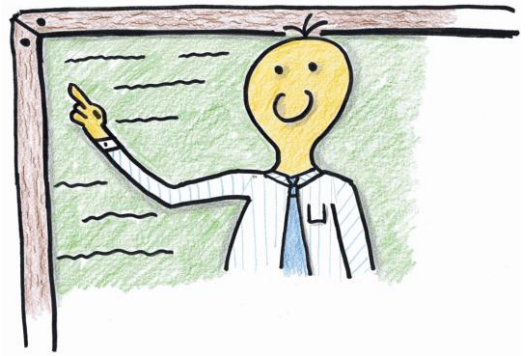


Webinar – Cybersecurity without surprises

Plan your work packages right!

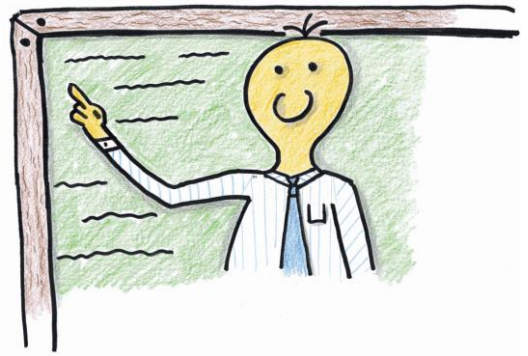
Agenda

1. Introduction
2. PM & Cybersecurity – hand in hand
3. What belongs in the cybersecurity package?
4. Integration into project management
5. Lessons learned & recommendations
6. Q&A and discussion



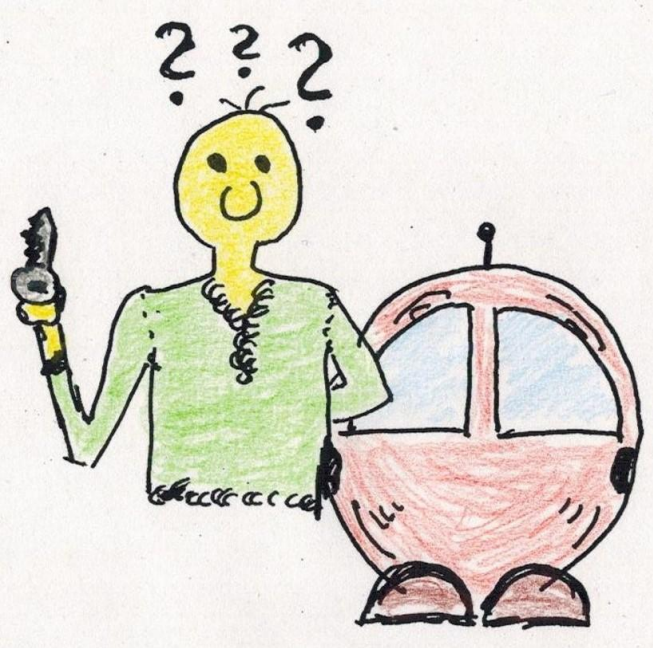
Agenda

1. **Introduction**
2. PM & Cybersecurity – hand in hand
3. What belongs in the cybersecurity package?
4. Integration into project management
5. Lessons learned & recommendations
6. Q&A and discussion



© 2026 Process Fellows

Why Cybersecurity Is Not "Just a Technical Topic"



Regulation & homologation

UN R155/R156: without a certified CSMS/SUMS no type approval – and no vehicle on the road.

Contracts & liability

OEMs require cybersecurity evidence from suppliers; responsibilities are fixed in the CIA.

Organization & people

Policy, roles, competence and culture are required by ISO/SAE 21434 – not just a good system/software.

Whole lifecycle

Monitoring, vulnerability management and updates continue long after SOP – until end of support.

Cybersecurity is a management task with technical content –
not a technical task with some documentation at the end.

© 2026 Process Fellows

Relevant Standards and Drivers

UN R155 / R156 Regulation	**ISO/SAE 21434** Standard	**ASPICE for Cybersecurity** Assessment model	**TISAX** Assessment & label	**NIS2** EU directive
CSMS & SUMS as prerequisite for type approval; mandatory in the EU for all new vehicles **since 07/2024**.	Cybersecurity engineering over the full lifecycle – from concept to decommissioning. State of the art for R155.	PAM 2.0 (2025): SEC.1–SEC.4, MAN.7, ACQ.2 – capability of CS engineering processes.	Information security of the company (VDA ISA) – e.g. protection of data and prototypes.	Cybersecurity risk management and reporting duties for essential / important entities.
Vehicle / OEM + supply chain	**Product & project**	**Process / project**	**Organization**	**Organization**

