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

Felix Thorwächter

19.06.2023, Bachelor’s Thesis Kick-Off

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

Introduction

- Motivation

Approach

- Research Questions
- Methodology

Initial Results

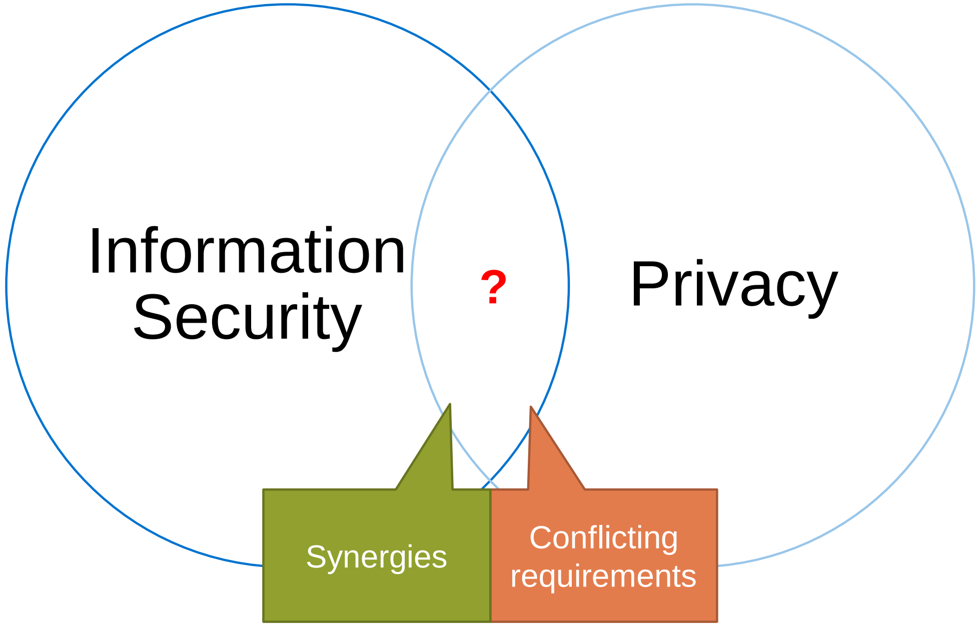
- Literature Review
- Draft of Concept Map
- First Feedback Workshop
- Draft of Decision Tree for Impact Evaluation

Next Steps

Timeline

Motivation(1/2)

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:

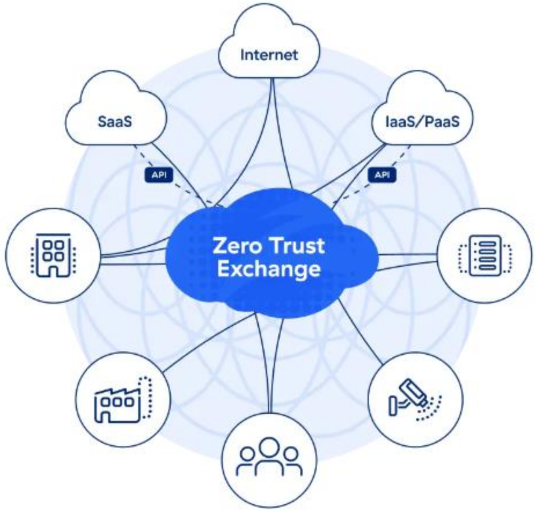
- Process for incident management
- Data protection from unauthorized access or disclosure

Examples for Conflicts:

- Data Retention vs Backup
- Data Minimization vs Monitoring

Motivation(2/2)

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/

Outline

Introduction

- Motivation

Approach

- Research Questions
- Methodology

Initial Results

- Literature Review
- Draft of Concept Map
- First Feedback Workshop
- Draft of Decision Tree for Impact Evaluation

Next Steps

Timeline

Research Questions

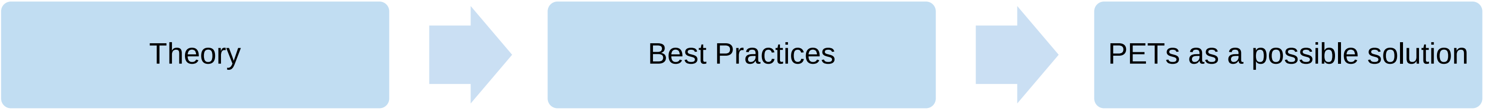
Theory → Best Practices → PETs as a possible solution

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



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 Workshops
→ 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

Outline

Introduction

- Motivation

Approach

- Research Questions
- Methodology

Initial Results

- Literature Review
- Draft of Concept Map
- First Feedback Workshop
- Draft of Decision Tree for Impact Evaluation

Next Steps

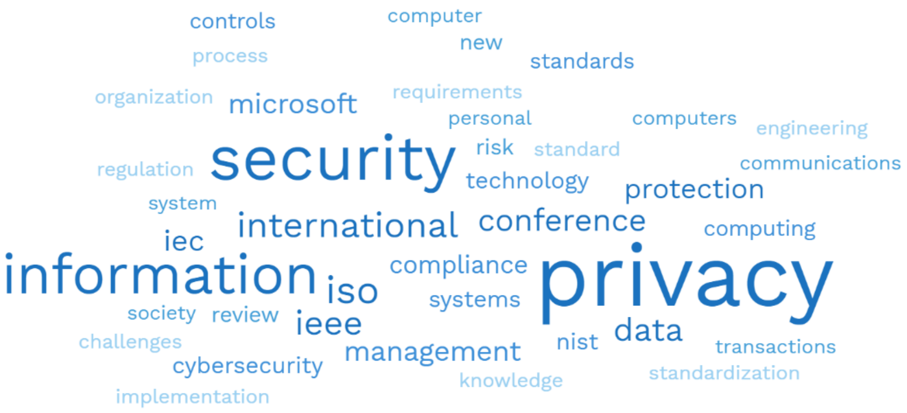
Timeline

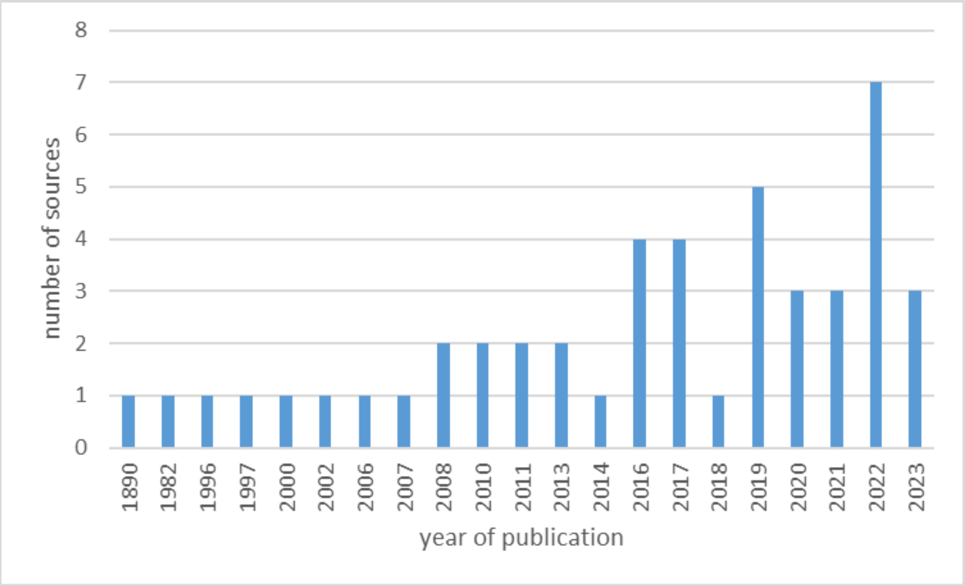
Literature review

1.5 of 2.5 months

- Currently 48 academic literature sources selected
- Search mainly in IEEE database
- Search queries combine “information security” and “privacy” with “information systems”, “standards”, “frameworks”, “regulations”
- For RQ3: “privacy enhancing technologies”

