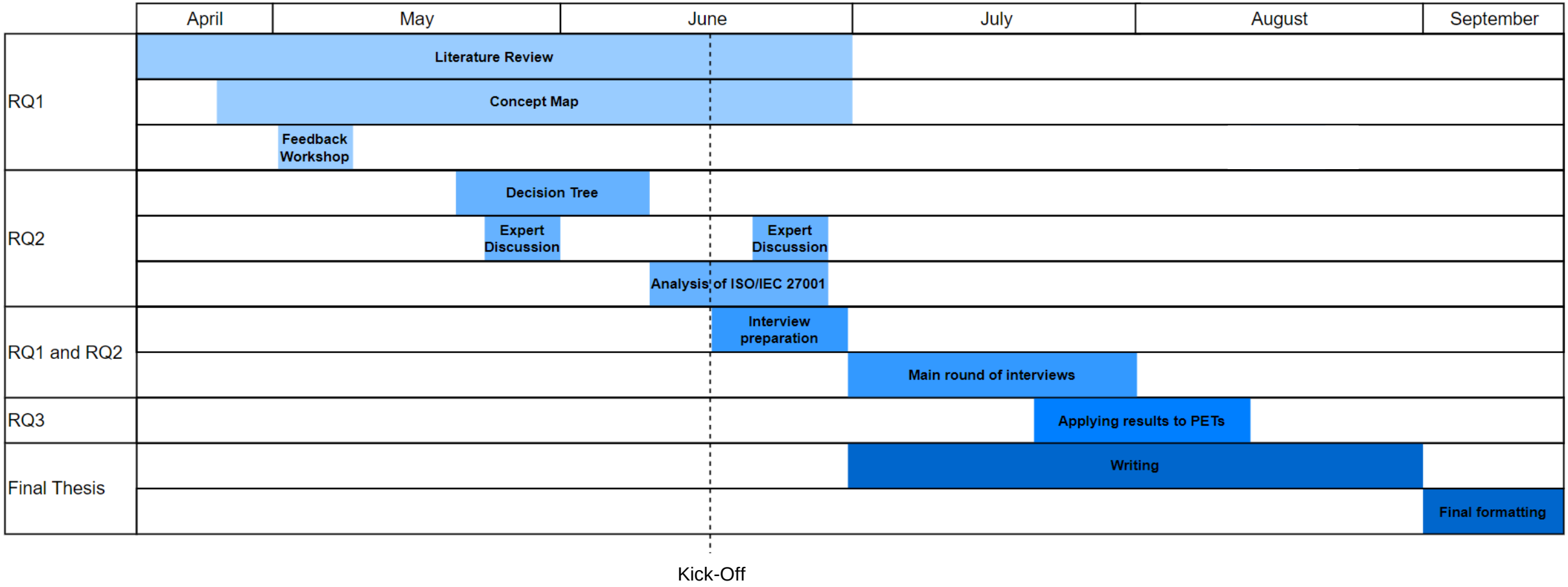
ISO/IEC 27002 Analysis

Control ID	Control Name	Is PII involved? (If yes, which)	Is any privacy principle breached? (If yes, which, if no: are there synergies?)	Category	Is the conflict solvable? (If yes, how)
8.11	Data masking	Yes, all kind of data	No: Synergies (Secrecy by PII masking)	Synergies	
8.12	Data leakage prevention	Yes, all kind of data	No: Synergies (Secrecy by PII protection)	Synergies	
8.13	Information backup	Yes, all kind of data	Yes: Data retention (right to erasure)	Possible conflict	No
8.14	Redundancy of information processing facilities	No			
8.15	Logging	Yes, metadata	Yes: Data Minimization (Logging)	Possible conflict	Yes, dependent on use anonymize or pseudonymize metadata
8.15			No: Synergies (Accountability)	Synergies	
8.16	Monitoring activities	Yes, metadata	Yes: Data Minimization (Analysis and documentation)	Possible conflict	Yes, pseudonymize metadata
8.17	Clock synchronization	No			
8.18	Use of privileged utility programs	No	(Out of scope, as only affects users of utility programs)		
8.19	Installation of software on operational systems	No			
8.20	Networks security	Yes, all kind of data	Yes, Data Minimization (Logging and monitoring)	Possible conflict	Yes, pseudonymize metadata
8.21	Security of network services	Yes, meta data	Yes, Data Minimization (Monitoring)	Possible conflict	Yes, pseudonymize metadata
8.22	Segregation of networks	No			
8.23	Web filtering	Yes, all kind of data	Yes, Data Minimization (Monitoring)	Possible conflict	Yes, dependent on use anonymize or pseudonymize metadata
8.24	Use of cryptography	Yes, all kind of data	No, Synergies with secrecy (PII protection)	Synergies	
8.25	Secure development life cycle	No			

ISO/IEC 27002 Analysis

Control ID	Control Name	Is PII involved? (If yes, which)	Is any privacy principle breached? (If yes, which, if no: are there synergies?)	Category	Is the conflict solvable? (If yes, how)
8.26	Application security requirements	No	No, Synergies due to consideration of need for privacy	Synergies	
8.27	Secure system architecture and engineering principles	Yes, all kind of data within projects	No, Synergies (encryption) already in place, could be extended (“privacy by design”, …)	Synergies	
8.28	Secure coding	No			
8.29	Security testing in development and acceptance	No			
8.30	Outsourced development	No			
8.31	Separation of development, test and production environments	Yes, all kind of data within projects	No, Synergies with privacy: Secrecy (PII protection),	Synergies	
8.32	Change management	No			
8.33	Test information	Yes, all kind of data within projects	No, Synergies with privacy (analog to 8.31)	Synergies	
8.34	Protection of information systems during audit testing	No			

Timeline


April
May
June
July
August
September
RQ1
Literature Review
Concept Map
Feedback Workshop
RQ2
Decision Tree
Expert Discussion
Expert Discussion
Analysis of ISO/IEC 27001
RQ1 and RQ2
Interview preparation
Main round of interviews
RQ3
Applying results to PETs
Final Thesis
Writing
Final formatting
Kick-Off