MUNI FI

lasaris LAB OF SOFTWARE ARCHITECTURES AND INFORMATION SYSTEMS

MUNI C4E

Aspects of Forensic-Ready Software Systems in Public Service Domain

Lukas Daubner, Tomas Pitner
{daubner,tomp}@mail.muni.cz

Information Technology for Practice 2021
November 18, 2021, Ostrava, Czech Republic

Forensic Readiness

- Systematic, proactive preparation for forensic investigation
  - Maximizing the usefulness of incident evidence data
  - Minimizing the cost of forensics during an incident response
- Approached as a set of general guidelines
  - Collection of evidence
  - Handling of evidence
  - Presentation of evidence
  - Staff training
  - Escalation policies

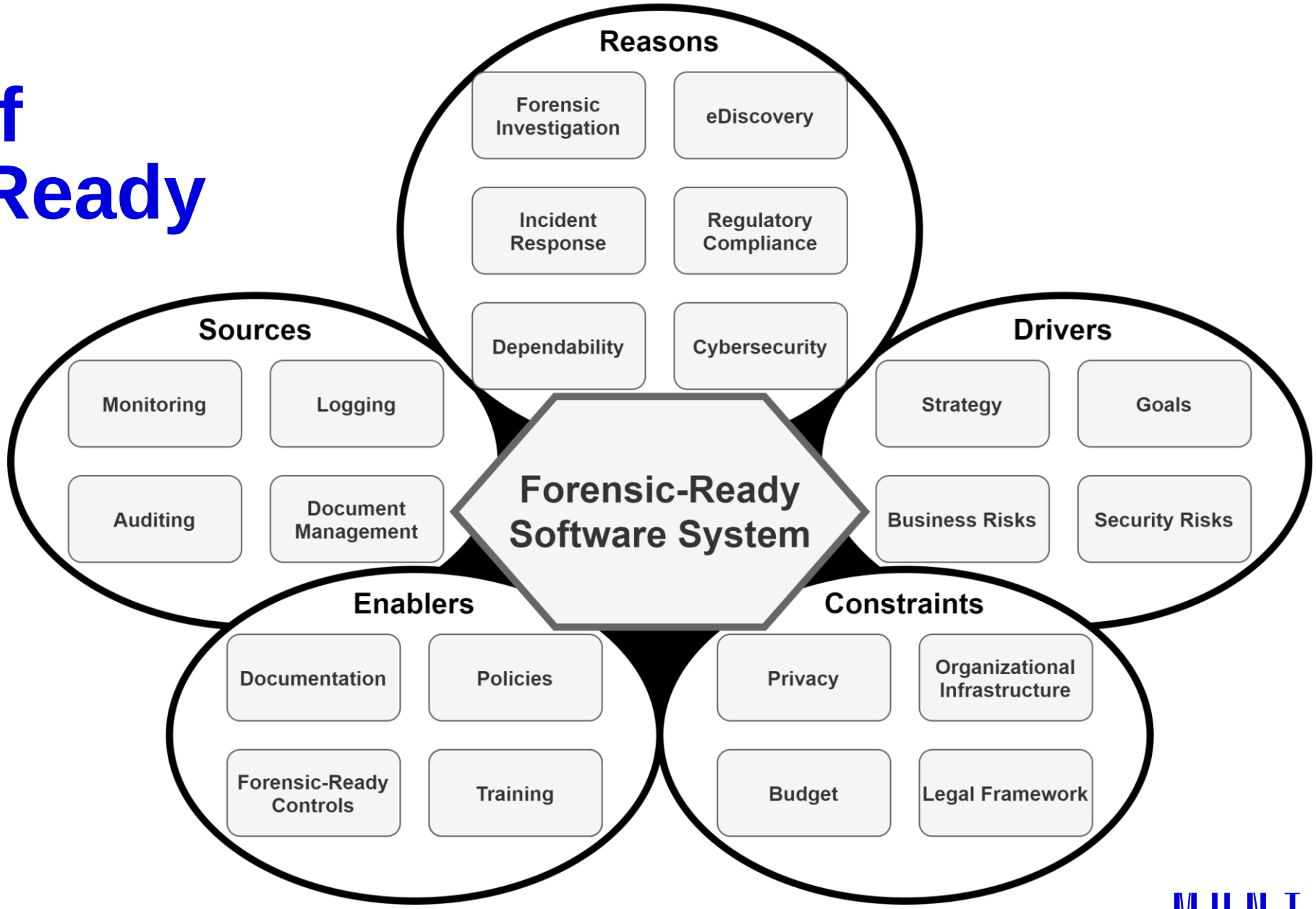
Why Forensic Readiness?

- Digital forensic investigation is:
  - Laborious
  - Costly
  - Time-consuming
  - Delicate
- Success is never assured
  - Data might be unavailable, corrupted, or tampered
  - Error in evidence handling jeopardies the process
- Data might me misleading

