Executive Cyber Security Risk Assessment

Webeo Bank AG

Confidential Report for Board & Executive Management

DEMO REPORT

Generated by Webeo GmbH

webeo.ch

performant static websites
impactful, privacy-first,

SECTION 1 OF 8

Risk Overview

OVERALL RISK RATING

Webeo Bank AG · February 2026

ELEVATED

Risk Rating

An **Elevated** rating indicates demonstrable control gaps that could result in operational disruption, regulatory sanction, or reputational harm if exploited. Immediate, structured remediation is required. This rating reflects control adequacy relative to the threat landscape applicable to a FINMA-supervised institution — not an assessment of imminent breach.

Key Risk Drivers

- Excessive and unreviewed privileged access across core banking systems
- Absence of immutable backup architecture — critical ransomware exposure
- Insufficient security event logging and real-time monitoring
- No formally tested Incident Response plan
- Remote access MFA not consistently enforced across all user segments

Webeo Bank AG operates in a high-assurance environment where client trust, data confidentiality, and regulatory compliance are non-negotiable. The identified gaps collectively represent a material risk to uninterrupted operations and expose the Board to potential liability in the event of a security incident.

SECTION 2 OF 8

Executive Summary

Sentinel AG was engaged to conduct an independent executive-level security assessment of Webeo Bank AG's information security posture. The assessment covered identity and access governance, infrastructure exposure, monitoring maturity, data protection controls, and incident readiness. Findings are cross-referenced against ISO 27001 control objectives and FINMA's Circular 2023/1 on operational risk.

Security Maturity

The organisation's current posture is **reactive**. Controls exist across most domains but were implemented incrementally without a unifying framework, resulting in coverage gaps, inconsistent enforcement, and limited real-time threat visibility. No current formal risk register or documented security roadmap aligned to business strategy was identified.

Concentration of Exposure

Risk is disproportionately concentrated in three areas: **Identity and Privileged Access**, **Backup and Recovery Resilience**, and **Security Monitoring**. These represent the primary attack surface for threat actors targeting financial institutions. Weakness in any one amplifies the impact of a security incident significantly.

Audit Readiness

The organisation is not currently positioned for audit readiness. Documentation of access reviews, security policies, and control testing is incomplete. A FINMA enquiry or ISO 27001 audit in the current state would likely result in significant findings requiring remediation commitments.

SECTION 3 OF 8

Prioritised Risk Register

Risk levels reflect likelihood of exploitation combined with potential business impact under current control conditions.

#	Risk Area	Business Impact	Likelihood	Timeframe	Level
1	**Excessive Privileged Access**	Misused admin credentials could enable full system compromise or data exfiltration.	High	0–30 d	Red
2	**Immutable Backup Absence**	Without write-protected backups, ransomware attacks may render recovery infeasible.	High	30–60 d	Red
3	**Inadequate SIEM / Monitoring**	Threat actors may operate undetected, increasing dwell time and breach severity.	Medium	30–90 d	Red
4	**Incident Response Gap**	No tested IR plan materially increases regulatory liability and recovery time.	Medium	30–60 d	Amber
5	**Inconsistent MFA**	Partial MFA coverage leaves credential attack vectors open across remote access.	High	0–30 d	Amber
6	**No Formal Access Reviews**	Accumulated entitlements increase insider threat risk and fail ISO 27001 requirements.	Low	30–60 d	Amber
7	**Patch Management Gaps**	Known vulnerabilities in unpatched systems provide exploitable footholds.	Medium	30–60 d	Amber
8	**Policy Documentation**	Absent or incomplete policies impair audit defensibility and staff accountability.	Low	60–90 d	Green

SECTION 4 OF 8

Business Impact Analysis

Operational Risk

A successful ransomware or destructive attack against core systems could interrupt banking operations for days to weeks. Without tested recovery procedures and immutable backups, mean time to recovery is unpredictable, carrying direct cost implications and potential contractual penalties with counterparties.

Financial Risk

Direct exposure arises from incident response costs, forensic investigation, legal counsel, regulatory fines, and potential client compensation. Indirect exposure includes asset outflows following a publicly disclosed breach. Industry benchmarks indicate total breach costs in the range of CHF 2–8 million for moderate-severity incidents at institutions of comparable size.

Regulatory Risk

FINMA expects regulated entities to maintain demonstrable operational resilience and sound information security governance. Material gaps in privileged access management, monitoring, and incident response are inconsistent with these expectations. A reportable incident under current conditions could result in enforcement action, increased supervisory intensity, or mandated remediation programmes.

Reputational Impact

Webeo Bank's business model depends on client confidence in the security and privacy of their assets. A publicised breach or FINMA enforcement action would materially damage this confidence. In the Swiss private banking segment, reputational recovery is measured in years.

Board-Level Accountability

Under Swiss law and FINMA guidance, the Board bears ultimate responsibility for the adequacy of internal controls, including information security. Where material weaknesses are identified and not addressed, individual directors may face personal liability exposure. Documented awareness of the risks identified here — combined with inaction — heightens this exposure.

