EIN ANSCHAULICHES BEISPIEL

ISCUE
embedded intelligence

CRA?

IEC 62443

CRA?

IEC 62443

EN 303645

CRA?

IEC 62443

EN 303645

ISO 27001

CRA?

IEC 62443

EN 303645

ISO 27001

ISO 21434

CRA?

IEC 62443

EN 303645

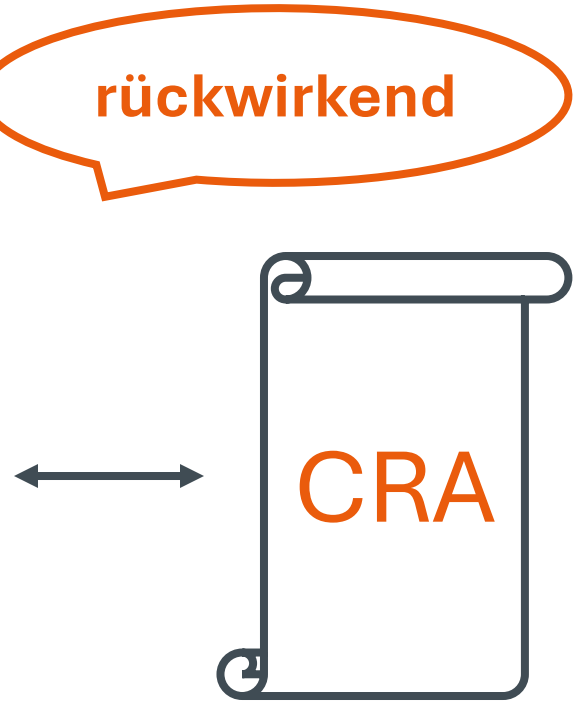
ISO 21434

ISO 27001

Risikoanalyse
schützenswerter Ziele,
Schwachstellenmanagement
...

CRA!