Focus today: product & project level

Context: organizational information security

© 2026 Process Fellows

Different Requirements for Organization and Project

Organization – Clause 5
Set up once, used by all projects

- Cybersecurity governance & policy
- Roles, responsibilities, competence & culture
- CS processes incl. monitoring, incident response
- Management systems & tool management
- Information security management
- Organizational cybersecurity audit

Checked by: ACSMS audit / CSMS certificate (company level, basis for UN R155 type approval)

Project – Clause 6
Planned and executed per project / item

- Assign responsibilities for CS activities **[RQ-06-01]**
- Identify reuse already in the acquisition phase **[RQ-06-02]**
- Tailoring based on reuse & impact analysis **[RQ-06-13 – 22]**
- Develop the cybersecurity plan **[RQ-06-03 – 07]**
- Identify need for external support **[RQ-06-10]**
- Identify need for CS assessment **[RQ-06-24]**
- Ensure completeness of the CS case **[RQ-06-23]**
- Perform the release for post-development **[RQ-06-33 – 34]**

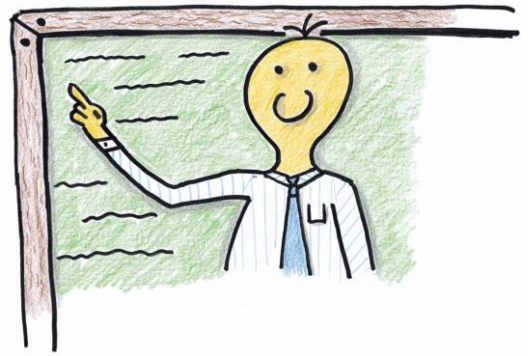
Checked by: ISO/SAE 21434 CS assessment (work products) & ASPICE for CS assessment (processes)

An ASPICE for Cybersecurity assessment cannot replace an ACSMS audit – and vice versa

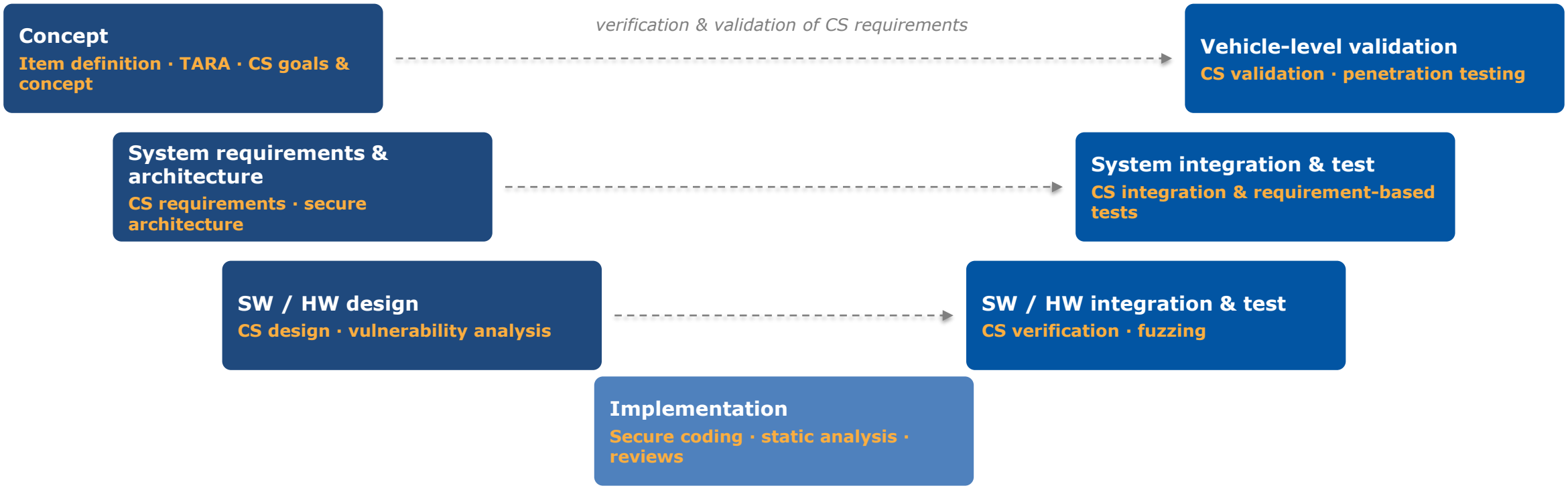
© 2026 Process Fellows

Agenda

1. Introduction
2. **PM & Cybersecurity – hand in hand**
3. What belongs in the cybersecurity package?
4. Integration into project management
5. Lessons learned & recommendations
6. Q&A and discussion