SECTION 5 OF 8

Immediate Action Plan · 0–30 Days

Actions are prioritised by risk severity and feasibility within 30 days. Each action materially reduces exposure and improves audit defensibility.

01 **Privileged Access Audit**

Commission an immediate audit of all administrative and privileged accounts. Disable or remove accounts that are inactive, shared, or lack documented business justification. This directly reduces the most probable vector for a significant breach.

02 **Enforce MFA Universally**

Mandate multi-factor authentication for all remote access, cloud services, and privileged accounts without exception. MFA is the single most effective control against credential-based attacks, which account for the majority of successful intrusions in the financial sector.

03 **Initiate Immutable Backup Implementation**

Scope and commence deployment of write-protected, air-gapped or immutable backup systems. Even partial implementation within 30 days meaningfully reduces ransomware exposure for the most critical data assets.

04 **Establish Logging Baseline**

Enable logging across critical systems — domain controllers, firewalls, core banking applications — centralised and retained for a minimum of 90 days. This provides the minimum viable forensic capability required by FINMA in the event of an incident.

05 **Appoint an Incident Response Lead**

Formally assign an internal IR coordinator and engage external IR retainer capability. Define escalation paths and communication protocols. This reduces regulatory liability and significantly improves response times in a crisis.

06 **Present Findings to the Full Board**

Table this assessment as a formal Board agenda item. Document the presentation and subsequent decisions. This creates an auditable record of governance engagement and protects directors in the event of future regulatory enquiry.

07 **Freeze Unsanctioned Privileged Account Creation**

Implement an interim policy requiring CISO approval for any new privileged account. This prevents further risk accumulation while the formal access governance programme is established.

SECTION 6 OF 8

Strategic Roadmap · 3–12 Months

Transition from reactive security posture to structured, defensible security governance aligned with ISO 27001 and FINMA expectations.

3–4 mo

Governance Framework

Formally adopt an ISMS framework (ISO 27001 or equivalent). Establish a Security Committee with Board representation. Develop and approve an Information Security Policy suite and a living risk register.

3–6 mo

Privileged Access Management

Deploy a PAM solution to govern, audit, and control all administrative credentials. Implement just-in-time provisioning and session recording for critical systems. Establish quarterly access review cycles.

4–8 mo

Security Monitoring & Detection

Deploy a SIEM platform with use-cases tuned to the financial services threat landscape. Establish a monitoring capability — in-house or via a managed security service provider — with defined escalation thresholds and SLAs.

3–6 mo

Backup Resilience & Recovery Testing

Complete immutable backup infrastructure across all critical systems. Conduct a full recovery exercise to validate RTO and RPO. Document and present recovery metrics to the Board.

4–6 mo

Incident Response Formalisation

Develop, test, and approve a formal IR Plan. Conduct at least one tabletop exercise involving executive management. Establish FINMA communication protocols and validate cyber insurance coverage.

6–12 mo

Security Awareness Programme

Launch role-appropriate security awareness training including phishing simulation. Track and report participation metrics to executive management quarterly.

SECTION 7 OF 8

Compliance Alignment

Findings mapped to principal compliance frameworks applicable to Webeo Bank AG. Maturity reflects current control evidence, not intent.

Control Domain	ISO 27001	FINMA	Maturity	Gap
Access Control & PAM	Partial	Partial	Developing	Significant
Privileged Account Mgmt	Insufficient	Insufficient	Ad-hoc	Critical
Security Monitoring / SIEM	Partial	Partial	Minimal	Significant
Incident Response	Insufficient	Insufficient	Undocumented	Critical
Backup & Recovery	Partial	Partial	Developing	Significant
Policy Documentation	Partial	Partial	Incomplete	Moderate
Security Awareness	Partial	Aligned	Informal	Moderate
Vulnerability Management	Partial	Partial	Reactive	Moderate

Documentation Readiness

Audit defensibility requires that controls are documented, tested, and evidenced — not merely that they exist. Formal records of access reviews, penetration testing, control testing, and security training completion are either absent or insufficiently structured to withstand regulatory scrutiny. Addressing this gap is a prerequisite for any future certification or audit engagement.

SECTION 8 OF 8

Conclusion for the Board

This assessment presents a clear and substantiated picture of Webeo Bank AG's current information security posture. The findings are significant but not exceptional for an organisation that has grown without commensurate investment in structured security governance. The risks identified are addressable. What is required is leadership commitment and structured execution.

The Board's responsibility in this context is unambiguous. FINMA's supervisory expectations and Swiss corporate governance standards hold the Board accountable for the adequacy of internal controls. Awareness of material security deficiencies — as documented in this report — combined with inaction constitutes a governance failure with direct legal and regulatory implications.

The recommended course of action is straightforward: formally acknowledge the risk, commission the immediate action plan, and mandate a structured 12-month remediation programme under executive ownership. Progress should be reported to the Board quarterly.

Sentinel AG is available to support Webeo Bank in the execution of this programme — in an advisory capacity or through direct programme management.

Sentinel AG
Cyber Security Advisory · Zürich

February 2026

Classification
Confidential — Board & Executive Management

Not for further distribution