How to establish a cybersecurity culture in automotive development work - Guidance beyond ISO/SAE 21434

ASRG: Secure our Streets Conference 2023

Manuel Sandler

Online, September 14, 2023

CYRES CONSULTING

How to establish a cybersecurity culture in automotive development work - Guidance beyond ISO/SAE 21434

— presented by

Manuel Sandler
Partner

- Master in mathematics
- More than 9 years of experience in different projects for automotive suppliers and OEMs
- Expert in engineering processes development, ISO/SAE 21434, UN R155, ISO 15288, ISO 26262, and ASPICE
- Author of **The Essential Guide to ISO/SAE 21434**, the world's first reference book on ISO/SAE 21434, officially licensed by ISO

CYRES CONSULTING

What ISO/SAE 21434 requires

ganization shall foster and maintain a strong cybersecurity culture.

B for examples.

Table B.1 — Examples of weak and strong cybersecurity culture

Examples indicative of a weak cybersecurity culture	Examples indicative of a strong cybersecurity culture
Accountability for decisions related to cybersecurity is not traceable.	The process ensures that accountability for decisions related to cybersecurity is traceable.
Performance (of the implemented functionality or feature), cost or schedule take precedence over cybersecurity.	Cybersecurity and safety have the highest priority.
The reward system favours cost and schedule over cybersecurity.	The reward system supports and motivates the effective achievement of cybersecurity and penalizes those who take shortcuts that jeopardize cybersecurity.
Cybersecurity personnel force inappropriate and very strict adherence to cybersecurity without considering specific needs of projects/activities.	Cybersecurity personnel act as role models with a good sense for appropriateness and practical implementation that leads to trust in their actions by the entire organization.
Personnel assessing cybersecurity and its governing processes are influenced unduly by those responsible for executing the processes.	The process provides adequate checks and balances, e.g. the appropriate degree of independence in cybersecurity assessment.
Passive attitude towards cybersecurity, e.g.: — heavy dependence on testing at the end of the development; — not being prepared for potential weaknesses or incidents in the field; — management reacting only when there is a cybersecurity incident in production, in the field or if there is a lot of attention in the media about competitor products.	Proactive attitude towards cybersecurity, e.g.: — cybersecurity issues are discovered and resolved from the earliest stage in the product lifecycle (cybersecurity by design); — the organization is prepared to react fast to vulnerabilities or incidents in the field.
The required resources for cybersecurity are not allocated.	The required resources for cybersecurity are allocated. Skilled resources have the competence commensurate with the activity assigned.

Table B.1 *(continued)*

Examples indicative of a weak cybersecurity culture	Examples indicative of a strong cybersecurity culture
— "Groupthink" confirmation bias (i.e. uncritical acceptance or conformity to prevailing points of view). — "Stacking the deck" (i.e. choose members to ensure desired outcome) when forming review groups to prevent potential dissention. — Dissenter is ostracized or labelled as "not a team player" (e.g. uncooperative, intransigent, toxic person). — Dissent reflects negatively on performance reviews. — Minority dissenter is labelled or treated as a "troublemaker", "not a team player" or a "whistle-blower" (i.e. agitator, undesirable or a snitch). — Employees who express concerns fear repercussion.	The process uses diversity to its advantage: — intellectual diversity is sought, valued and integrated in all processes; — behaviour which counters the use of diversity is discouraged and penalized. The supporting communication and decision-making channels exist and the management encourages their usage: — self-disclosure is encouraged; — responsible disclosure by anyone (internal or external) of potential vulnerability is encouraged; — the discovery and resolution process continues in the field, in manufacturing and in development of other products.
No systematic continuous improvement processes, learning cycles or other forms of lessons learned.	Continuous improvement is integral to all processes.
Processes are ad hoc or implicit.	Defined, traceable, and controlled processes are followed.

Cybersecurity Culture

A word without hard facts

Cognitions/Knowledge

Employees awareness, proven knowledge and beliefs

KNOW

ACT

Behaviors

Handling and responding cybersecurity topics

Attitudes

Feelings and emotions of employees about cybersecurity risks

FEEL

Making cybersecurity an integral part of employees' work and habits – more than just pushing policies and standards

The need of a strong Cybersecurity Culture

Two examples

We are human beings

- **Global** development & **cultural** differences
- **Separated teams** with different cybersecurity knowledge and awareness
- **Mistakes happen** – most IT breaches are caused by humans (82% in 2021)
  according to Forbes article

