A Model of Qualitative Factors in Forensic-Ready Software Systems

Lukas Daubner, Raimundas Matulevičius, Barbora Buhnova

Research Challenges in Information Science (RCIS) 2023

Corfu, May 23-26, 2023

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

Forensic-Ready Software Systems

- Preparation for an incident investigation
  - Proactively collect potential digital evidence
  - Soundly conduct forensic processes

- Builds on (security) risk management
  - We know the risks
  - We set the investigation goals – What we might need to know
  - We formulate the scenarios – How is the goal addressed, given the risk

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

Forensic-Ready Software Systems

- What should be implemented?
- How to fulfil the goal?
- Is it implemented correctly?
- Is it enough?
- Are there any alternatives?
- Is it really what we want?

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

MUNI
C4E

Co-funded by the European Union

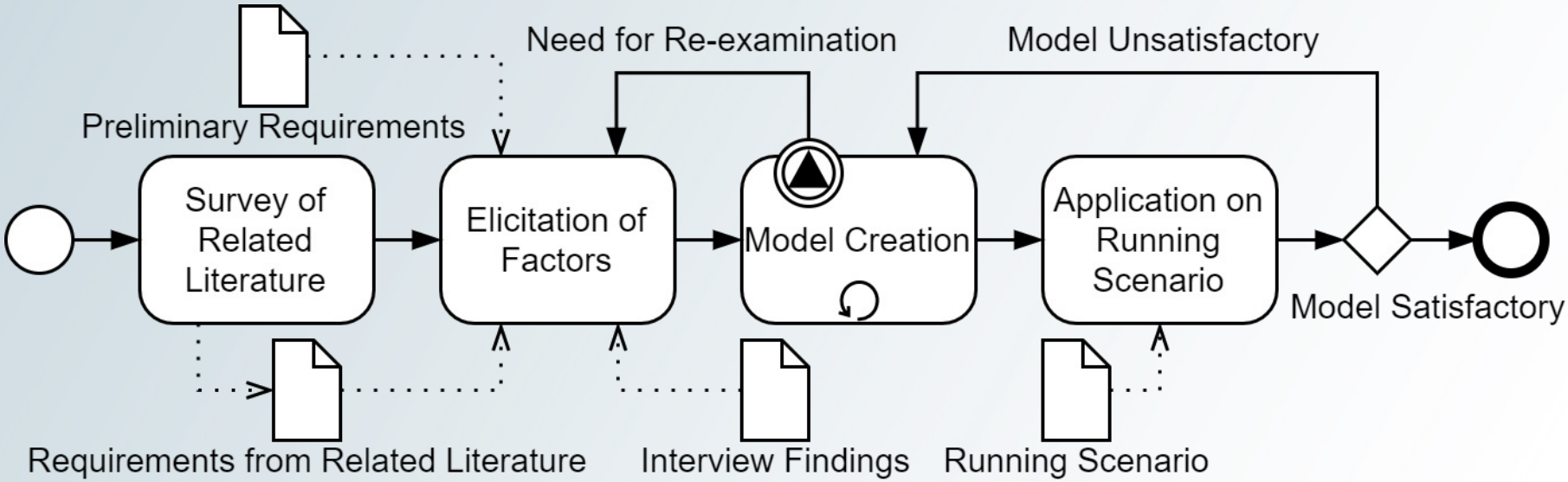
Research Questions

- What are the factors that form the forensic readiness requirements?

- How can the factors be manifested as a concrete requirement?

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL 1632 UNIVERSITAS TARTUENSIS
MUNI C4E
Co-funded by the European Union

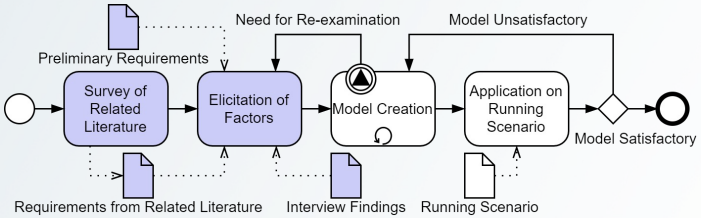
Research Method



CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632
MUNI
C4E
Co-funded by the European Union

