

Cyber-Risikobericht an den Verwaltungsrat – CH

Berichte / Board Security Briefing · Vorlage mit Ausfüllhilfe

Dokumenttyp: Bericht (Vorlage)

Version: V1.0 · Status: Published Version · Datum: 09.10.2026

Owner: Martin Bischoff · 4T2 Solutions GmbH

Public · Publierte Version



Dokumentkontrolle

Feld	Wert
Titel	Cyber-Risikobericht an den Verwaltungsrat – CH
Dokumentart	Berichte · Führung · Board Security Briefing
Gültigkeit	Unternehmen · Schweiz. Hinweise für FinanzCH und für Deutschland in Abschnitt B6.
Version	V1.0
Status	Published Version
Stand	2026-10-09
Review	jährlich sowie bei Änderung von OR, FINMA-Vorgaben oder ISG
Rechtsraumunterschiede	Abschnitt B6
Vertraulichkeit	Public (die ausgefüllte Fassung ist vertraulich)
Owner	Martin Bischoff · 4T2 Solutions GmbH

So verwenden Sie diese Vorlage

Teil A ist der Bericht selbst. Er ist auf rund zwei Seiten ausgelegt und wird pro Berichtsperiode ausgefüllt. Text in eckigen Klammern ist ein Platzhalter. Teil B erklärt, warum der Bericht so aufgebaut ist, wie Kennzahlen definiert werden und welche Pflichten des Verwaltungsrats er unterstützt. Die zugehörige Excel-Arbeitsmappe enthält den Kennzahlenkatalog und ein ausgefülltes Beispiel.

Der Bericht ersetzt keine Rechtsberatung. Er strukturiert die Information, auf deren Grundlage der Verwaltungsrat entscheidet und seine Oberaufsicht dokumentiert.

Teil A – Bericht

A1 Berichtskopf

Feld	Eintrag
Unternehmen	[Unternehmen]
Berichtsperiode / Stichtag	[z. B. Q3 2026 / 30.09.2026]
Adressat	[Verwaltungsrat / Prüfungs- und Risikoausschuss]
Verfasst von	[CISO, Name]
Freigegeben durch	[Mitglied der Geschäftsleitung]
Vertraulichkeit	Vertraulich

A2 Gesamtlage auf einen Blick

Element	Eintrag
Gesamteinschätzung	[Grün / Gelb / Rot] im Vergleich zur genehmigten Risikotoleranz
Was hat sich verändert?	[ein Satz: wesentliche Veränderung seit dem letzten Bericht]
Grösstes Risiko	[ein Satz: Risiko, betroffene Geschäftsleistung, Trend]
Was soll der VR entscheiden?	[ein Satz: Verweis auf A3]

A3 Erbetene Entscheide

Nur Punkte, die der Verwaltungsrat tatsächlich entscheiden muss. Kenntnisnahmen gehören nicht hierher.

Nr.	Entscheid	Empfehlung	Folge ohne Entscheid	Frist
1	[z. B. Erhöhung Budget Wiederherstellungstests]	[Option, Kosten]	[Restrisiko, betroffene Leistung]	[Datum]
2	[z. B. Akzeptanz eines Restrisikos]	[befristet bis ...]	[...]	[Datum]

A4 Top-Risiken

Höchstens fünf Risiken, formuliert als Geschäftsauswirkung. Trend: ↑ steigend, → stabil, ↓ sinkend.

Risiko	Betroffene Leistung	Bewertung	Trend	Risikoeigner	Behandlung / Status	Toleranz
[z. B. Ransomware verschlüsselt Kernsysteme]	[Zahlungsverkehr]	[hoch]	[→]	[GL-Mitglied]	[Massnahme, Termin]	[in / über]
[...]	[...]	[...]	[...]	[...]	[...]	[...]

A5 Kennzahlen

Sechs bis acht Kennzahlen mit vorab festgelegten Schwellen. Definitionen im Kennzahlenkatalog der Excel-Arbeitsmappe.