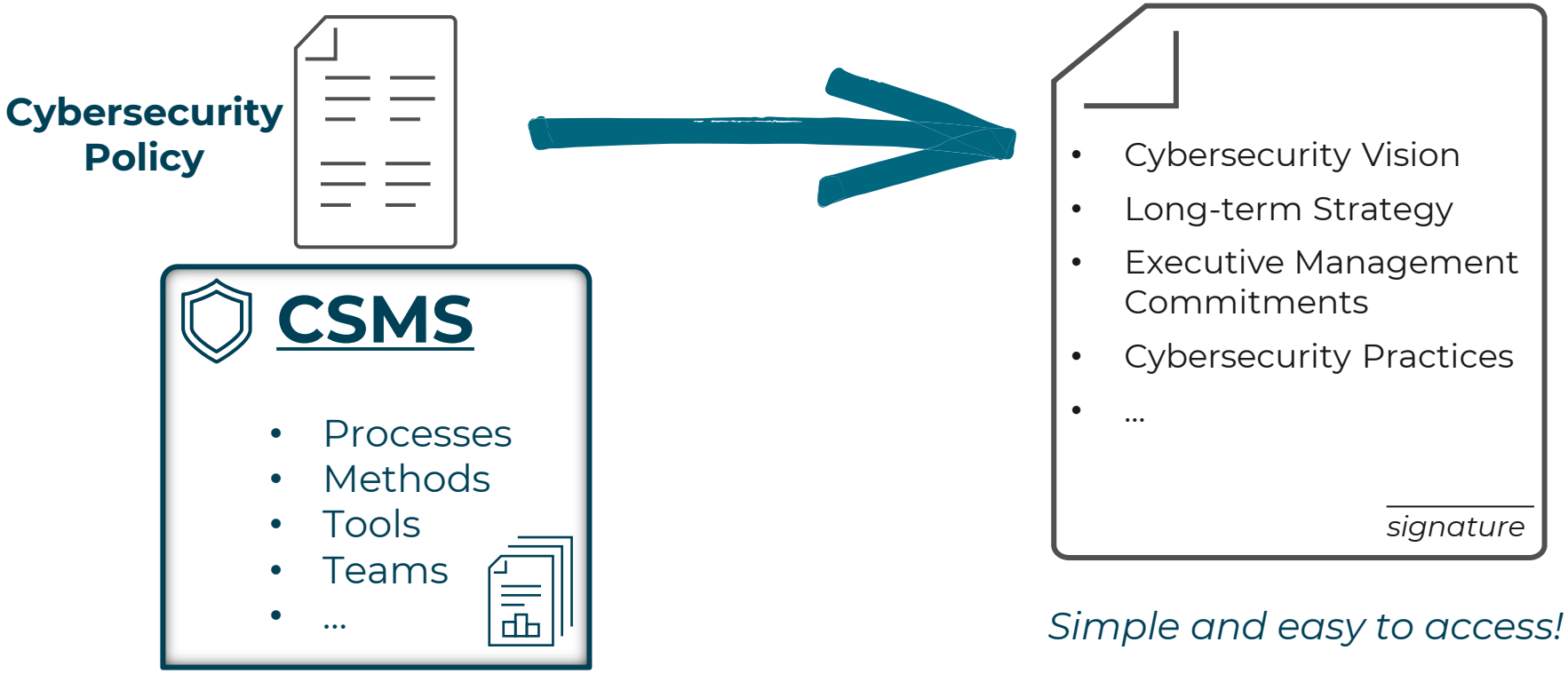
Time is not only linear

- Cybersecurity affects activities across the **whole life cycle**
- Cybersecurity means **anticipating** to the future
- Threats will always be **there** and even **evolve**

Measures to establish Cybersecurity Culture

Management point of view

Meaningful Top-Down Approach

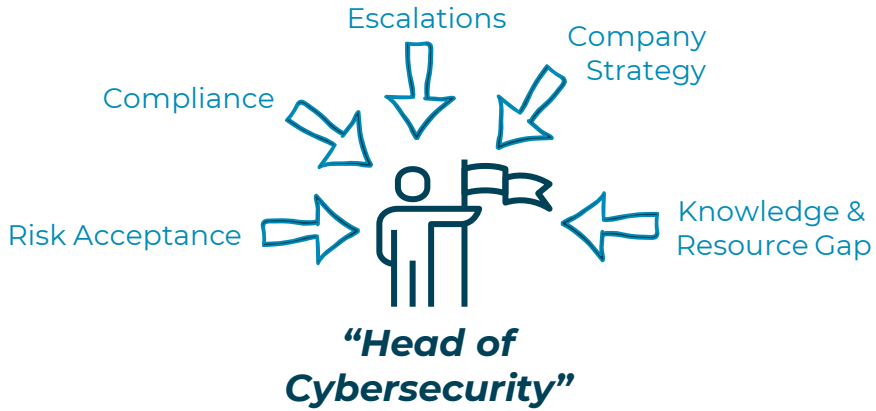


Simple and easy to access!

Measures to establish Cybersecurity Culture

Management point of view

Meaningful Top-Down Approach



- Overloaded
- Frustrated
- No decision making
- Missing support
- Mistakes

- **Vulnerabilities**

Development

Production

HR

IT

...