Elicitation of Factors

Preliminary Requirements

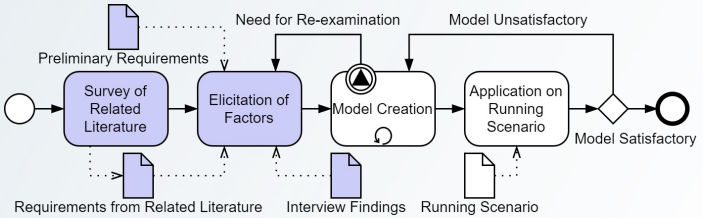


Availability	• Evidence is preserved and retrievable
Relevance	• Evidence is relevant to considered scenarios
Minimality	• Unnecessary evidence is not preserved
Linkability	• Evidence can be linked with other pieces
Completeness	• Evidence is sufficient to satisfy/refute a hypothesis
Non-Repudiation (Admissibility)	• Evidence integrity and authenticity are ensured
Data Provenance	• Evidence handling is recorded
Legal Compliance	• Compliant with laws and regulations

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL UNIVERSITAS TARTUENSIS 1632
MUNI C4E
Co-funded by the European Union

Elicitation of Factors

Interview Findings



"It's not just about maintaining logs about what comes in or out, but about **maintaining logs about what's going on**."

"...if it (data) would be structured, if there would be **some data dictionary, some documentation,** then it could be approached more programmatically, meaning data processing."

"I would like to have a way to **know who was there at the given time** or which user performed the action."

"Ensuring the **data is valid and accurate**, tamper-evident, calibrated, tested, if you like."

"...also, for the certification of common systems ... there can be a requirement for a **generation of reliable metadata**."

"Lots of observations are just an estimation of something happening. ... and there should be an **additional source which would support or refute it**"

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

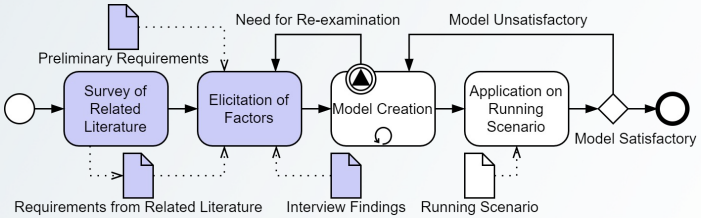
TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

MUNI
C4E

Co-funded by the European Union

Elicitation of Factors

Requirements from Literature



Verifying that **evidential data is created** within a (system) and that this evidential data satisfies the various **business scenarios** that could require digital evidence.
[Grispos at el., 2017]

An **audit trail** or other record of all processes applied to computer based electronic evidence should be created and preserved. An independent third party should be able to examine those processes and achieve the same result.
[CESG, 2015]

When designing forensic strategies, it's important to consider international and local **legal and regulatory** requirements, because different national laws and regulations might have different evidence requirements.
[Ab Rahman at el., 2016]

The various logs may each contain indications of the same event or activity. **Duplication** may provide a form of **corroboration** if, for example, independent monitoring detects similar activity or independent confirmation of the involvement of a suspect.
[Rowlingson, 2004]

Have all **errors** been reasonably identified and satisfactorily explained so as to remove any doubt over the reliability of the evidence.
[McKemmish, 2008]

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

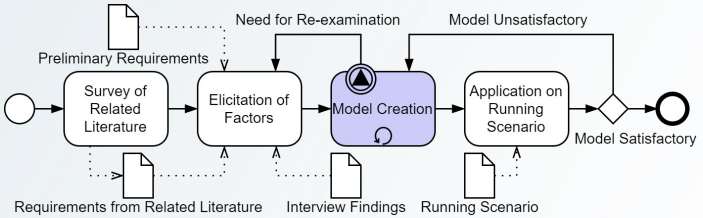
TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

MUNI
C4E

Co-funded by the European Union

Model Creation

Forensic Readiness Requitements



- From forensic-ready risk management we know:
  - Goals of forensic readiness – Why do we want it
  - Scenarios – What do we want to protect/investigate
  - Treatments – What do we want to enhance

- Requirements
  - What do we want to enhance?
  - When are we done?
  - How to verify their implementation?

