Product Management Thinking
How to Integrate Security?

Florian Angermeir
06.11.2024

fortiss

BLEKINGE TEKNISKA HÖGSKOLA · BTH ·

Disclaimer

⚠️ This talk can't and doesn't attempt to capture the entire security (compliance) domain

⚠️ Even though this talk is grounded in research findings, your experiences might be different

About Me

Currently

- Researcher at fortiss
- PhD student at Blekinge Institute of Technology

Past

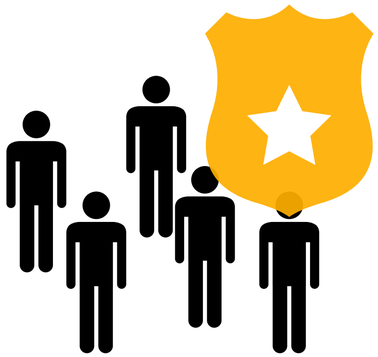
- Research and implementation of security (compliance) in agile/DevOps for 5 years at Siemens
- System administrator at Technical University of Munich for 5 years

Security & Compliance

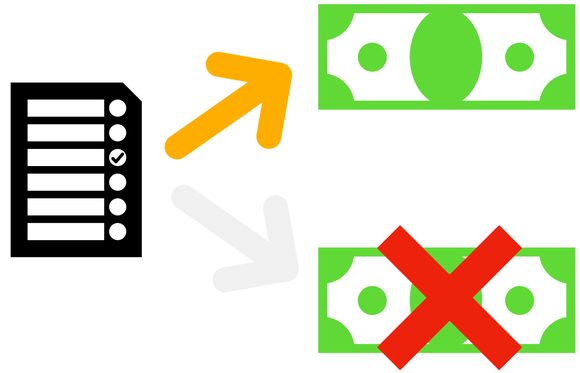
Why Security?

Secure Product

Protect Business or Reputation



Protect Customers



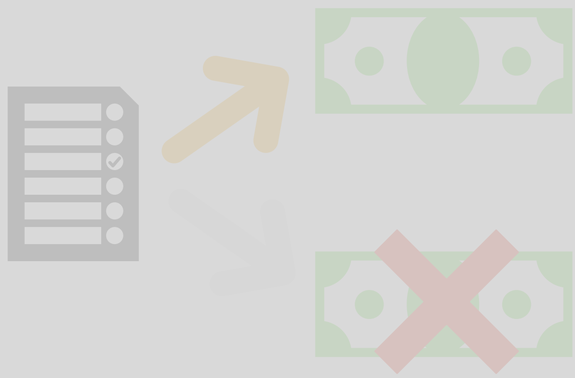
Requirement to Enter Market

Why Security?

Secure Product

Protect Business or Reputation

Protect Customers



Requirement to Enter Market

1. Motivations are intertwined
2. Affect all parts of the business
3. Market becomes increasingly regulated

Structure to Approach Security

Organisational Security

- Is information classified according to business needs? (ISO 27001 5.12)
- Is information security addressed in supplier agreements? (ISO 27001 5.20)

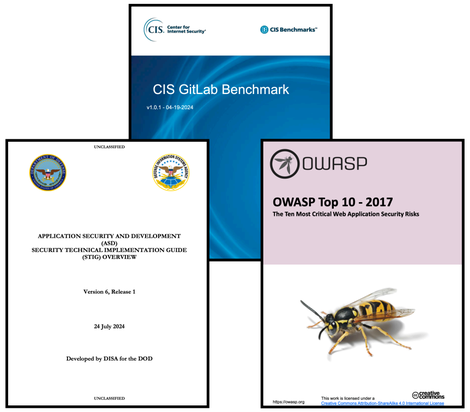
Product Development Process Security

- Is a threat modelling analysis process in place? (IEC 62443-4-1 SR 2)
- Does the product design document external interfaces? (IEC 62443-4-1 SD 1)