Cybersecurity in the V-Model

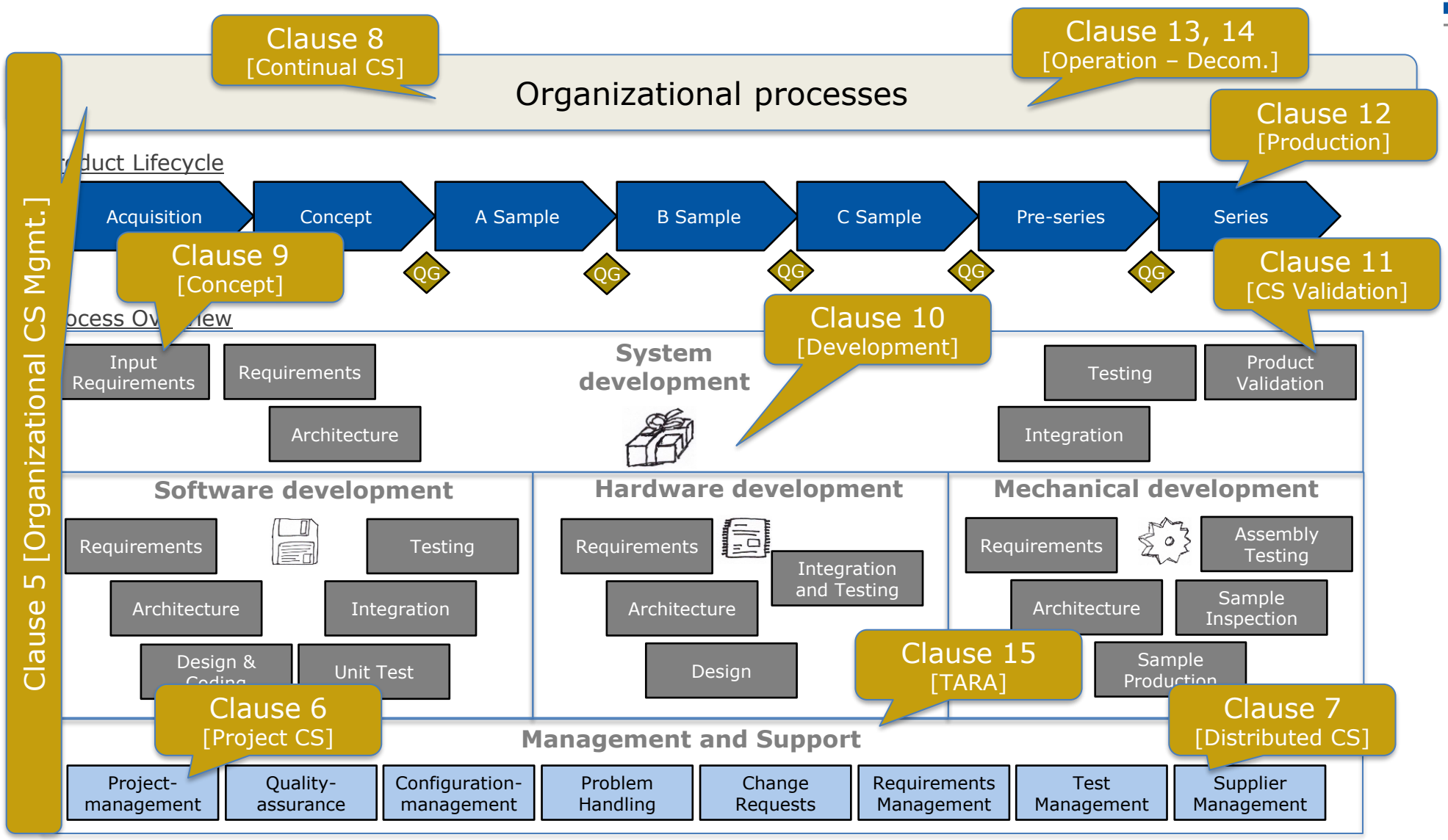


CS management: CS plan · CIA with suppliers · CS case & assessment · release for post-development

Continual activities: CS monitoring · vulnerability analysis & management – beyond SOP

© 2026 Process Fellows

Where Do We Address ISO/SAE 21434 in the Project?