Sources about	#
privacy	24
security	9
privacy and security	13

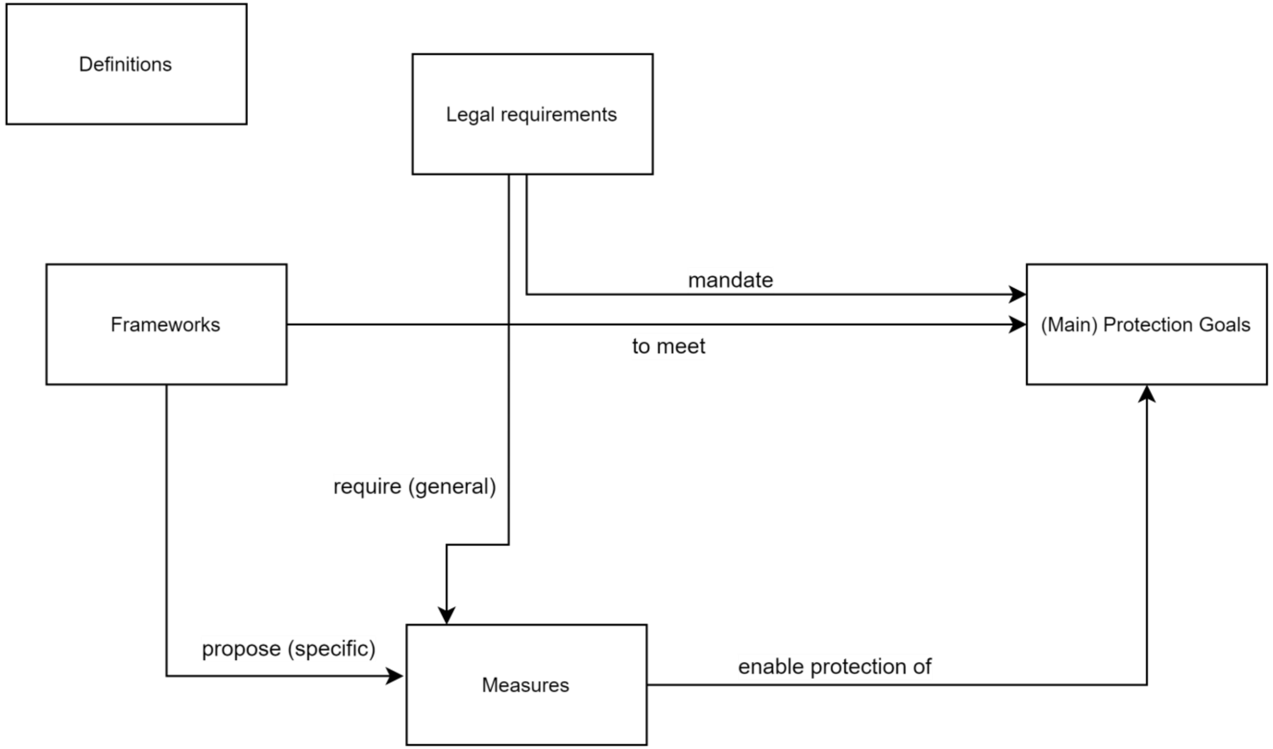




Draft of Concept Map(1/4) – Overview

Problem: How to display the relationship between privacy and security?

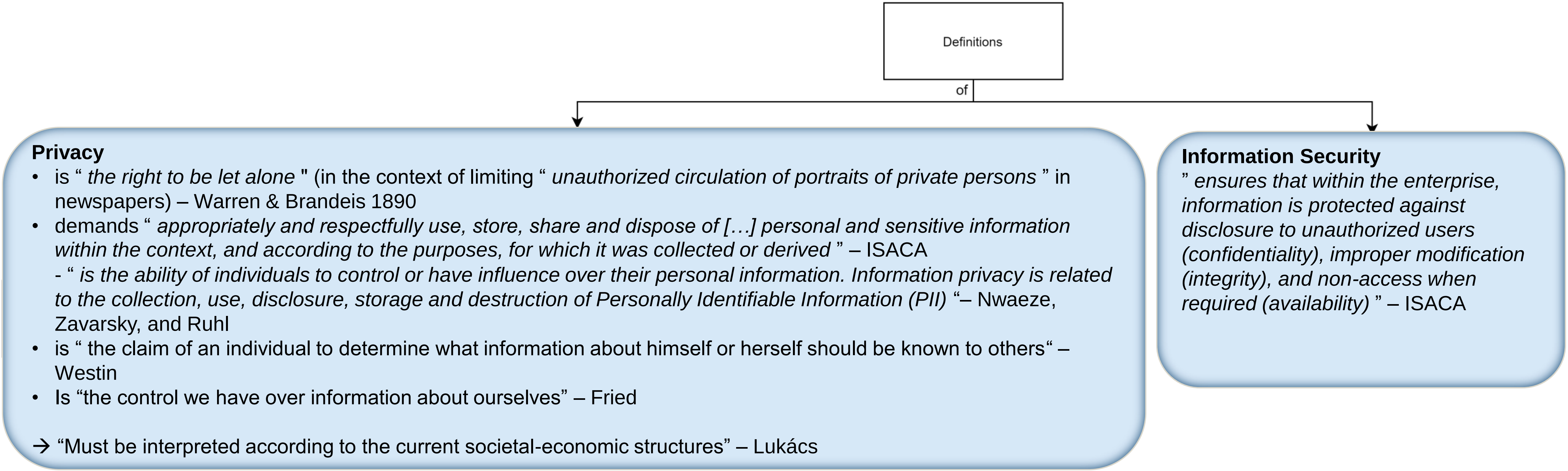
Initial solution:



Draft of Concept Map(2/4)

Problem: How to display the relationship between privacy and security?

Initial solution:



Privacy

- is " *the right to be let alone* " (in the context of limiting " *unauthorized circulation of portraits of private persons* " in newspapers) – Warren & Brandeis 1890
- demands " *appropriately and respectfully use, store, share and dispose of […] personal and sensitive information within the context, and according to the purposes, for which it was collected or derived* " – ISACA
  - " *is the ability of individuals to control or have influence over their personal information. Information privacy is related to the collection, use, disclosure, storage and destruction of Personally Identifiable Information (PII)* "– Nwaeze, Zavarsky, and Ruhl
- is " the claim of an individual to determine what information about himself or herself should be known to others" – Westin
- Is "the control we have over information about ourselves" – Fried

→ "Must be interpreted according to the current societal-economic structures" – Lukács

Information Security

" *ensures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity), and non-access when required (availability)* " – ISACA

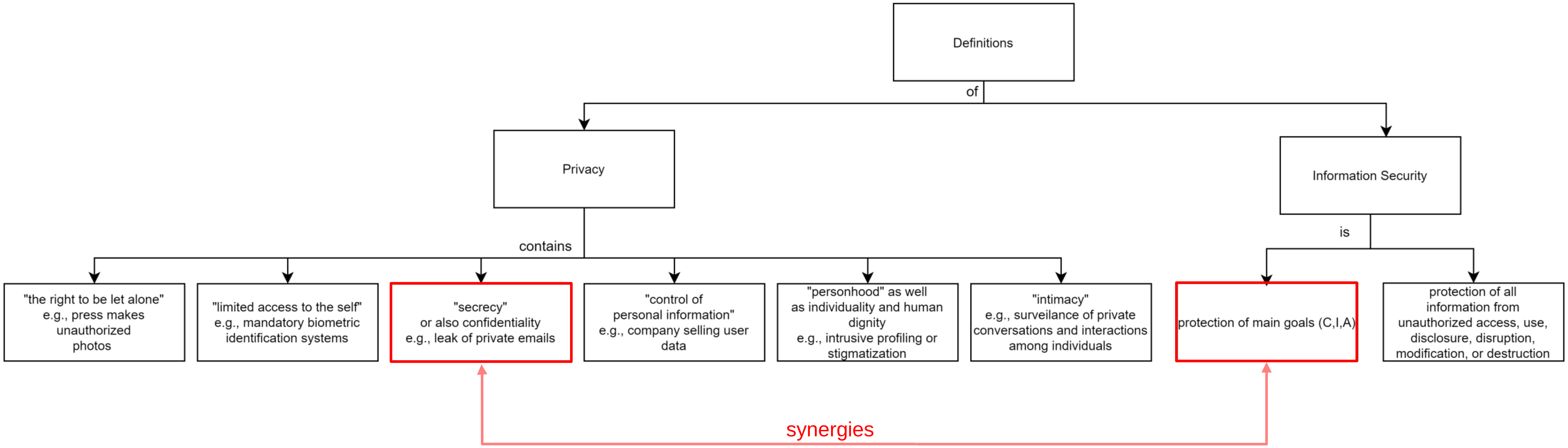
Observation 1: There are different definitions of privacy

Observations 2: Privacy is often mentioned in literature, but rarely defined
→ Confusion which definition is used in the context

Draft of Concept Map(2/4)

Problem: How to display the relationship between privacy and security?

