CHESS
Cyber-security Excellence Hub in
Estonia and South Moravia

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

Forensic-Ready Information Security

Risk-Based Approach for Information Systems

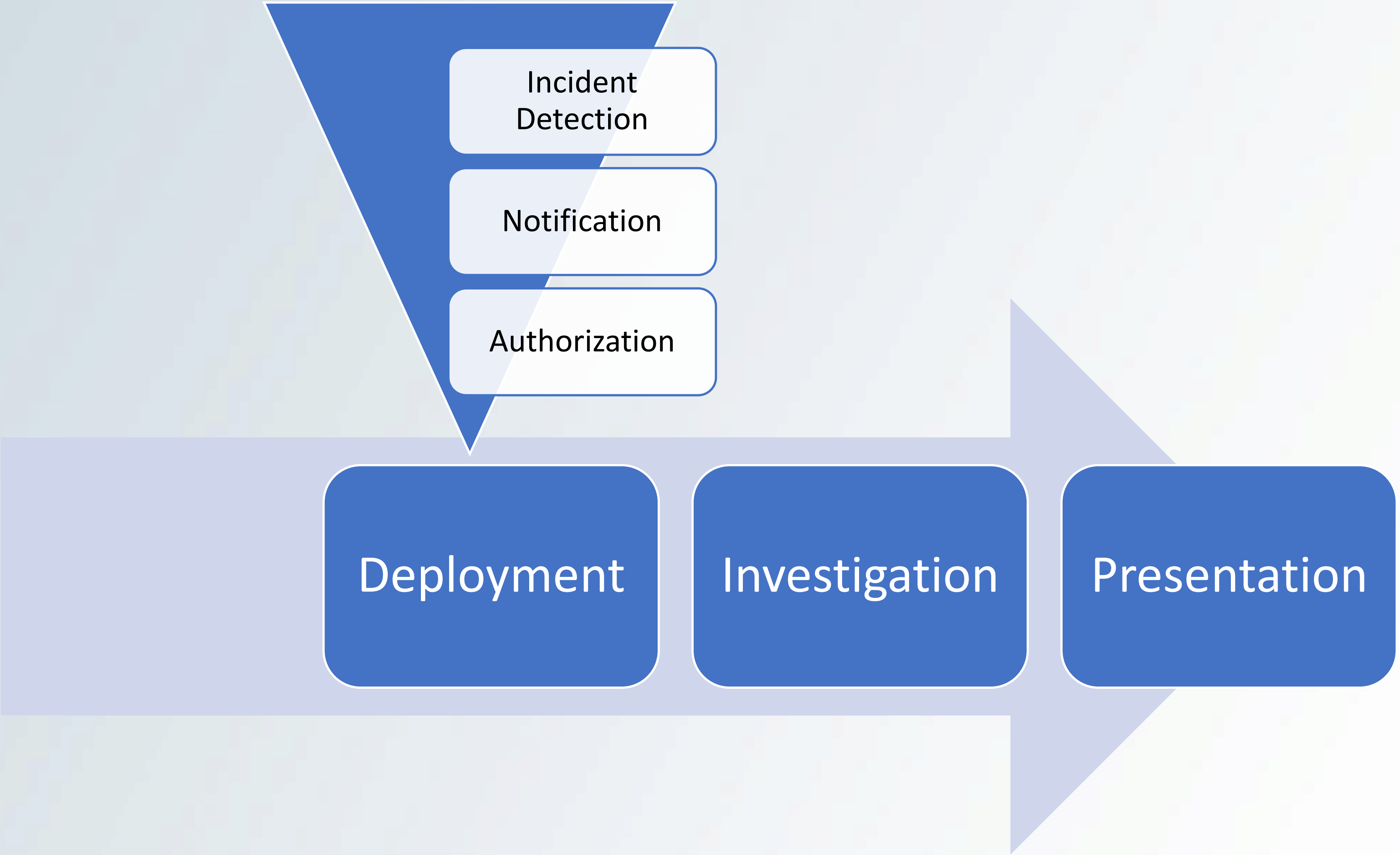
Lukáš Daubner (lukas.daubner@ut.ee)
Raimundas Matulevičius (raimundas.matulevicius@ut.ee)

Tallinn, March 19, 2026

Funded by the European Union under Grant Agreement No. 101087529. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Research Executive Agency. Neither the European Union nor the granting authority can be held responsible for them.

Co-funded by
the European Union

Forensics Timeline



Incident Detection

Notification

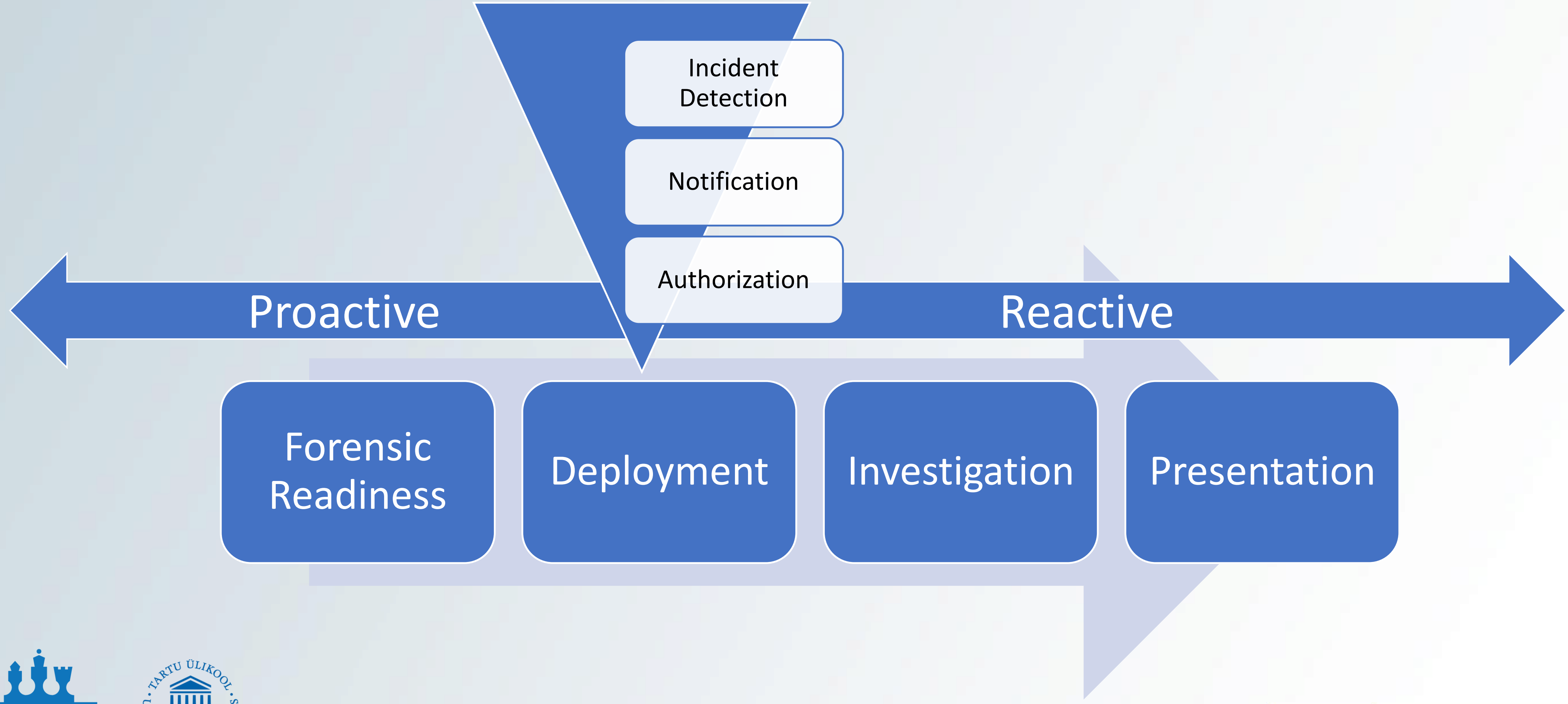
Authorization

Deployment

Investigation

Presentation

Forensics Timeline



CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European Union

Forensic Readiness

- Proactive steps towards incident investigation

Incident Response

Useful Evidence

Cost Effective

- Forensic-ready systems (forensic-by-design)
  - **Prepare systems during development**
  - **Ensure rich and forensically sound evidence for future use**

WHY Forensic Readiness?

Effective Investigation

WHY Forensic Readiness?

Effective Investigation

Compliance

Co-funded by the European Union

WHY Forensic Readiness?

- Effective Investigation
- Compliance
- Legal Actions Support

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European Union

WHY Forensic Readiness?