Project A

Project B

Project C

Measures to establish Cybersecurity Culture

Management point of view

Meaningful Top-Down Approach

- Represent departments' interests
- Ensure decision making progress
- Integrate individual experience and knowledge
- Share responsibilities
- Escalate to Executive Management

Cybersecurity Decision Board
("Cybersecurity Committee")

Development

Production

HR

IT

...

Project A

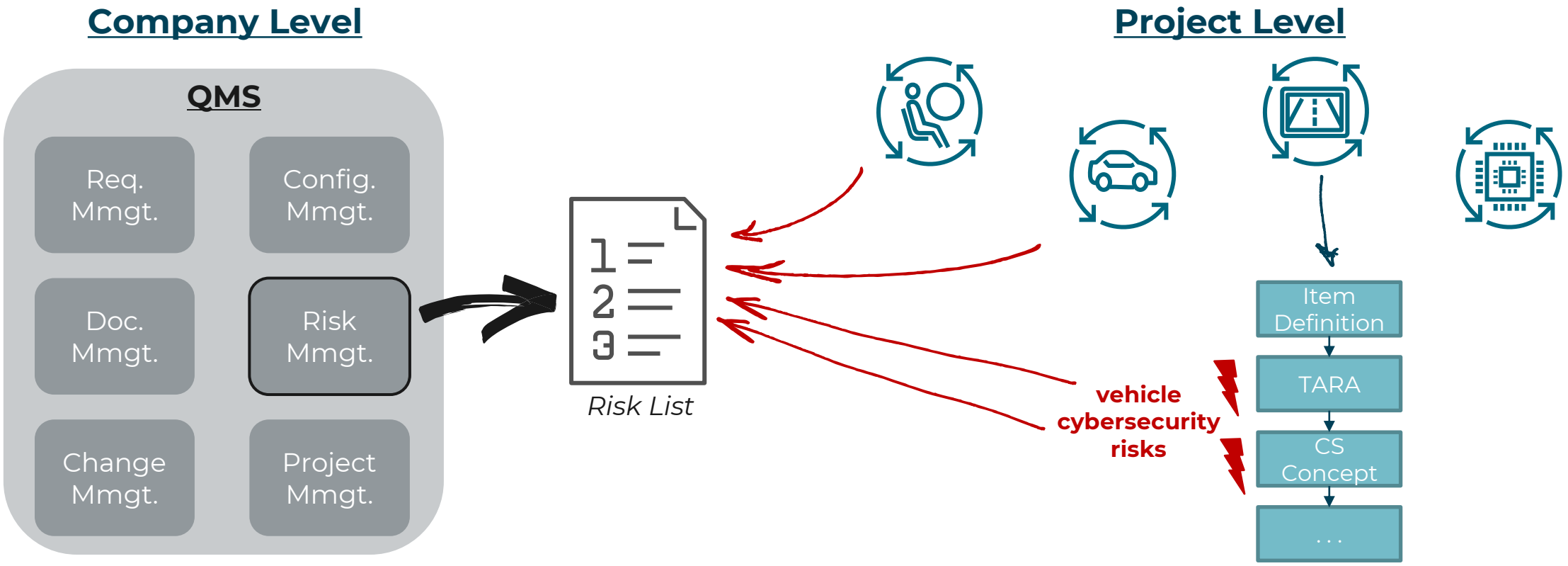
Project B

Project C

Measures to establish Cybersecurity Culture

Management point of view

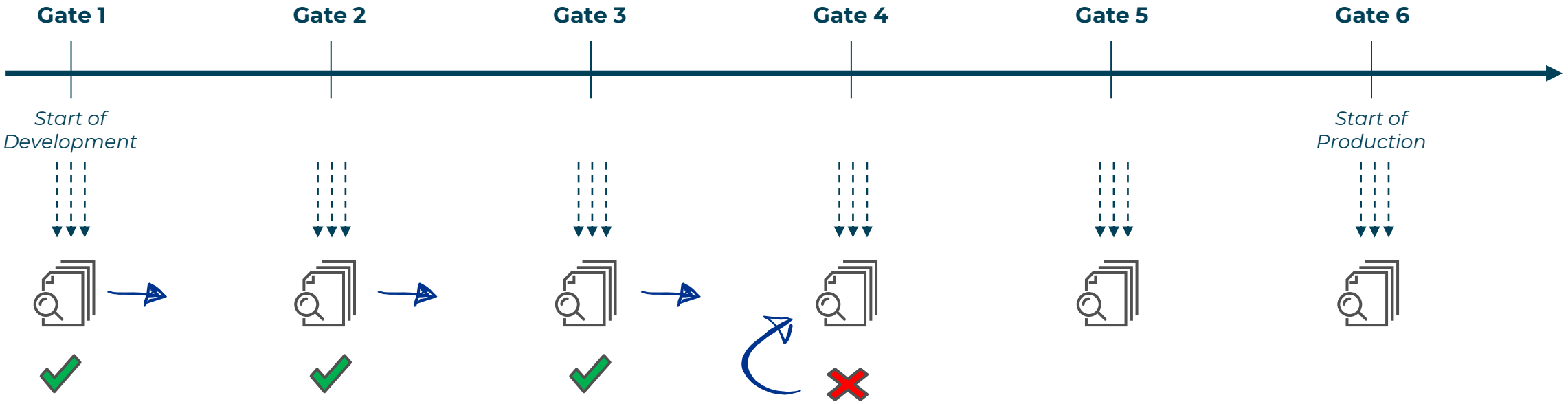
Holistic Risk Mmgt. Approach



Measures to establish Cybersecurity Culture