Forensic-Ready Software Systems

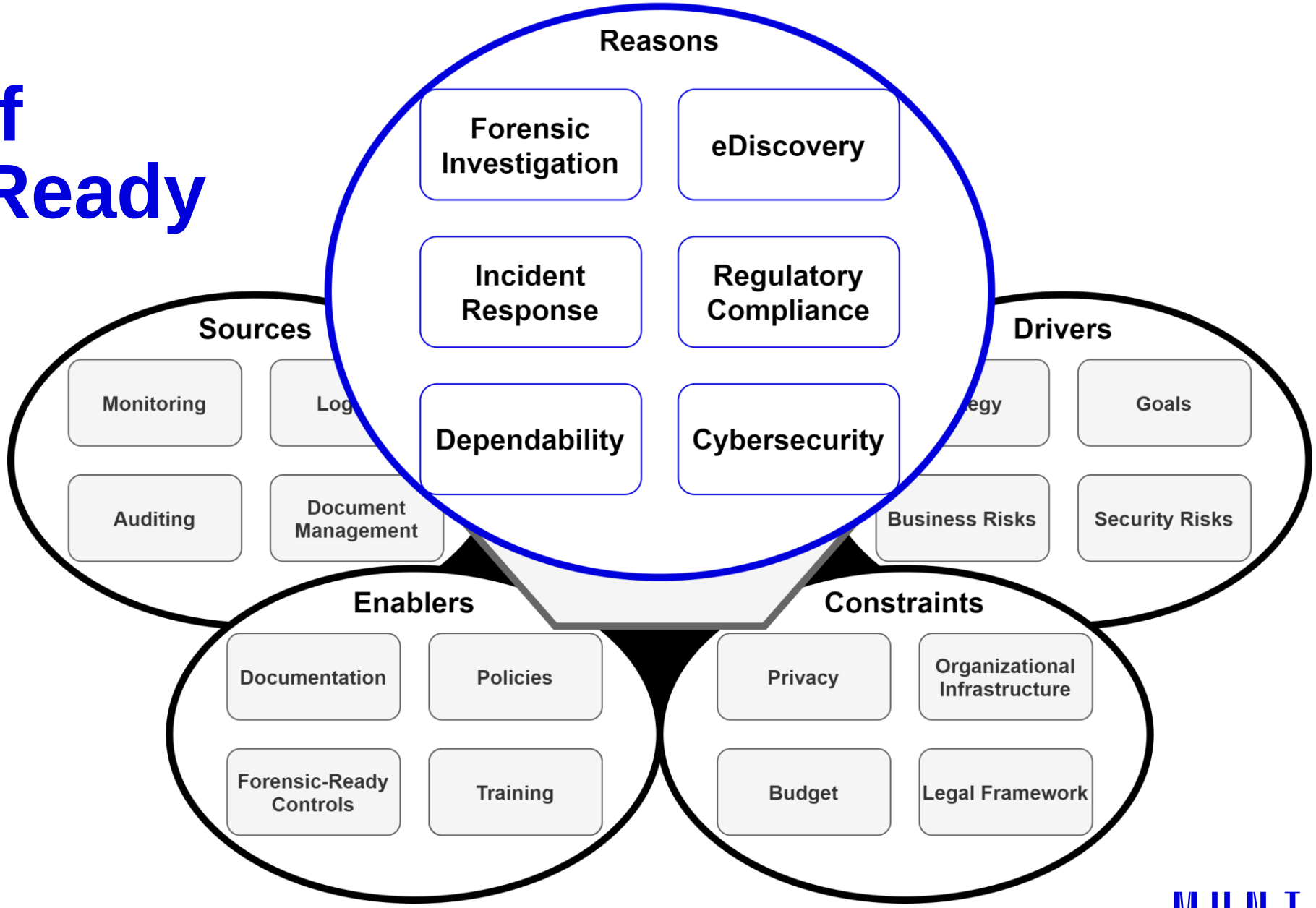
- Software system are prepared during development
  - A.k.a. forensic-by-design
- Capable of:
  - Conducting digital forensic processes in a forensically sound way
  - Producing forensically sound evidence
- High-level non-functional requirement