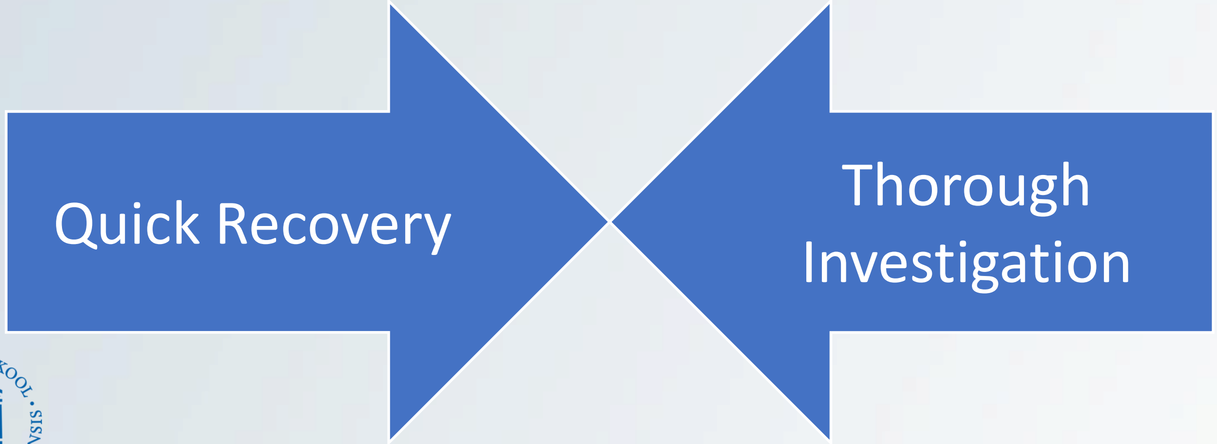
- Effective Investigation
- Compliance
- Legal Actions Support
- Disclosure Orders

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Co-funded by the European Union

WHY ELSE Forensic Readiness?

- Security – Not IF, but WHEN
- Insight – What? When? Where? Who? How?
- Softening the incident response dilemma



Quick Recovery

Thorough Investigation

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Co-funded by the European Union

HOW Forensic Readiness?

Organisation

- Strategy
- Policy
- Staff Training
- Documentation

Technology

- Evidence Preservation
- Secure Storage
- Evidence Production
  - Logs
  - Audit Trails

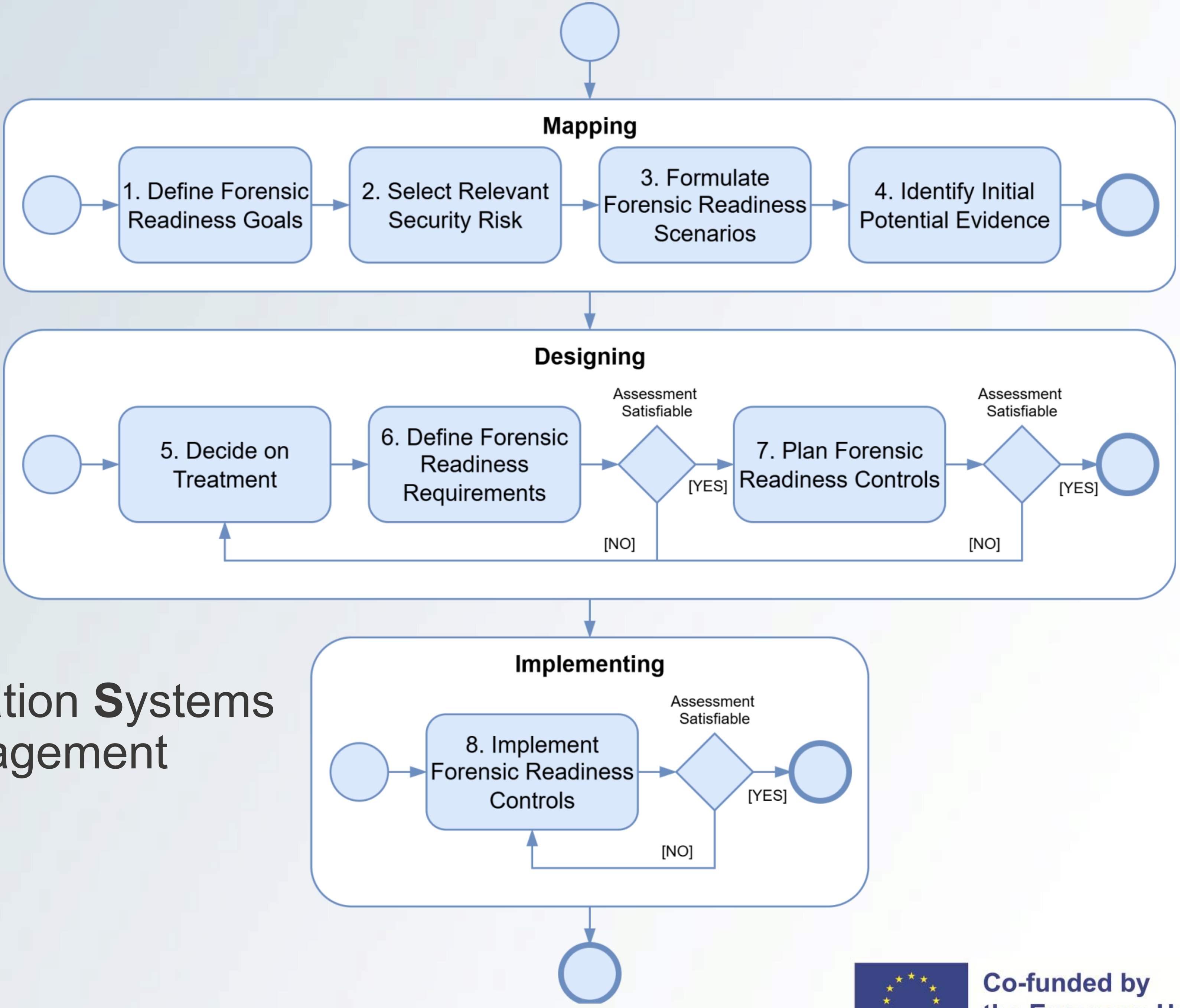
Forensic-Ready Information Security

1. Forensic readiness complements security
2. Risk assessment to guide implementation
3. Building forensic readiness on top of information security

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Co-funded by the European Union

FR-ISSRM Process


Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

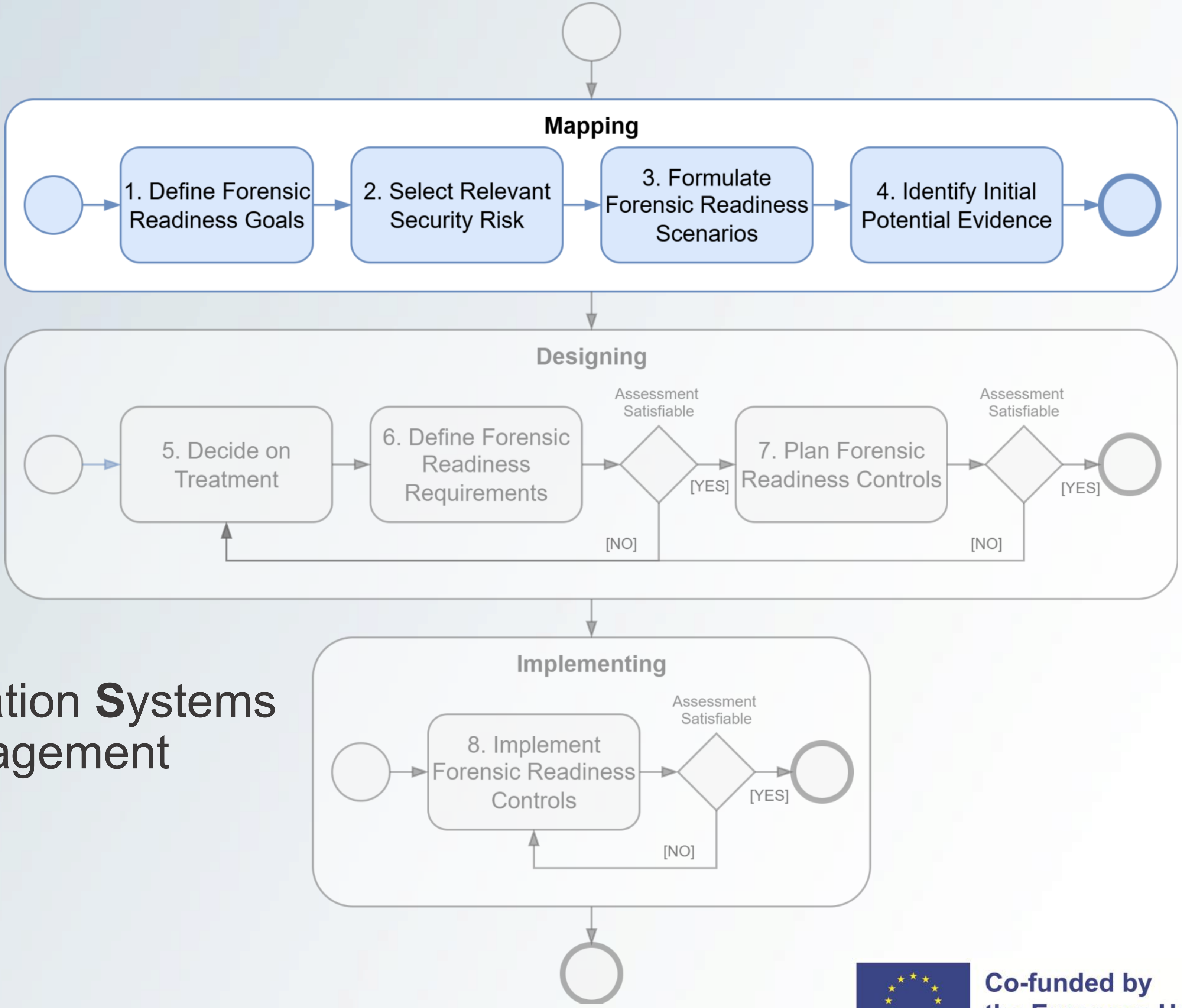
Forensic-**R**eady **I**nformation **S**ystems **S**ecurity **R**isk **M**anagement