Project point of view

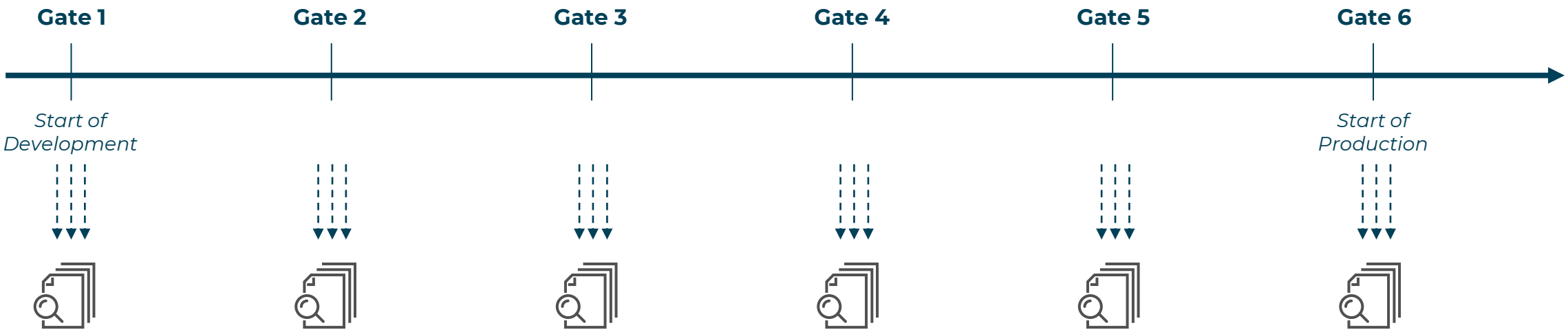
Overall Development Process



Measures to establish Cybersecurity Culture

Project point of view

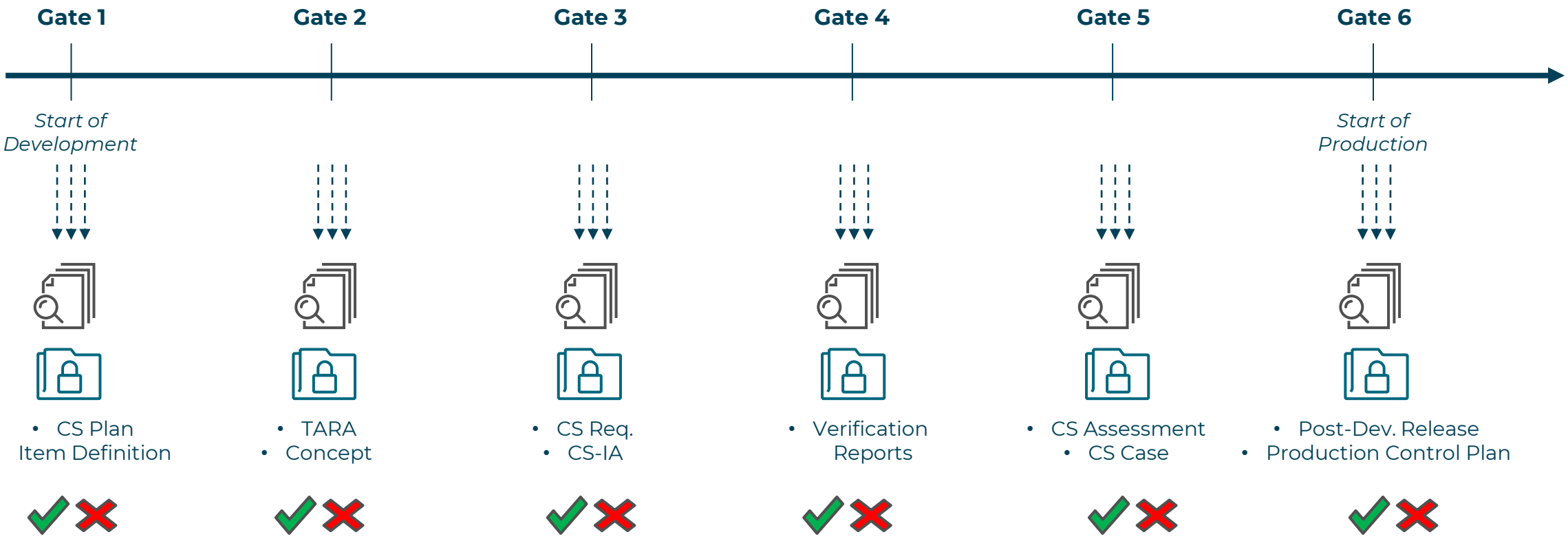
Overall Development Process



Measures to establish Cybersecurity Culture

Project point of view

Overall Development Process



Measures to establish Cybersecurity Culture

Project point of view

Shared Governance

Different cybersecurity related work products have different owners and creators

Work Product	CS Plan	Item Definition	TARA	CS Concept	CIA	CS SW Req	Production Control Plan
Owner	CS Manager	System Team	CS Engineer	CS Engineer	Purchase	SW Team	Man. Engineering