Aspects of Forensic-Ready Software Systems



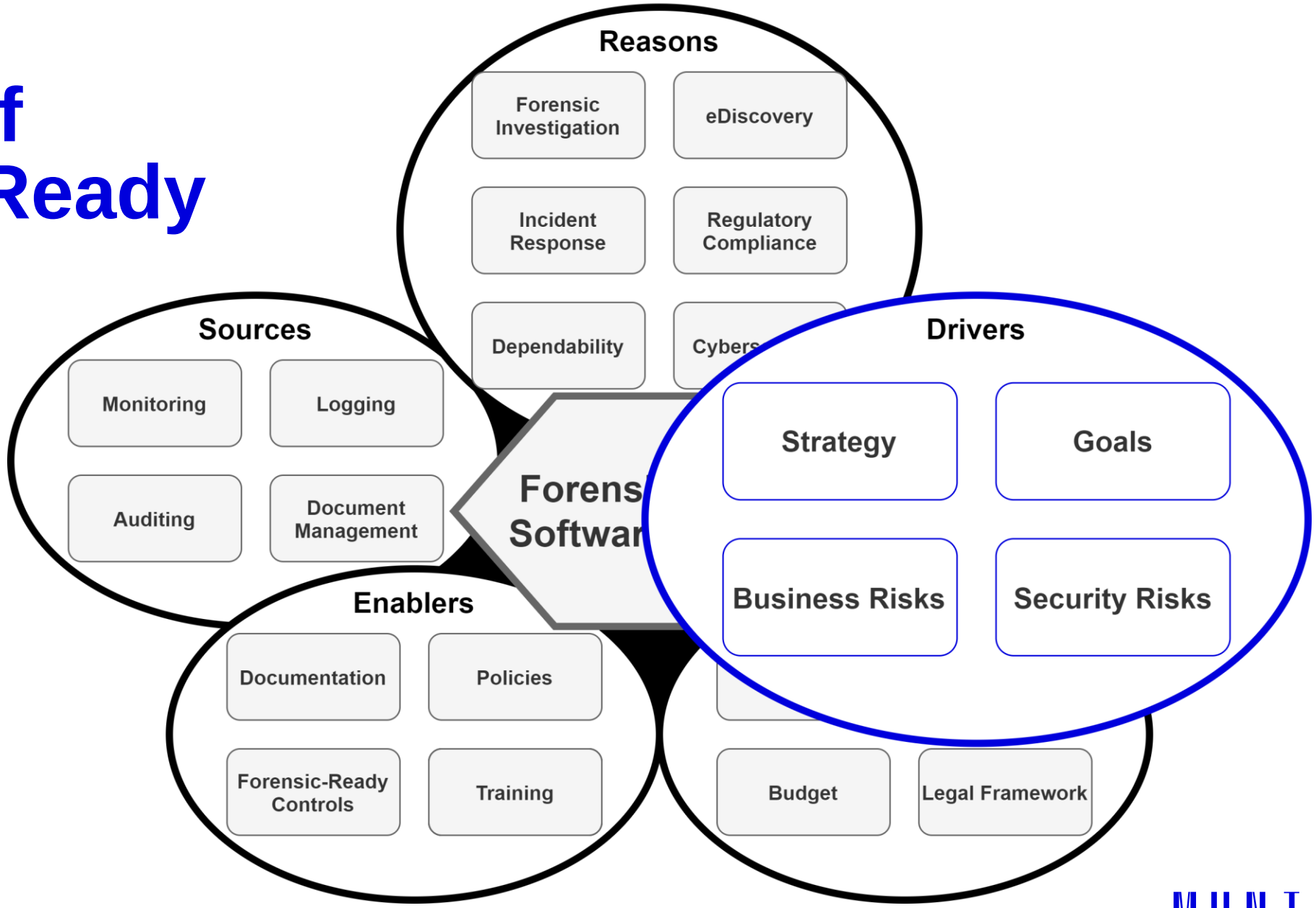
MUNI FI

Aspects of Forensic-Ready