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European Union

FR-ISSRM Process



Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

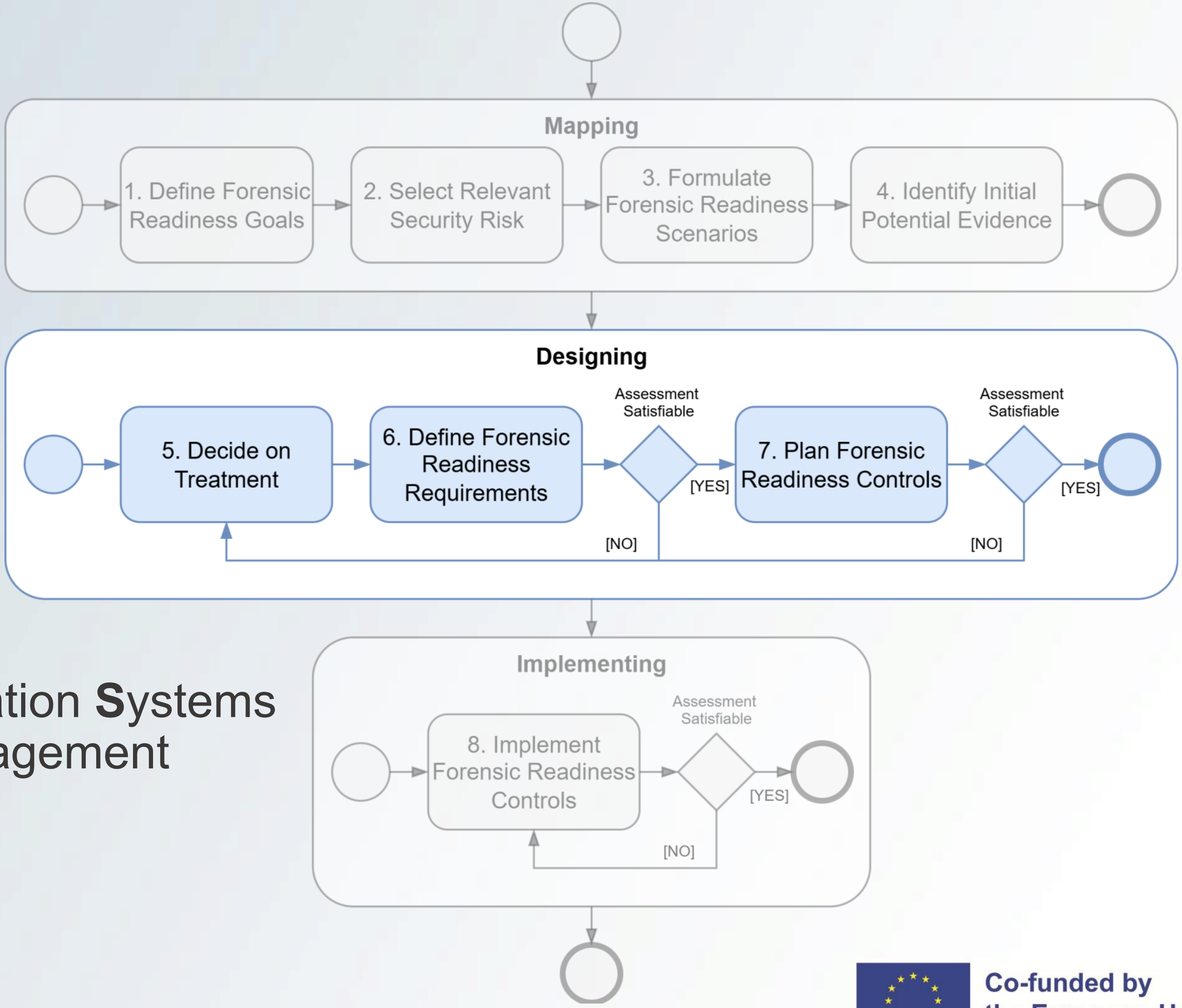
Forensic-**R**eady **I**nformation **S**ystems **S**ecurity **R**isk **M**anagement

CHESS Cyber-security Excellence Hub in Estonia and South Moravia

Tartu Ülikool · Universitas Tartuensis 1632

Co-funded by the European Union

FR-ISSRM Process



Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

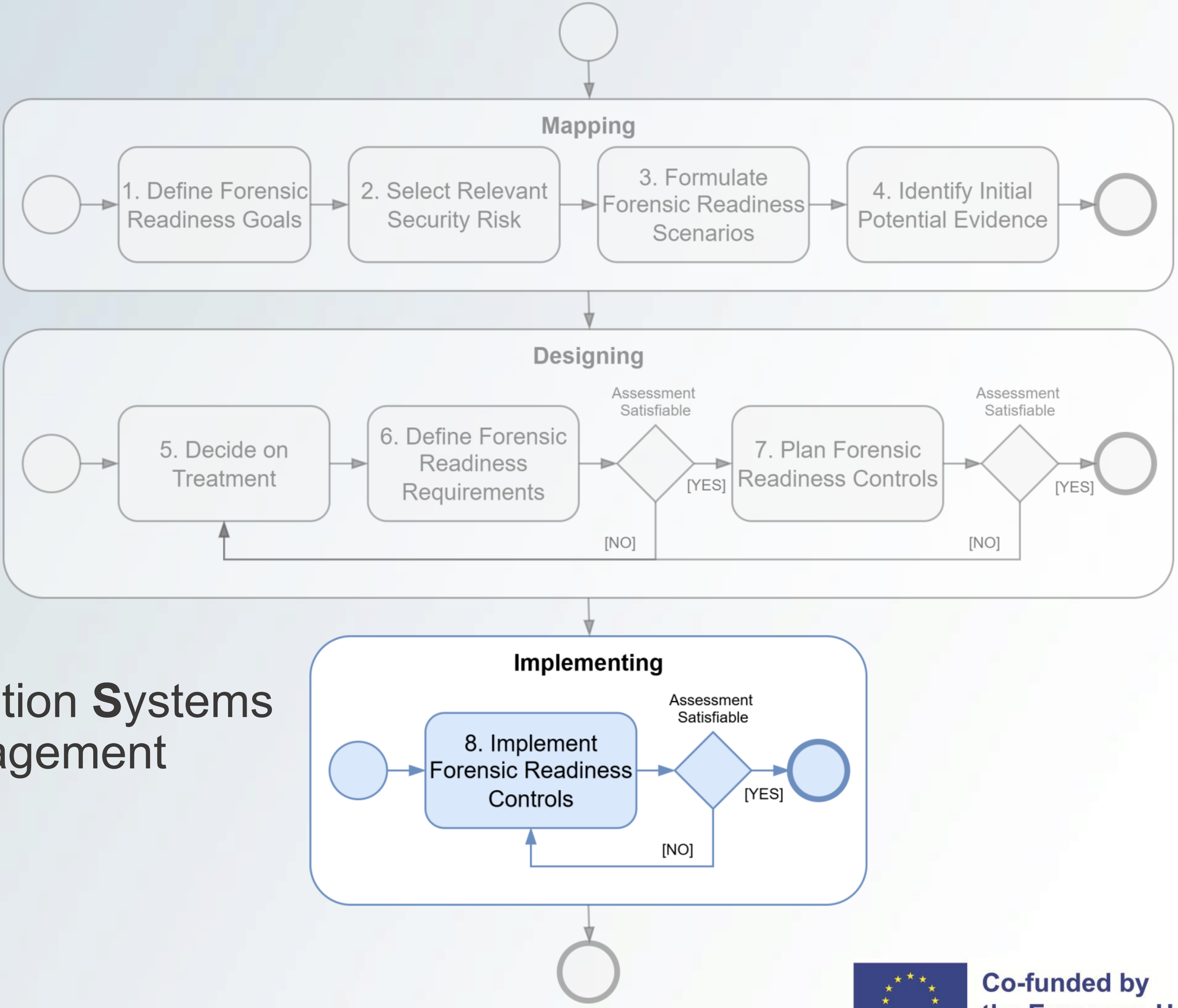
Forensic-**R**eady **I**nformation **S**ystems **S**ecurity **R**isk **M**anagement

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Tartu Ülikool · Universitas Tartuensis 1632

Co-funded by the European Union

FR-ISSRM Process



Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

Forensic-**R**eady **I**nformation **S**ystems **S**ecurity **R**isk **M**anagement