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

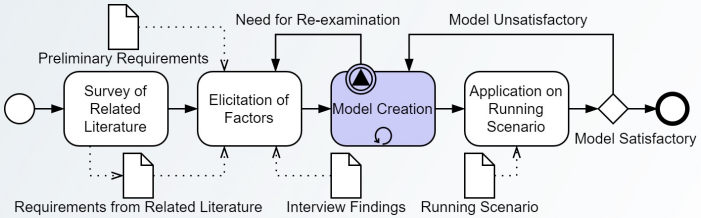
TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

MUNI
C4E

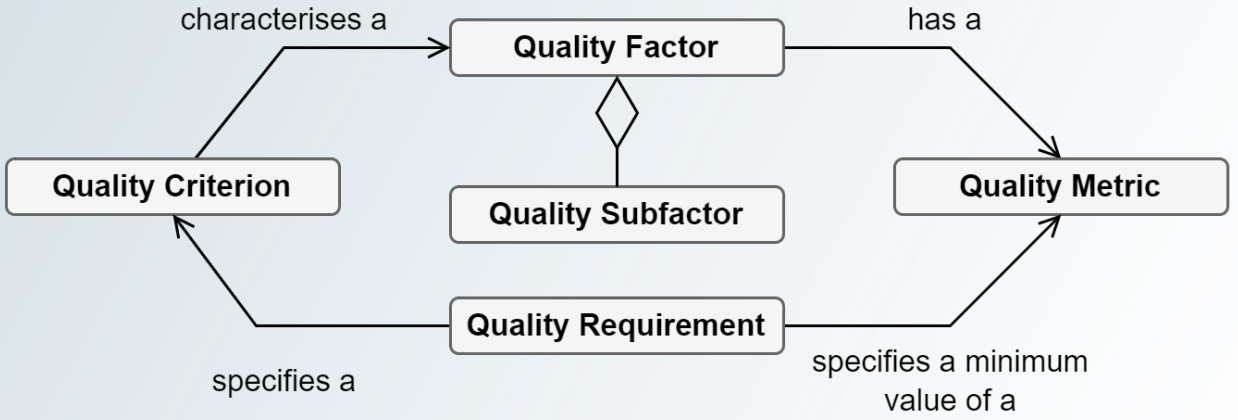
Co-funded by the European Union

Model Creation

Forensic Readiness as Software Quality



- It is all about the quality
  - A quality requirement specifies a minimum amount of a quality factor [Firesmith, 2003]
- Making the implementation verifiable



CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

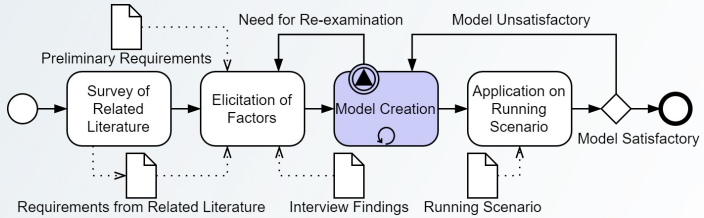
TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

MUNI
C4E

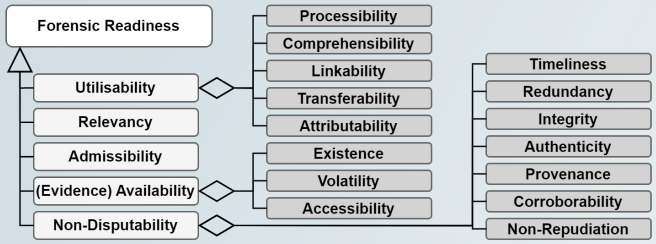
Co-funded by the European Union

Model Creation

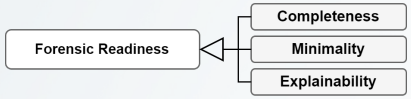
Forensic Readiness Qualitative Factors



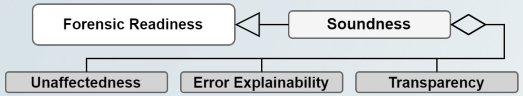
Evidence Factors



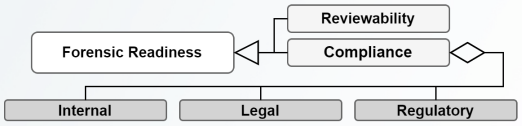
Scenario Factors



Process Factors



Cross-Cutting Factors



CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

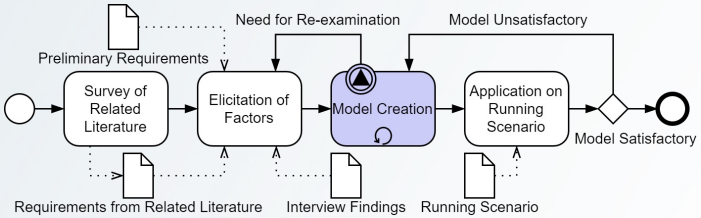
TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

