UNIVERSITY OF TARTU
Institute of Computer Science

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

# Evaluating Organization Security: User Stories of European Union NIS2 Directive

Mari Seeba[1,2], Magnus Valgre[1], Raimundas Matulevičius[1]

[1]University of Tartu

[2]NCSC-EE

CAISE 2025

Co-funded by the European Union

Investing in your future

**GDPR: Global impact**
– Awareness of privacy & data protection

**Hope for NIS2 Directive**
– Similar shift in cybersecurity culture

**... but ...**

**Only 6 of 27 EU Member States**
– transposed NIS2 on time

**Key obstacle:**
– Disconnect between **policy-makers (lawyers)** and **implementers (engineers)**

## Lawyers' View (Policy-Makers)

**What must be done**
**Static rules**

Focus on **compliance**
Noncompliance = **sanction & penalty**

Use **regulatory language**
Clause interpretation can change due clause sequence and role

Work in **norms in different levels (EU, Membes State, regulative standard)**

Kiyavitskaya *et al* (2008), Islam *et al* (2010)

| Lawyers' View (Policy-Makers) | Engineers' View (Implementers) |
| --- | --- |
| **What must be done**<br>**Static rules** | **How things work**<br>**Adaptive systems** |
| Focus on **compliance**<br>Noncompliance = **sanction & penalty** | Focus on **efficiency & resilience**<br>Gaps = risk & **opportunity to improve** |
| Use **regulatory language**<br>Clause interpretation can change due clause sequence and role | Use **technical terminology**<br>Avoid multiple interpretations |
| Work in **norms in different levels (EU, Membes State, regulative standard)** | Work in **infrastructure & code** & with humans |

Kiyavitskaya *et al* (2008), Islam *et al* (2010)

# User stories as the bridge between Policymakers and Engineers



Lucassen et al. (2016), by Alsaadi et al. (2019), Hassani et al. (2024)

