QUALIFICATION REPORT (SAMPLE)

Hypothetical example. The company, findings, and evidence are entirely fictitious and serve solely to illustrate the methodology.

Report No.: MZG-2026-014 (example)
Date: 21 September 2026
Prepared by: Jan Richter, qualification expert for IT security (GxP methodology)
Client: SAMPLEWORKS GROUP (fictional), a global industrial conglomerate with EU subsidiaries in Germany and the Czech Republic, annual revenue above EUR 500 million

Scope: The EU IT unit of SAMPLEWORKS GROUP: 180 employees, hosting on Azure EU, 4 critical applications, 11 data processing agreements with processors.
Sources of requirements: GDPR Art. 28, 32, 33; NIS2UmsuCG (DE transposition act) § 30, § 33, § 38, § 39; BSI IT-Grundschutz modules APP / CLA / ORP.
Method: Qualification in three stages per measure:

- I – Installation: Is the measure configured correctly (configuration, policies, roles)?
- O – Operation: Does it run permanently and verifiably (logs, reports, repeat checks)?
- P – Performance: Does it hold under pressure (test, load, attack or failure scenario)?

Evidence classes (verification method stated per finding):

- CLIENT-COLLECTED: Raw evidence self-collected by the client via versioned, checksummed qualification protocols (raw script output, no assessments), methodically reviewed by the qualification expert.
- LIVE-OBSERVED: Performance test executed in a joint session under supervision of the qualification expert.
- NOT VERIFIABLE: [illegible] accepted.

---

1. Overall assessment

Metric	Value
Measures examined	20
Passed (I+O+P)	6
Partially passed (I ok, O or P missing)	9
Failed	5
Audit-readiness vis-à-vis authorities	limited

Key takeaway: The organization has good paperwork. 15 of 20 measures are documented. Only 6 of 20 can be defended today with execution evidence in an audit. This very gap between documented and operated measures is the sanction pattern of recent proceedings (CNIL/France Travail, Jan 2026: measures identified in the DPIA but not effectively implemented, EUR 5M; ANSPDCP/Renault, Mar 2026: appropriate measures and processor governance not evidenced; UODO/Poland, 2025: recognized risk without implemented mitigation).

---

2. Exemplary findings (excerpt, 5 of 20)

F1 – MFA for administrative and remote access

- Source: GDPR Art. 32(1)(b); NIS2UmsuCG § 30 (access control)

• I – Installation: CORRECT. MFA policy in place, Azure Conditional Access configured.

• O – Operation: DEFICIENT. Verifiable enforcement limited to VPN and mail. Admin consoles and the HR system authenticate via legacy authentication without MFA (login log export, 30 days: 1,214 admin logins without MFA).

• P – Performance: NOT TESTED. No test whether the policy actually blocks access when the second factor is denied.

• Assessment: Partially passed. On paper MFA applies everywhere; execution shows it does not apply where it counts. This is the exact "partial MFA" pattern criticized in CNIL and EDPB cases.

• Provable in an audit today: No.

F2 – Backup and recovery capability

• Source: GDPR Art. 32(1)(c) (restorability); NIS2UmsuCG § 30 (restoration)

• I: CORRECT. Immutable backups configured, schedule documented.

• O: PASSED. Daily job reports available and archived.

• P: FAILED. Last documented restore test: 19 months ago, one application of four.

• Assessment: Partially passed. Art. 32 requires the ability to restore, not a backup job. Untested backups are treated as deficient (EDPB breach examples; UODO case law: security must function in the failure scenario).

• Provable in an audit today: Partially (installation/operation), not performance.

F3 – Processor governance (Art. 28)

• Source: GDPR Art. 28(1); NIS2UmsuCG § 30 (supplier governance)

• I: CORRECT. 11 data processing agreements in place with control clauses.

• O: FAILED. No evidence of a single exercise of audit rights in 3 years (Art. 28(3)(h)). Processor risk assessment only at contract signature, no periodic reassessment.

• P: FAILED. No guarantees review (sub-processor lists, log access, leak tests) for 8 of 11 processors.

• Assessment: Failed. The verification duty is continuous; years of cooperation without audits do not constitute sufficient guarantees (UODO 2025; EDPB Guidelines 07/2020 para. 99).

• Provable in an audit today: No.

F4 – Registration and BSI obligations

• Source: NIS2UmsuCG § 33, § 38, § 39

• I: CORRECT. Registration completed in the BSI portal (evidence: portal confirmation).

• O: DEFICIENT. No process for updating changed data (2 weeks, § 33(5)). An IP-range change from June was updated after 31 days.

• P: OPEN. Management training evidence available, but no oversight report on implementation (reporting process never rehearsed; the 24h/72h/1-month deadlines never simulated).

• Assessment: Partially passed. From 2028, proof obligations apply under § 39; today's state would not survive an unannounced check of management duties (Directive Art. 34, § 38).

• Provable in an audit today: Registration yes, management oversight no.

F5 – Mobile device encryption

• Source: GDPR Art. 25, Art. 32(1)(a)

• I: CORRECT. Intune BitLocker policy, exception group "Field Engineering" (9 devices).

• O: FAILED. Exception without compensating control: no technical substitute, no time-boxed

sunset list, no quarterly review.

• P: Not reached (blocked by O failure).

• Assessment: Failed. Risk identified, measure on paper, permanent gap in execution: this is the lever for gross negligence in proceedings, because knowledge of the risk is established (UODO 2025: "knowledge of a risk without appropriate mitigation weighs more heavily than the absence of an analysis").

• Provable in an audit today: No.

---

3. Prioritized remediation plan (excerpt)

Priority	Action	Effort	Evidence target
1	MFA on all privileged systems, legacy authentication off	2–3 weeks	O+P: 30-day logs plus lockout test
1	Restore test of all 4 applications, quarterly	1 week per cycle	O+P: restore report plus sign-off
2	Processor audit cycle: 11 agreements, risk-based, payments first	one audit slot per agreement	O: audit reports, sub-processor evidence
2	Field Engineering: dissolve Intune exception, sunset list	2 weeks	I+O: configuration export, quarterly evidence
3	Reporting-process rehearsal (24h/72h) with management	1 day	O+P: exercise evidence per § 32/§ 38

4. Handover and validity

This report hands over 20 single assessments, 5 finished evidence packages and the remediation plan. Validity: 12 months or until the first revalidation trigger (new cloud provider, new critical systems, security incident, material change in the processor landscape). On expiry or on a trigger, the client decides anew, without obligation and without minimum term.

Legal notice: Professional qualification by an independent qualification expert. Not a certification, not a governmental audit, not legal advice.