Product Security

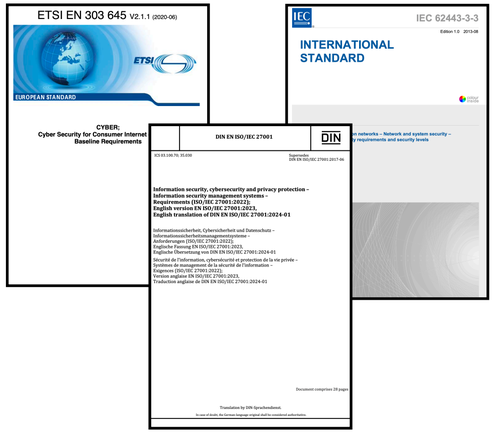
- Does the product limit unsuccessful login attempts? (IEC 62443-3-3 SR 1.11)
- Is the software application running with least necessary privileges? (ETSI EN 303 645 5.6-7)

Available Guidance



Best Practices

- Voluntary guidelines
- Cover the most common security issues
- Often easily applicable



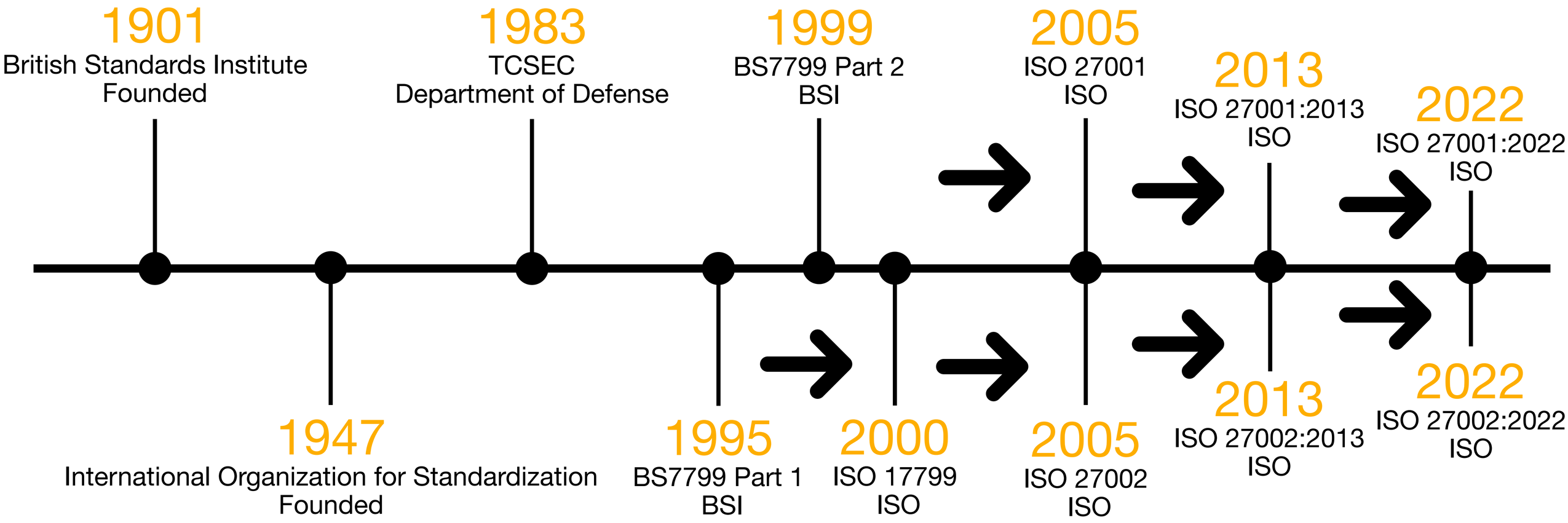
Security Standards

- Voluntary/Mandatory guidelines
- Offer high level of security posture
- Provided by standardisation bodies (e.g. ISO)

Regulations

- Mandatory guidelines
- Dictate security posture - explicit consequences
- Provided by governmental authorities (e.g. EU)