Software Systems



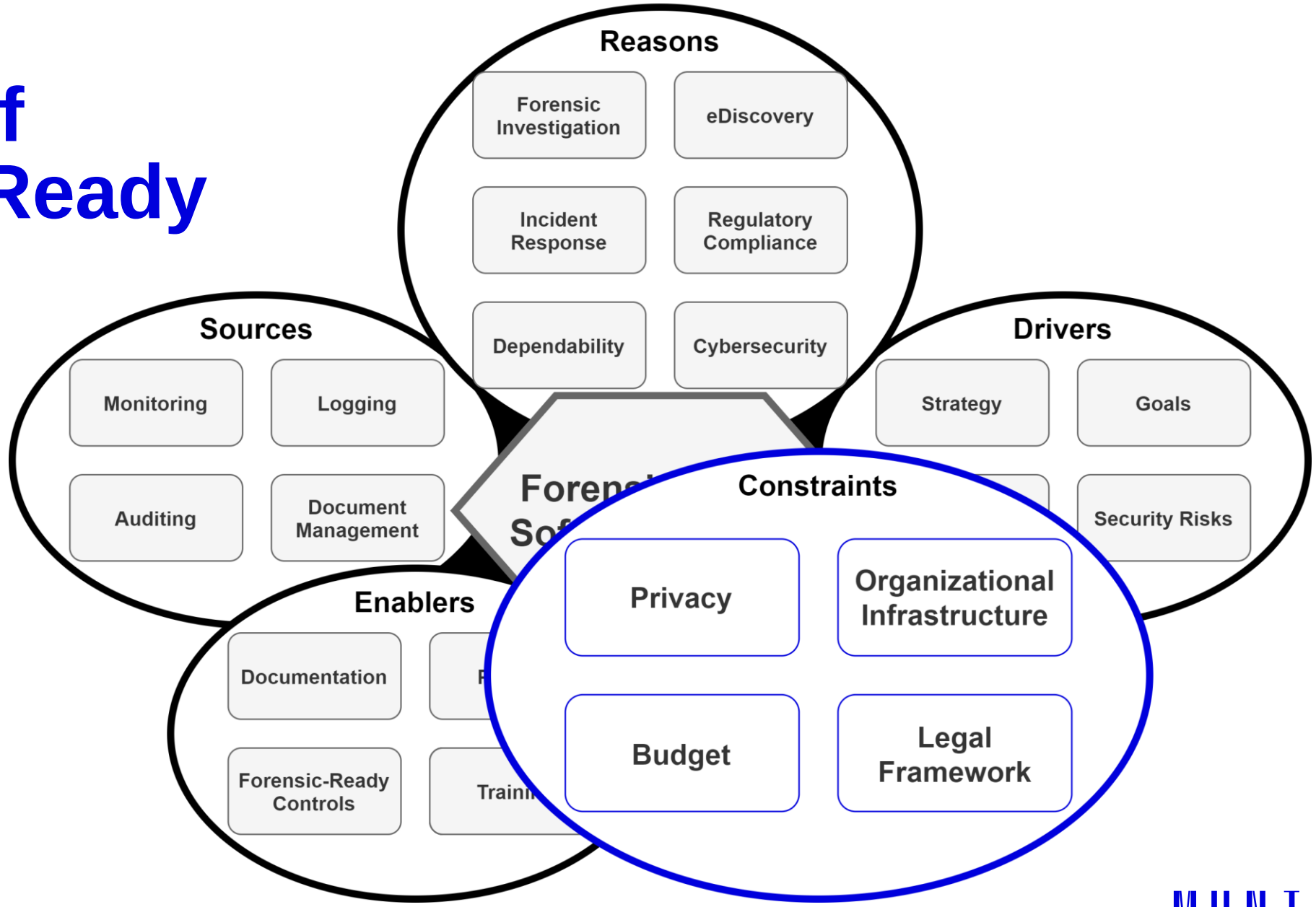
MUNI FI

Aspects of Forensic-Ready Software Systems