Initial solution:



Definitions

of

Privacy

Information Security

contains

"the right to be let alone" e.g., press makes unauthorized photos

"limited access to the self" e.g., mandatory biometric identification systems

"secrecy" or also confidentiality e.g., leak of private emails

"control of personal information" e.g., company selling user data

"personhood" as well as individuality and human dignity e.g., intrusive profiling or stigmatization

"intimacy" e.g., surveilance of private conversations and interactions among individuals

is

protection of main goals (C,I,A)

protection of all information from unauthorized access, use, disclosure, disruption, modification, or destruction

synergies

Observation 1: There are different definitions of privacy

Observations 2: Privacy is often mentioned in literature, but rarely defined
→ Confusion which definition is used in the context

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

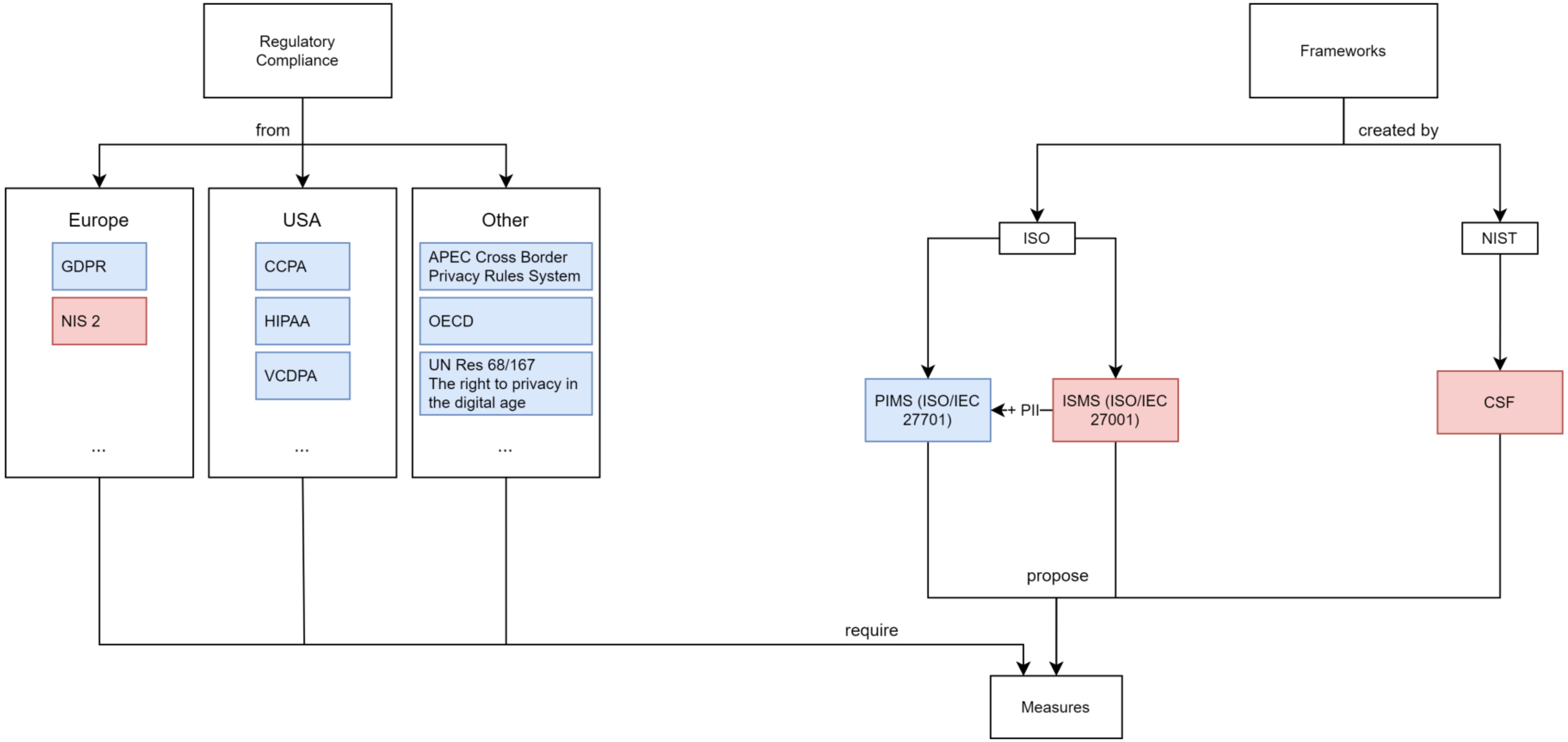
Draft of Concept Map(3/4)

Colour key:

Blue	Privacy
Red	Security
Green	Both

Problem: How to display the relationship between privacy and security?

Initial solution:



Regulatory Compliance

from

Europe: GDPR, NIS 2, ...

USA: CCPA, HIPAA, VCDPA, ...

Other: APEC Cross Border Privacy Rules System, OECD, UN Res 68/167 The right to privacy in the digital age, ...

require

Frameworks

created by

ISO

NIST

PIMS (ISO/IEC 27701)

PII

ISMS (ISO/IEC 27001)

CSF

propose

Measures

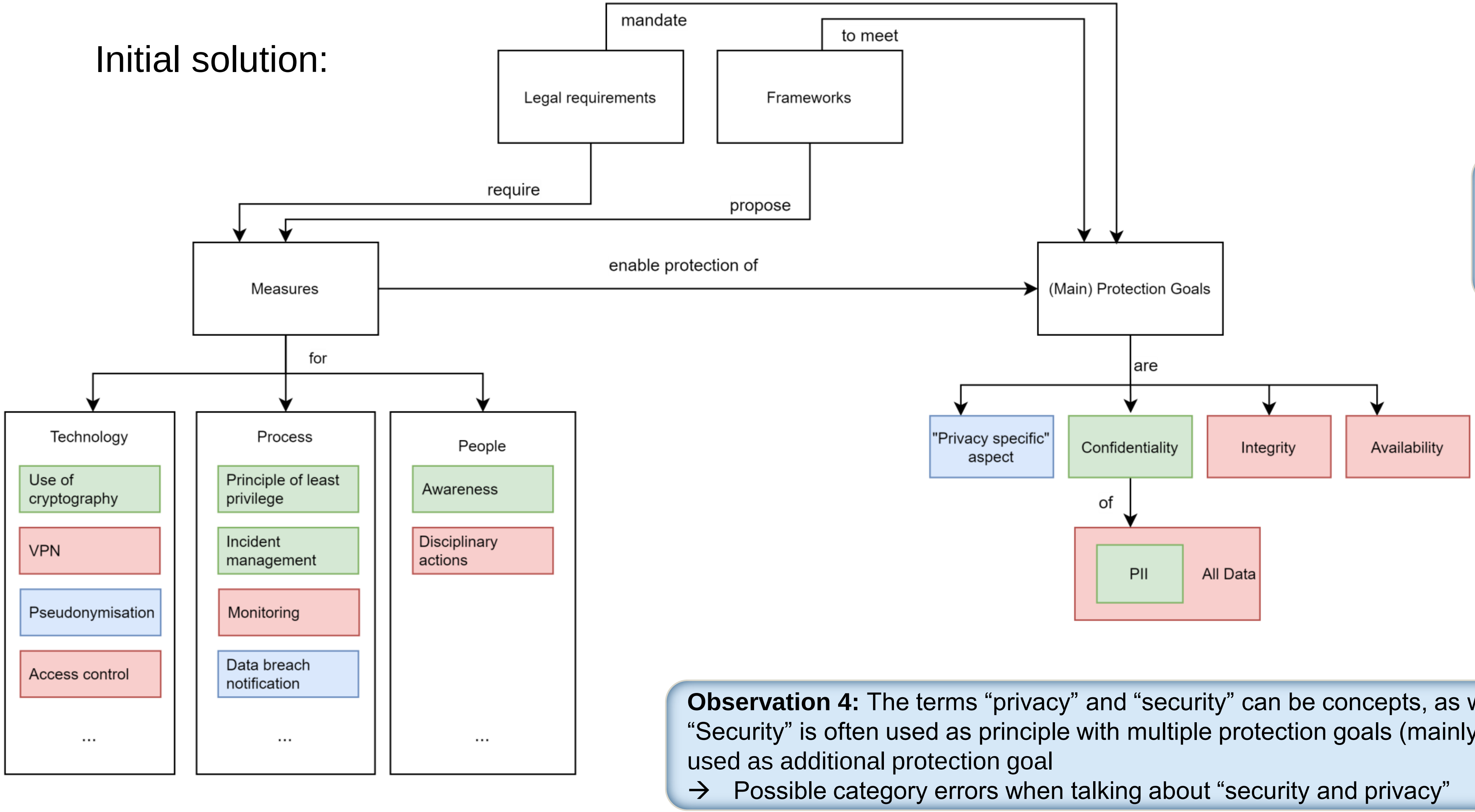
Draft of Concept Map(4/4)