→Not all cybersecurity work products are in responsibility of the Cybersecurity Team

But: Cybersecurity Team needs evidences for Cybersecurity Case and/or Type Approval

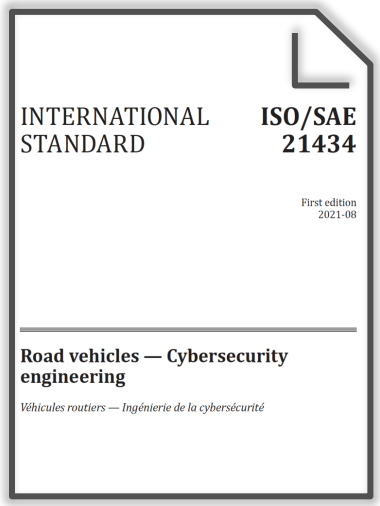
Shared governance between different team

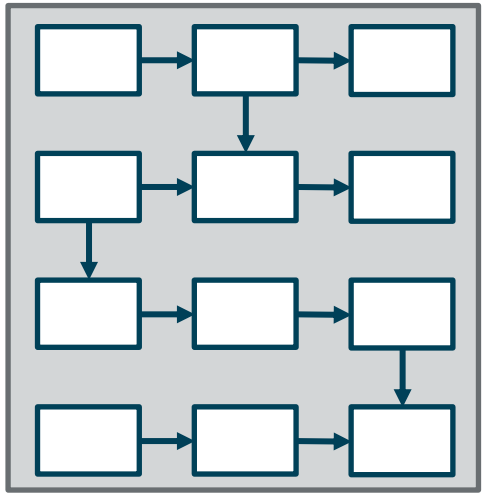
Measures to establish Cybersecurity Culture

Process point of view

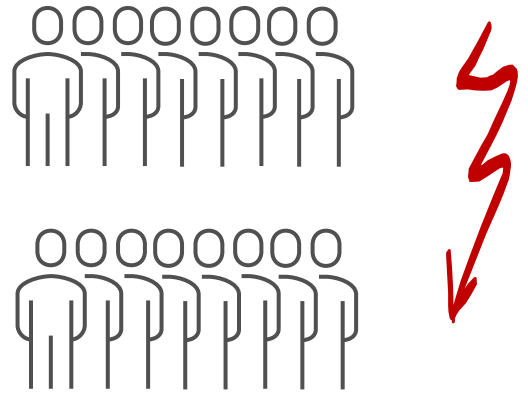
Strategic Process Roll-out and Training

→ *Blind compliance to ISO/SAE 21434*
→ *Overwhelmed Project Teams*
→ ***Missing acceptance***