# NIS2 Directive

**DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL**

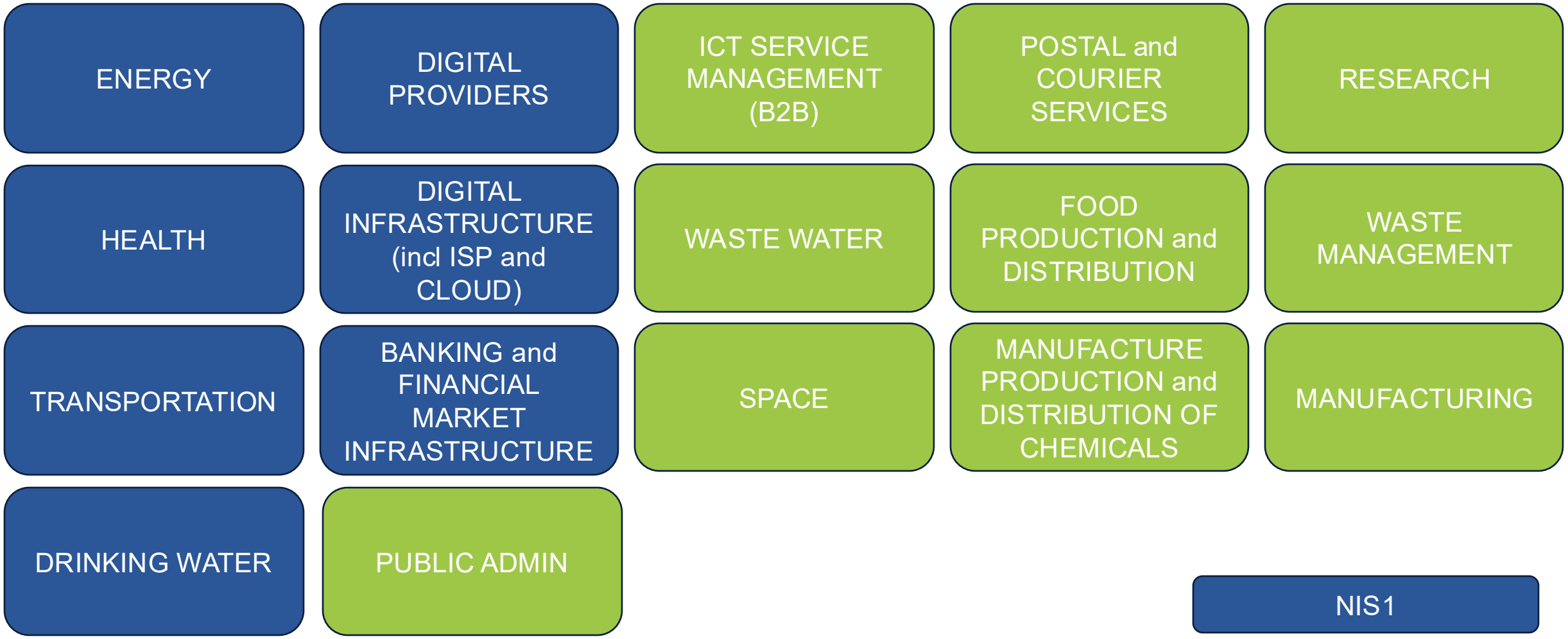
**of 14 December 2022**

**on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)**

- Aims at a high common level of cybersecurity
- Applies to essential and important entities
  - *Critical infrastructure and service providers*
- Focuses
  - *Risk-management measures*
  - *Incident handling on Member State level*
  - *Supervision*

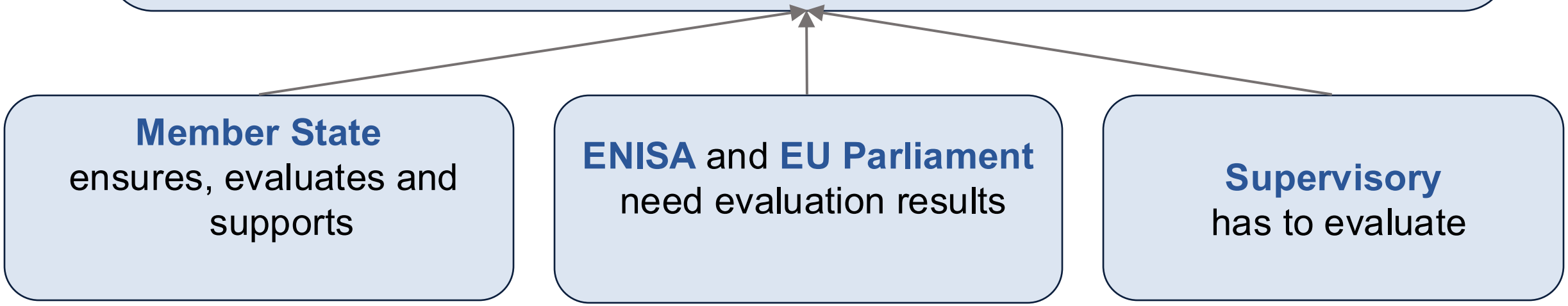
- All-hazards and risk-based approach required

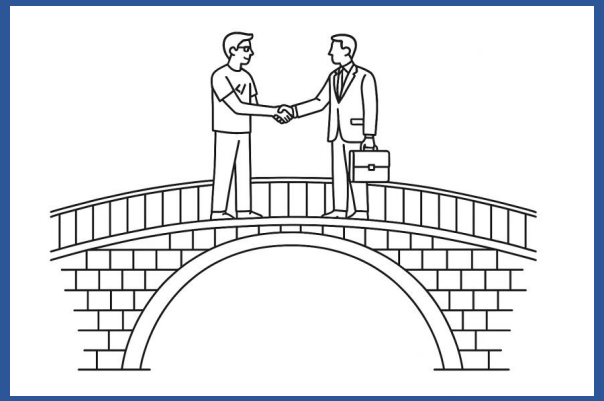
# NIS2 Critical sectors



# Scope:
# NIS2 Directive Security Level Evaluation Context

**Entity**:
- implements risk management measures
  - implements policies and procedures **to assess the effectiveness** of cybersecurity risk-management measures
  - assesses **supply chain**





What are the **user stories of NIS2**
in the context of security level evaluation of organizations?

As a <*type of user*>,

I can <*some goal*> so that <*some reason*>.