Colour key:

Blue	Privacy
Red	Security
Green	Both

Problem: How to display the relationship between privacy and security?

Initial solution:



Observation 3: Privacy only considers the confidentiality of PII, Information Security includes all data

Observation 4: The terms “privacy” and “security” can be concepts, as well as protection goals: “Security” is often used as principle with multiple protection goals (mainly C,I,A) while “privacy” is used as additional protection goal

→ Possible category errors when talking about “security and privacy”

First Feedback Workshop

Problem: How to verify the practical validity of the (first) results?

Solution: Workshop with security experts (~30 minutes on May 3rd)

Participants:

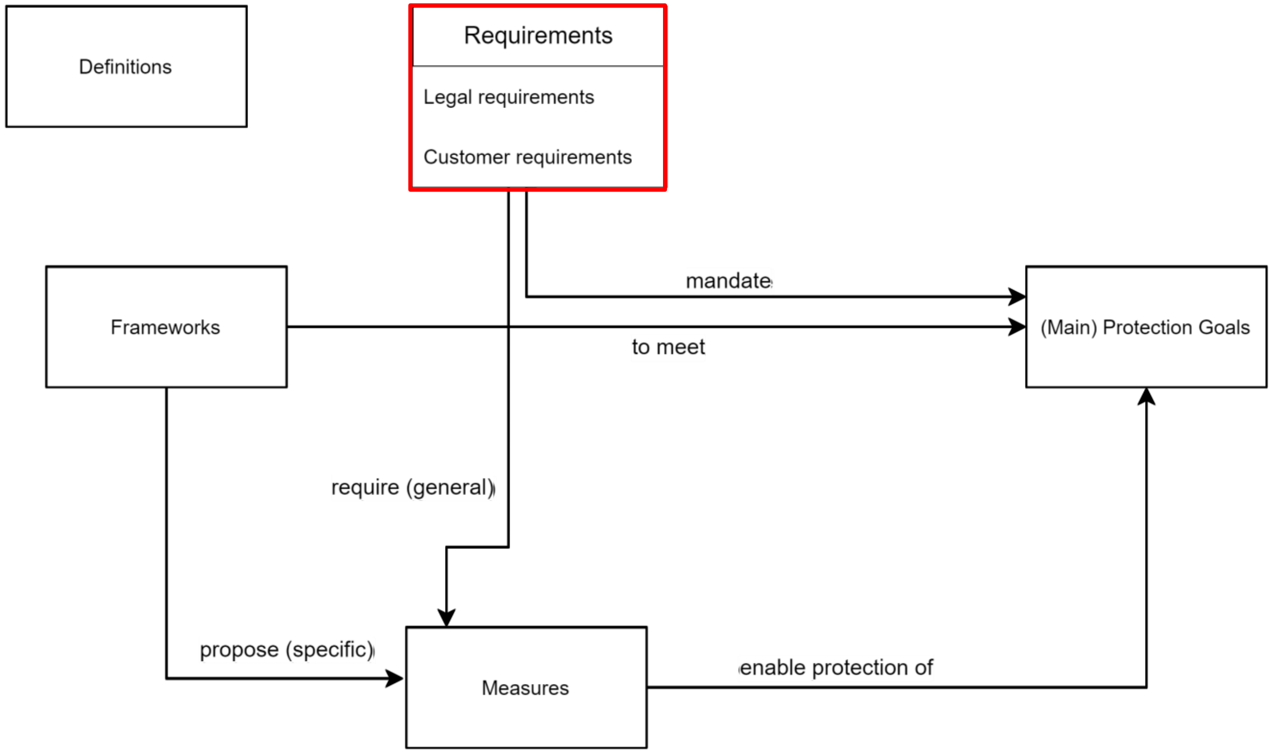
#	Company Size	Sector	(Main) Region	Position (* also ISO)
1	Large (~500)	Build + Construct	USA	* Director Information Security
2				GRC Manager
3	(Holding of all other companies)			Corporate Information Security Officer
4				Security Architect
5	Small (~75)	Operate + Manage	Europe	* Team Lead Internal IT
6	Large (~650)	Planning + Design	Europe	* Team Lead Infrastructure and Security
7	Small (~50)	Digital Twin	Europe	* Security Consultant
8	Large (~1200)	Planning + Design	Europe	* Global IT Security and Business Operations Manager
9	Medium (~350)	Planning + Design	USA	Senior Corporate Security Engineer
10	Medium (~250)	Build + Construct	Europe	* Team Lead IT Network and Infrastructure

Results of Feedback Workshop(1/2)