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Co-funded by the European Union

CHESS

Cyber-security Excellence Hub in Estonia and South Moravia

Example Implementation – SensitiveCloud

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

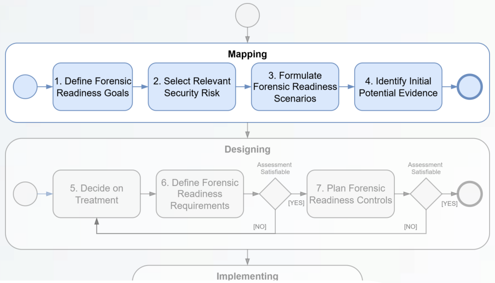
Sensitive Cloud

- Platform for storage and processing of sensitive data
  - Supporting life sciences research
  - Strong security needs
  - Build on Kubernetes (K8s), accessible by VPN

- Aspiring for ISO/IEC 27k certification

- Interested in systematization of “logging”

Sensitive Cloud


Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing

Forensic Readiness Goals

Prove access to user data

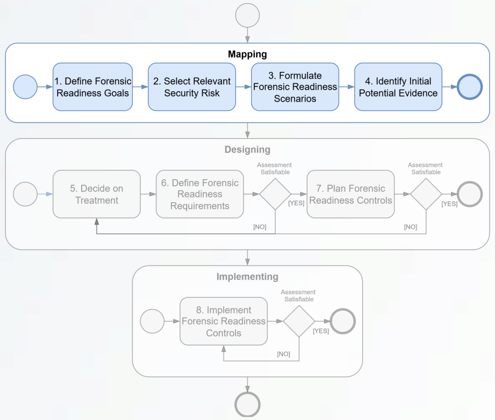
Enable investigation of logical perimeter access process breach

Prove misuse of user identity

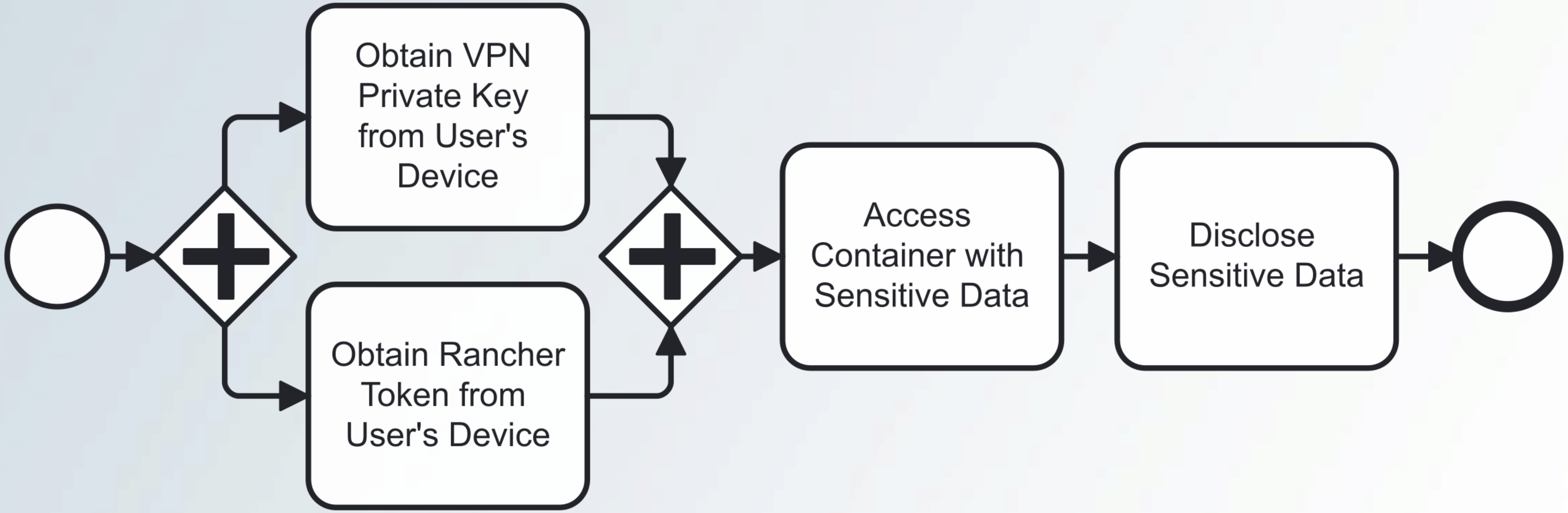
Enable evidence release of perimeter access process

Co-funded by the European Union

Sensitive Cloud



Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

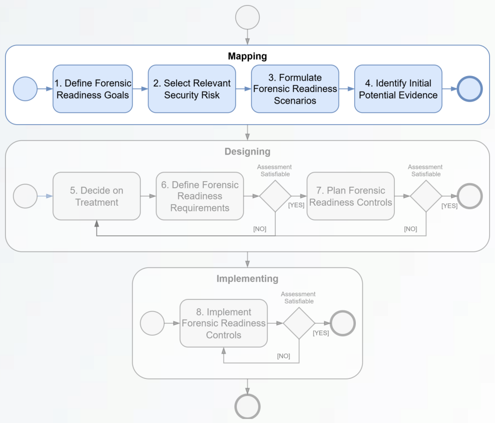


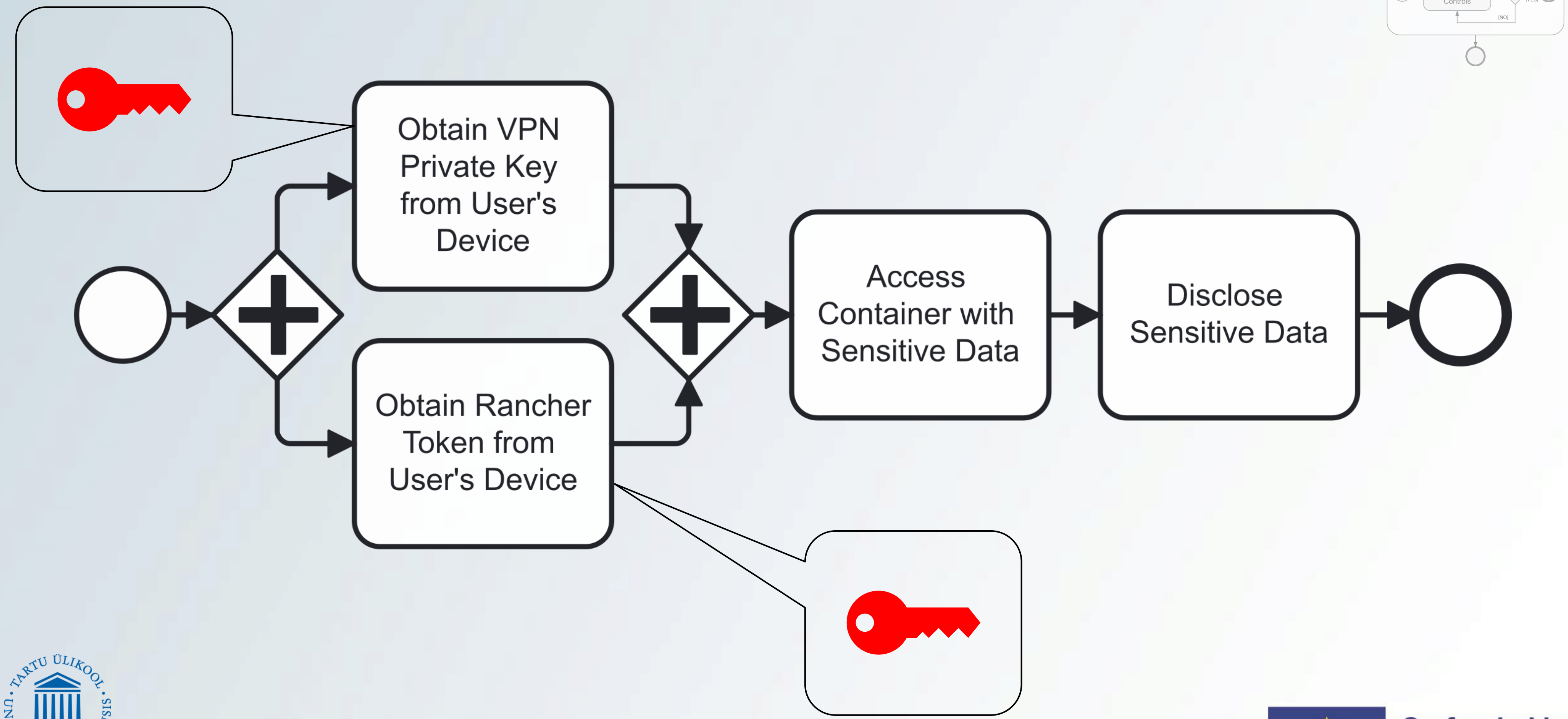
Obtain VPN Private Key from User's Device
Obtain Rancher Token from User's Device
Access Container with Sensitive Data
Disclose Sensitive Data

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Co-funded by the European Union