© 2026 Process Fellows

What We See in Practice: Extra Topic vs. Integrated Topic

Cybersecurity as an extra topic

- ✗ CS activities are **planned too late** – after architecture and sourcing
- ✗ **Own schedule**, own milestones – **not synced** with the project lifecycle
- ✗ "We'll do that later" – until gate or assessment
- ✗ CS experts only called in when needed – no planned capacity
- ✗ Evidence is produced for the assessment, not for the product

Cybersecurity as an integrated topic

- ✓ **CS work packages** in the project plan **from day one**
- ✓ CS milestones = project gates and releases
- ✓ Project **plan** and cybersecurity plan are **consistent**
- ✓ **CS roles** defined and assigned, capacity planned and monitored
- ✓ Evidence grows with the product – the CS case is always current

Impact of the extra-topic approach:



Schedule
late changes, blocked gates, SOP at risk

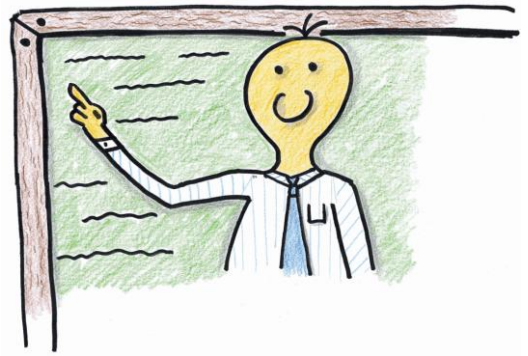
Quality
bolted-on measures, unknown residual risk

Compliance
incomplete CS case, type approval at risk

© 2026 Process Fellows

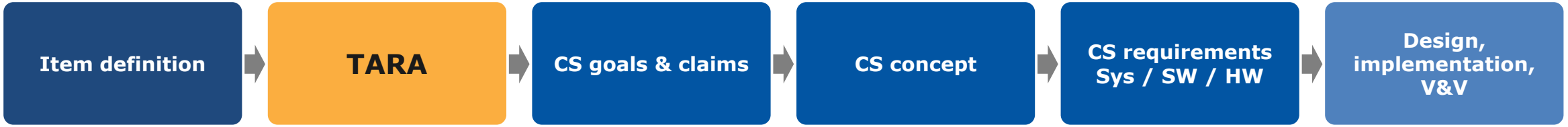
Agenda

1. Introduction
2. PM & Cybersecurity – hand in hand
3. **What belongs in the cybersecurity package?**
4. Integration into project management
5. Lessons learned & recommendations
6. Q&A and discussion



© 2026 Process Fellows

The TARA Is the Anchor for Cybersecurity Development



TARA steps (ISO/SAE 21434, Clause 15)

1	2	3	4	5	6	7
Asset identification	Threat scenario identification	Impact rating	Attack path analysis	Attack feasibility rating	Risk value determination	Risk treatment decision

On the critical path

Plan the TARA directly after the item definition – in the concept phase, before architecture freeze and sourcing decisions.

Everything depends on it

CS requirements, test and validation scope, supplier requirements and effort estimates are derived from the TARA.

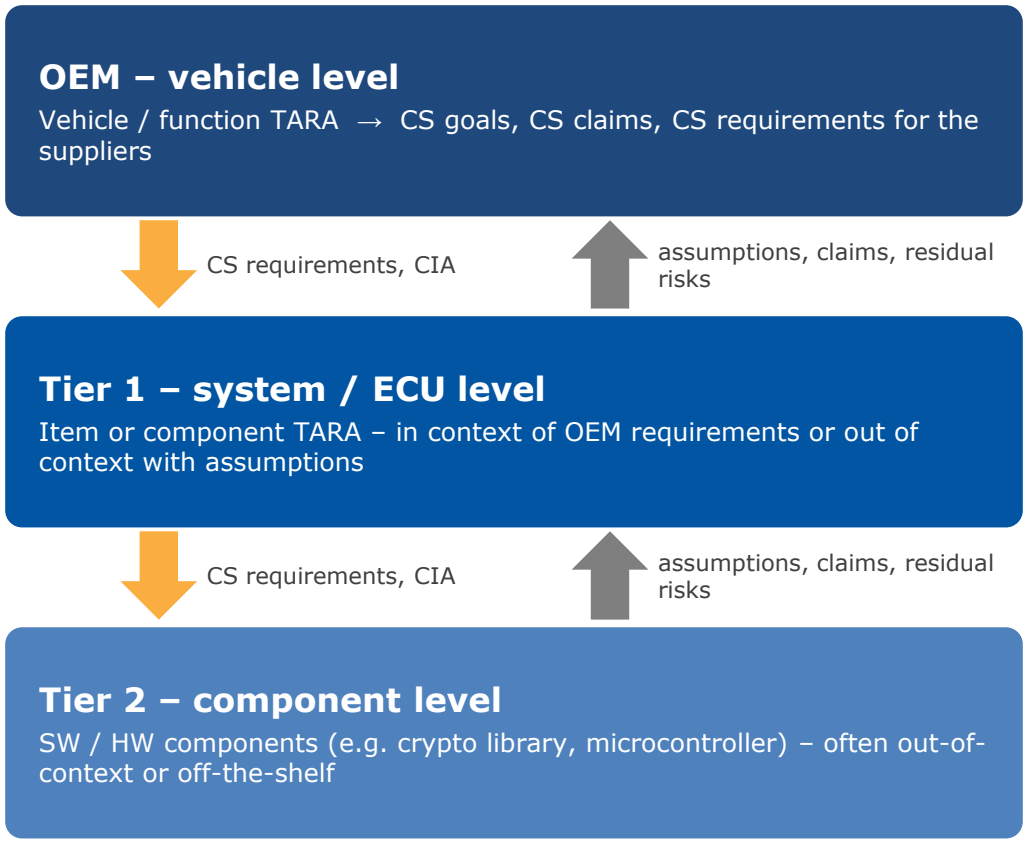
Never "done"