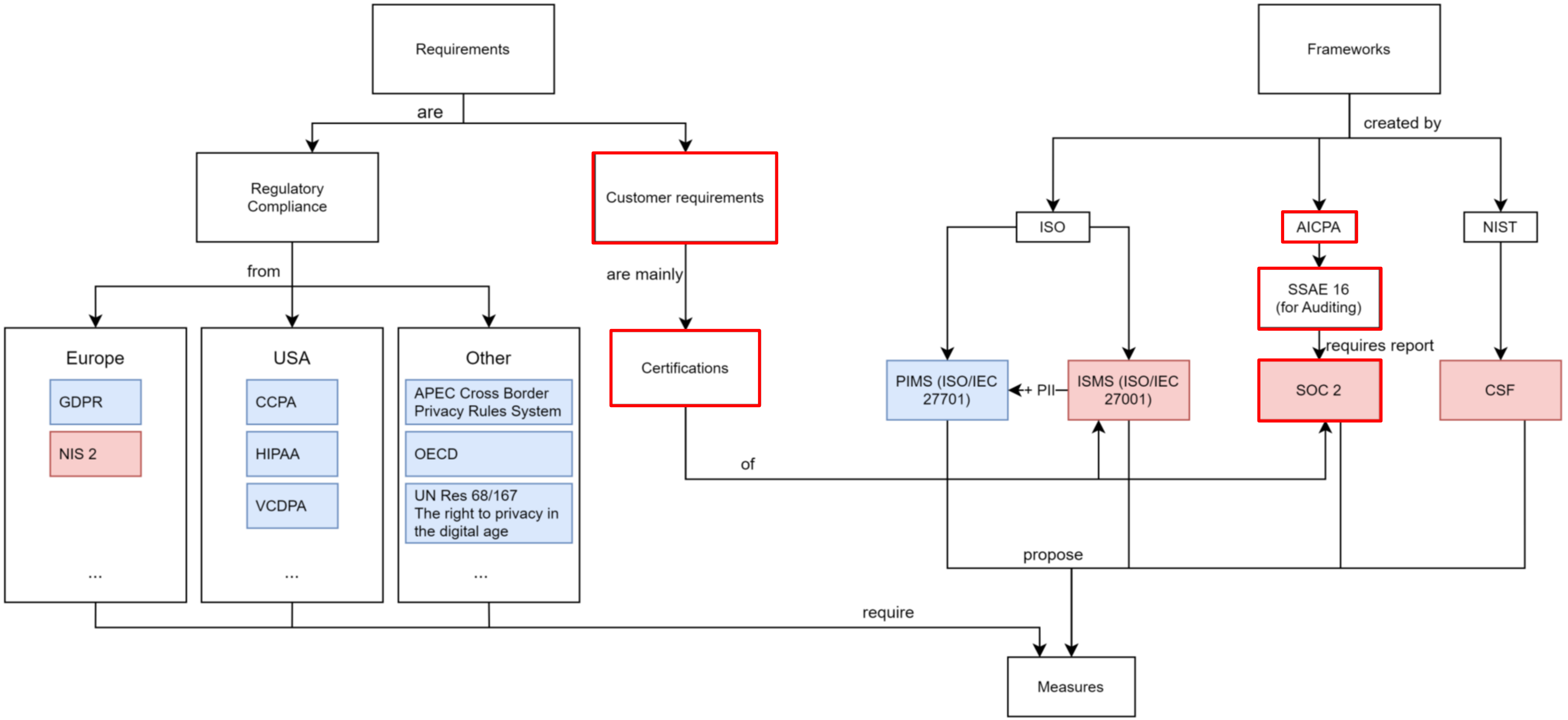
Insight 1: Unclear differentiation in practice
→ Motivation confirmed

Insight 2: Great interest in the topic
→ Agreed to second feedback workshop

Insight 3: Customers have security requirements
→ Additions in Concept map



Results of Feedback Workshop(2/2)



Insight 4: Many customers require security certifications
→ Additions in Concept map

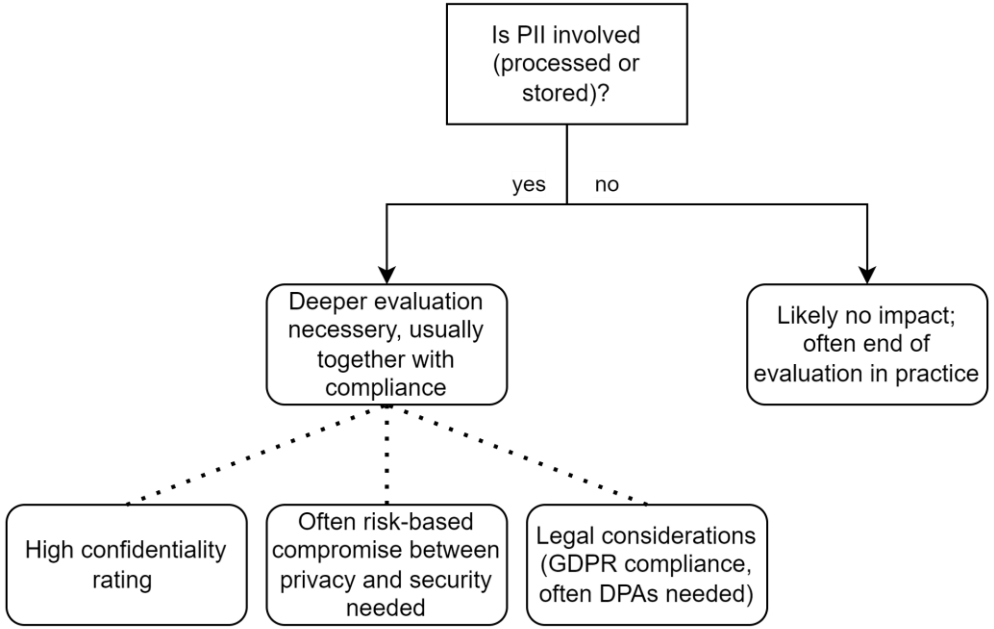
Insight 5: American companies often use SOC 2 as alternative to ISO
→ Additions in Concept map

Draft of Decision Tree for Impact Evaluation(1/2)

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

Method: Discussion with security expert (#3)

Solution:


Is PII involved (processed or stored)?
yes
no
Deeper evaluation necessery, usually together with compliance
Likely no impact; often end of evaluation in practice
High confidentiality rating
Often risk-based compromise between privacy and security needed
Legal considerations (GDPR compliance, often DPAs needed)

Insight 6: PII leads to high confidentiality rating

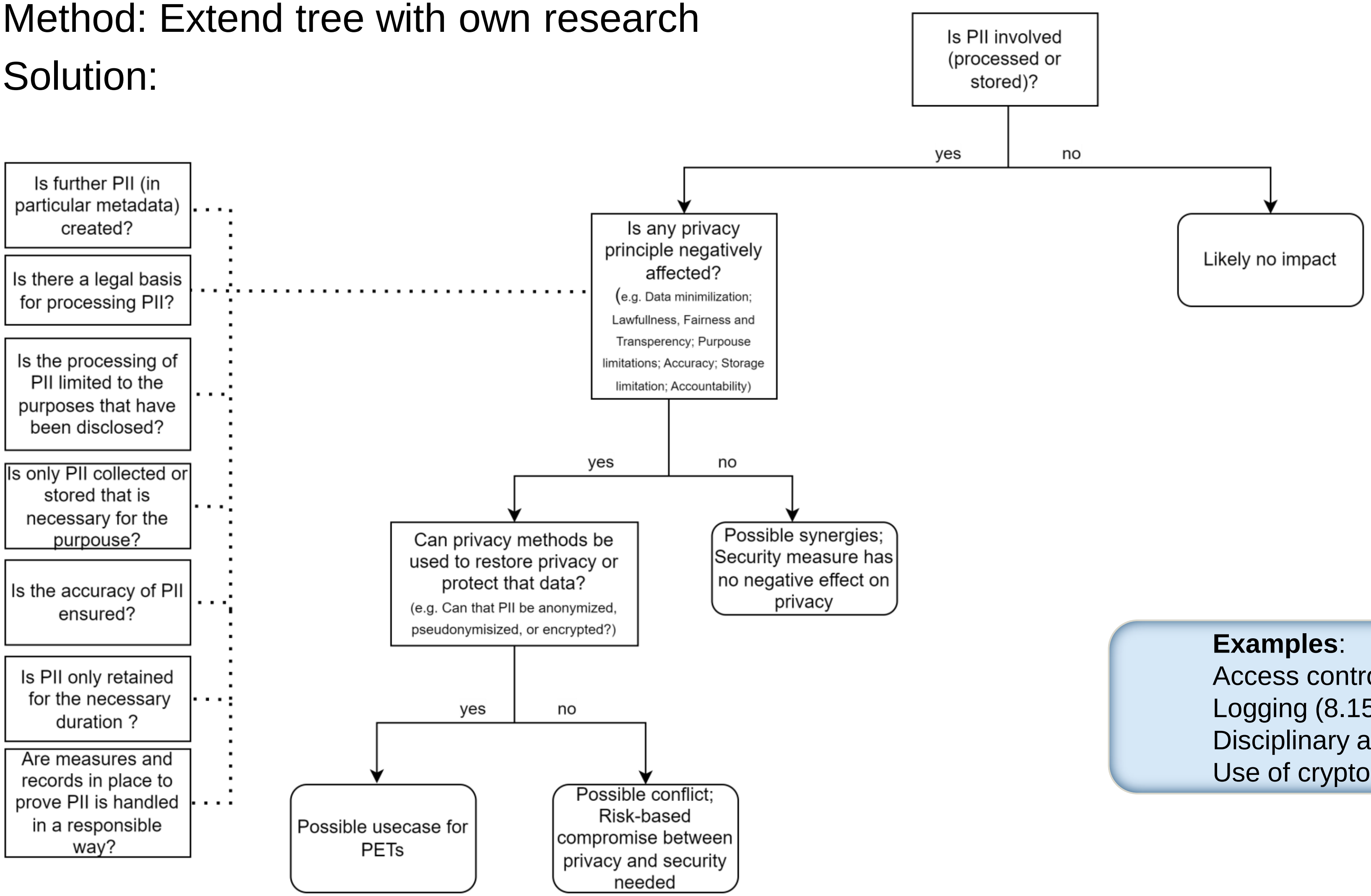
Insight 7: Privacy is currently mainly a compliance topic

Draft of Decision Tree for Impact Evaluation (2/2)

Problem: How can this be extended to evaluate the impact of (ISO 27001) security measure on privacy?