Sensitive Cloud

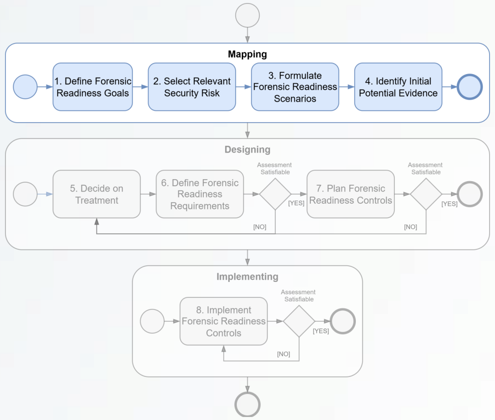

Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

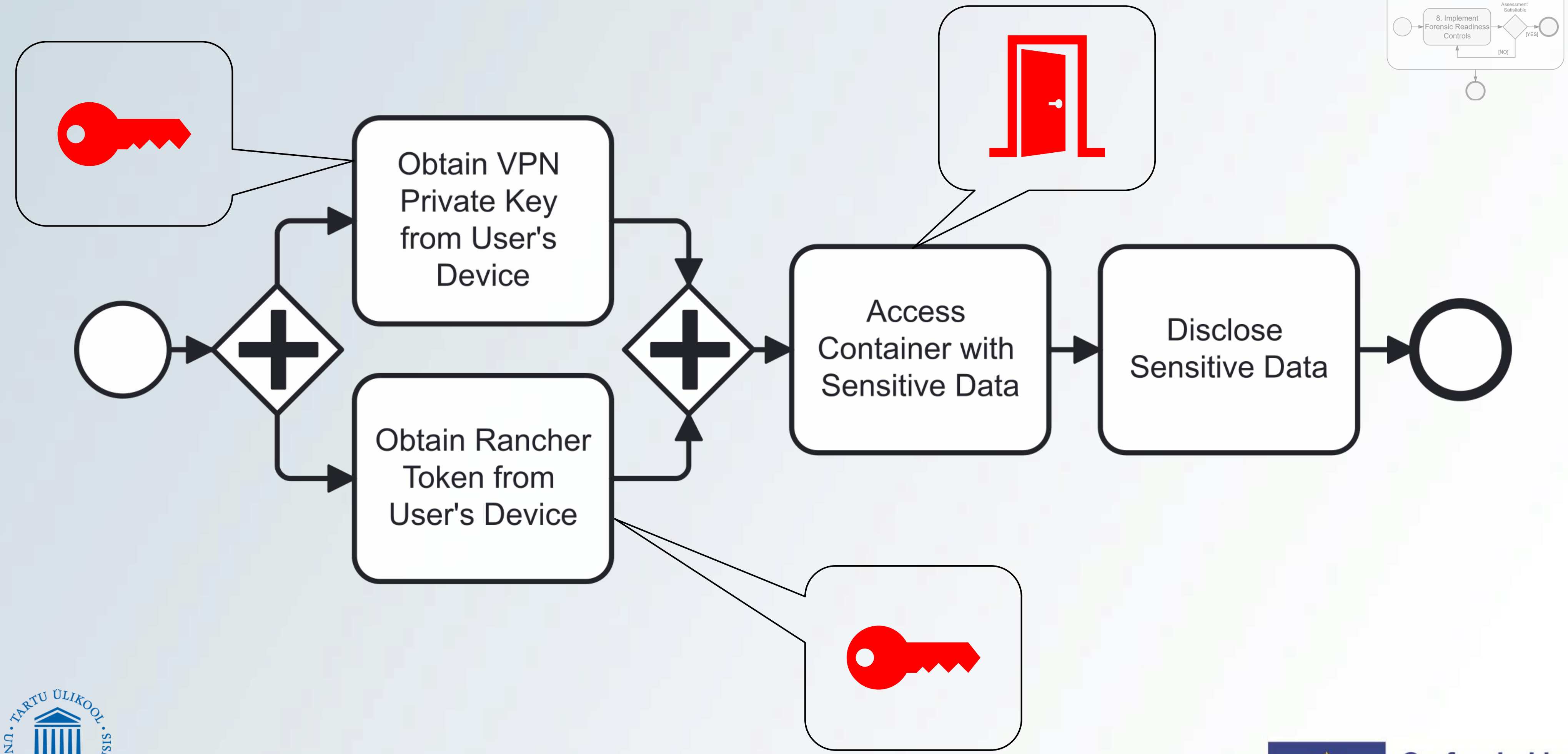

Obtain VPN Private Key from User's Device
Obtain Rancher Token from User's Device
Access Container with Sensitive Data
Disclose Sensitive Data

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Co-funded by the European Union

Sensitive Cloud

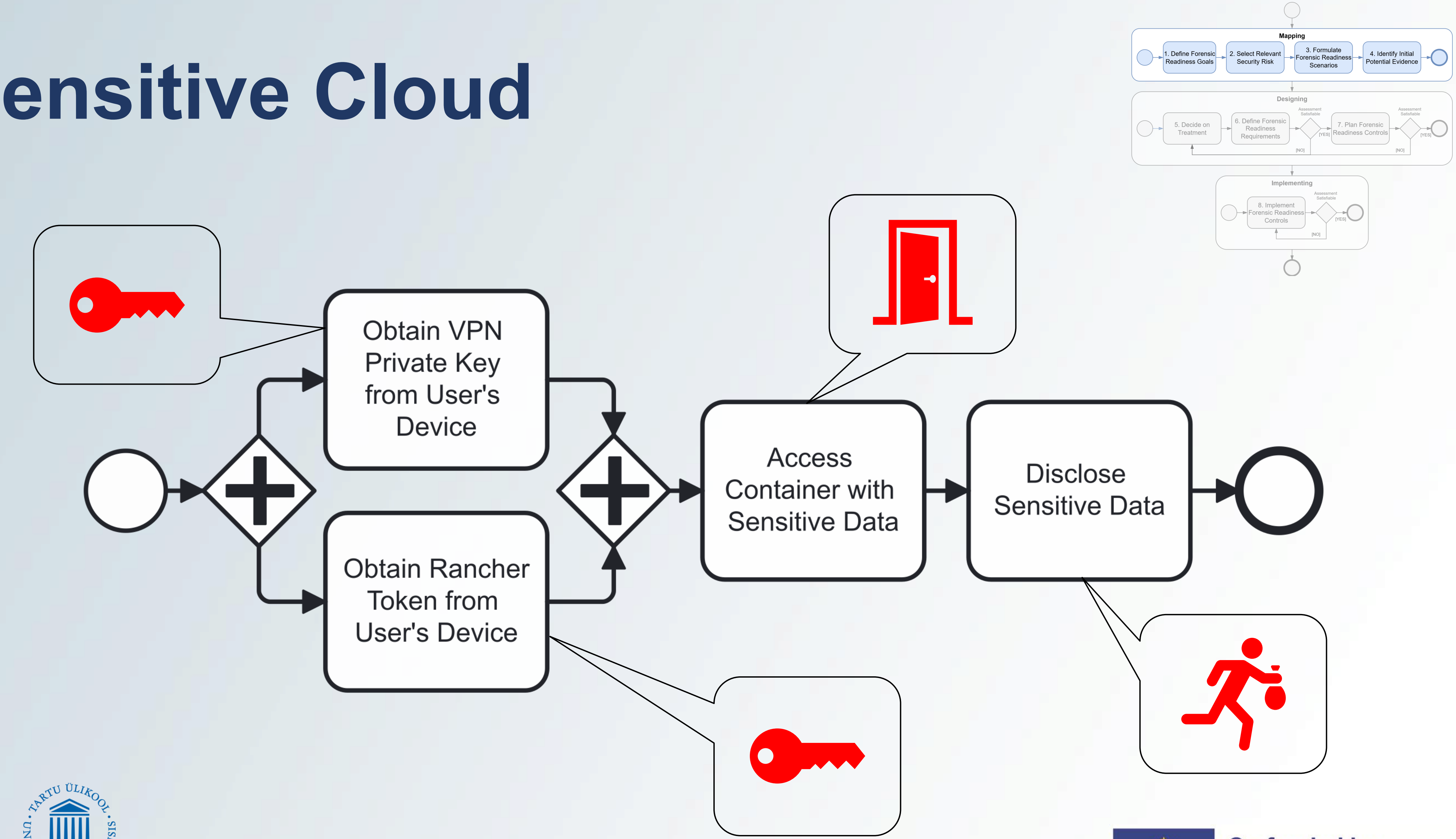

Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]


Obtain VPN Private Key from User's Device
Obtain Rancher Token from User's Device
Access Container with Sensitive Data
Disclose Sensitive Data

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Co-funded by the European Union

Sensitive Cloud

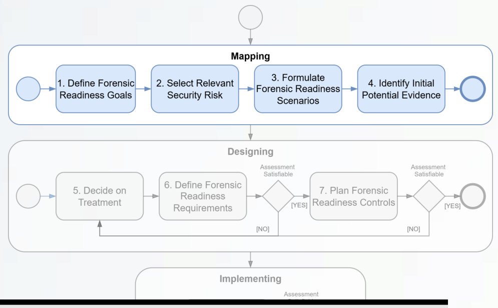

Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Obtain VPN Private Key from User's Device
Obtain Rancher Token from User's Device
Access Container with Sensitive Data
Disclose Sensitive Data