Update triggers: design changes, new threats, vulnerabilities, field findings – plan TARA updates as recurring tasks.

Without a TARA, there is nothing to plan the cybersecurity work against.

© 2026 Process Fellows

TARAs on OEM and Supplier Level

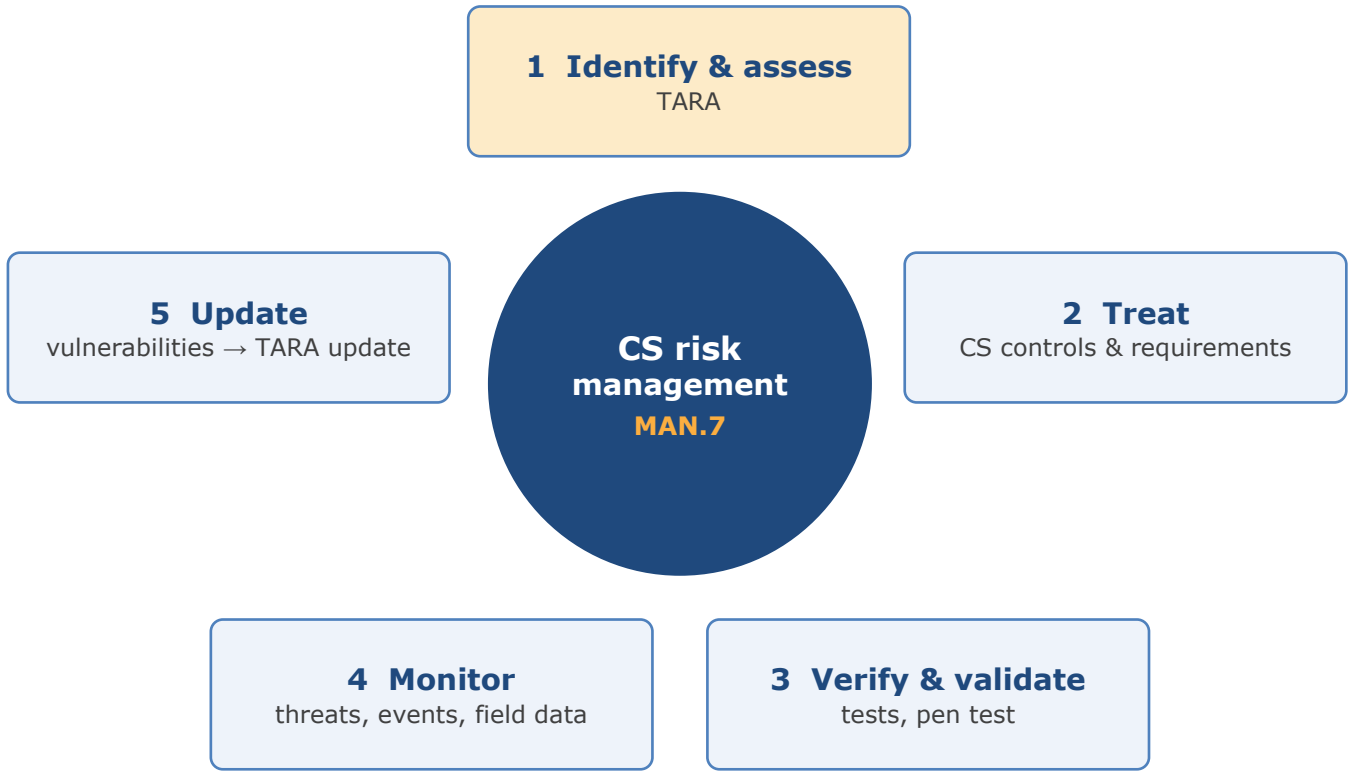


What this means for planning

- **Handover = milestone:** the date for OEM CS requirements belongs in both project plans
- **No input yet?** Start out of context with documented assumptions – and plan the rework once OEM input arrives
- **Align methods early:** impact and feasibility scales, risk matrix agreed in the CIA
- **Consistency across levels:** each level owns its TARA – results must fit at the interfaces
- **Change propagates:** a change on one level triggers TARA updates on the other levels

© 2026 Process Fellows

Cybersecurity Risk Management Is Continuous



What this means for planning

- TARA updates as **recurring tasks** – per release and per relevant change
- **CS impact analysis** in every change request (SUP.10)
- Vulnerabilities and incidents handled **via problem resolution** (SUP.9)
- CS risks and treatment status as a fixed item in project reporting
- Capacity for monitoring & vulnerability management until end of support
- CS risks also visible in project risk management (MAN.5)

