SWISS DIGITAL NETWORK

MANAGED RELIABILITY / OBSERVE

Observability Check

OBSERVE

FOKUSSIERTE SELBSTEINSCHÄTZUNG

Erstellt für Beispiel Bank AG

Alex Muster / Head of IT / Operations / 22.10.2026

READINESS-SCORE

50 / 100

REIFEGRAD

Im Aufbau

Einige Praktiken sind vorhanden, wirken aber fragmentiert, manuell oder vom Wissen einzelner Personen abhängig.

GESCHÄFTSRISIKO

Mittel

Abgeleitet aus vier selbst bewerteten Kontrollen.

Score: vier ursprüngliche Kontrollen. Zwei zusätzliche Diagnose-Ergebnisse werden separat ausgewiesen und nicht bewertet.

BEWERTETE FÄHIGKEIT

Observability

50 / 100

WICHTIGSTER NÄCHSTER SCHRITT

Observability-Grundlage

Schaffen Sie zuerst eine gemeinsame Sicht auf eine kritische Journey und verbinden Sie aussagekräftige Signale mit einer klar verantworteten Incident-Reaktion. Weitere relevante Ergebnisse sind auf der nächsten Seite priorisiert.

PRIORISIERTE MASSNAHMENFOLGE

Ihre Prioritäten

Der wichtigste nächste Schritt steht an erster Stelle. Die folgenden Prioritäten decken die übrigen wesentlichen Ergebnisse dieses fokussierten Observability Checks ab.

READINESS-SCORE	EINSTUFUNG	WESENTLICHE LÜCKEN
50 / 100	**Im Aufbau** Geschäftsrisiko: Mittel	**2 / 4** mit Stufe 0-1 bewertet

PRIORISIERTER MASSNAHMENPLAN

Selbsteinschätzung, noch nicht anhand technischer Nachweise validiert.

FOKUS 01

HIER STARTEN

UMSETZEN

Eine gemeinsame Sicht auf den Servicezustand schaffen

Eine verlässliche Service-Sicht, SLOs und direkten Telemetrie-Zugriff für Einsatzteams schaffen.

BASIEREND AUF VIS-01 / VIS-03 / ACC-01

NACHWEIS DER UMSETZUNG

Verlässliche SLO-Sicht und direkter Telemetrie-Zugriff.

VERANTWORTLICH Service Owner / Observability

FOKUS 02

DANACH AUFBAUEN

UMSETZEN

Verantwortliche für Störungen benennen und üben

Alerting nach Kundenauswirkung, Incident Command, On-Call, Eskalation und Runbooks festlegen; einmal üben.

BASIEREND AUF VIS-02

NACHWEIS DER UMSETZUNG

Zeitlich gemessene Übung mit benannten Verantwortlichen und abgeschlossenen Folgemassnahmen.

VERANTWORTLICH Service Owner / IT-Betrieb

DIESE WOCHE STARTEN Wählen Sie einen kritischen Service, benennen Sie die verantwortliche Person und prüfen Sie diesen Plan anhand aktueller Nachweise.

AKTUELLER STAND UND ERFORDERLICHE MASSNAHME

Massnahmenregister 01-04

KONTROLLE	AKTUELLER STAND / ERFORDERLICHE MASSNAHME
VIS-01 OBSERVE	Haben Sie ein Live-Dashboard für die Customer Journey? Eine Journey-Sicht existiert, wird aber nicht überall vertraut MASSNAHME: Erstellen Sie ein Management- und ein technisches Dashboard (Grafana) für die kritische Service-Journey.
VIS-02 OBSERVE	Warnen Alerts Sie, bevor Kunden etwas merken? Alerts sind laut oder häufig zu spät MASSNAHME: Reduzieren Sie Fehlalarme, indem Sie das Alerting auf SLOs aufbauen, damit ein Alarm echte Kundenauswirkung bedeutet. Prüfen Sie das mit einer Incident-Simulation.
VIS-03 OBSERVE	Sind Metriken, Logs und Traces verknüpft und SLOs definiert? Teilweise zentralisiert, aber nicht korreliert MASSNAHME: Führen Sie Metriken, Logs und Traces in einer Grafana-basierten Sicht zusammen und definieren Sie SLOs für die kritische Journey.
ACC-01 OBSERVE	Kommen Einsatzteams ohne Wartezeit an die Incident-Daten? Kerndaten sind zugänglich, der Zugriff variiert MASSNAHME: Geben Sie rollenbasierten Self-Service-Zugriff auf Metriken, Logs und Traces für jeden kritischen Service, mit klarer Verantwortung und Zugriffskontrollen.