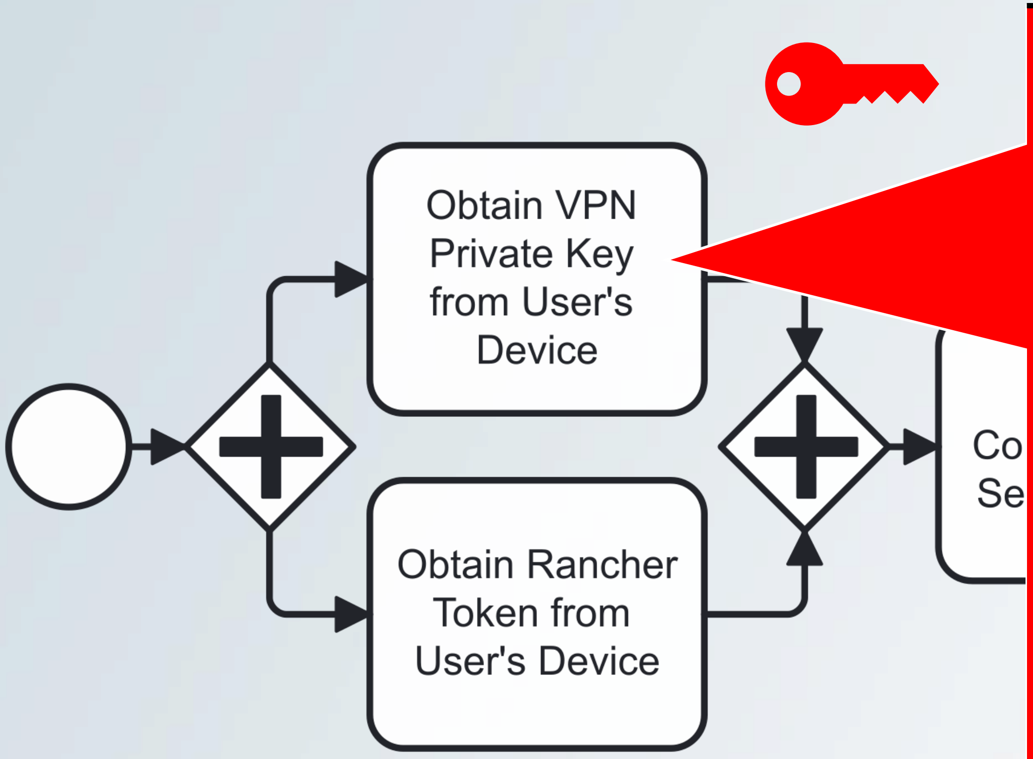
CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European Union

Sensitive Cloud


Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
Assessment


Obtain VPN Private Key from User's Device
Obtain Rancher Token from User's Device
Co
Se

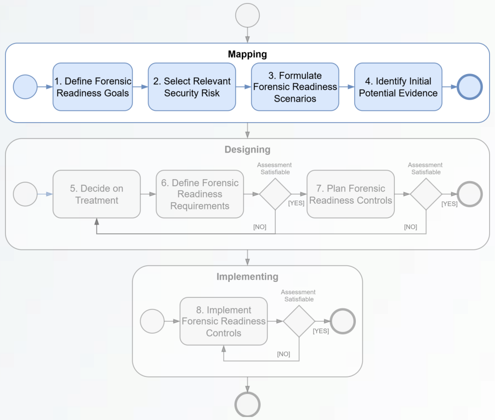
Vulnerability	1. VPN key is unprotected on User Device 2. VPN key is sufficient to access internal network
Threat	An attacker with the capability to access the VPN key on a User Device steals the VPN key and then uses it to access the Internal Network
Impact	1. Loss of User Identity integrity 2. Breach of Perimeter Access Process
Goal	Enable investigation of logical perimeter access process breach

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL UNIVERSITAS TARTUENSIS 1632

Co-funded by the European Union

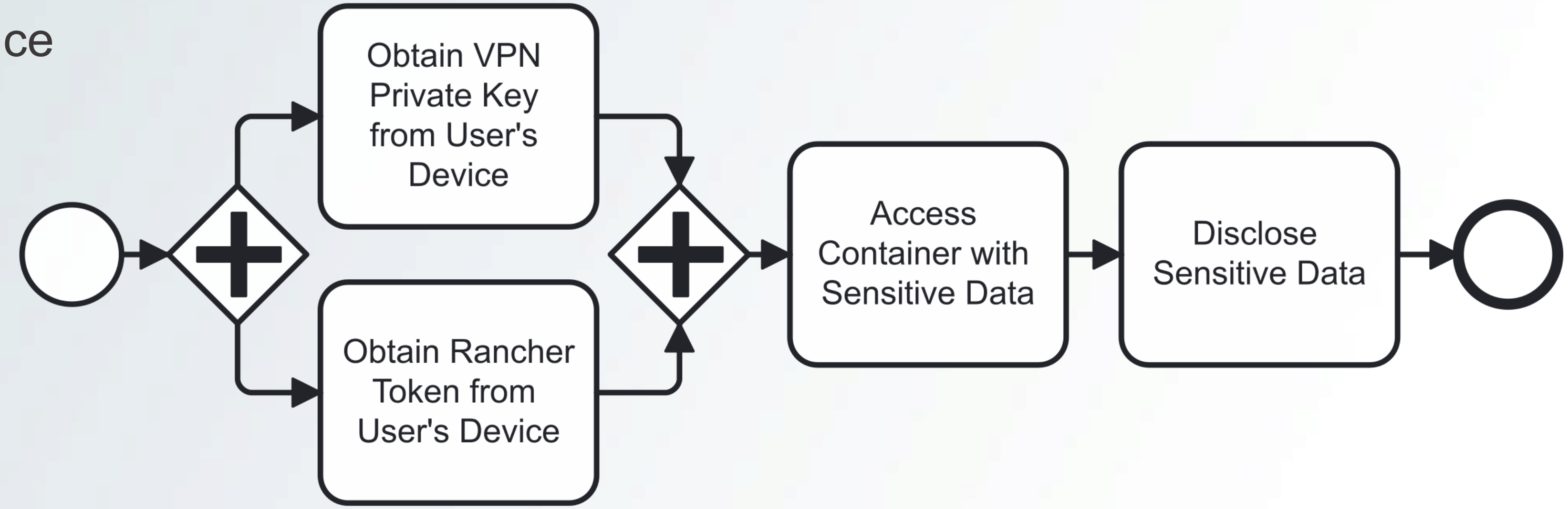
Scenario Modelling


Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

- Capture scenario as a business process

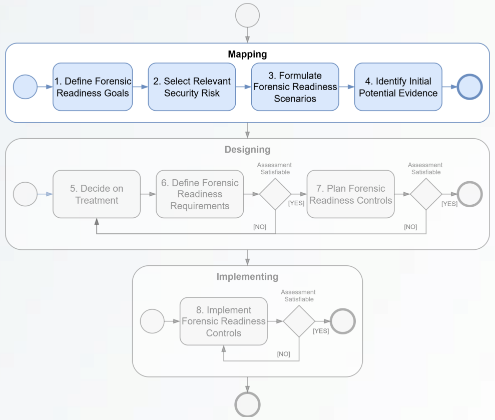
- Mapping phase
  - Enumerating known evidence

- Designing phase
  - Alternatives
  - Analysis
  - FREAS tool


Obtain VPN Private Key from User's Device
Obtain Rancher Token from User's Device
Access Container with Sensitive Data
Disclose Sensitive Data