Process Creation
- *by isolated process teams*
- *only based on ISO/SAE 21434*

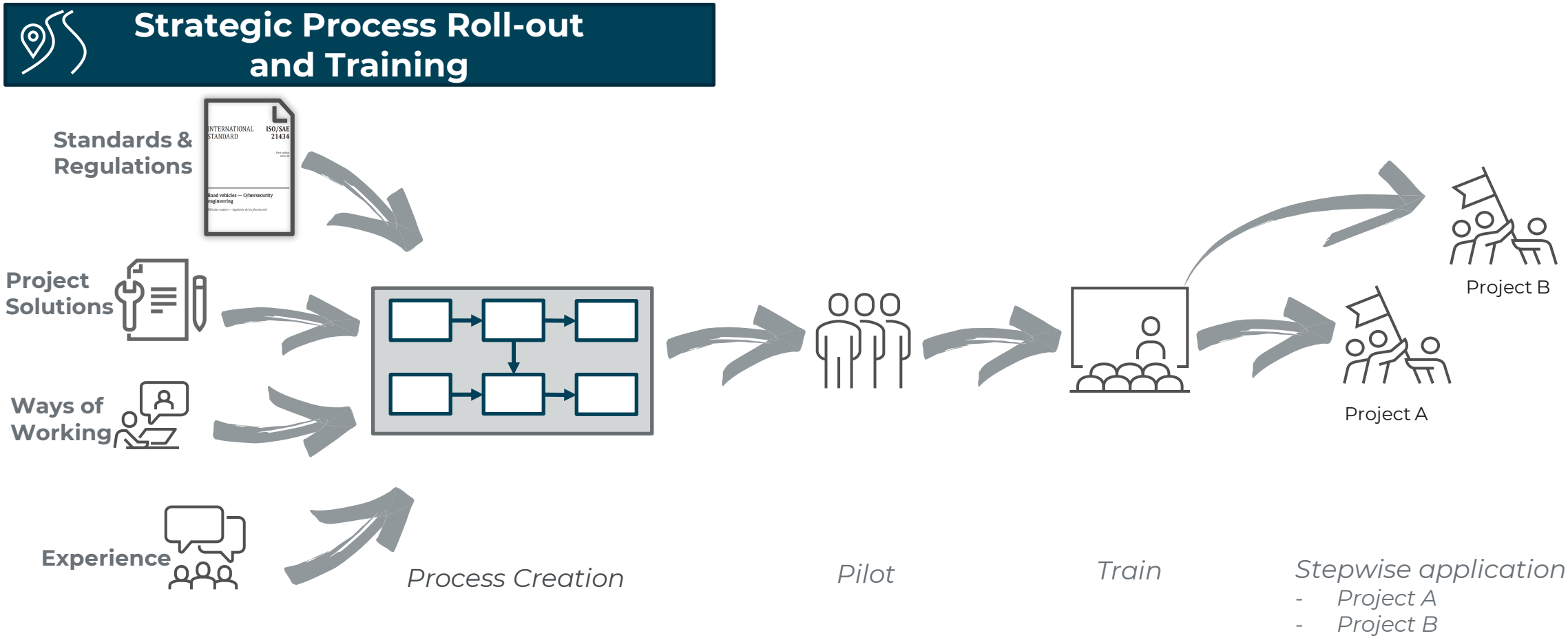


Process Roll-out
- *without verification*
- *without preparation*

"Big Bang"

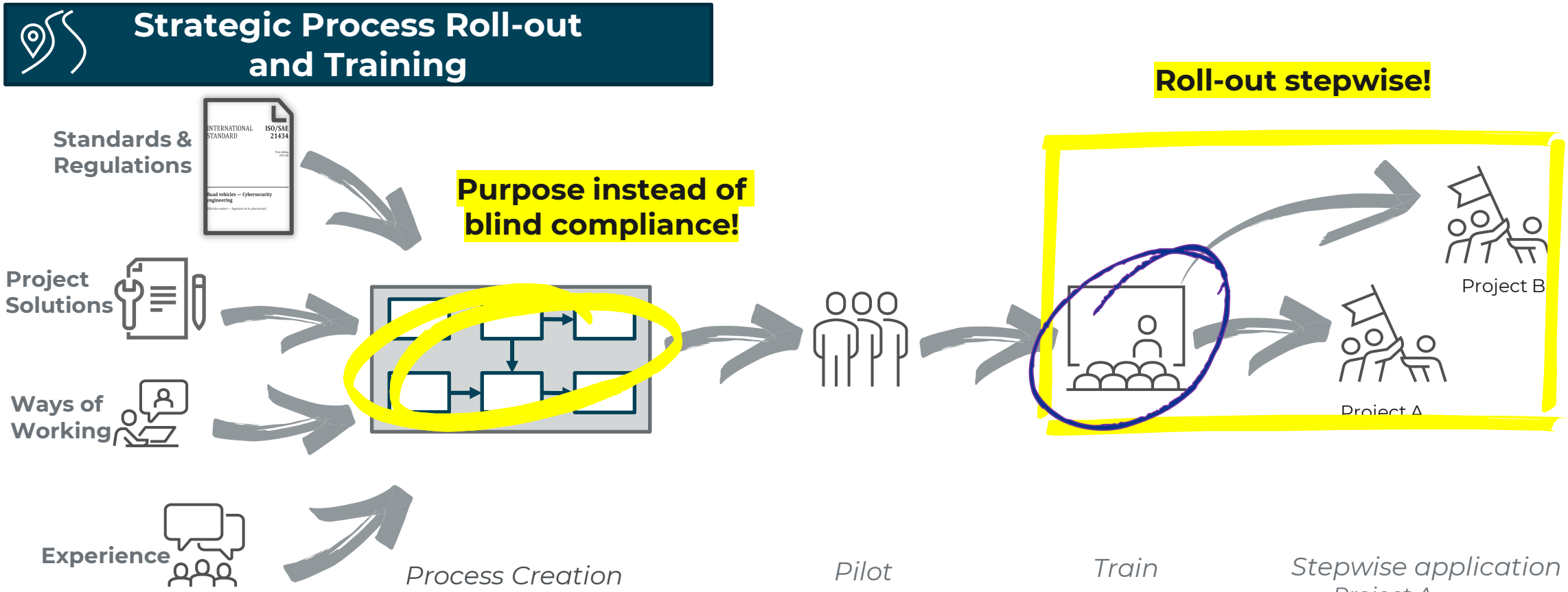
Measures to establish Cybersecurity Culture