Risikoanalyse
schützenswerter Ziele,
Schwachstellenmanagement
…



Beispiel

Damals

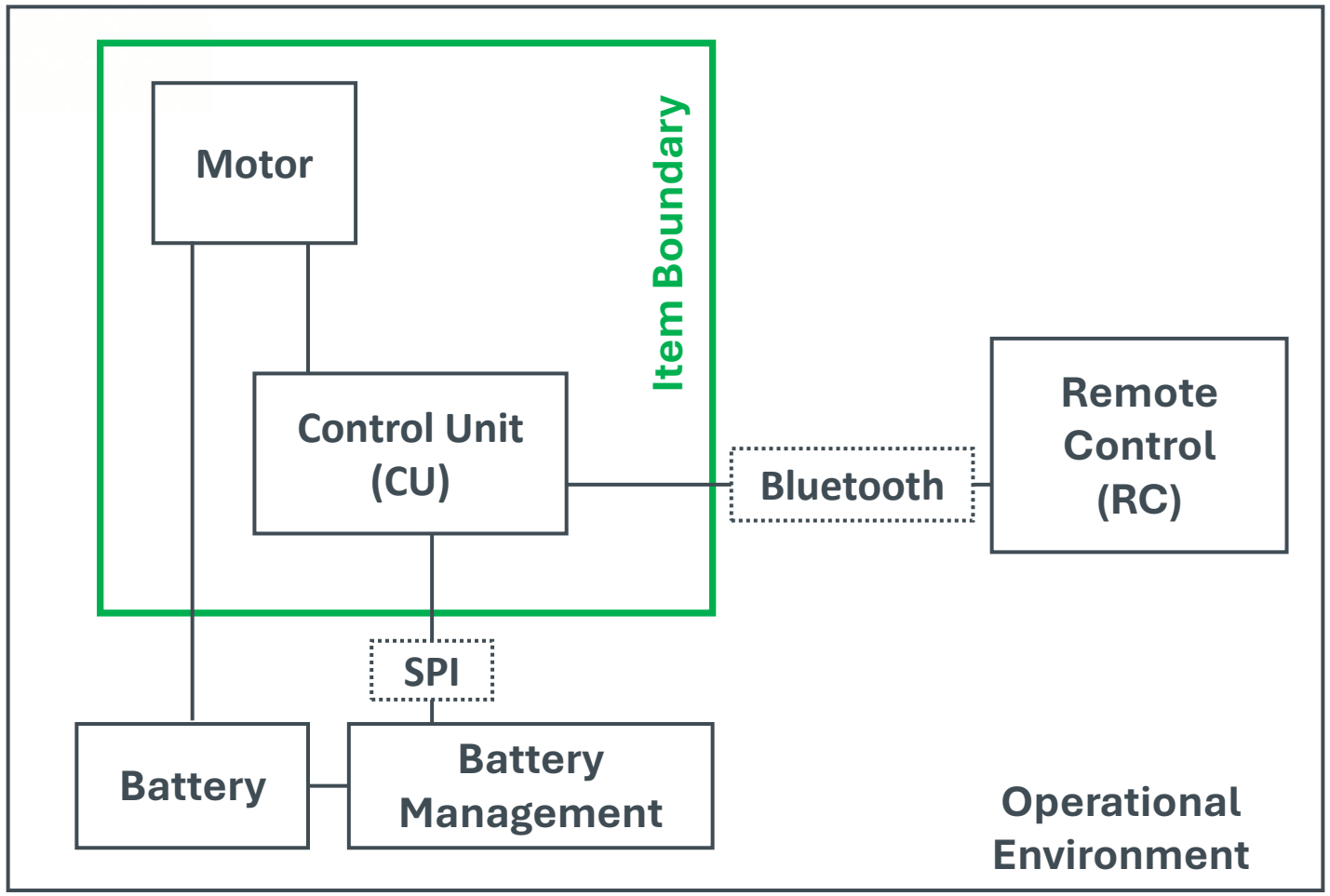
Risikoanalyse

Heute

CRA

Produktbeschreibung
Risikoanalyse
Szenarien
Konformitätserklärung
Prozesse
Security by Design
...