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

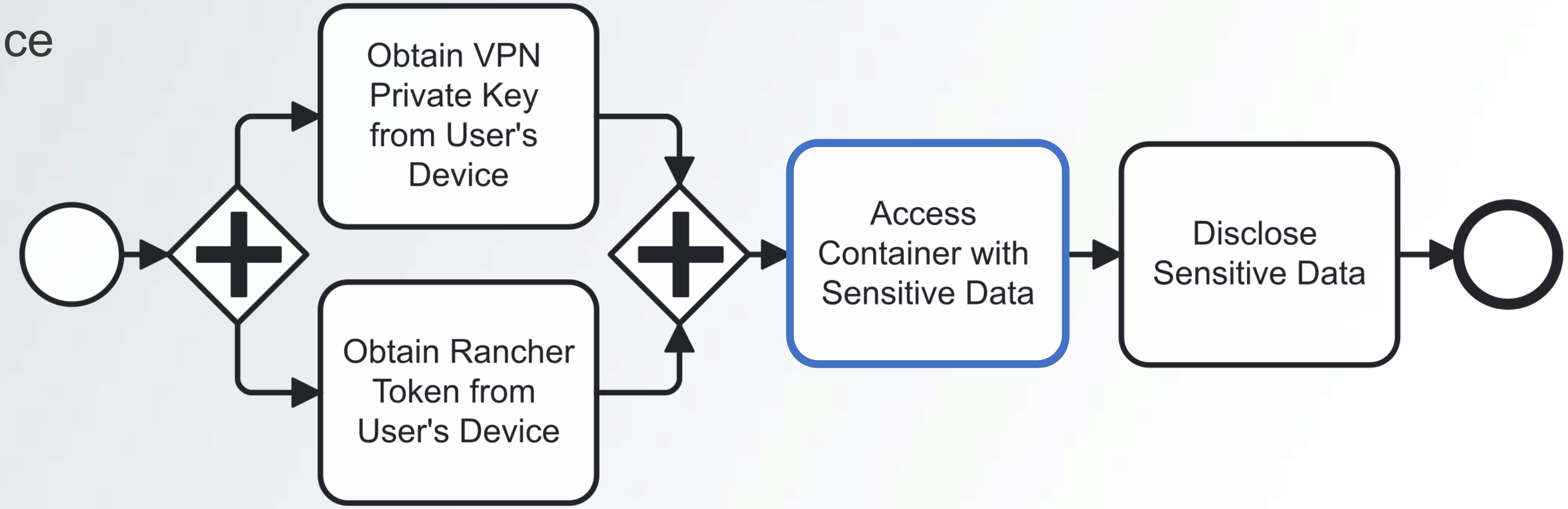
Scenario Modelling


Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

- Capture scenario as a business process

- Mapping phase
  - Enumerating known evidence

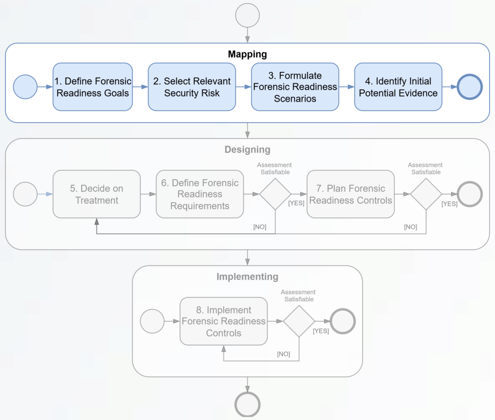
- Designing phase
  - Alternatives
  - Analysis
  - FREAS tool


Obtain VPN Private Key from User's Device
Obtain Rancher Token from User's Device
Access Container with Sensitive Data
Disclose Sensitive Data

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

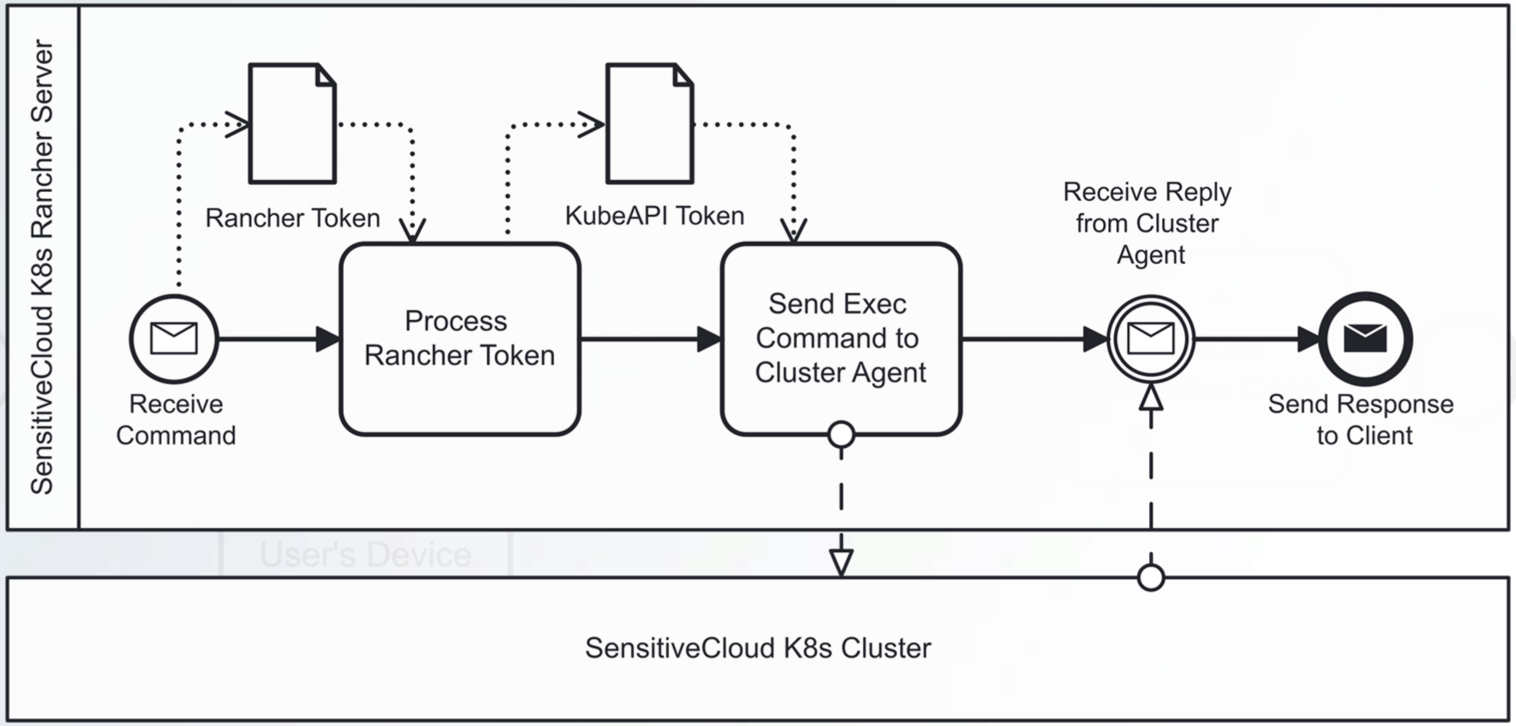
Scenario Modelling


Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

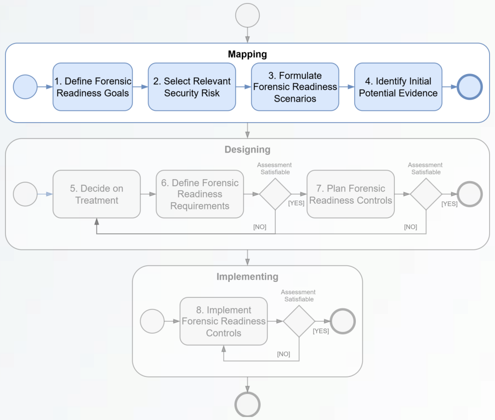
- Capture scenario as a business process

- **Mapping phase**
  - **Enumerating known evidence**

- Designing phase
  - Alternatives
  - Analysis
  - FREAS tool


SensitiveCloud K8s Rancher Server
Rancher Token
KubeAPI Token
Receive Reply from Cluster Agent
Receive Command
Process Rancher Token
Send Exec Command to Cluster Agent
Send Response to Client
SensitiveCloud K8s Cluster