User Story template by Cohn (2004, 2017)

# Method


- Entire text
- Filtering relevant parts
- For double-check words seach:
  - *ensure, level, assess..., oversee, measure...*
- Finding Actors, their activities, resources
- Dependency model in i*

- 10 User Stories for 6 Actors
  - based on text analysis and dependency model

- existing security evaluation methods and instruments

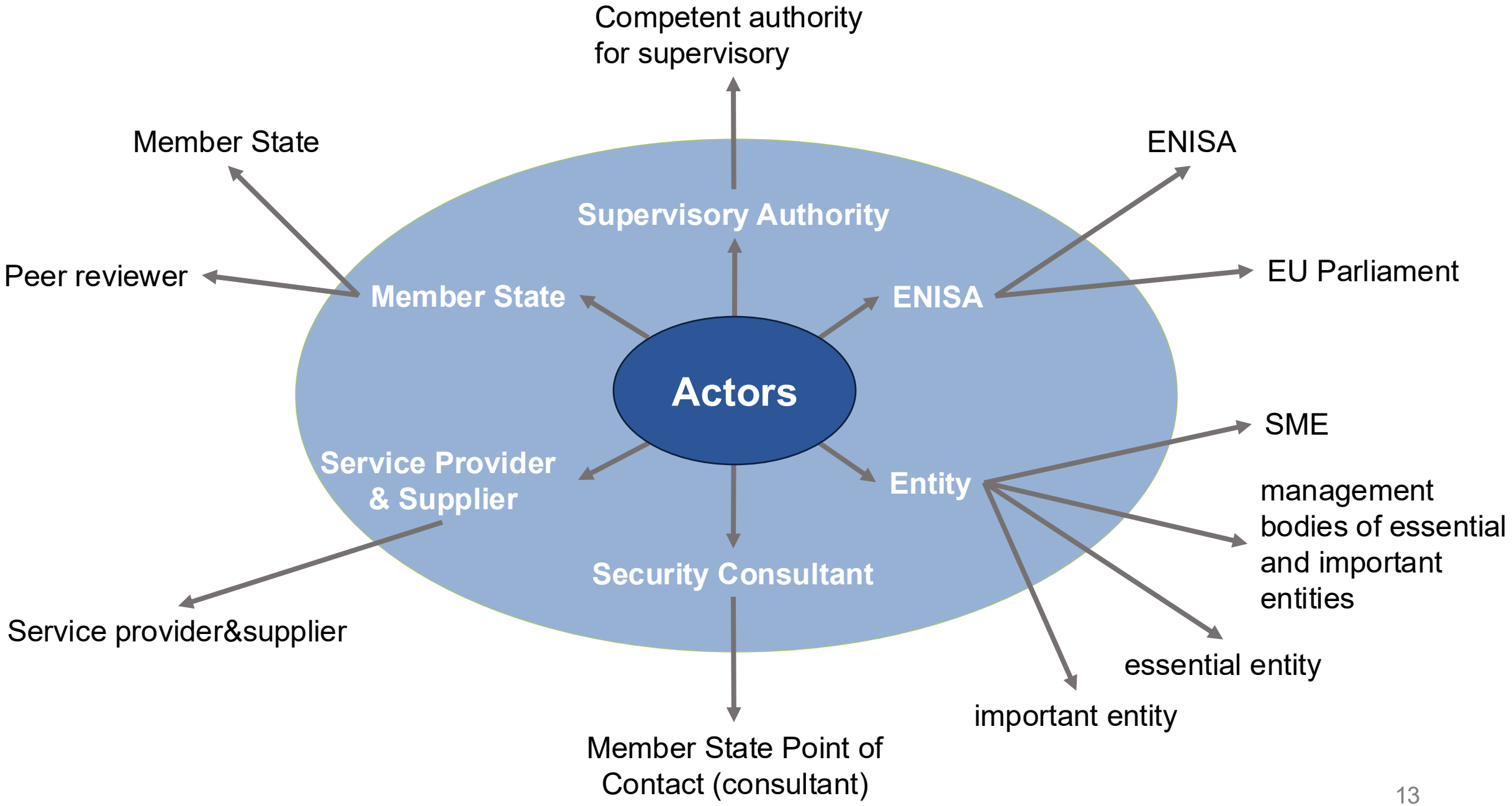
by Islam *et al.* (2010), Jorshari *et al.* (2012), Fatema *et al.* (2016), Hassani *et al.* (2024)