Brief History of Security Standards



Ever Present Challenges

1. Security standards are difficult to understand & Interpretative
2. Stakeholders lack security knowledge

   Security is a big field - you can't know everything, especially if is not your job

3. Security experts scarce

   1 (=One) Security expert for 100 developers [1]

4. Ensuring you satisfy security requirements (e.g. audits) is resource-intensive

[1] https://www.sonatype.com/hubfs/SON_Survey2018_final.pdf

The World Changed

IOT & Cloud Computing: Smaller, faster devices, highly distributed systems

Big data: Data-driven applications, personal data processing

Machine Learning & AI: Non-determinism

Contemporary Product Development: High development velocity

Contemporary Product Development & Security Compliance

DevOps, Agile & Security Compliance

Traditional Software Development

Long release cycles
Testing at end of cycle
Heavy-weight change management
Lots of documentation

Traditional Security Compliance

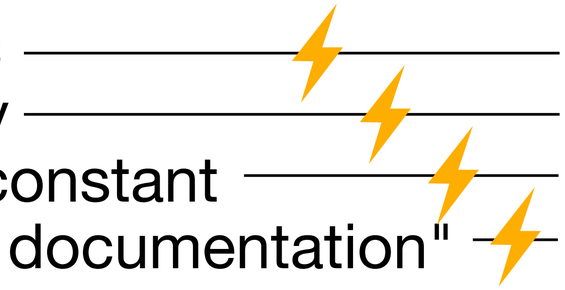
Resource-intensive
Process oriented
Doesn't handle frequent changes
Requires extensive documentation

Modern Software Development

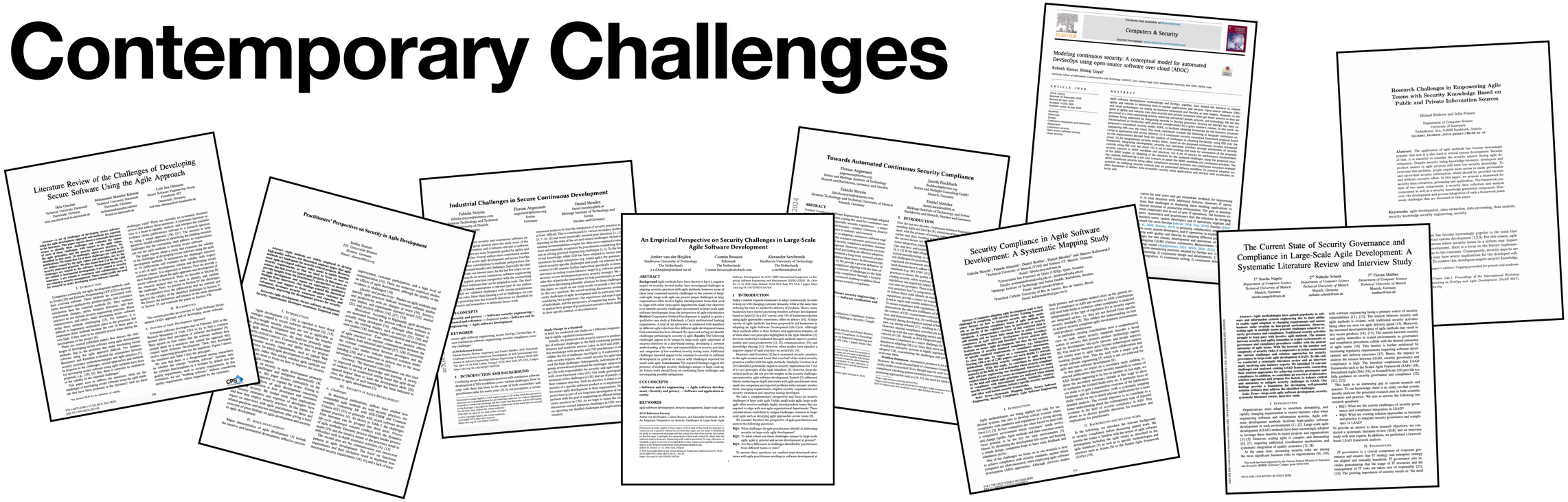
Short release cycles
Testing continuously
Change is the only constant
"Working code over documentation"

Modern Security Compliance

?
?
?
?



