BSides Munich 2026

Beyond the Checkbox

Can Your NIS-2 Evidence Survive Reality?

Younes Ahmadzei
9 November 2026

“Yes, we have backups.”

Three fictional SMEs. The same answer.

A

A signed backup policy

B

Recent successful job logs

C

A successful restore test

What would you need before relying on that answer?

What the evidence supports

Evidence supplied	Supported conclusion	Still open
Signed policy	An approved recovery design	Whether teams follow it
Recent job logs	Recorded backup jobs ran	Whether recovery works
Successful restore test	The tested recovery worked	Coverage beyond that test

Confidence belongs to a specific claim, scope and date.

The practical starting point

1,800

German SMEs contacted

17

semi-structured interviews

Exploratory research and an SME self-assessment model

Non-representative sample. Examples today are synthetic.

The evidence lens

Claim	What exactly are we asserting?
Design	How should the measure work?
Operation	What shows consistent execution?
Effectiveness	What shows the intended outcome?

A teaching device. No official maturity levels or combined score.

A claim needs a service and a target

“We can recover MW-ERP for production planning.”

4 hours

maximum data loss

8 hours

target recovery time

Musterwerk 180: fictional manufacturer with 180 employees. In-scope status is a scenario assumption.

The ERP recovery test missed its targets

Criterion	Target	Recorded result
Data age at test start	At most 4 h	9 h 30 m
Operational recovery	Within 8 h	Stopped after 8 h 35 m
Business validation	Orders and schedules work	Not completed

12 June 2026 exercise: FAILED. Open actions at the 4 August evidence cut-off.

A useful evidence request

“Please provide the latest end-to-end MW-ERP restore-test record, including the recovery point, elapsed time, business validation and open corrective actions.”

Service scope + recent record + outcome + exceptions

A closed ticket can hide an open incident

17:40 Endpoint ticket closed

21:05 ERP restored and validated

A 3 h 25 m gap between ticket closure and business recovery

17 August 2026, synthetic case. Closure evidence must cover the affected service.

Reporting needs a defensible awareness time

Case benchmark: 17 August, 14:45

Case milestone	Early warning	Incident notification
Case deadline	18 Aug, 14:45	20 Aug, 14:45
Recorded submission	18 Aug, 15:48	20 Aug, 17:05
Delay against benchmark	1 h 03 m	2 h 20 m

§ 32 BSIG: without undue delay, at most 24 h / 72 h after awareness of a significant incident.

The headline says green

4 overdue high-risk actions

The dashboard’s own rule says red when more than two high-risk actions are overdue.

G-05 dashboard, data as at 24 June 2026. Reported overall status: Green.

Management oversight leaves a decision trail

Risk and consequence	What does management understand?
Decision and owner	Who accepts or treats the risk?
Date and resources	What will happen, and when?
Follow-up evidence	How will management verify progress?

A future meeting or training booking remains a plan until it happens.

Evidence gaps and observed failures differ

Evidence situation	Assessment language
Relevant evidence supports the claim	Demonstrated
Evidence covers only part of the claim	Partially demonstrated
Evidence shows the target was missed	Not demonstrated
Evidence cannot support a conclusion	Cannot be determined

Every judgement needs a scope, an evidence reference and a reason.

The evidence survival test

01 What exactly is the claim and its scope?

02 Who owns it, and how should it work?

03 What recent evidence shows consistent operation?

04 How was effectiveness tested, including failures?

05 What gap, owner and deadline follow?

Five questions to reuse in your next assessment

A finding that someone can close

MW-ERP recovery within the agreed targets is not demonstrated.

Field	Example
Evidence	B-07: 9 h 30 m data age, test stopped without acceptance
Action and owner	Head of IT fixes log protection and secret access, then retests
Proposed deadline	30 days from approval, with interim risk treatment now
Closure evidence	A dated ERP test meets both targets with business acceptance

Proposed remediation example. An action plan does not prove completion.

Priority follows the security consequence

Recovery	Can production planning resume?
Incident handling	Can people escalate and report on time?
Governance	Can leaders make and track informed decisions?

Ownership, urgency and completion evidence make a gap actionable.

Before the next “Yes”

“This evidence supports this claim, for this scope, at this date.”

Then name the gap, the owner and the evidence needed to close it.

Questions

Which “Yes” would you challenge first?

Younes Ahmadzei
linkedin.com/in/younes-ahmadzei-7536b42a3

Reporting clock: case detail

Event	Timestamp
Documented serious-impact assessment	17 Aug 2026, 14:45
External legal confirmation	18 Aug 2026, 14:30
Early warning submitted	18 Aug 2026, 15:48
Incident notification submitted	20 Aug 2026, 17:05

The case uses 14:45 as a conservative benchmark. Earlier awareness remains a question for assessment.

Official references

Published session	pretalx.com/bsides-munich-2026/talk/YVSF7Z/
§ 30 BSIG	Risk measures, documentation and effectiveness assessment
§ 32 BSIG	Staged reporting after awareness of a significant incident
§ 38 BSIG	Management implementation, oversight and regular training

German references checked 8 November 2026. Scope and sector-specific rules still matter.

Case evidence and limits

Backup	B-07 recovery exercise, 12 June 2026 Open-action status at 4 August
Incident	I-06 timeline, I-07 impact and I-08 receipts Scenario review at 21 August
Governance	G-05 dashboard and G-07 decision trail Scenario review at 21 August

All case records are synthetic. No customer evidence, prevalence estimates or claim of full compliance.