Item Definition



Grobe Architektur
Systemgrenze
Operationsumgebung
Funktionsbeschreibung

STRIDE

HEAVENS

OCTAVE

TARA

Risikoanalyse

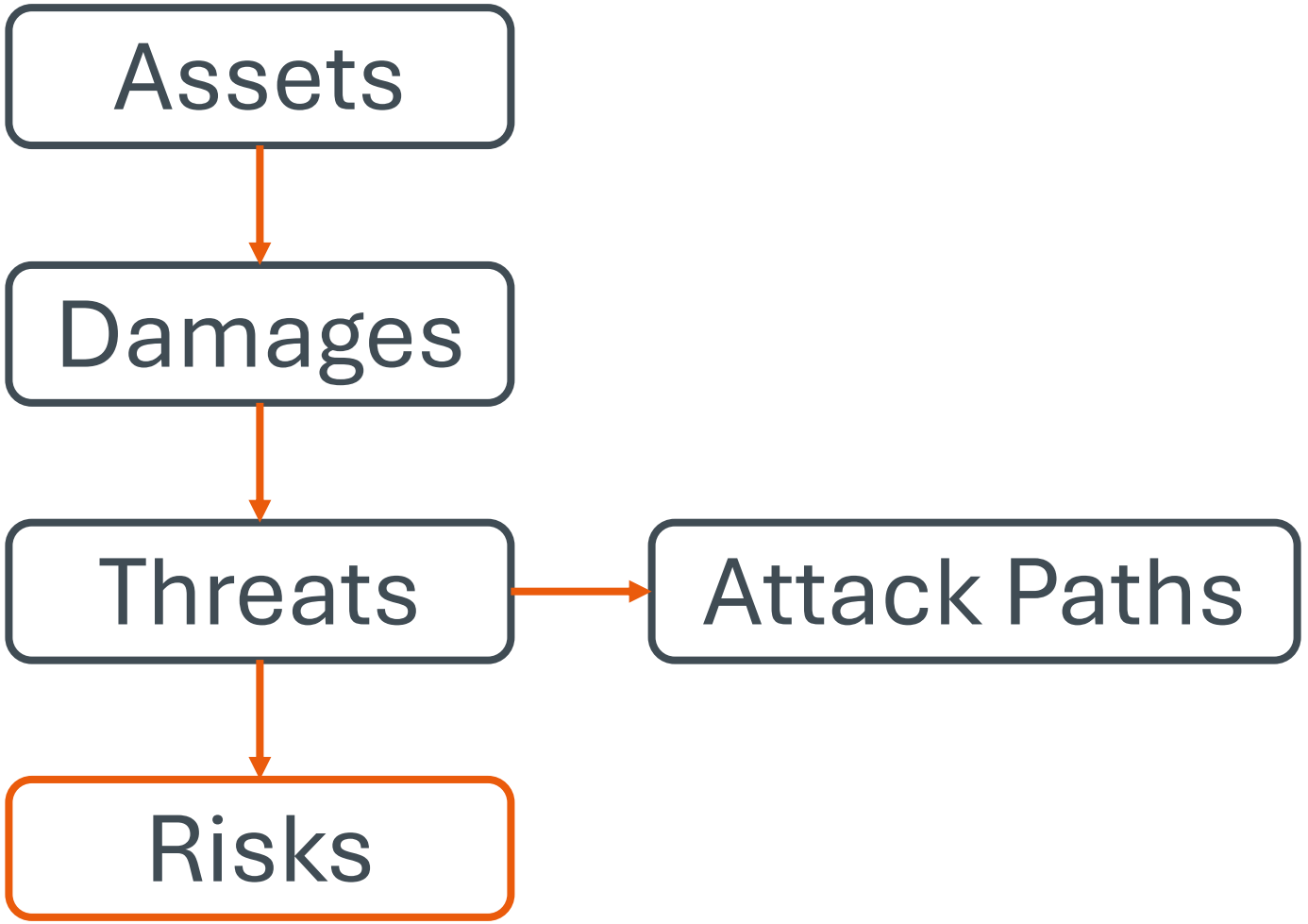
STRIDE

HEAVENS

OCTAVE

TARA

TARA



ID	Summary	Description	CS Property	Lifecycle States
AS1	Battery level signal	The battery level communicated by the BMS to the control unit via UART	Integrity, Availability	In Use, In Transit
AS2	Local speed level	The speed level locally used by the control unit	Integrity	In Use
AS3	Speed level signal	The new speed level requested by the user via the remote control; received via Bluetooth	Integrity, Availability	In Transit

Assets | Damages | Threats | Attack Paths | Risks | Goals | Claims

				Impact Rating			
ID	**Asset ID**	**Summary**	**Description**	**Safety**	**Financial**	**Operational**	**Privacy**
			damage is the missing indication and not the empty battery itself				
DI2	AS2	The longboard accelerates without user intention due to manipulated local speed level	The longboard unexpectedly accelerates without user input because the local speed level is changed by an attacker *Impact rating:* The unexpected movement can cause the user to fall off the board which can cause serious injuries	Major	Negligible	Negligible	Negligible
		The longboard	The longboard unexpectedly accelerates without user input because a manipulated speed level				

Assets | **Damages** | Threats | Attack Paths | Risks | Goals | Claims

TARA

ID	Damage ID	Summary	Description
TS1	DI1, DI4	Tampering with battery level signal on SPI	The attacker manipulates the battery level signal transmitted from the BMS to the CU
TS3	DI2	Tampering with the local speed level	The attacker manipulates the speed level in the CU memory so that the longboard accelerates without user intention.
TS2	DI3	Tampering with or spoofing	The attacker sends a malicious speed level signal via Bluetooth as if it