Scenario Modelling

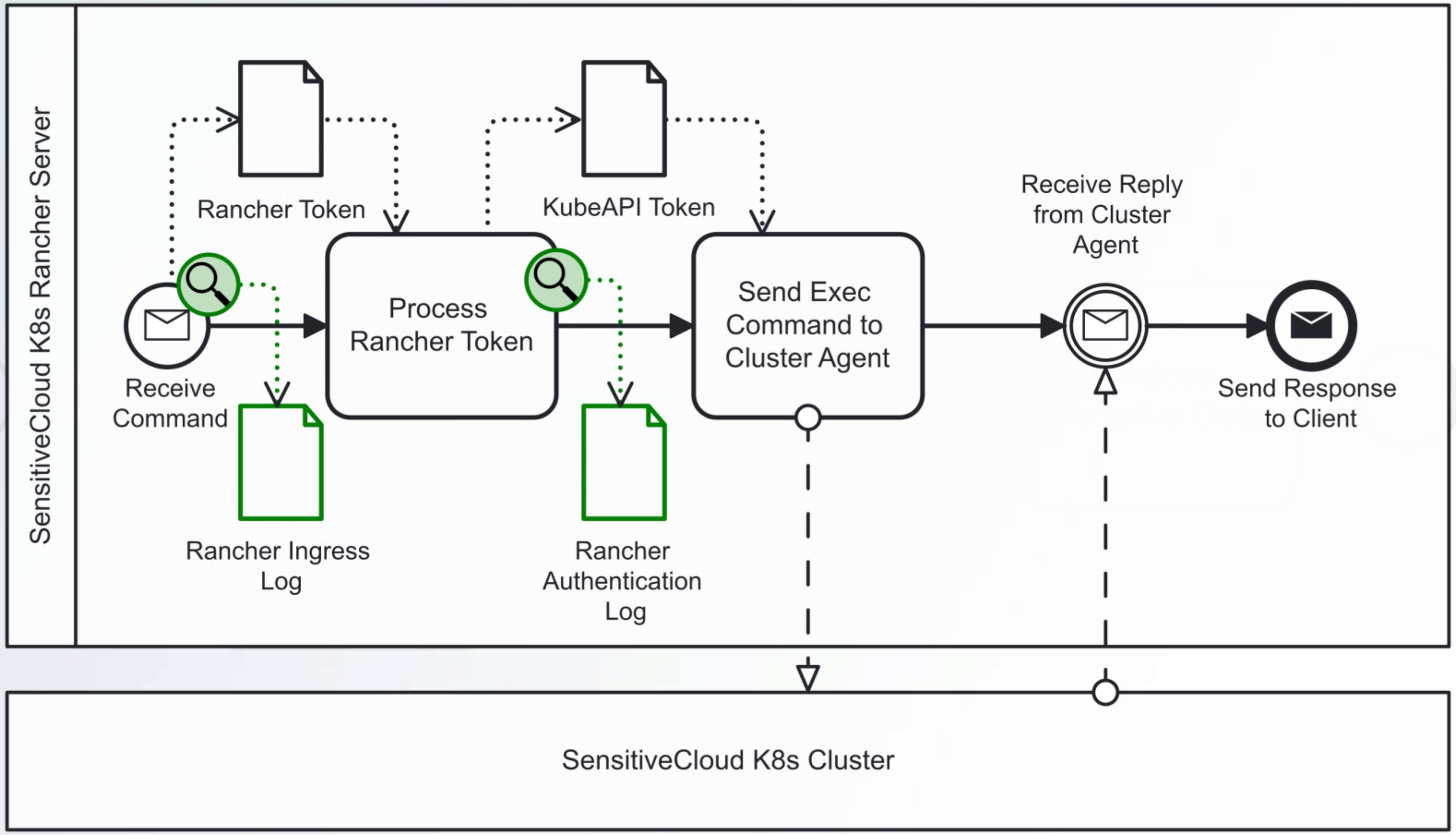


Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

- Capture scenario as a business process

- **Mapping phase**
  - **Enumerating known evidence**

- Designing phase
  - Alternatives
  - Analysis
  - FREAS tool

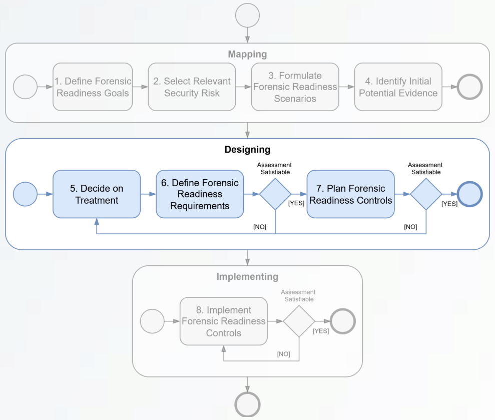


SensitiveCloud K8s Rancher Server
Rancher Token
KubeAPI Token
Receive Reply from Cluster Agent
Receive Command
Process Rancher Token
Send Exec Command to Cluster Agent
Send Response to Client
Rancher Ingress Log
Rancher Authentication Log
SensitiveCloud K8s Cluster

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL UNIVERSITAS TARTUENSIS 1632

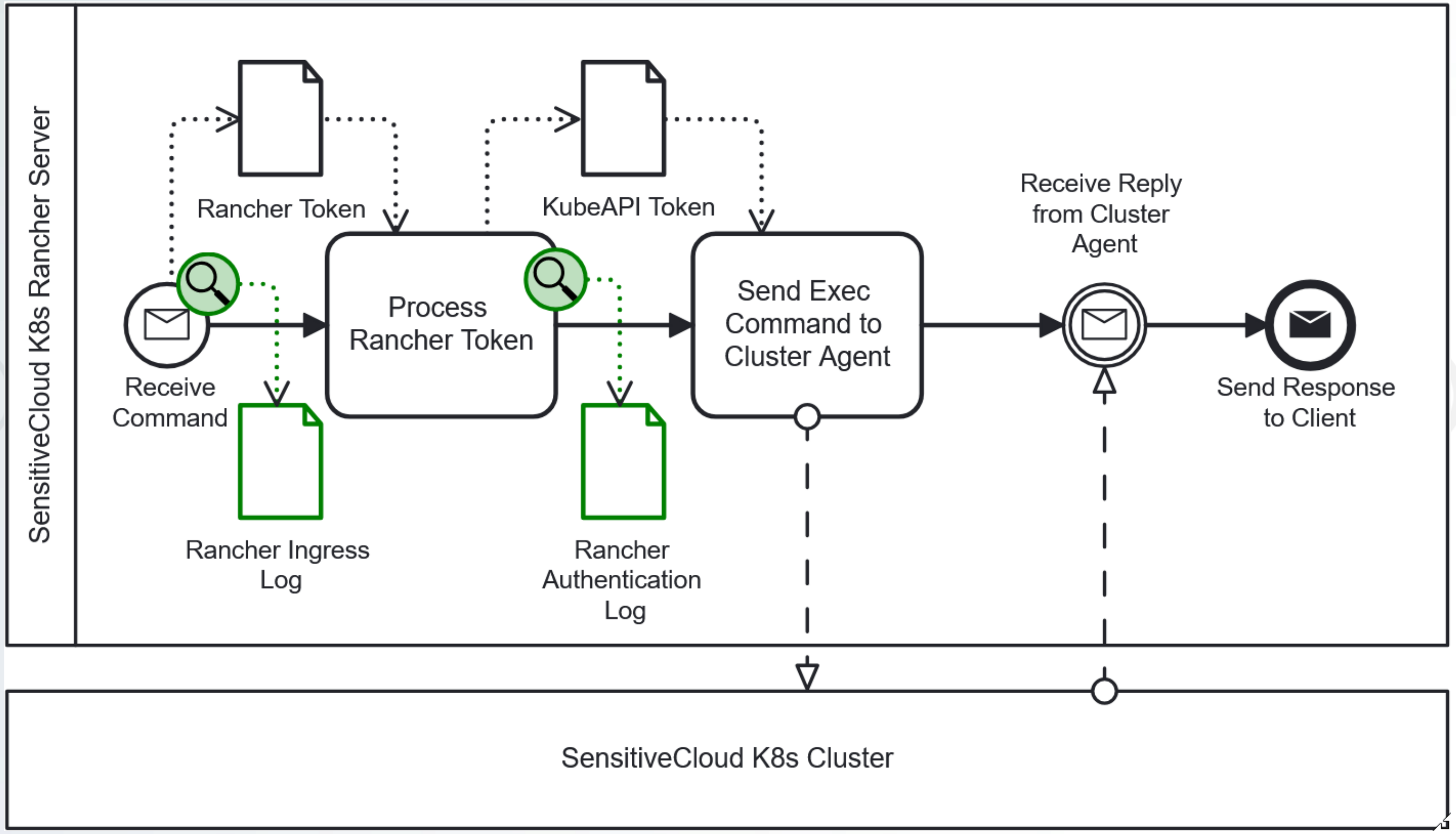
Scenario Modelling


Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

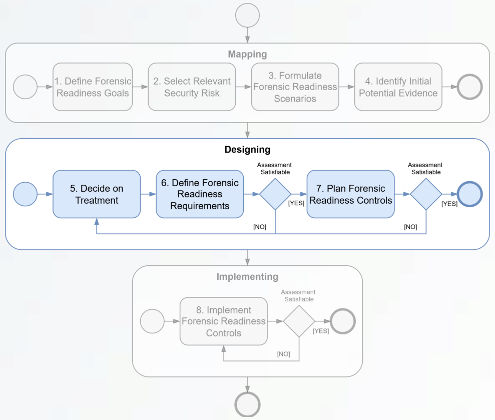
- Capture scenario as a business process

- Mapping phase
  - Enumerating known evidence

- **Designing phase**
  - **Alternatives**
  - **Analysis**
  - **FREAS tool**


SensitiveCloud K8s Rancher Server
Rancher Token
KubeAPI Token
Receive Command
Process Rancher Token
Send Exec Command to Cluster Agent
Receive Reply from Cluster Agent
Send Response to Client
Rancher Ingress Log
Rancher Authentication Log
SensitiveCloud K8s Cluster

Sensitive Cloud


Mapping
1. Define Forensic Readiness Goals
2. Select Relevant Security Risk
3. Formulate Forensic Readiness Scenarios
4. Identify Initial Potential Evidence
Designing
5. Decide on Treatment
6. Define Forensic Readiness Requirements
Assessment Satisfiable
[YES]
[NO]
7. Plan Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]
Implementing
8. Implement Forensic Readiness Controls
Assessment Satisfiable
[YES]
[NO]

- Simulated incident evaluation
  - Simulate attack based on the scenario
  - Activates incident handling plan
- Investigation uncovered serious issues
  - Some avoidable
- Practical complement to ISO/IEC 27k certification

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL · UNIVERSITAS TARTUENSIS · 1632

Co-funded by the European Union

Conclusion

- Forensic readiness is a complement to information security

FR-ISSRM Method

https://frssdesign.github.io/

Tool

https://freas-tools.github.io/wiki/

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

Co-funded by the European Union