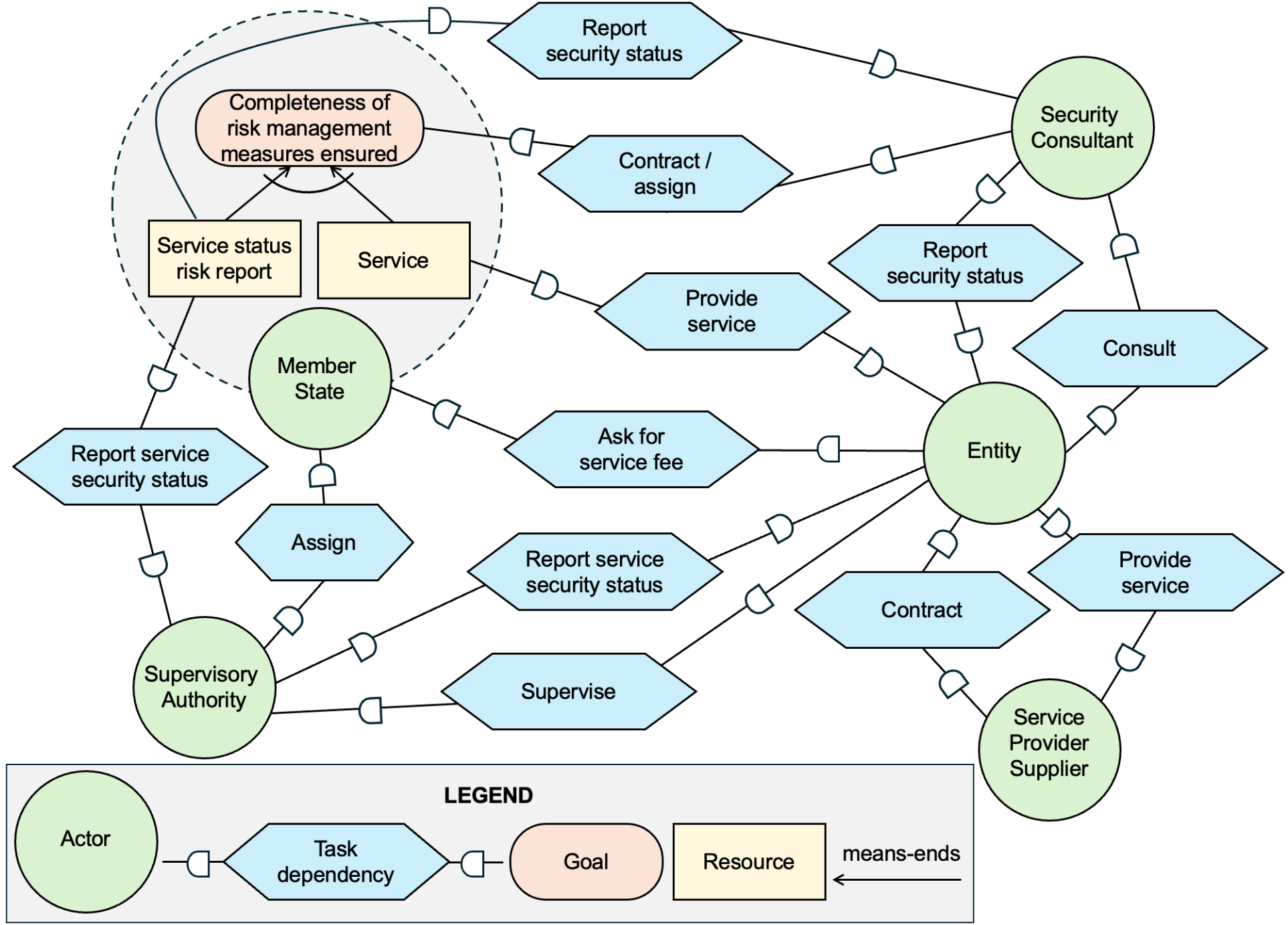
As a <*type of user*>,

I can <*some goal*> so that <*some reason*>.