Assets | Damages | **Threats** | Attack Paths | Risks | Goals | Claims

TARA

				Feasibility (Attack potential based approach)					
ID	**Threat ID**	**Summary**	**Description**	**Time**	**Expertise**	**Knowledge**	**Opportunity**	**Equipment**	***Feasibility***
			3. Using the buffer overflow the attacker changes the local speed level in the memory of the CU						
AP2	TS3	Attacker sends invalid Bluetooth signal to attack the CU memory	1. The attacker sends an invalid Bluetooth signal 2. The transceiver picks up the signal and stores the message in a buffer 3. The CU software reads the invalid signal and due to incorrect handling of unexpected input a buffer overflow occurs	1 month	Expert	Public	Easy	Standard	*High*
			1. The attacker presents a device which intercepts the						

Assets | Damages | Threats | **Attack Paths** | Risks | Goals | Claims

TARA

ID	Threat	*Aggregated Impact*	*Aggregated Feasibility*	*Value*	CAL	Risk Treatment Decision
R1	TS2	*Financial: Moderate, Operational: Moderate*	*High*	*4*	4	Reducing the Risk
R2	TS3	*Safety: Major*	*High*	*4*	4	Reducing the Risk
R3	TS1	*Financial: Moderate, Operational: Moderate*	*High*	*3*	2	Retaining the Risk

Assets | Damages | Threats | Attack Paths | **Risks** | Goals | Claims

ISO 21434

ID	Risk ID	*Threat*	*CAL*	Summary	Description
G2	R2	*Tampering with the local speed level*	*4*	Firewall for Bluetooth	All messages received via Bluetooth shall be checked for consistency; invalid messages shall be rejected
G3	R2	*Tampering with the local speed level*	*4*	Static code analysis / coding guidelines	Coding Guidelines (e.g. CERT C) shall be used and the code shall be checked via static code analysis to reduce the risk of vulnerabilities like buffer overflows
G4	R1	*Tampering with or spoofing of the speed level signal*	*4*	Minimum length for Bluetooth session keys	Enforce a minimum length for Bluetooth session keys so that bruteforcing is prevented

Assets | Damages | Threats | Attack Paths | Risks | **Goals** | Claims


Bibliotheken
Firmware
Abhängigkeiten
SBOM


Änderung
Fremdsoftware
Schwachstelle
Dokumentenpflege

Schwach stellen

Kunden
Experten
...

Meldesystem

Schwach stellen

Kunden
Experten
...