Method: Extend tree with own research

Solution:



Is PII involved (processed or stored)?

yes → Is any privacy principle negatively affected? (e.g. Data minimilization; Lawfullness, Fairness and Transperency; Purpouse limitations; Accuracy; Storage limitation; Accountability)

no → Likely no impact

Is any privacy principle negatively affected?

yes → Can privacy methods be used to restore privacy or protect that data? (e.g. Can that PII be anonymized, pseudonymisized, or encrypted?)

no → Possible synergies; Security measure has no negative effect on privacy

Can privacy methods be used to restore privacy or protect that data?

yes → Possible usecase for PETs

no → Possible conflict; Risk-based compromise between privacy and security needed

Is further PII (in particular metadata) created?

Is there a legal basis for processing PII?

Is the processing of PII limited to the purposes that have been disclosed?

Is only PII collected or stored that is necessary for the purpouse?

Is the accuracy of PII ensured?

Is PII only retained for the necessary duration ?

Are measures and records in place to prove PII is handled in a responsible way?

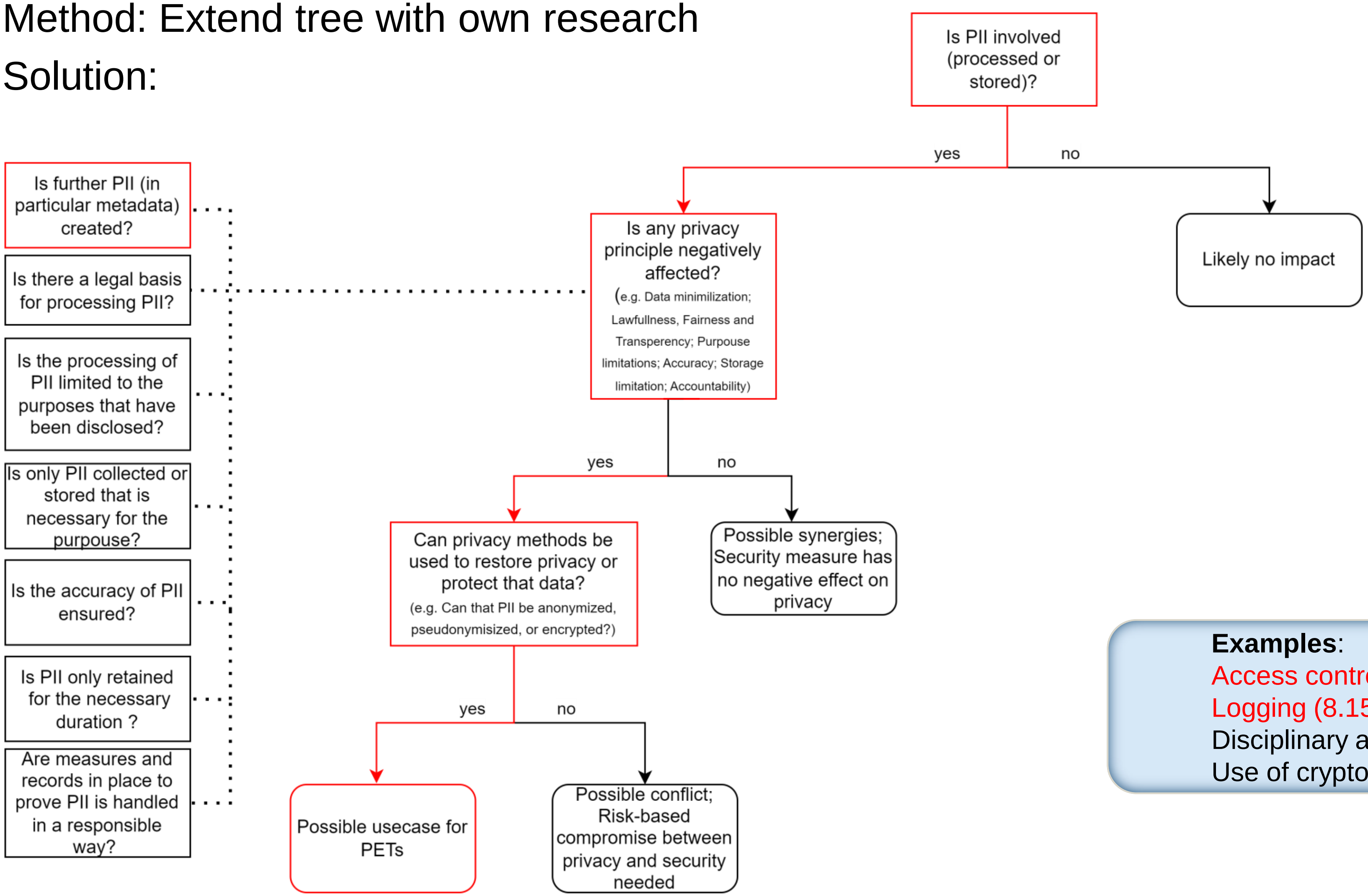
Examples:
Access control (5.15) → Possible use case for PETs
Logging (8.15) → Possible use case for PETs
Disciplinary actions (6.4) → Possible conflict
Use of cryptography (8.24) → Synergies

Draft of Decision Tree for Impact Evaluation(2/2)

Problem: How can this be extended to evaluate the impact of (ISO 27001) security measure on privacy?

Method: Extend tree with own research

Solution:



Is PII involved (processed or stored)?

yes

no

Likely no impact

Is any privacy principle negatively affected? (e.g. Data minimilization; Lawfullness, Fairness and Transperency; Purpouse limitations; Accuracy; Storage limitation; Accountability)

Is further PII (in particular metadata) created?

Is there a legal basis for processing PII?

Is the processing of PII limited to the purposes that have been disclosed?

Is only PII collected or stored that is necessary for the purpouse?

Is the accuracy of PII ensured?

Is PII only retained for the necessary duration ?

Are measures and records in place to prove PII is handled in a responsible way?

yes

no

Possible synergies; Security measure has no negative effect on privacy

Can privacy methods be used to restore privacy or protect that data? (e.g. Can that PII be anonymized, pseudonymisized, or encrypted?)