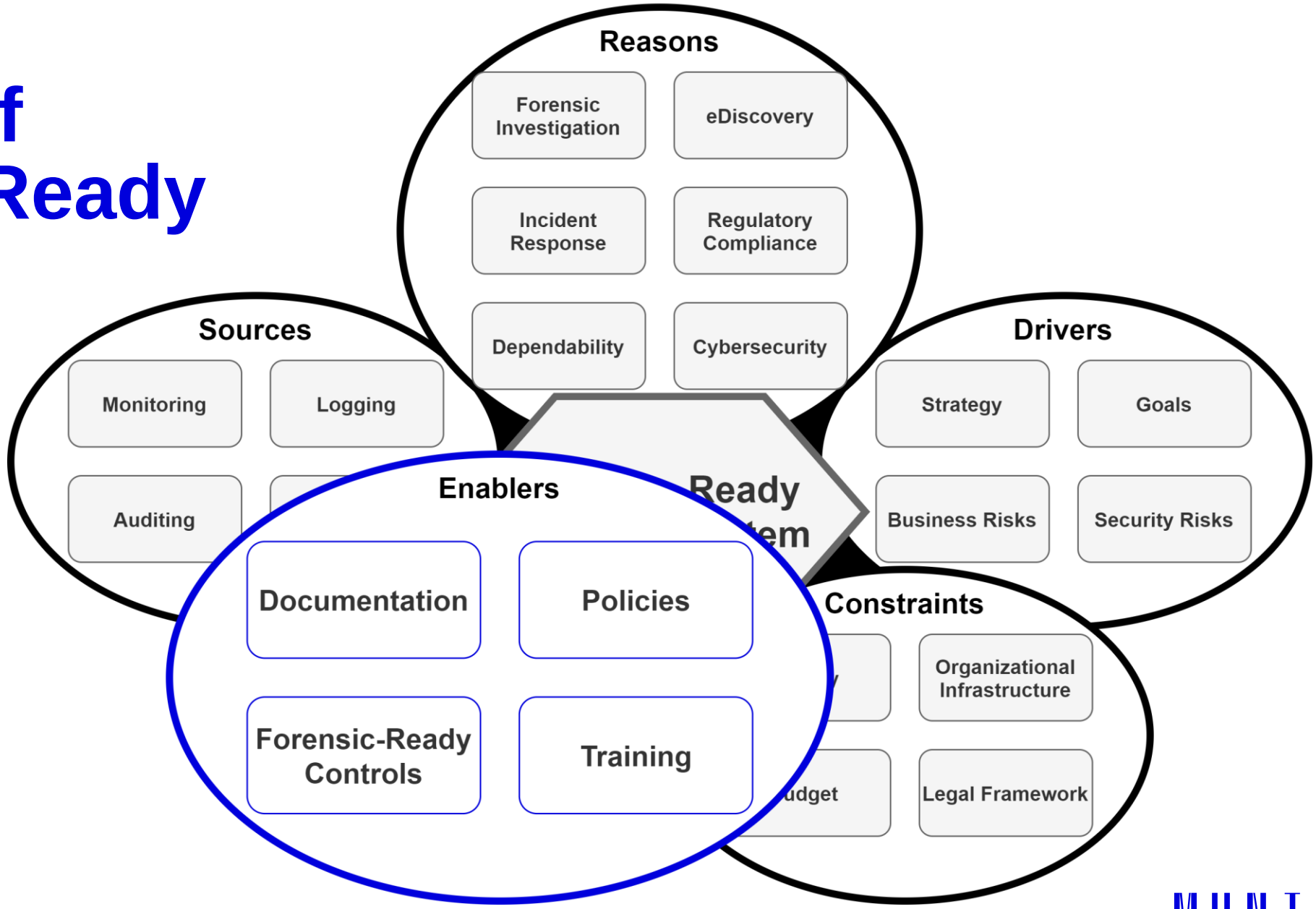
MUNI FI

Aspects of Forensic-Ready Software Systems



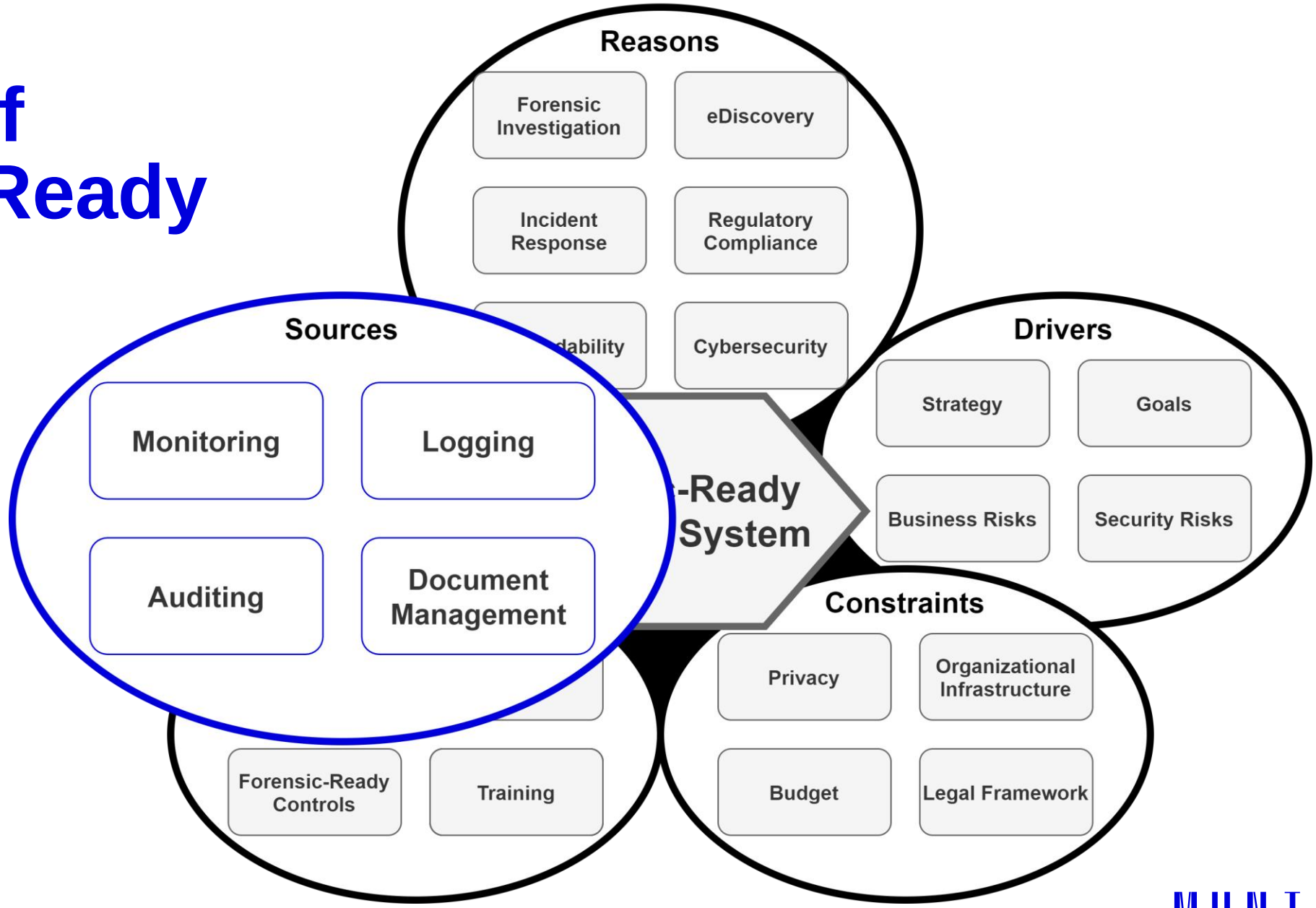
