SWISS DIGITAL NETWORK

MANAGED RELIABILITY / OBSERVE

Observability Check

OBSERVE

FOCUSED SELF-ASSESSMENT

Prepared for Example Bank AG

Alex Muster / Head of IT / Operations / 22.10.2026

FOCUSED READINESS

50 / 100

MATURITY

Emerging

Some practices are present, but they appear fragmented, manual, or dependent on individual knowledge.

BUSINESS RISK

Medium

Derived from four self-reported controls.

Score: four original controls. Two additional diagnostic findings are reported separately and are not scored.

ASSESSED CAPABILITY

Observability

50 / 100

MOST CRITICAL NEXT STEP

Observability Foundation

Prioritise a shared view of one critical journey and connect meaningful signals to accountable incident response. Additional relevant findings are prioritised on the following page.

PRIORITISED ACTION SEQUENCE

Your reliability priorities

The most critical next step is highlighted first. The priorities below cover the other material findings from this focused Observability Check.

FOCUSED READINESS	POSTURE	MATERIAL GAPS
50 / 100	**Emerging** Medium business risk	**2 / 4** scored at level 0-1

PRIORITISED ACTION PLAN

Self-assessed and not yet validated against technical evidence.

FOCUS 01

START HERE

ACT

Create a shared view of service health

Create one trusted service view, SLOs and direct telemetry access for responders.

BASED ON VIS-01 / VIS-03 / ACC-01

EVIDENCE OF DONE

Trusted SLO view and direct telemetry access.

OWNER Service owner / observability

FOCUS 02

BUILD NEXT

ACT

Name who responds to outages and practise the response

Define customer-impact alerting, incident command, on-call, escalation and runbooks; rehearse once.

BASED ON VIS-02

EVIDENCE OF DONE

Timed rehearsal with named ownership and closed follow-ups.

OWNER Service owner / IT operations

START THIS WEEK

Select one critical service, name its accountable owner, and validate this plan against current evidence.

CURRENT STATE AND REQUIRED ACTION

Detailed action register 01-04

CONTROL	CURRENT STATE / REQUIRED ACTION
VIS-01 OBSERVE	Do you have one live dashboard for the customer journey? One journey view exists; not trusted by everyone **REQUIRED ACTION** Create one executive and one technical dashboard (Grafana) for the critical service journey.
VIS-02 OBSERVE	Do alerts warn you before customers notice? Alerts exist but are noisy or often too late **REQUIRED ACTION** Cut alert noise by rebuilding alerting on SLOs so a page means customer impact. Verify it with one incident simulation.
VIS-03 OBSERVE	Are metrics, logs and traces linked, with SLOs defined? Partly centralised; no correlation across signals **REQUIRED ACTION** Consolidate metrics, logs and traces into one Grafana-based view and define SLOs for the critical journey.
ACC-01 OBSERVE	Can responders access incident data without waiting? Core telemetry is accessible; access varies by team **REQUIRED ACTION** Provide role-based self-service access to metrics, logs and traces for every critical service, with clear ownership and access controls.

REQUEST PATHS AND RECENT CHANGES

Additional diagnostic findings

Separate from the four-control score. Unknown answers require verification. Diagnostic version 1.0.0.

OBS-ADD-01 / GAP TO ADDRESS

Can you locate where a request slows down or fails?

Your answer: Only for parts of the request path

NEXT ACTION

Map one critical request path. Connect missing service and dependency telemetry, then use a safe test to locate a slow or failing step.

Suggested owner: Service owner + observability lead

EVIDENCE TO CHECK

A recorded investigation or safe test identifies the slow or failing step; remaining blind spots have owners.

OBS-ADD-02 / GAP TO ADDRESS

Can you see what changed before an incident?

Your answer: No, we ask around or search separate records

NEXT ACTION

Bring deployment and configuration events into the service timeline. Include timestamps, affected services and links to change records. Investigate correlation before assigning a cause.

Suggested owner: Service owner + delivery / platform team

EVIDENCE TO CHECK

A service timeline shows a deployment and a configuration change alongside signals, with links to the underlying records.

ROUTING INPUTS / FINAL APPENDIX

Scope and interpretation

P-03

Do you operate business-critical applications?

Yes

Critical workloads are operated by the organisation.

SCORE BASIS

The score uses the four original observability controls and their existing weights. It reflects your answers, not verified incident performance.

DIAGNOSTIC FINDINGS

The two additional answers inform actions only. Unknown means not yet checked. A change near an incident does not prove it caused the incident.

INTERPRETATION AND LIMITS

Use these findings to investigate one critical application. Validate the suggested actions against your telemetry and incident experience. This report does not measure how quickly your team can diagnose an incident.

This focused Observability Check reflects only the selected questions. It is not a complete reliability assessment, technical audit, certification, legal advice, regulatory assessment, or external benchmark.