REQUEST-PFADE UND LETZTE ÄNDERUNGEN

Zusätzliche Diagnose-Ergebnisse

Getrennt vom Score der vier Kontrollen. Unbekannte Antworten müssen geprüft werden. Diagnoseversion 1.0.0.

OBS-ADD-01 / LÜCKE SCHLIESSEN

Finden Sie heraus, wo ein Request langsam wird oder fehlschlägt?

Ihre Antwort: Nur für Teile des Request-Pfads

NÄCHSTE MASSNAHME

Bilden Sie einen kritischen Request-Pfad ab. Ergänzen Sie fehlende Telemetrie für Services und Abhängigkeiten und lokalisieren Sie dann in einem sicheren Test einen langsamen oder fehlerhaften Schritt.

Vorgeschlagene Verantwortung: Service Owner + Observability Lead

ZU PRÜFENDER NACHWEIS

Eine dokumentierte Untersuchung oder ein sicherer Test zeigt den langsamen oder fehlerhaften Schritt; verbleibende blinde Flecken haben Verantwortliche.

OBS-ADD-02 / LÜCKE SCHLIESSEN

Sehen Sie, was sich vor einem Incident geändert hat?

Ihre Antwort: Nein, wir fragen nach oder suchen in getrennten Aufzeichnungen

NÄCHSTE MASSNAHME

Bringen Sie Deployment- und Konfigurationsereignisse in die Service-Zeitachse, mit Zeitstempeln, betroffenen Services und Links zu den Change Records. Prüfen Sie Zusammenhänge, bevor Sie eine Ursache festlegen.

Vorgeschlagene Verantwortung: Service Owner + Delivery- / Plattform-Team

ZU PRÜFENDER NACHWEIS

Eine Service-Zeitachse zeigt ein Deployment und eine Konfigurationsänderung neben den Signalen, mit Links zu den zugrunde liegenden Aufzeichnungen.

KONTEXTANGABEN / ANHANG

Umfang und Einordnung

P-03

Betreiben Sie geschäftskritische Anwendungen?

Ja

Kritische Workloads werden von der Organisation betrieben.

GRUNDLAGE DES SCORES

Der Score nutzt die vier ursprünglichen Observability-Kontrollen und ihre bestehende Gewichtung. Er spiegelt Ihre Antworten, nicht die nachgewiesene Leistung bei Incidents.

DIAGNOSE-ERGEBNISSE

Die zwei zusätzlichen Antworten fliessen nur in Massnahmen ein. Unbekannt heisst: noch nicht geprüft. Eine Änderung kurz vor einem Incident beweist nicht, dass sie ihn verursacht hat.

EINORDNUNG UND GRENZEN

Nutzen Sie diese Ergebnisse, um eine kritische Anwendung zu untersuchen. Prüfen Sie die vorgeschlagenen Massnahmen anhand Ihrer Telemetrie und Ihrer Erfahrung mit Incidents. Dieser Report misst nicht, wie schnell Ihr Team einen Incident diagnostizieren kann.

Dieser fokussierte Observability Check bildet nur die ausgewählten Fragen ab. Er ist keine vollständige Reliability-Bewertung, kein technisches Audit, keine Zertifizierung, keine Rechtsberatung, keine regulatorische Beurteilung und keine externe Benchmark.