yes

no

Possible usecase for PETs

Possible conflict; Risk-based compromise between privacy and security needed

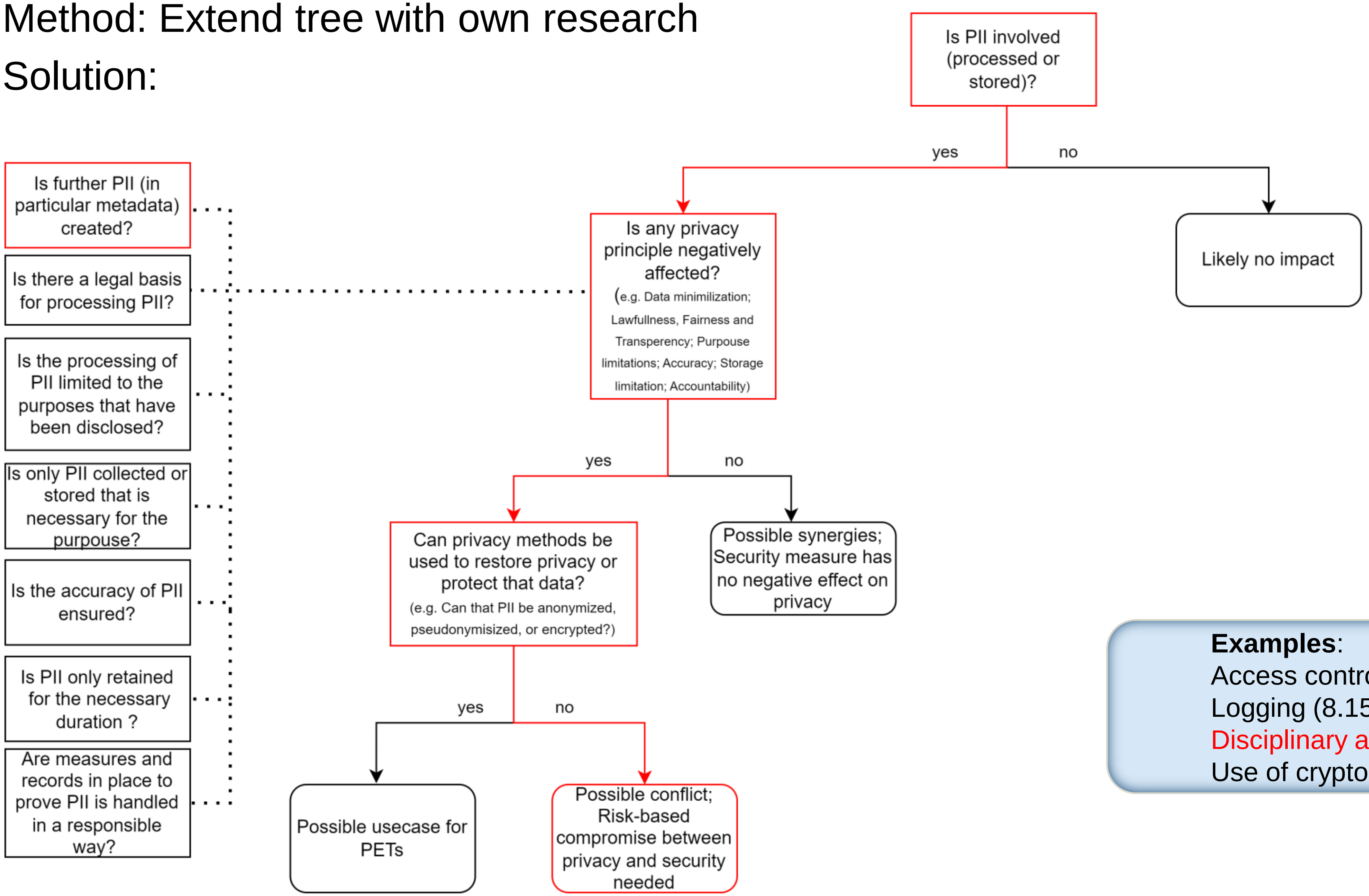
Examples:
Access control (5.15) → Possible use case for PETs
Logging (8.15) → Possible use case for PETs
Disciplinary actions (6.4) → Possible conflict
Use of cryptography (8.24) → Synergies

Draft of Decision Tree for Impact Evaluation(2/2)

Problem: How can this be extended to evaluate the impact of (ISO 27001) security measure on privacy?

Method: Extend tree with own research

Solution:



Is PII involved (processed or stored)?

yes → Is any privacy principle negatively affected? (e.g. Data minimilization; Lawfullness, Fairness and Transperency; Purpouse limitations; Accuracy; Storage limitation; Accountability)

no → Likely no impact

Is any privacy principle negatively affected?

yes → Can privacy methods be used to restore privacy or protect that data? (e.g. Can that PII be anonymized, pseudonymisized, or encrypted?)

no → Possible synergies; Security measure has no negative effect on privacy

Can privacy methods be used to restore privacy or protect that data?

yes → Possible usecase for PETs

no → Possible conflict; Risk-based compromise between privacy and security needed

Is further PII (in particular metadata) created?

Is there a legal basis for processing PII?

Is the processing of PII limited to the purposes that have been disclosed?

Is only PII collected or stored that is necessary for the purpouse?

Is the accuracy of PII ensured?

Is PII only retained for the necessary duration ?

Are measures and records in place to prove PII is handled in a responsible way?

Examples:

Access control (5.15) → Possible use case for PETs

Logging (8.15) → Possible use case for PETs

Disciplinary actions (6.4) → Possible conflict

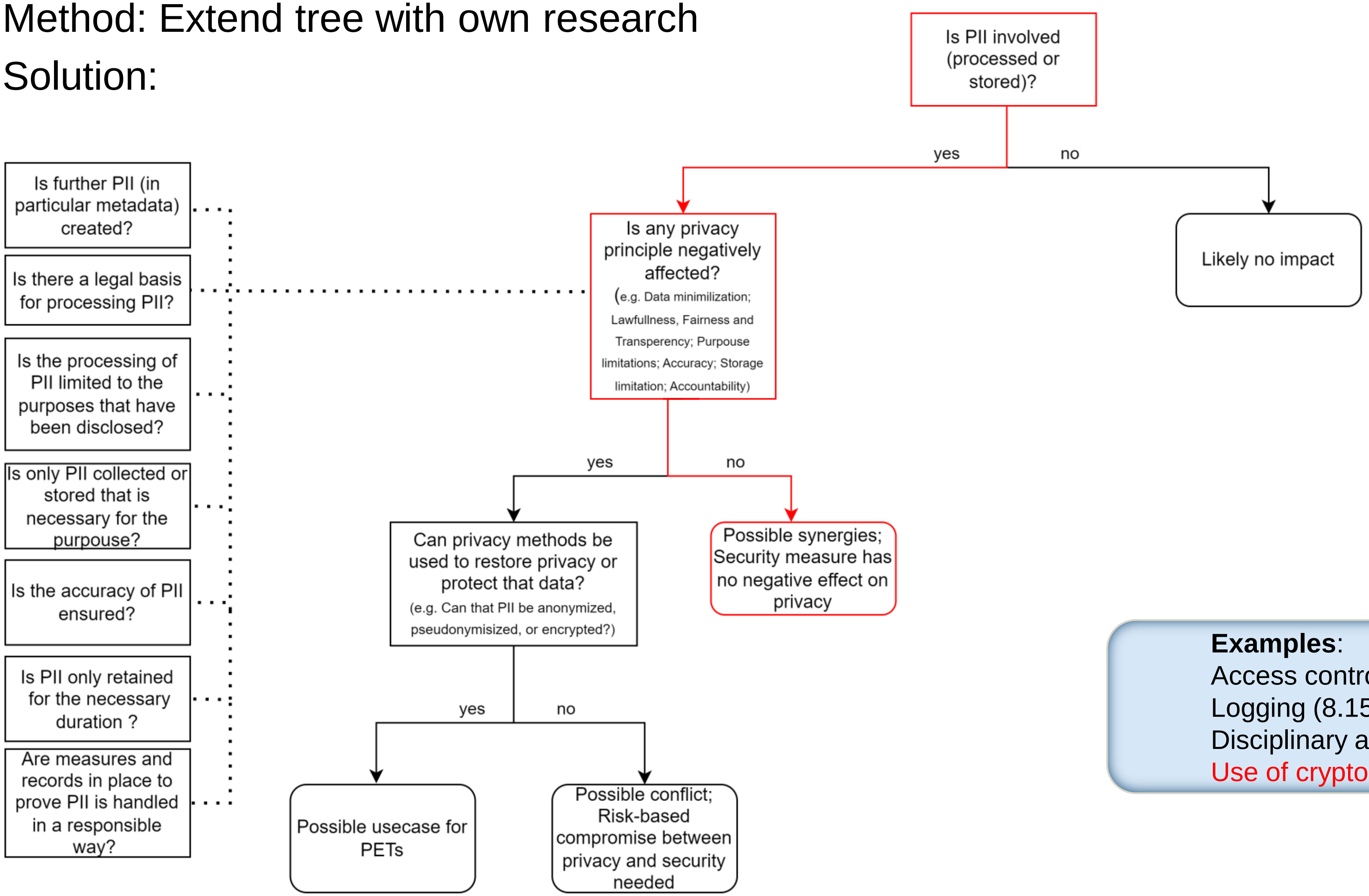
Use of cryptography (8.24) → Synergies

Draft of Decision Tree for Impact Evaluation(2/2)

Problem: How can this be extended to evaluate the impact of (ISO 27001) security measure on privacy?