Meldesystem

Offenlegen

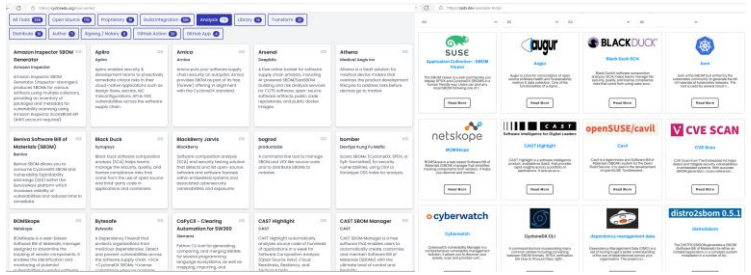
Schwach stellen

SBOM

CycloneDX

SPDX®

Online Tools



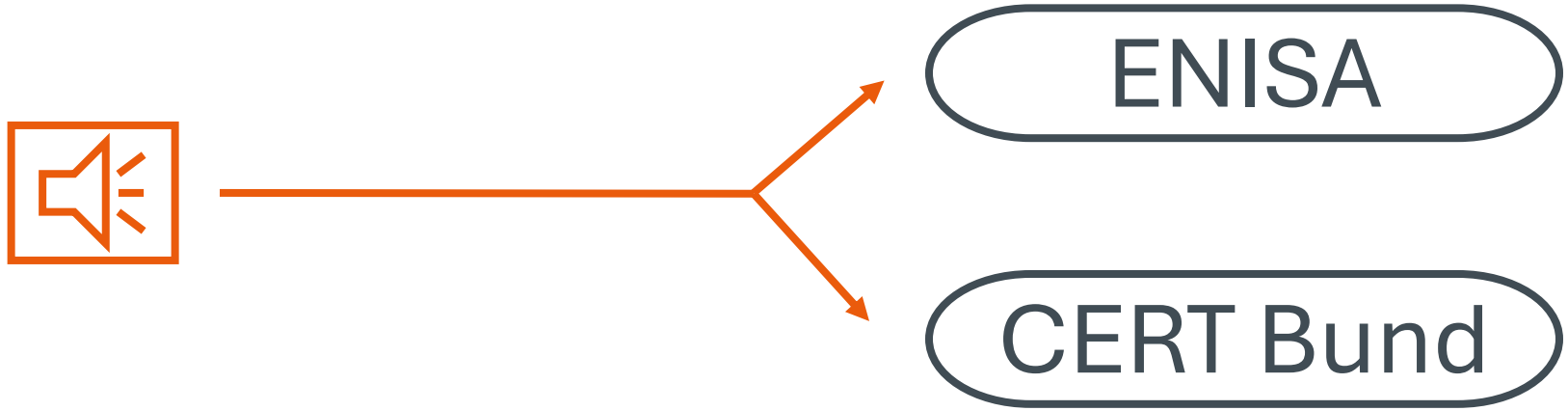
!