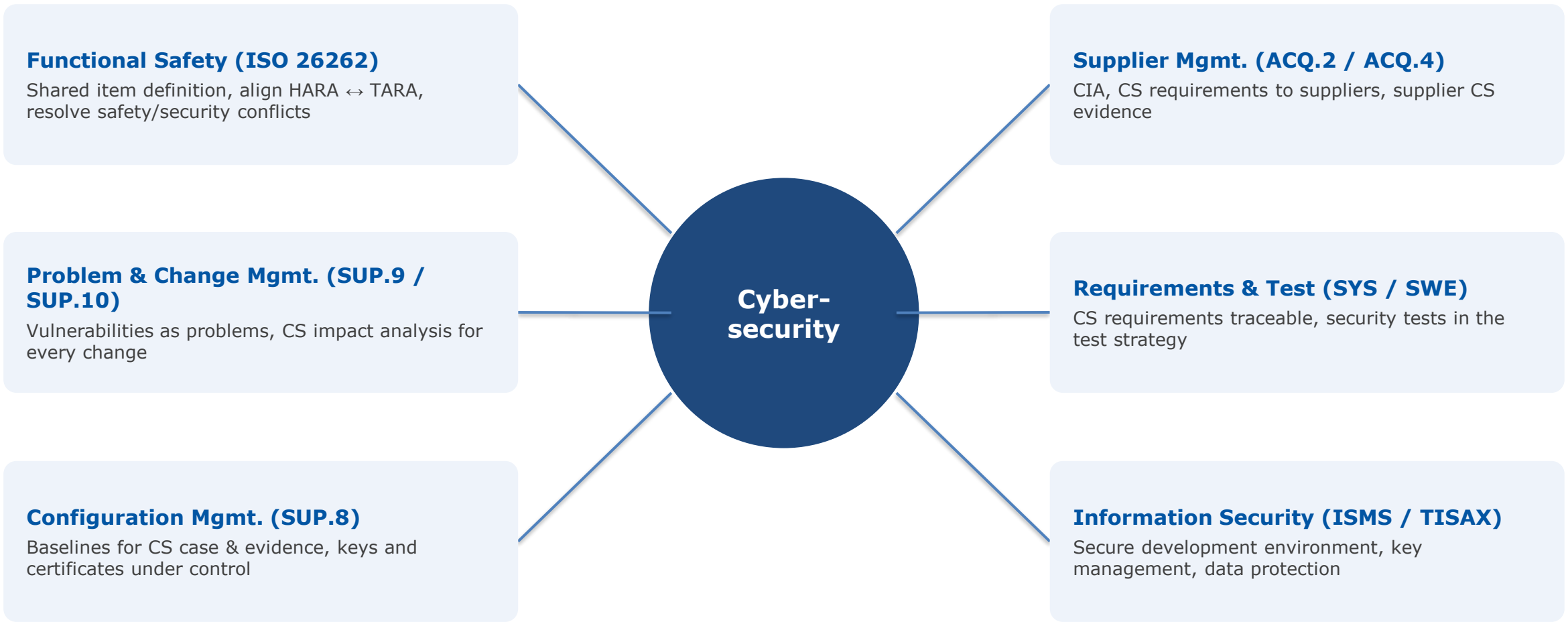
© 2026 Process Fellows

Cybersecurity Work Packages Along the Lifecycle

#	Work package	Key outputs	Typical owner
1	CS planning & tailoring	**CS plan, tailoring rationale, role assignment**	CS manager + PM
2	Supplier management (CIA)	**CIA / RASIC, CS requirements to suppliers**	Purchasing + CS manager
3	Item definition	**Item boundary, functions, interfaces, assumptions**	System architect
4	TARA	**Assets, threat scenarios, risk values, treatment decisions**	CS engineer
5	CS goals & concept	**CS goals, claims, CS requirements & allocation**	CS engineer + architect
6	CS design (Sys / SW / HW)	**Refined CS requirements, secure architecture, vulnerability analysis**	Architects + CS engineer
7	Implementation & verification	**Secure coding, static analysis, reviews, CS tests, fuzzing**	Development + test
8	CS validation	**Penetration test, validation report, residual risk**	CS engineer + pen-testers
9	CS case & assessment	**CS case, independent CS assessment report**	CS manager + assessor
10	Post-development readiness	**Incident response plan, update concept, production control plan**	CS manager + PSIRT

© 2026 Process Fellows

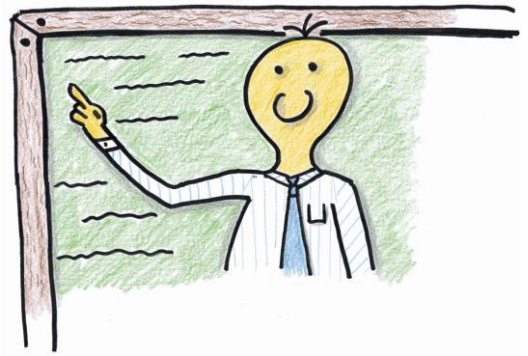
Cybersecurity Interfaces



© 2026 Process Fellows

Agenda

1. Introduction
2. PM & Cybersecurity – hand in hand
3. What belongs in the cybersecurity package?
4. **Integration into project management**
5. Lessons learned & recommendations
6. Q&A and discussion



© 2026 Process Fellows

MAN.3 Project Management from a Cybersecurity Perspective

Base practice	What it means for cybersecurity
BP1 Define the scope of work	**CS is part of the scope definition** – CS goals and boundaries of the CS development are defined
BP2 Define project life cycle	**CS phases and milestones** are synchronized with the project lifecycle
BP3 Evaluate feasibility	**CS know-how**, stakeholder CS goals and requirements are evaluated – external support may be needed