MUNI
C4E

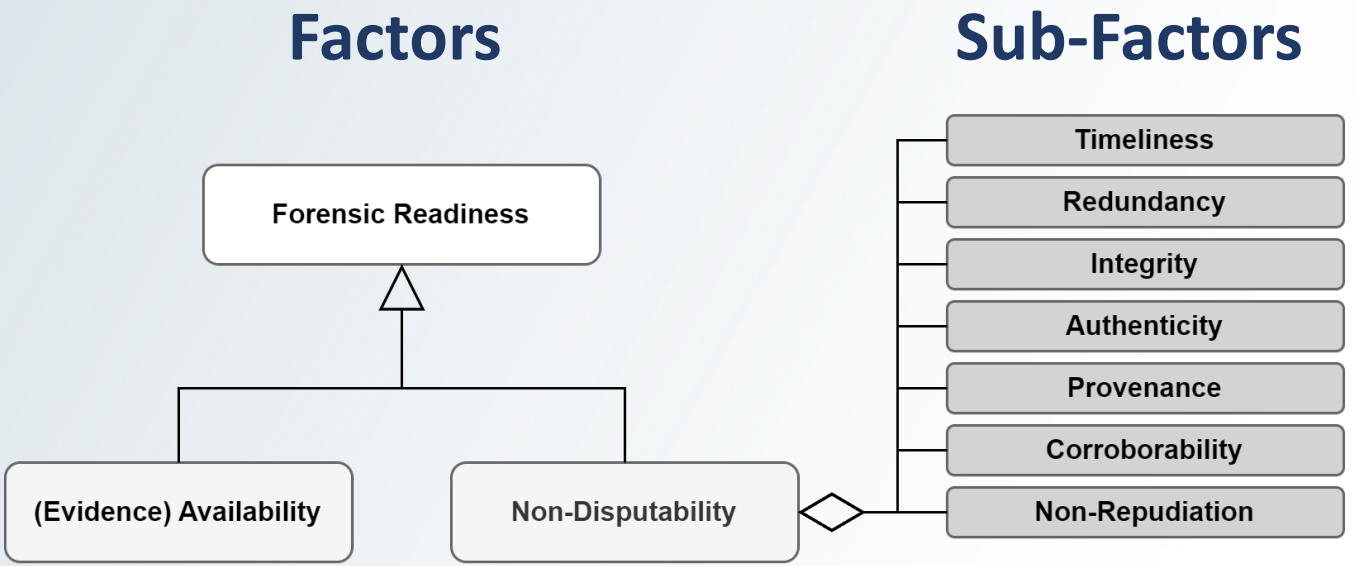
Co-funded by the European Union

Model Creation

Forensic Readiness Qualitative Factors



- Factors
  - High-level aspect
- Sub-Factors
  - Component
  - Overlapping
  - Alternatives



CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

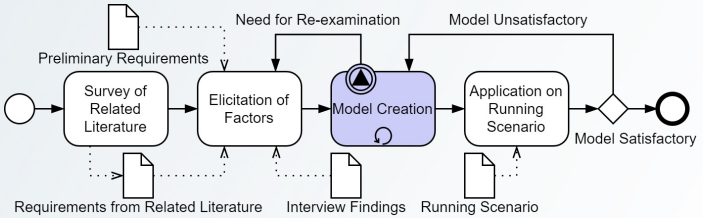
TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