Schwach stellen

Meldepflicht

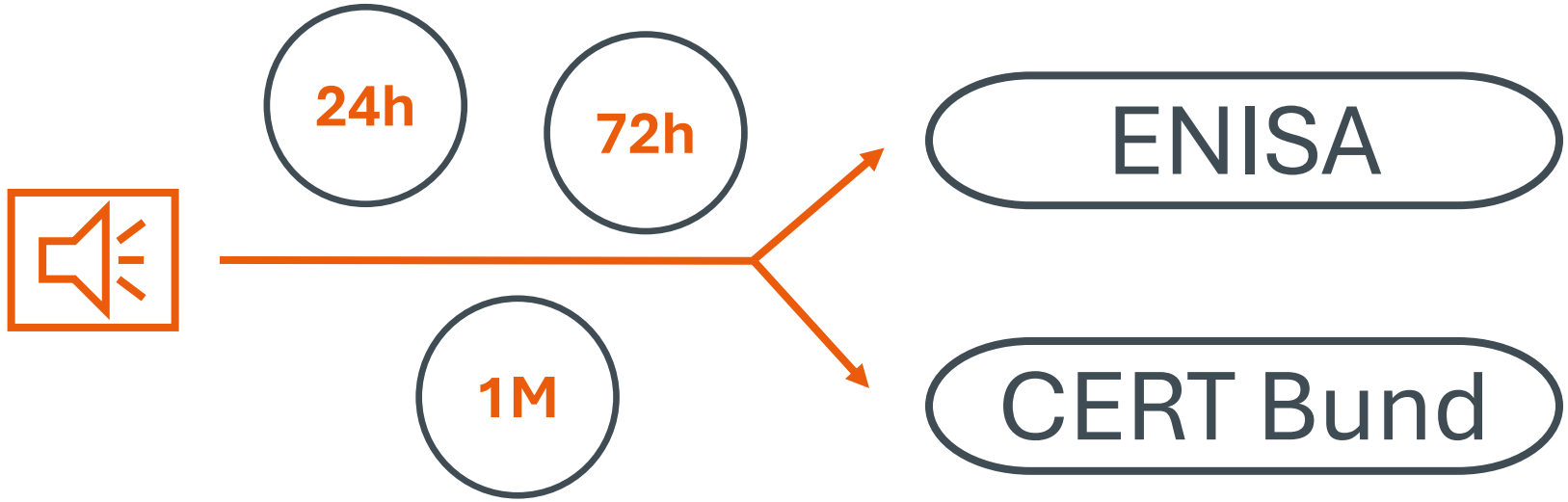
Schwach stellen

Meldepflicht

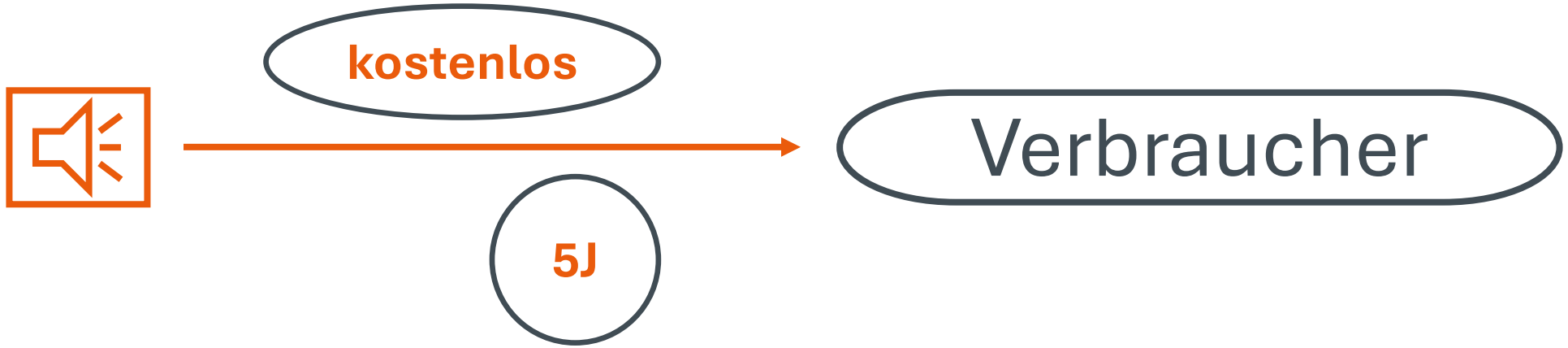


Schwach stellen

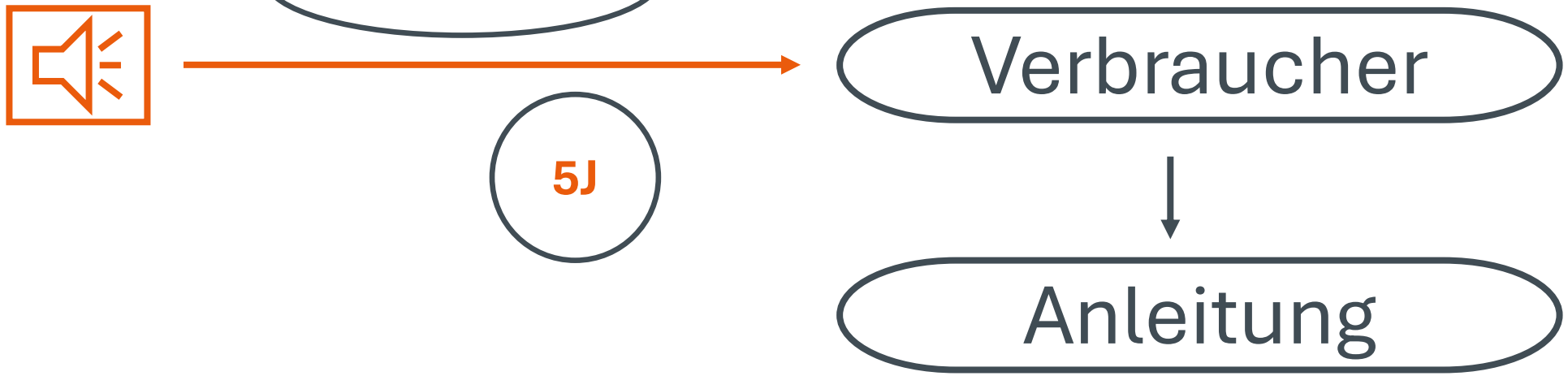
Meldepflicht



Sicherheitsupdate



Sicherheitsupdate



Prüfung?