MUNI FI

Aspects of Forensic-Ready Software Systems

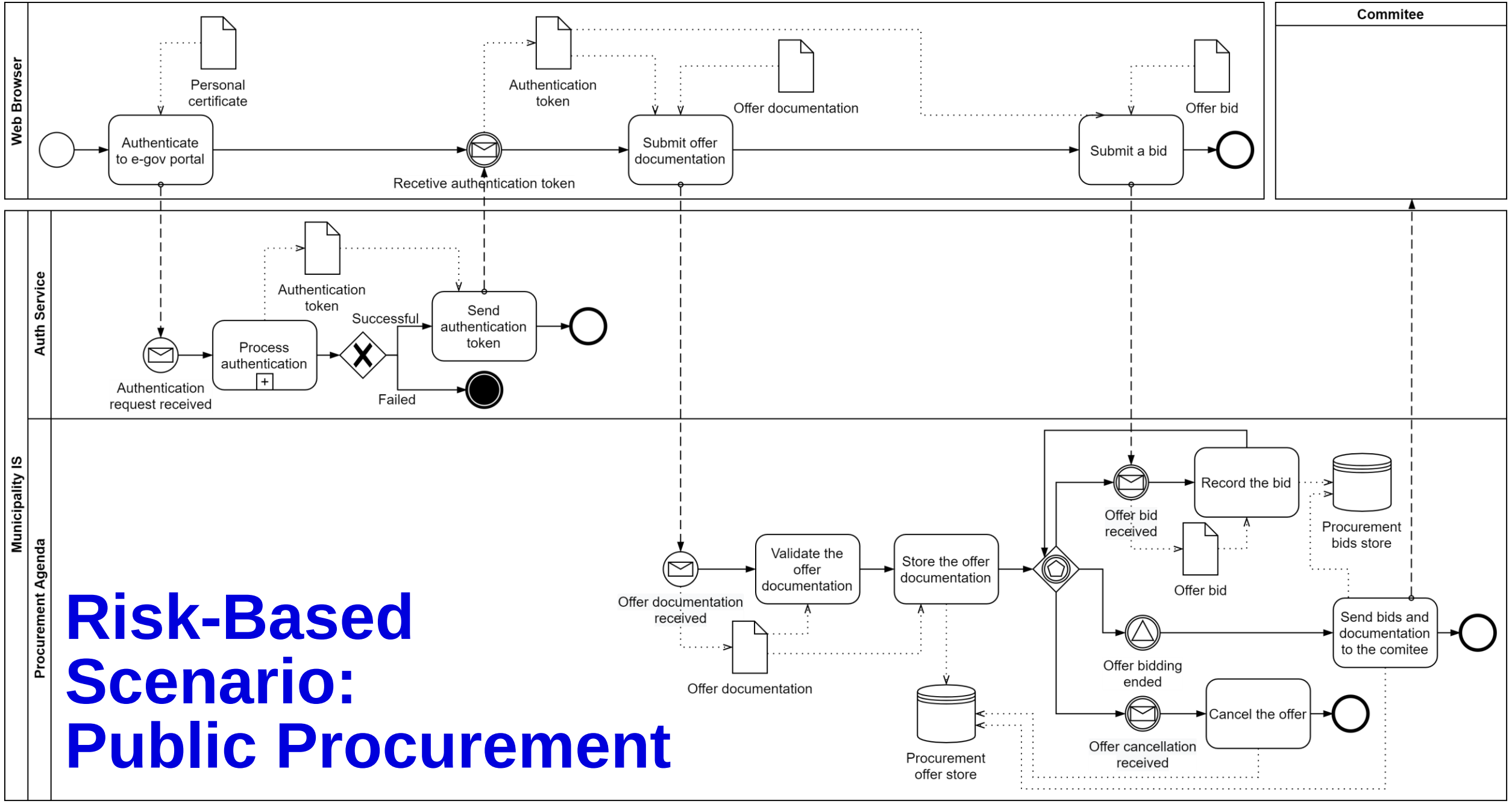