MUNI
C4E

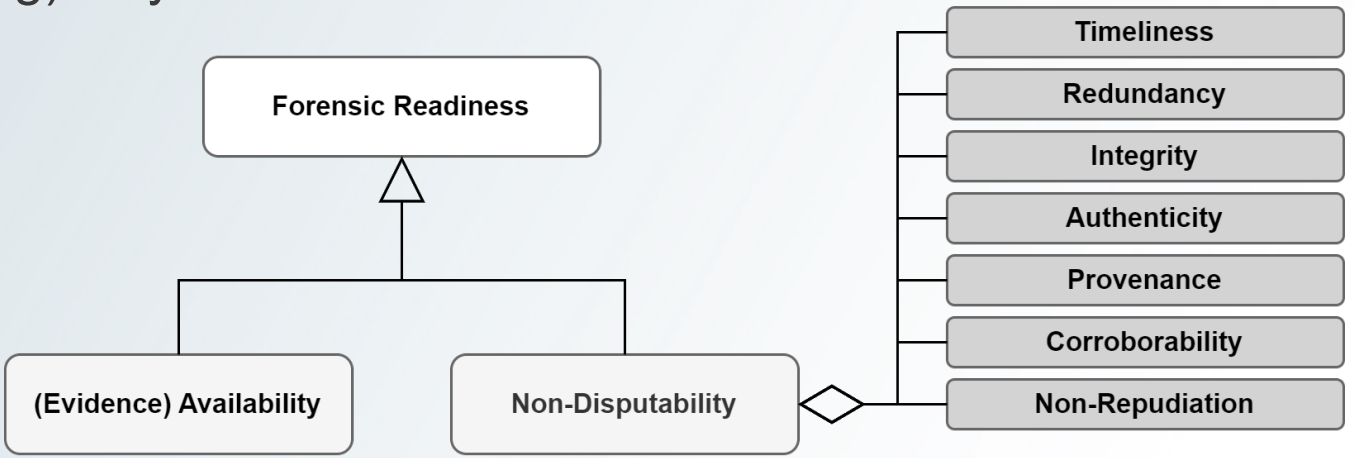
Co-funded by the European Union

Model Creation

Forensic Readiness Qualitative Factors



- Non-Disputability
  - Preventing disputes regarding the evidence
  - Addresses dangers of tampering or corruption
  - Many (overlapping) ways to achieve it



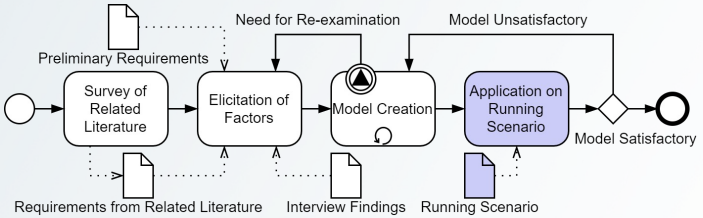
CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

MUNI
C4E

Co-funded by the European Union

Application on Scenario



- Automated valet parking scenario
  - Autonomous Vehicle (AV) – Under user's ownership and control
  - Parking Service Provider (PSP) – Contact point, deployed on cloud
  - Parking lot terminal (PLT) – Edge IoT device, controls the parking area

- Automated issuing of parking permit
  - AV sends a **parking request** to PSP, who forwards it to PLT
  - If there is a space, PSP creates **parking reservation** and sent it to PLT
  - PLT generates a **parking permit**, which PSP sends back to AV

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

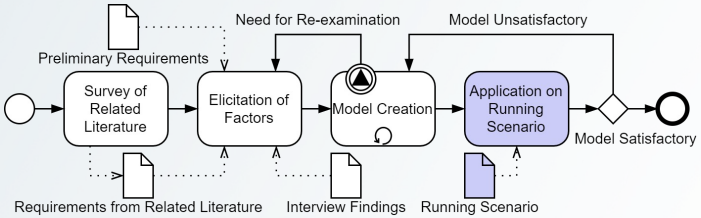
TARTU ÜLIKOOL UNIVERSITAS TARTUENSIS 1632

MUNI C4E

Co-funded by the European Union

Application on Scenario

Risks, Forensic Readiness Goals, and Gaps

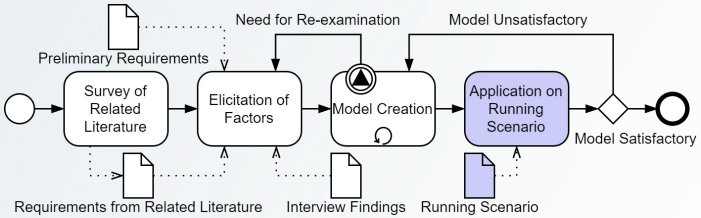


Permit injection	Covert disruption	Permit repudiation
Insiders injects a parking permit into a storage to get free parking	Attacker intercepts and forges custom replies on behalf of parking lot terminal	Dishonest customer repudiates a parking permit, demanding a reimbursement
Prove loss of parking permit integrity	**Prove loss of reservation process availability**	**Defend against repudiation parking permit**
How the Parking permit was stored cannot be determined	The link between the logs uses only circumstantial data	Correct delivery of the Parking permit cannot be proven

