BSIDES MUNICH 2026 • FOUR-HOUR PRACTITIONER WORKSHOP

From Checkbox to Evidence

A Hands-On NIS-2 Assessment for a Fictional SME

PARTICIPANT BRIEFING / MUSTERWERK 180 GMBH

FORMAT	CASE	EVIDENCE	OUTPUT
4 hours	1 fictional SME	3 assessment rounds	90-day action plan

Your mission

Musterwerk 180 has answered “Yes” to three important security questions. Your team must determine what the available evidence actually demonstrates—and what remains assumption.

> **The practical question**
> Can the organisation support its claim with evidence of design, operation and effectiveness?

By the end of the workshop, you will be able to

- turn a broad “Yes” into a precise, assessable claim;
- distinguish written design from evidence of operation and effectiveness;
- identify contradictions, missing evidence and dangerous assumptions;
- formulate focused follow-up evidence requests; and
- translate findings into a prioritised 90-day improvement plan.

All organisations, people, records and incidents in this packet are synthetic. This workshop does not provide legal, certification or audit advice.

01 / CASE FILE

Meet Musterwerk 180

A growing Bavarian manufacturer whose management wants to know whether its security statements can withstand scrutiny.

Legal name	Musterwerk 180 GmbH (MW180)
Business	Manufacture of electrical drive and industrial automation components
Workforce	180 employees, including production, engineering, sales and administration
Location	One headquarters and production site in Bavaria, Germany
Operations	Two-shift production; customer delivery commitments depend on digital production planning
Customers	Industrial equipment manufacturers and system integrators in Germany and the EU
Quality context	ISO 9001-certified quality management; no formally certified information security management system
Assessment premise	For this exercise, MW180 is assumed to fall within the applicable NIS-2/BSIG scope. Applicability analysis is out of scope.

Why management commissioned the assessment

A customer questionnaire, insurer renewal and new regulatory expectations produced similar questions—but different internal answers. The executive team wants an evidence-based view of three topics before approving the next security budget.

> **Management request**
> Do not perform a certification audit or produce a binary compliance verdict. Show us which claims are supported, which are only partially demonstrated and what should happen next.

Scenario boundaries

- Treat the case information and evidence supplied by the facilitator as the complete exercise universe.
- Do not debate whether MW180 is legally in scope; use the stated premise.
- Assess the evidence—not the people who created it.

02 / OPERATING CONTEXT

How MW180 works

Use this baseline to understand business dependence and ownership. It is context—not proof that any control works.

Core systems and services

SYSTEM / SERVICE	BUSINESS USE	PRIMARY DEPENDENCE
Microsoft 365	Email, collaboration and document exchange	Customer, supplier and internal communication
MW-ERP	Orders, purchasing, production planning and dispatch	Production scheduling and delivery commitments
CAD/PDM	Product design files and engineering change records	Engineering and product continuity
Identity services	Active Directory and Microsoft Entra ID	User authentication and access management
File services	Departmental and project information	Daily work across office and engineering teams
Production-adjacent systems	Machine interfaces, PLC engineering and quality data	Manufacturing availability and product quality
Remote access	VPN and vendor support access	Remote work and external maintenance
Ticketing & backup	IT requests, incident records and protected copies	Operational support and recovery capability

Organisation and accountability

Executive management	CEO, COO and CFO; the management team approves budgets and business priorities.
Head of IT	Reports to the CFO and coordinates day-to-day IT operations and the internal NIS-2 workstream.
Internal IT	A small team supports users, infrastructure, applications and external providers.
Production	The COO and production leadership own manufacturing continuity and operational priorities.
External MSP	Provides infrastructure monitoring, selected administrative support and escalation assistance.
ERP vendor	Provides application maintenance and specialist support for MW-ERP.

03 / ASSESSMENT MANDATE

Three “Yes” answers to test

These statements come from MW180’s internal self-assessment. Your task is to assess what each one really means and what the evidence supports.

01	BACKUP & RECOVERY **“Backups for all business-critical systems are performed regularly and can be restored within business requirements.”**
02	INCIDENT HANDLING & REPORTING **“MW180 can identify, escalate, handle and report significant security incidents within required timelines.”**
03	CYBERSECURITY GOVERNANCE **“Management has assigned responsibility, oversees cybersecurity risk and fulfils its NIS-2 governance obligations.”**

Regulatory context for the exercise

Germany’s NIS-2 implementation framework gives particular relevance to incident reporting and management responsibility. For the workshop, use the following as orientation—not as a legal opinion:

Incident reporting	The German BSIG reporting process includes staged reporting duties, including early and 72-hour notifications for significant incidents.
Management responsibility	Management is expected to implement and monitor risk-management measures and to participate in relevant training.
Assessment focus	Evidence should show more than a policy statement: assess whether the intended process exists, is used and achieves its purpose.