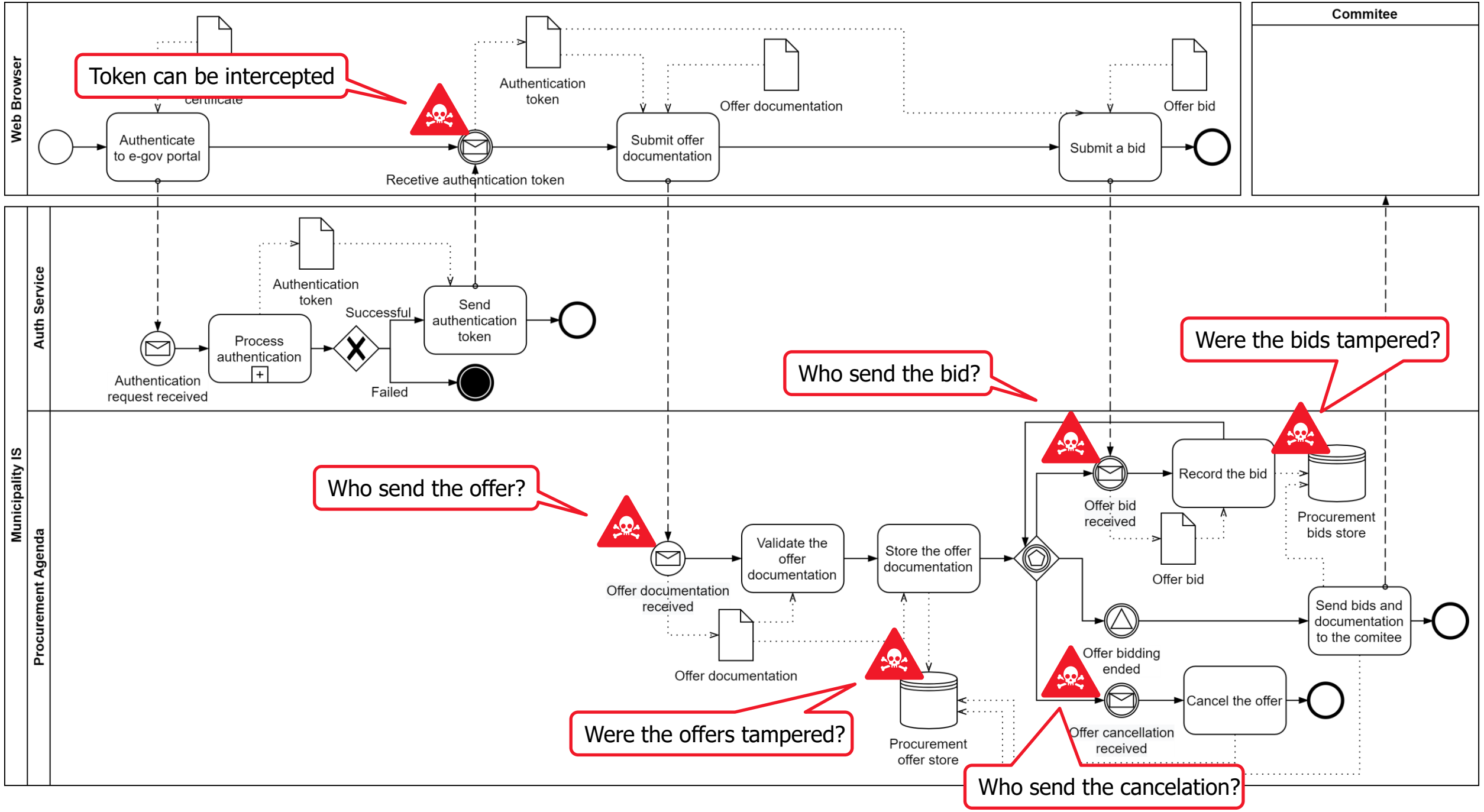
MUNI FI

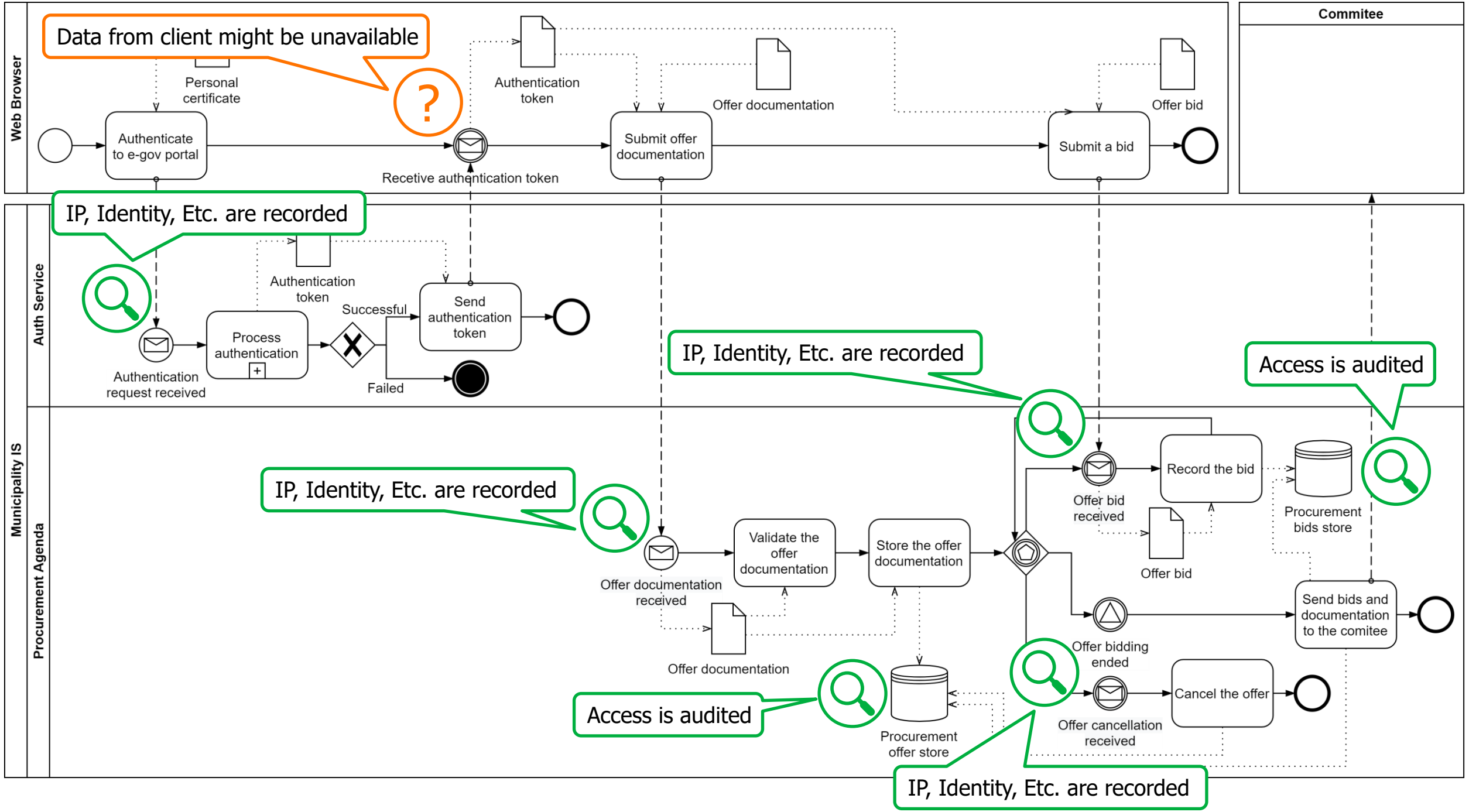
Aspects of Forensic-Ready Software Systems