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia
TARTU ÜLIKOOL UNIVERSITAS TARTUENSIS 1632
MUNI C4E
Co-funded by the European Union

Application on Scenario

Forensic Readiness Requirements



Completeness	Covert disruption	Utilisability	Availability
Permit injection	Permit injection	Covert disruption	Permit repudiation
Known scenarios of parking permit generation tampering **shall contain evidence**	Parking permit storage audit log **shall be non-disputable**	Availability request log **shall be linkable** with provider's potential evidence	Evidence of Parking permit reception **shall be available**
At least **90% Scenario Coverage**	At least **2 Relative Evidentiary Value**	At least **1 link**	For at least **99.9% of delivered parking permits**

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

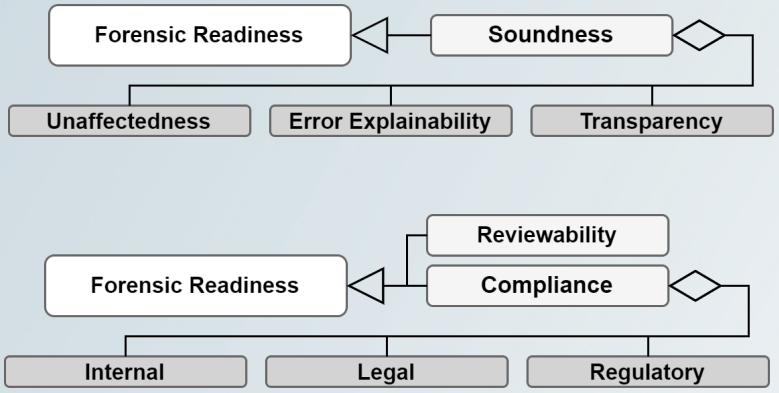
MUNI
C4E

Co-funded by the European Union

Conclusion

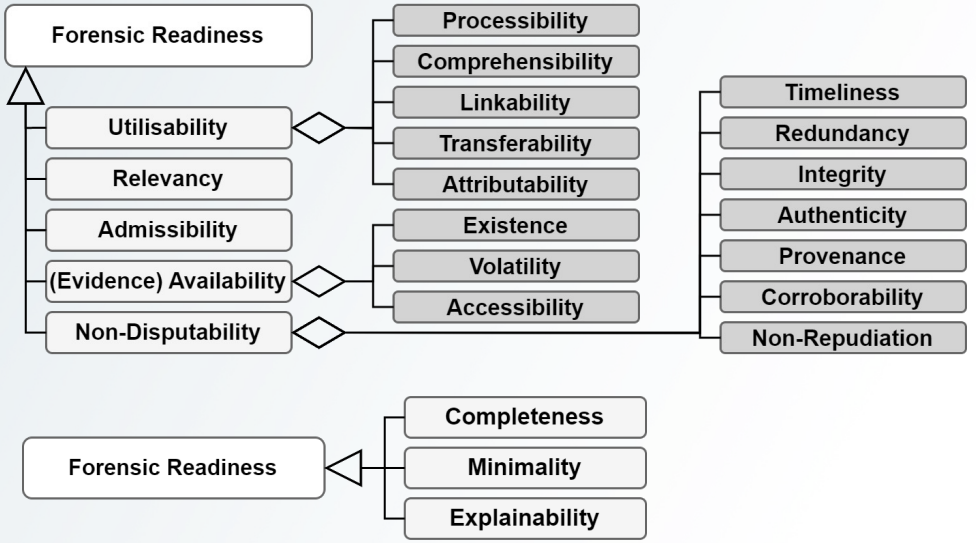
What are the factors that form the forensic readiness requirements?

- Forensic readiness as software quality
- Grouping qualities with the same goal
- Towards verifiable requirements



How can the factors be manifested as a concrete requirement?

- Process based on risk management
- Criteria with a minimum acceptable value



CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

TARTU ÜLIKOOL
UNIVERSITAS TARTUENSIS
1632

MUNI
C4E

Co-funded by the European Union