BP4 Define and monitor work packages	**CS activities** are planned and monitored – included in or referenced from the project plan
BP5 Estimates and resources	**Resources for CS** are identified and made available
BP6 Skills, knowledge, experience	Building up or acquiring **CS know-how** is addressed early in the project
BP7 Interfaces and commitments	**Additional stakeholders:** CS management, external partners, production, organizational CS
BP8 Project schedule	As in BP4 – CS activities are scheduled and monitored
BP9 Ensure consistency	Project plan ↔ **cybersecurity plan**
BP10 Review and report progress	**Status of CS activities** is reported – additional stakeholders are addressed

© 2026 Process Fellows

Cybersecurity Gate Criteria: What Must Be Ready When?

Gate	Gate question	Cybersecurity evidence
QG1 Nomination	***Is cybersecurity set up and offered?***	CS plan (draft), roles, CIA, preliminary TARA / CS scope in the offer
QG2 Concept	***Do we know what we protect – and why?***	Item definition, TARA, CS goals & claims, CS concept
QG3 A-Sample	***Are CS requirements in the design?***	CS requirements allocated (Sys/SW/HW), secure architecture, vulnerability analysis, TARA update
QG4 B-Sample	***Are the controls implemented and verified?***	CS verification results, static analysis, open vulnerabilities rated
QG5 C-Sample	***Does it hold against attacks?***	CS validation incl. pen test, residual risks, CS case (draft)
SOP release	***Can we release – and operate?***	CS case final, CS assessment, release for post-dev., incident response & update process ready

© 2026 Process Fellows

Releases, Sprints, Tracking & Effort Estimation



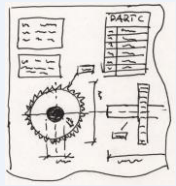
Releases & sprints

- CS work packages as epics / backlog items
- Security user stories & abuse cases
- TARA impact check in refinement for every new feature
- Definition of Done: CS requirements verified, static analysis clean, review done
- Release plan: CS evidence per release, not only at SOP