Item Definition

Risikoanalyse

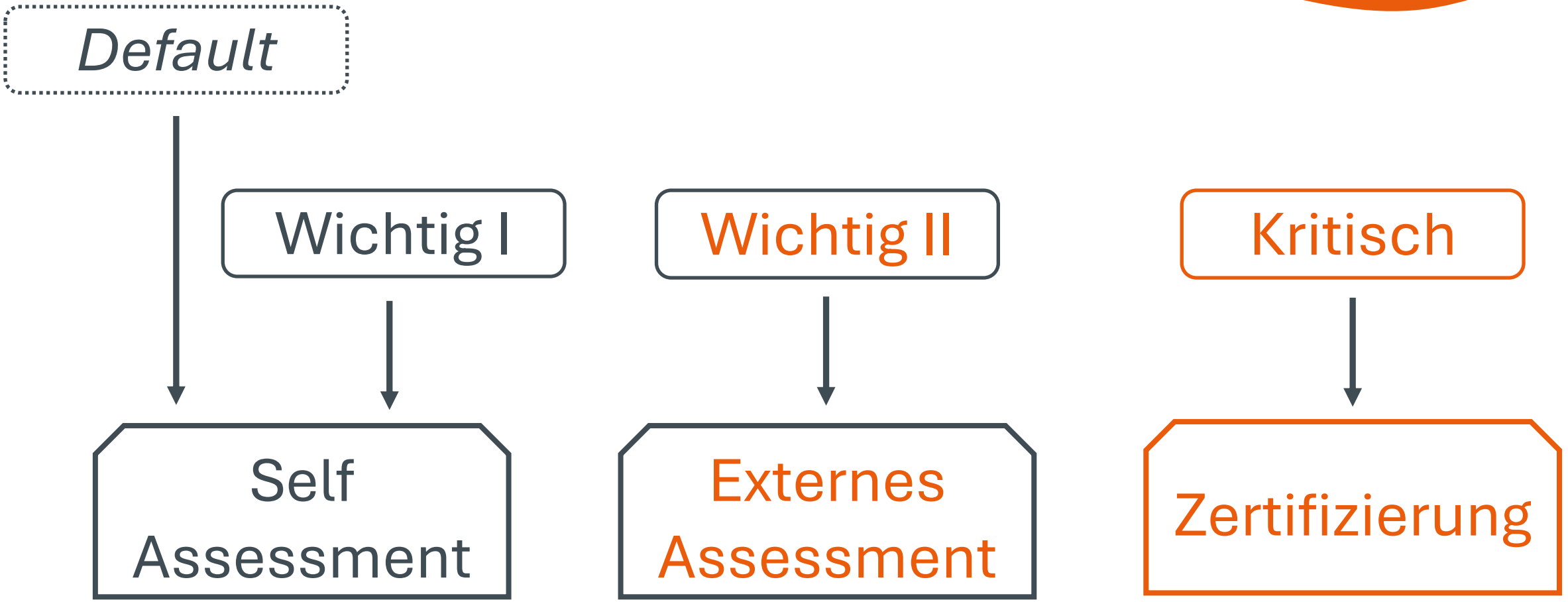
SBOM

Dokumentenpflege

Schwachstellen management

Meldepflicht

Assessment


Default
Wichtig I
Wichtig II
Kritisch
Self Assessment
Externes Assessment
Zertifizierung


35 Mitarbeiter, vor Ort in Nürnberg – wir spielen Ihnen den Ball zu
www.iscue.com
ISCUE
embedded intelligence