Process point of view



Measures to establish Cybersecurity Culture

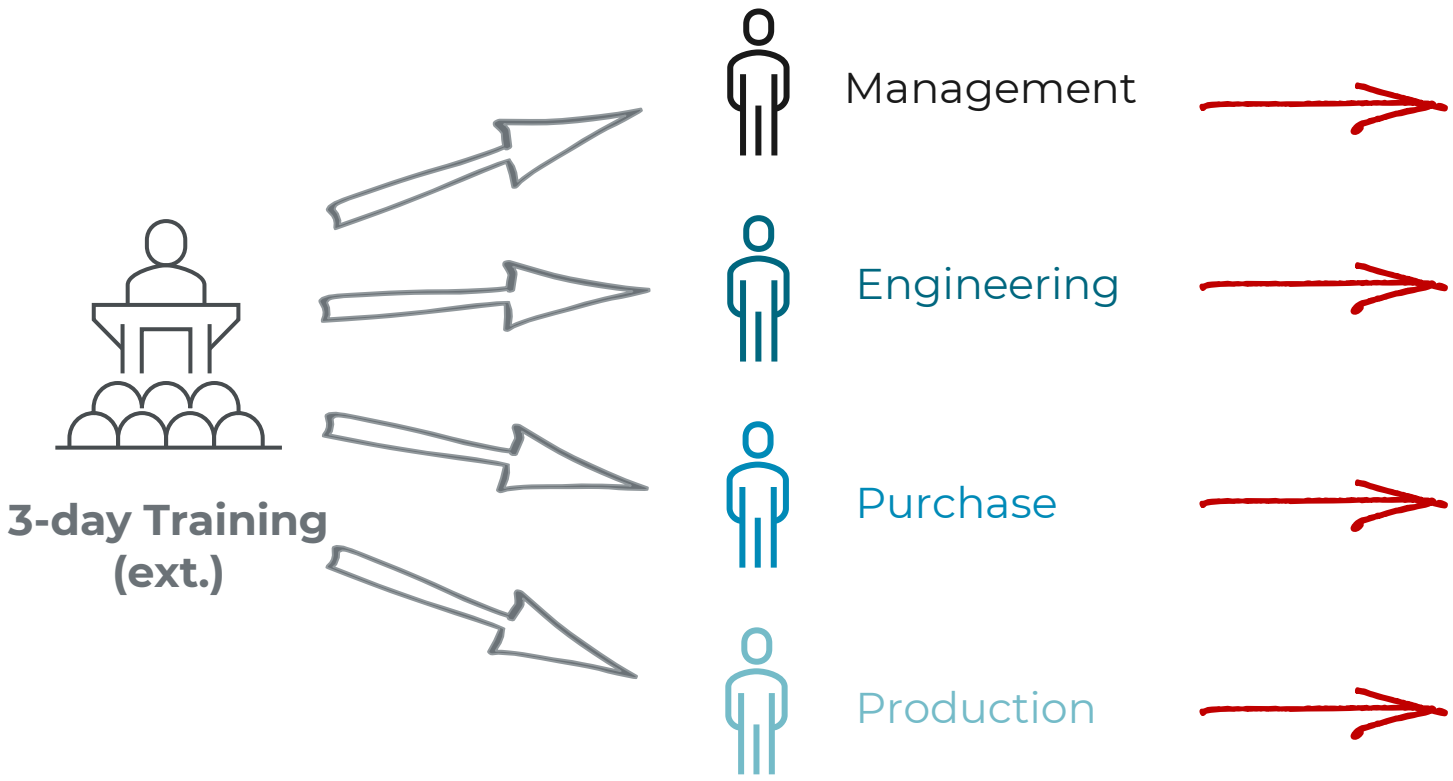
Process point of view



Measures to establish Cybersecurity Culture

Process point of view

Strategic Process Roll-out and Training



Employees...

- ... have to invest a lot of **time**
- ... are trained in **areas not relevant** for daily work
- ... only learn theory and **not company specific** approaches
- ... still **do not know** what changes for them

Measures to establish Cybersecurity Culture

Process point of view

Strategic Process Roll-out and Training

Cybersecurity **Training**

Technical knowhow

→ *Different levels for different needs*

- Awareness → *Get in touch*
- Basic → *Cybersecurity Interface*
- Advanced → *Apply Cybersecurity*

Company Processes

→ *Different teams: Same questions – different answers*

- What is my actual to-do?
- How can I solve it?
- Who to go in contract?
- Where to find needed info?
- . . .