04 / ASSESSMENT LENS

Claim → Design → Operation → Effectiveness

A practical workshop lens for examining evidence. It is not an official NIS-2 framework, certification method or maturity model.

LAYER	QUESTION	TYPICAL EVIDENCE
Claim	What exactly is the organisation saying—and for which scope?	Self-assessment answer, management statement, customer response
Design	Is there a defined process, responsibility or control that could achieve the intended result?	Policy, procedure, role description, system configuration, contractual requirement
Operation	Is the design actually being followed over time and within the stated scope?	Logs, tickets, approvals, meeting records, samples, training records
Effectiveness	Does the implemented measure achieve its intended outcome in realistic conditions?	Test result, restored service, exercise outcome, trend, incident review, verified completion

Use one status per assessed layer

Demonstrated	Relevant and sufficiently reliable evidence supports the layer for the stated scope.
Partially demonstrated	Some relevant evidence exists, but scope, consistency, recency or completeness is limited.
Not demonstrated	Available evidence contradicts the claim or shows that the intended practice did not occur.
Cannot be determined	The supplied evidence is insufficient to reach a defensible conclusion.

No mathematical average

Do not collapse Design, Operation and Effectiveness into one score. Preserve the evidence trail and explain your judgement layer by layer.

Evidence rules

- Use only the evidence supplied in the exercise.
- Do not assume that a plausible process is actually performed.
- Absence of evidence usually means “Cannot be determined”, not automatic failure.
- Record contradictions and differences in scope, date, owner or system.
- Cite the evidence ID and the exact passage, field or record that supports your judgement.
- Prefer a focused follow-up request over “send us everything”.

Do not jump to “compliant” or “non-compliant”

This case is designed to practise evidence-based judgement. A missing document may mean “Cannot be determined”; it is not automatically proof of legal non-compliance.

05 / TEAM WORKFLOW

Work like an assessment team

Each evidence round follows the same method. Roles rotate so everyone practises judgement, challenge and communication.

Suggested group roles

ROLE	RESPONSIBILITY	WORKING QUESTION
Lead assessor	Keeps scope and claim precise	What exactly are we assessing?
Evidence analyst	Finds and cites relevant material	What does the record actually show?
Challenger	Tests assumptions and contradictions	What would make this conclusion wrong?
Recorder	Maintains the worksheet and rationale	Can another team follow our reasoning?
Spokesperson / timekeeper	Controls time and reports the result	What is the clearest decision-relevant message?

Eight steps for every evidence round

1. Rewrite or confirm the exact claim and its scope.
2. Inventory the initial evidence and identify relevant items.
3. Map evidence to Design, Operation and Effectiveness.
4. Assign a status to each assessed layer and record the rationale.
5. Document contradictions, gaps and dangerous assumptions.
6. Formulate up to three precise follow-up evidence requests.
7. Review the follow-up evidence and update the assessment.
8. Draft one concise finding and one practical improvement action.

Progressive evidence release

The first evidence pack will not answer every question. Your follow-up requests determine what your team is trying to prove—not which answer it hopes to find.

Required output from each round

Exact claim • evidence references • layer-by-layer status • contradictions/gaps • follow-up requests • one finding • one improvement action

06 / FINAL SYNTHESIS

Turn evidence into a 90-day plan

The workshop ends with a management-ready plan—not a long list of observations.

Prioritised action plan

FIELD	WHAT TO CAPTURE	QUALITY TEST
Action	Maximum five concrete actions across the three assessment areas	Does it address an evidenced gap or risk?
Owner	One accountable role for each action	Is ownership unambiguous?
Time horizon	0–30, 31–60 or 61–90 days	Is the timing realistic and risk-informed?
Evidence of completion	The record or observable result that will show completion	Could an independent reviewer verify it?

Your 60-second management briefing

- One claim that is supported—and why
- One dangerous assumption that management should stop relying on
- Three priority actions for the next 90 days

A strong final message

separates fact from assumption, states the scope, cites the decisive evidence and gives management a concrete next step.

Official reference points

- BSI information on Germany's NIS-2 implementation and registration
- German BSIG § 32 — staged reporting duties for significant incidents
- German BSIG § 38 — management implementation, monitoring and training
- Directive (EU) 2022/2555 (NIS 2)

Version note: participant briefing v1.0. The facilitator will provide separate evidence packs and worksheets during the workshop. The legal references above are provided for learning context only.