Method: Extend tree with own research

Solution:



Is PII involved (processed or stored)?

yes

no

Likely no impact

Is any privacy principle negatively affected? (e.g. Data minimilization; Lawfullness, Fairness and Transperency; Purpouse limitations; Accuracy; Storage limitation; Accountability)

Is further PII (in particular metadata) created?

Is there a legal basis for processing PII?

Is the processing of PII limited to the purposes that have been disclosed?

Is only PII collected or stored that is necessary for the purpouse?

Is the accuracy of PII ensured?

Is PII only retained for the necessary duration ?

Are measures and records in place to prove PII is handled in a responsible way?

yes

no

Can privacy methods be used to restore privacy or protect that data? (e.g. Can that PII be anonymized, pseudonymisized, or encrypted?)

Possible synergies; Security measure has no negative effect on privacy

yes

no

Possible usecase for PETs

Possible conflict; Risk-based compromise between privacy and security needed

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

Outline

Introduction

- Motivation

Approach

- Research Questions
- Methodology

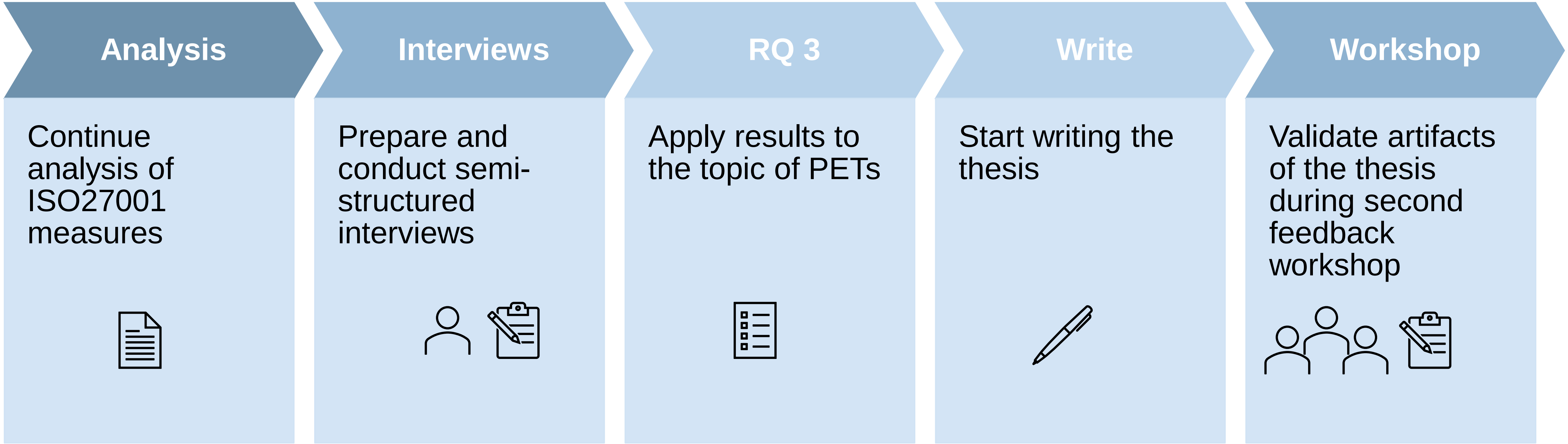
Initial Results

- Literature Review
- Draft of Concept Map
- First Feedback Workshop
- Draft of Decision Tree for Impact Evaluation

Next Steps

Timeline

Next Steps



Analysis

Continue analysis of ISO27001 measures

Interviews

Prepare and conduct semi-structured interviews

RQ 3

Apply results to the topic of PETs

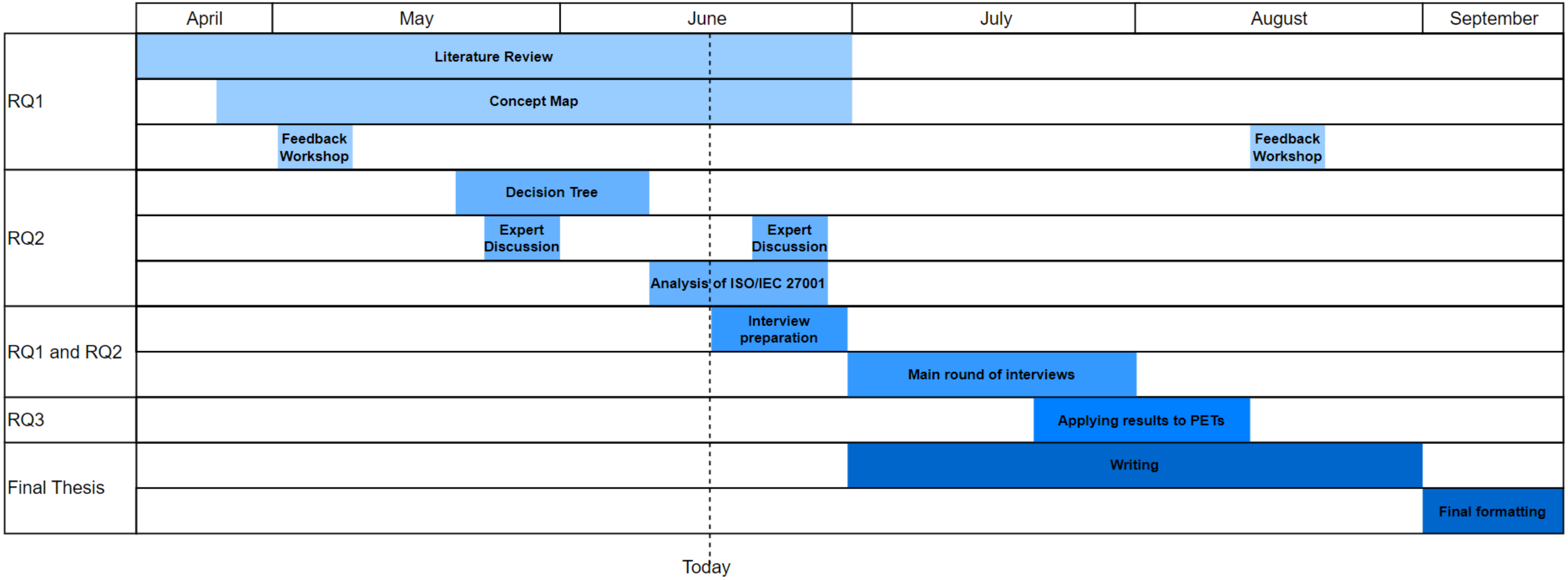
Write

Start writing the thesis

Workshop

Validate artifacts of the thesis during second feedback workshop

Timeline



April May June July August September

RQ1

Literature Review

Concept Map

Feedback Workshop

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

Today

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!

References

[1] Elmimouni, H., Shusas, E., Skeba, P., Baumer, E.P.S., Forte, A. (2023). *What Makes a Technology Privacy Enhancing? Laypersons' and Experts' Descriptions, Uses, and Perceptions of Privacy Enhancing Technologies*. In: , *et al.* Information for a Better World: Normality, Virtuality, Physicality, Inclusivity. iConference 2023. Lecture Notes in Computer Science, vol 13972. Springer, Cham. https://doi.org/10.1007/978-3-031-28032-0_20

[2] NIST Joint Task Force Transformation Initiative (2013). *Security and Privacy Controls for Federal Information Systems and Organizations*. In: NIST Special Publication 800-53. Revision 4 http://dx.doi.org/10.6028/NIST.SP.800-53r4

[3] ISO https://www.iso.org/standard/27001