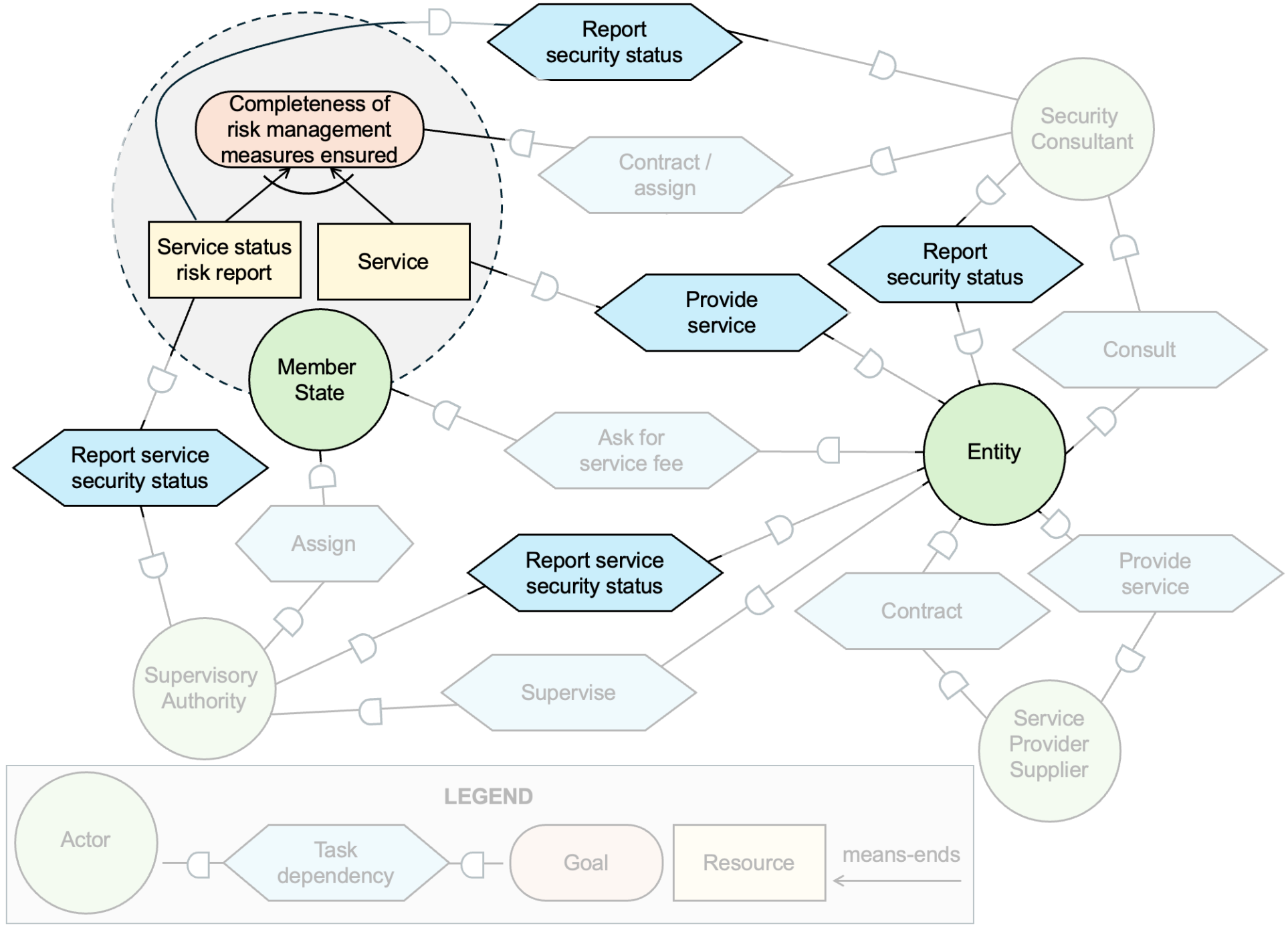
User Story template by Cohn (2004, 2017)


Competent authority for supervisory
Member State
ENISA
Supervisory Authority
Peer reviewer
Member State
ENISA
EU Parliament
Actors
SME
Service Provider & Supplier
Entity
management bodies of essential and important entities
Security Consultant
Service provider&supplier
essential entity
important entity
Member State Point of Contact (consultant)