Contemporary Challenges



- Workshop with 3 companies over 2 years (Moyón et al. [1])
- Literature review (Angermeier et al. [2]) & Survey
- 27 challenges in 6 categories

[1] https://arxiv.org/pdf/2401.06529
[2] https://arxiv.org/pdf/2407.21494

Contemporary Challenges

Category: Security in Continuous Development
e.g. Perform threat modelling and consistently increment/adapt it throughout sprints

Category: Security in the Value Stream
e.g. Prioritisation of security requirements vs. system functionalities

Category: Security Implementation Efficiency
e.g. Security compliance evidence generation and documentation too time consuming

Category: Security Knowledge
e.g. Enable security knowledge and ownership in engineering teams

Category: Security into CI/CD pipelines
e.g. Achieve efficient handling of security tool findings and involve into regular issue handling process

Category: Security Strategy Success
e.g. Insufficient leadership on security

Source: https://arxiv.org/pdf/2407.21494

High-Level Solution Streams

Agile/DevOps team security skill improvement

Implementation of continuous security feedback loop

Continuous automatic security compliance

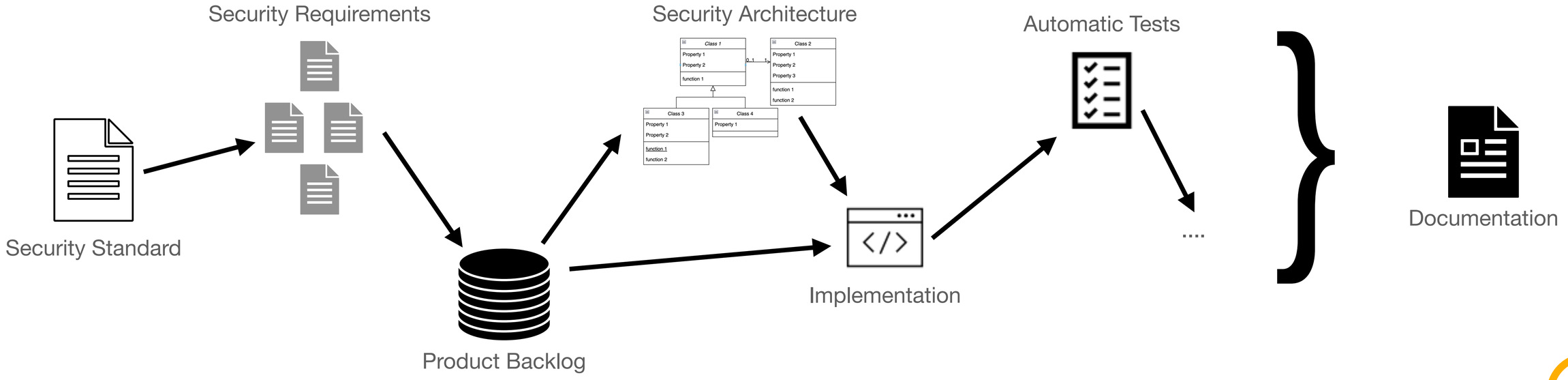
Visibility & assessment of security practices maturity