Tracking

- CS work packages in the PM tool with owner, due date and gate
- KPI: assets / interfaces covered by TARA
- KPI: CS requirements verified vs. total
- KPI: open vulnerabilities by risk level
- CS status as standard item in status report & gate review



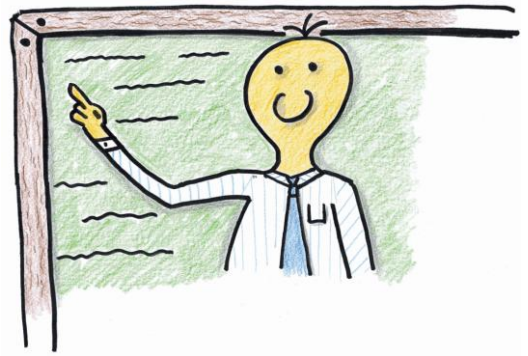
Effort estimation

- Bottom-up per work package
- Drivers: attack surface & interfaces, new vs. carry-over, CAL / risk level
- Supplier share and number of CIAs
- External services: pen test, CS assessment
- Post-SOP effort: monitoring & updates until end of support

© 2026 Process Fellows

Agenda

1. Introduction
2. PM & Cybersecurity – hand in hand
3. What belongs in the cybersecurity package?
4. Integration into project management
5. **Lessons learned & recommendations**
6. Q&A and discussion



© 2026 Process Fellows

Typical Pitfalls from Our Projects

1 Late TARA

"We'll do security once the architecture is ready."

Avoid it: Plan the TARA in the concept – make it a QG2 criterion.

2 "We'll do it later"

CS consciously postponed – until the gate or assessment.

Avoid it: CS work packages in the project plan from kick-off (MAN.3 BP4).

3 Missing roles & capacity

No CS manager; cybersecurity 'on top' of the day job.

Avoid it: Name CS roles at kick-off and plan their capacity (BP5 / BP6).

4 TARA levels not aligned

OEM and supplier TARAs use different scales and assumptions.

Avoid it: Align methods in the CIA; plan the OEM input as a milestone.

5 One-shot risk assessment

TARA done once, never updated; no budget after SOP.

Avoid it: Recurring TARA updates, CS impact analysis per change, post-SOP budget.

6 Pen test at the last minute

No slot, no time to fix the findings.

Avoid it: Book testers early and plan a fix-and-retest loop before SOP.

© 2026 Process Fellows

Key Takeaways

1. **The TARA is the starting signal.**
   Plan it first and early – it is on the critical path.

2. **Integrate, don't add on.**
   CS work packages, milestones and reporting inside the project plan (MAN.3).

3. **Align TARAs across levels.**
   OEM–supplier dependencies are schedule dependencies.

4. **Risk management is continuous.**
   Plan TARA updates, monitoring and capacity beyond SOP.

5. **Organization ≠ project.**
   Use the organizational framework – plan the project work.



Project manager
schedule, resources, gates, tracking

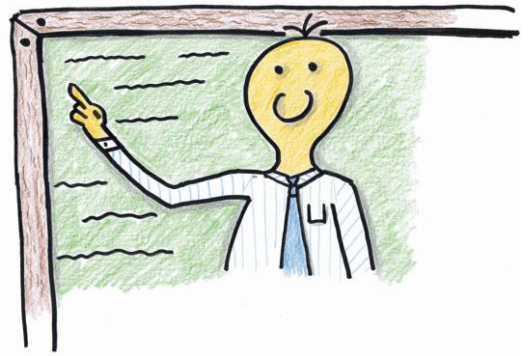
Security expert
risks, requirements, methods, evidence

Together: cybersecurity without surprises.

© 2026 Process Fellows

Agenda

1. Introduction
2. PM & Cybersecurity – hand in hand
3. What belongs in the cybersecurity package?
4. Integration into project management
5. Lessons learned & recommendations
6. **Q&A and discussion**



Q&A and Discussion

- What is your biggest challenge when integrating cybersecurity into projects?
- When does the TARA start in your projects – and who owns it?
- How do you align TARAs between OEM and supplier?
- Are cybersecurity deliverables part of your gate criteria today?
- Who plans and funds continuous risk management after SOP?



Let's discuss!

© 2026 Process Fellows



Process Fellows GmbH | Schlegelleithe 8 | 91320 Ebermannstadt | GERMANY Phone: +49 9194 3719 957

Website: www.processfellows.de | E-Mail: info@processfellows.de