

ILLUSTRATIVE REPORT / NOT REAL CUSTOMER DATA

Cyber Risk and Action Summary for the Board

Example organization / October 2026



Executive summary

Daily operations continue. Management needs evidence that critical controls work, clear action owners and visibility into risks that may recur.

This example presents five fictional risks, business impacts and corrective actions. It does not estimate financial loss. Applicable legal obligations and actual risk exposure require organization-specific evidence.

Decision requested from management

Agree priorities, accountable owners and target dates; allocate resources and document any residual risk accepted by authorized management.

Risks on the management agenda

01 / EXAMPLE RISK

Recovery of a critical application is unverified.

Business impact: Recovery time for orders, collections and service delivery may remain uncertain.

Technical observation: Backup jobs report success, but evidence of a recent restore test is absent.

Corrective action: Run an authorized restore test and record the recovery time and outcome.

Owner: IT / business continuity owner

Target date: 30.10.2026 / Next control: 15.11.2026

02 / EXAMPLE RISK

A former employee account has been reactivated.

Business impact: Unnecessary access may expose data or enable unauthorized transactions.

Technical observation: An illustrative account appears active despite a previous closure record.

Corrective action: Review the business justification and approval; examine offboarding and reactivation controls.

Owner: IT / HR process owner

Target date: 27.10.2026 / Next control: 15.11.2026

03 / EXAMPLE RISK

Purchased protection is not active on every critical server.

Business impact: Assets outside the protection scope may affect business operations.

Technical observation: Protection agents are inactive on two sampled critical servers.

Corrective action: Reconcile the asset scope, deploy protection and independently verify effective operation.

Owner: IT security owner

Target date: 29.10.2026 / Next control: 15.11.2026

Action and verification follow-up

04 / EXAMPLE RISK

Office-to-production access boundaries are unverified.

Business impact: An incident on an office system may reach production services.

Technical observation: An example network rule exceeds the documented business need; an authorized test is pending.

Corrective action: Agree the required access scope with IT and OT teams and perform approved tests.

Owner: IT / OT operations owners

Target date: 06.11.2026 / Next control: 15.11.2026

05 / EXAMPLE RISK

A completed action lacks independent closure evidence.

Business impact: Management may retain an assurance gap for a risk believed to be resolved.

Technical observation: A completion statement exists, but no independent retest record is available.

Corrective action: Attach technical evidence and an independent verification result before closure.

Owner: Action owner / independent auditor

Target date: 03.11.2026 / Next control: 15.11.2026

Control period and scope

An IT completion statement is not independent closure approval. Remediation requires evidence and retesting. Monthly periodic controls provide visibility into new and recurring in-scope risks; they are not continuous real-time monitoring.

This sample is not legal advice, a compliance certificate or a security guarantee. The image is an AI-generated illustrative scene. Contact: destek@siberkobi.co