Source: https://arxiv.org/pdf/2401.06529

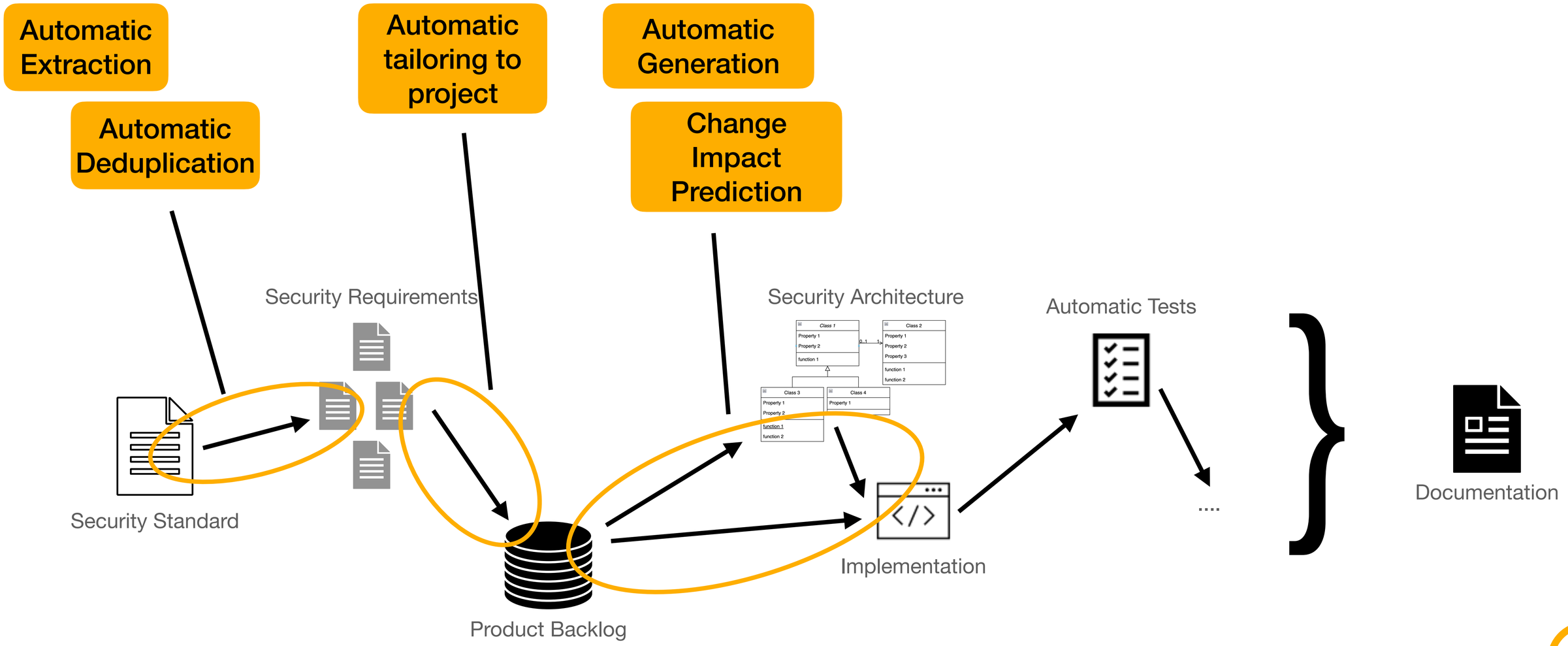
Let's Make One Deeper Dive

Challenge
Make Security Architecture visible in Backlog and Documentation

Solution (Continuous automatic security compliance)
Automatic artefact generation & traceability over the entire workflow



Let's Make One Deeper Dive



Final Consideration

Security as End in Itself?

Often security - especially if imposed from outside - feels like an end in itself.

BUT...

Most often its not - it serves a purpose for our business (goals or constraints).

NEVERTHELESS...

Too often business goals and constraints conflict.

My Takeaway

Security needs to become better at supporting other business goals.

Let's Discuss!

Takeaway 1
Three areas to structure your security posture plans: Organizational, Process, Product

Takeaway 2
Best practices, security standards & regulations support planning, prioritising, and integrating security in your product management thinking

Takeaway 3
Security has to be integrated across the entire product development flow with minimal impact on other business goals

Contact

Florian Angermeir
angemeir@fortiss.org
https://angermeir.me

fortiss GmbH, Germany
Blekinge Institute of Technology, Sweden