Report security status
Completeness of risk management measures ensured
Contract / assign
Security Consultant
Service status risk report
Service
Report security status
Provide service
Consult
Member State
Ask for service fee
Entity
Report service security status
Assign
Report service security status
Contract
Provide service
Supervisory Authority
Supervise
Service Provider Supplier
LEGEND
Actor
Task dependency
Goal
Resource
means-ends

# Example of User Stories

| Role | Member State |
|---|---|
| Goal: | Factual proof of achieving a high common level of cybersecurity in all sectors and entities to avoid cyber incidents causing major damage to economics and society. |
| Reference: | Art1(1); Art7(2); Art19(1.a); Art20(1),(2); Art21(1),(2),(3),(4) of NIS2 |
| **US1.1:** As a Member State, I can oversee the security posture of Entities through structured security level evaluation results, so that I achieve awareness of compliance with regulations.<br>**US1.2:** As a Member State, I can evaluate an entity's cybersecurity level using an all-hazards approach, so that I can allocate resources to address directly on identified vulnerabilities. | |


Report security status
Completeness of risk management measures ensured
Contract / assign
Security Consultant
Service status risk report
Service
Report security status
Provide service
Consult
Member State
Report service security status
Ask for service fee
Entity
Assign
Report service security status
Contract
Provide service
Supervisory Authority
Supervise
Service Provider Supplier
LEGEND
Actor
Task dependency
Goal
Resource
means-ends

# Real usage of User Stories

| Instruments | US1 Member State | US2 Supervisory | US3 ENISA | US4 Consultant | US5 Entity | US6 Supplier |
|---|---|---|---|---|---|---|
| NUKIB Report | + | + | | | | |
| ENISA EU CSI | + | | + | | | |
| NCSI, GCI | + | | | | | |
| State Audit Office(EE, LT), Statistics Authority | + | v | v | | | |
| ENISA Self Assesment Tool, ES, IE, GR, C2M2 (Maturity Model), certification audits | | | | v | + | v |
| F4SLE (EE), Kybermittari (FI) | + | + | v | + | + | + |

original purpose

can be used

# Concluding remarks

- Optimization to reduce burden of Entities
  - Collect and reuse data
  - Standardization of security level evaluation
  - Instruments to multiple users
- Integrate  security evaluation into security management

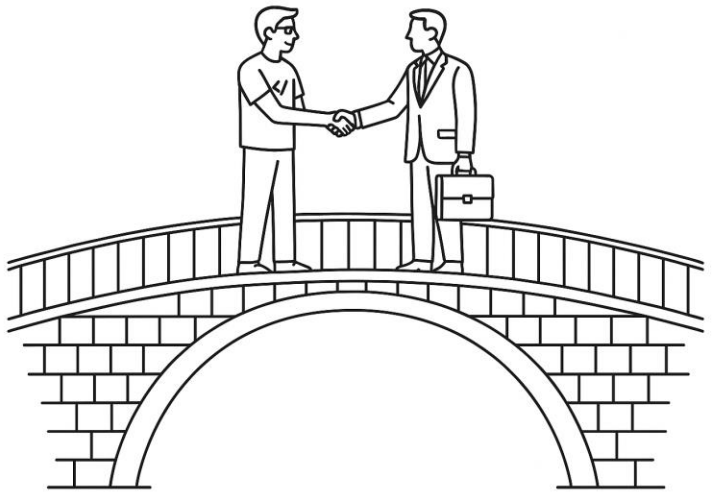
**Limitations**

- Scope coveres only NIS2
- High abstraction level – details from Member State

Compliance ≠ security

# Summary

- To bridge the silos between Lawyers and Engineers
  - 10  NIS2 User Stories for 6 Actors in the context of security level evaluation of organizations
- Avoiding burden of organisations
  - Optimization via standardization



**Further work**

- Testing user stories in real life with F4SLE (Framework for Security Level Evaluation)
- Detailing the User Stories to suit for our Member State
- Meet NIS2 via real resilience, not just checkbox compliance.

CHESS
Cyber-security Excellence Hub in Estonia and South Moravia

UNIVERSITY OF TARTU
Institute of Computer Science

# Thank you!
# Questions?

https://infosec.cs.ut.ee/

https://doi.org/10.1007/978-3-031-94569-4_4

mari.seeba@ut.ee