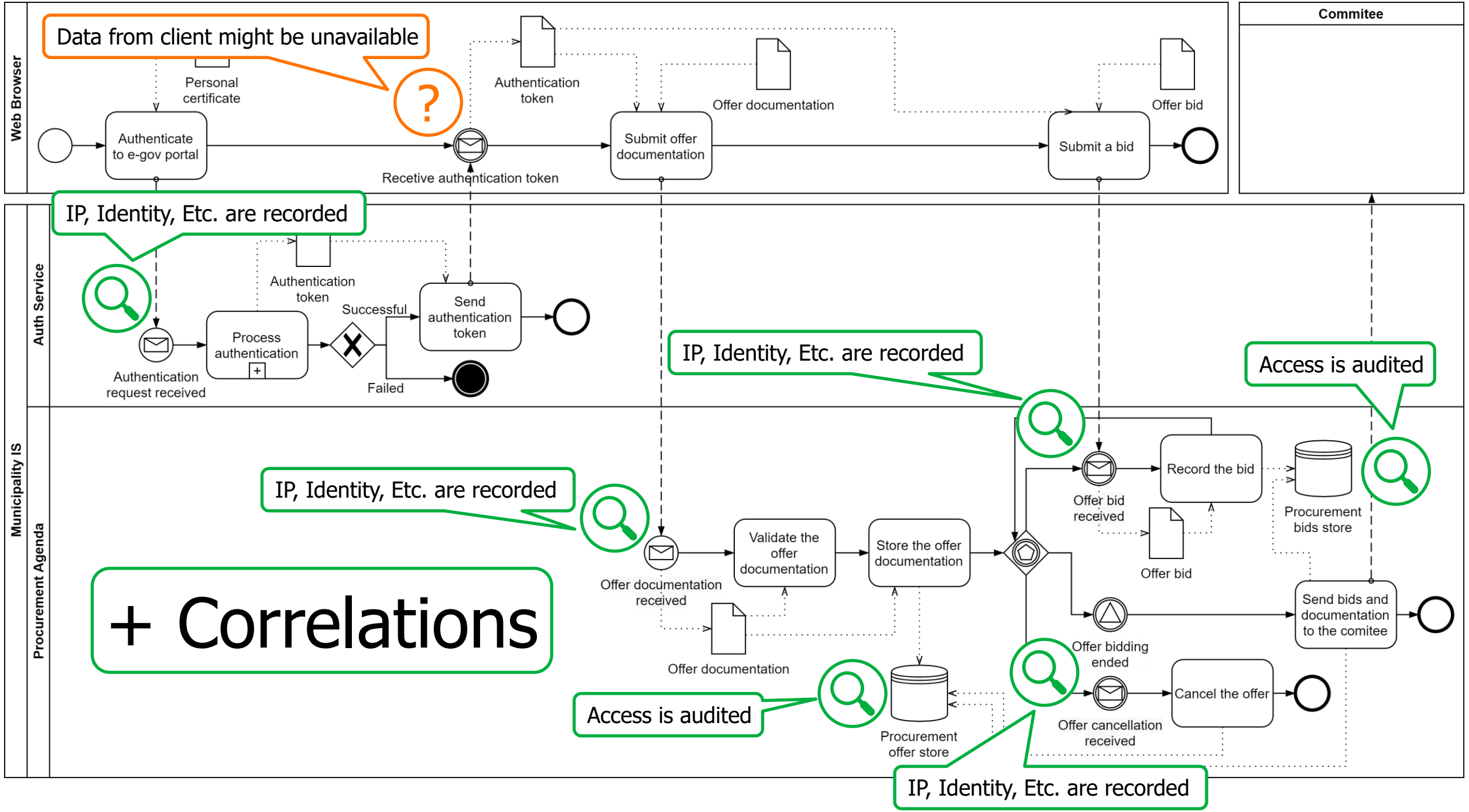


MUNI FI


Web Browser
Commitee
Personal certificate
Authentication token
Offer documentation
Offer bid
Authenticate to e-gov portal
Recetive authentication token
Submit offer documentation
Submit a bid
Municipality IS
Auth Service
Procurement Agenda
Authentication token
Successful
Send authentication token
Process authentication
Authentication request received
Failed
Offer documentation received
Validate the offer documentation
Store the offer documentation
Offer documentation
Procurement offer store
Offer bid received
Record the bid
Procurement bids store
Offer bid
Offer bidding ended
Send bids and documentation to the comitee
Offer cancellation received
Cancel the offer
Risk-Based Scenario: Public Procurement


Web Browser
Commitee
Token can be intercepted
Authentication token
Offer documentation
Offer bid
Authenticate to e-gov portal
Recetive authentication token
Submit offer documentation
Submit a bid
Municipality IS
Auth Service
Procurement Agenda
Authentication token
Successful
Send authentication token
Process authentication
Authentication request received
Failed
Were the bids tampered?
Who send the bid?
Who send the offer?
Record the bid
Offer bid received
Procurement bids store
Offer bid
Validate the offer documentation
Store the offer documentation
Offer documentation received
Offer documentation
Send bids and documentation to the comitee
Offer bidding ended
Were the offers tampered?
Procurement offer store
Cancel the offer
Offer cancellation received
Who send the cancelation?


Web Browser
Data from client might be unavailable
?
Personal certificate
Authentication token
Offer documentation
Offer bid
Authenticate to e-gov portal
Recetive authentication token
Submit offer documentation
Submit a bid
Commitee
Municipality IS
Auth Service
IP, Identity, Etc. are recorded
Authentication token
Successful
Send authentication token
Process authentication
Authentication request received
Failed
IP, Identity, Etc. are recorded
Access is audited
Procurement Agenda
IP, Identity, Etc. are recorded
Record the bid
Offer bid received
Procurement bids store
Offer bid
Offer documentation received
Validate the offer documentation
Store the offer documentation
Send bids and documentation to the comitee
Offer bidding ended
Offer documentation
Access is audited
Procurement offer store
Cancel the offer
Offer cancellation received
IP, Identity, Etc. are recorded


Web Browser
Data from client might be unavailable
?
Personal certificate
Authenticate to e-gov portal
Authentication token
Recetive authentication token
Offer documentation
Submit offer documentation
Offer bid
Submit a bid
Commitee
Municipality IS
Auth Service
IP, Identity, Etc. are recorded
Authentication token
Successful
Send authentication token
Process authentication
Authentication request received
Failed
Procurement Agenda
IP, Identity, Etc. are recorded
IP, Identity, Etc. are recorded
Access is audited
Record the bid
Offer bid received
Procurement bids store
Offer bid
Validate the offer documentation
Store the offer documentation
Offer documentation received
Offer documentation
Send bids and documentation to the comitee
Offer bidding ended
Cancel the offer
Offer cancellation received
Access is audited
Procurement offer store
IP, Identity, Etc. are recorded
+ Correlations

Conclusion

MUNI C4E

- Forensic-ready software systems are prepared for investigations
  - Their aspects are cross-cutting across multiple fields
- Various parts are already tackled, but it might not be sufficient
  - Is it securely stored?
  - What does it say?
  - Are we covered?

EUROPEAN UNION
European Structural and Investment Funds
Operational Programme Research,
Development and Education

MINISTRY OF EDUCATION,
YOUTH AND SPORTS

MUNI FI