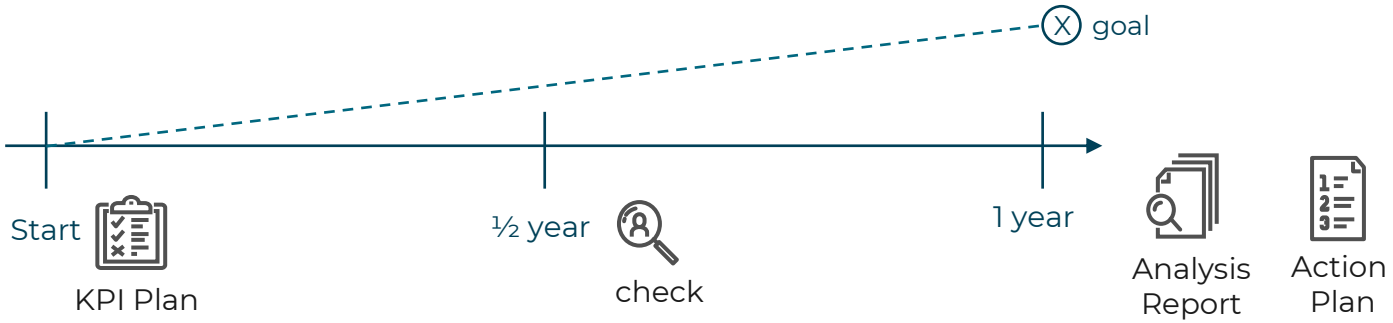
Tailored and **Modular** Training Approach required

Evidences for Cybersecurity Culture

ISO/SAE 21434 and UN R155 are **evidence** based

→ **Key Performance Indicators**

- *"quantifiable measure of a performance over time for a specific goal"*



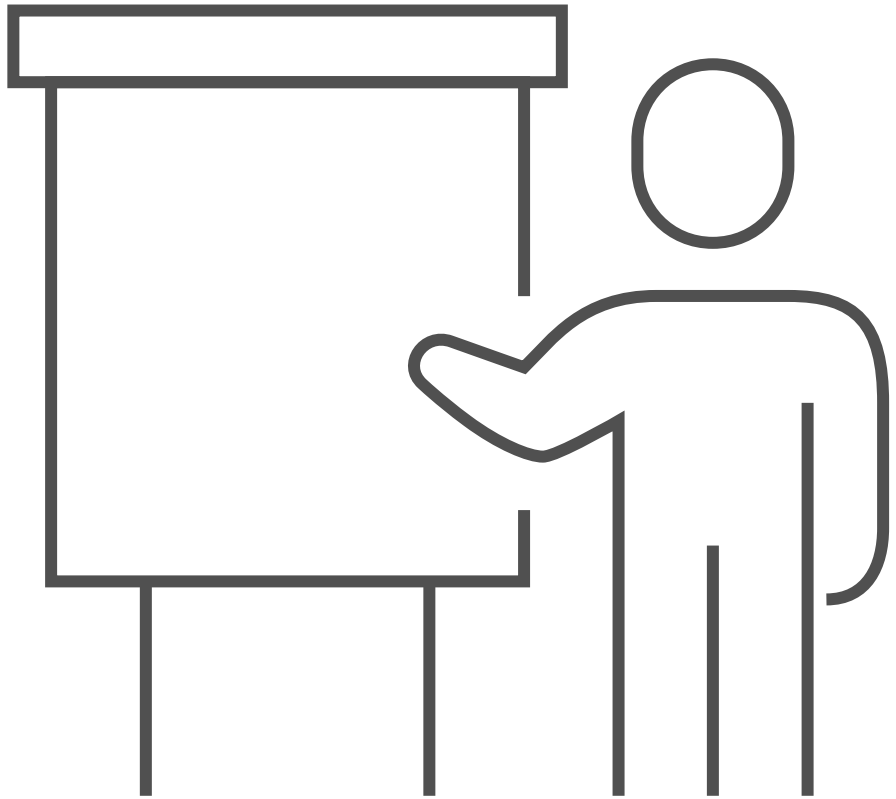
1. Goals derived from Cybersecurity Culture measures
2. KPIs defined in Cybersecurity KPI Plan
3. Check progress
4. KPI Plan, Analysis Report and Action Plan build evidence for Audit and Assessments

KPI examples

Area	Objective	KPI	Target Value
Org. Cybersecurity Management	Ensure Management Commitment	Number of executed CS Committee Meetings	1 per quarter
		Member of CS Committee participating in meetings	> 90% in average > 75% per meeting
	Establish CS Awareness	Number of trained engineers	> 80%
		Ratio between planned and attended training participants	> 90%
Project specific Cybersecurity Management	Integrate Cybersecurity into projects	Available deliverables per project milestone	> 90 % per milestone
	Identify supplier related risks	Received Cybersecurity deliverable from supplier acc. to CIA	> 80% per supplier
Cybersecurity Engineering	Ensure cybersecure product	Number of CS Requirement not been verified	< 10 %

Conclusion

- There is **no short-cut** for establishing a strong Cybersecurity Culture
- Cybersecurity Culture is about **people** management
- Cybersecurity Culture is an investment now which **pays off later**



CYRES

CONSULTING

CYRES Consulting Services GmbH
Highlight Towers
Mies-van-der-Rohe-Str. 8
80807 Munich
Germany

+49 (0) 89 9542 808 00
office@cyres-consulting.com

CYRES
CONSULTING