Kennzahl	Ist	Schwelle	Trend	Kommentar
K1 Kritische Schwachstellen auf exponierten Systemen über Behebungsfrist	[Anzahl]	[0]	[]	[]
K2 Phishing-resistente MFA für privilegierte und Fernzugänge	[%]	[100 %]	[]	[]
K3 Kritische Services mit erfolgreich getesteter Wiederherstellung innerhalb RTO	[%]	[≥ 90 %]	[]	[]
K4 Meldepflichtige Vorfälle mit fristgerechter Meldung	[% (n von n)]	[100 %]	[]	[]
K5 Kritische Dienstleister mit aktueller Sicherheitsbeurteilung	[%]	[≥ 90 %]	[]	[]
K6 Risikoakzeptanzen und Ausnahmen nach Ablaufdatum	[Anzahl]	[0]	[]	[]
K7 Zeit bis zur Eindämmung wesentlicher Vorfälle (Median)	[Stunden]	[≤ 24 h]	[]	[]
K8 Meilensteine des Sicherheitsprogramms im Plan	[%]	[≥ 80 %]	[]	[]

A6 Regulatorik und Pflichten

Regelwerk	Betroffenheit	Status	Nächste Frist
[ISG (Meldepflicht)]	[ja / nein, Begründung]	[Meldeprozess getestet am ...]	[laufend, 24 h]
[revDSG]	[ja]	[...]	[...]
[FINMA / DORA / NIS2, falls anwendbar]	[...]	[...]	[...]

A7 Risikoakzeptanzen und Ausnahmen

Akzeptiertes Risiko	Begründung	Akzeptiert durch	Gültig bis
[...]	[...]	[Gremium / Person]	[Datum]

A8 Wesentliche Ereignisse seit dem letzten Bericht

Vorfälle, Prüfungsfeststellungen, relevante externe Ereignisse (z. B. Angriffe auf Branchenkollegen) – jeweils mit Konsequenz für das Unternehmen.

Datum	Ereignis	Konsequenz / Massnahme
[...]	[...]	[...]

A9 Anhänge auf Nachfrage

[Technische Detailberichte, Prüfberichte, Testprotokolle. Sie werden nicht vorgelesen, müssen aber auf Nachfrage verfügbar sein.]

Teil B – Ausfüllhilfe

B1 Wozu der Bericht dient

Der Verwaltungsrat einer Aktiengesellschaft hat unübertragbare und unentziehbare Aufgaben, darunter die Oberleitung der Gesellschaft, die Festlegung der Organisation und die Oberaufsicht über die mit der Geschäftsführung betrauten Personen (Art. 716a Abs. 1 OR). Für Schäden aus absichtlicher oder fahrlässiger Verletzung ihrer Pflichten haften die Mitglieder des Verwaltungsrats persönlich (Art. 754 OR). Cyberrisiken sind Teil dieser Verantwortung, soweit sie die Geschäftstätigkeit wesentlich gefährden.

Gerichte überprüfen Geschäftsentscheide nur zurückhaltend, wenn sie in einem einwandfreien Verfahren, auf angemessener Informationsbasis und frei von Interessenkonflikten getroffen wurden (Business Judgment Rule, vgl. Bundesgericht, Urteil 4A_306/2009 vom 8. Februar 2010, E. 7.2.4). Der Bericht liefert genau diese Informationsbasis und dokumentiert, worüber der Verwaltungsrat entschieden hat.

B2 Grundsätze eines guten Board-Berichts

- Entscheidungsorientiert: Er beginnt mit dem, was der Verwaltungsrat entscheiden soll, nicht mit Technik.
- Portfoliosicht: Wenige Risiken mit Geschäftsauswirkung statt einer Liste von Massnahmen.
- Vergleich mit der Risikotoleranz: Jede Aussage zeigt, ob das Risiko innerhalb der genehmigten Toleranz liegt.
- Trends statt Momentaufnahmen: Dieselben Kennzahlen über mehrere Perioden, mit vorab festgelegten Schwellen.
- Belegbarkeit: Jede Zahl hat eine Datenquelle und einen Eigner. Details liegen im Anhang vor.
- Kürze: Zwei Seiten. Was nicht entscheidungsrelevant ist, gehört in den Anhang.

B3 Kennzahlen definieren

Eine Kennzahl ist nur brauchbar, wenn Formel, Datenquelle, Schwelle, Eigner und Frequenz festgelegt sind, bevor der erste Wert berichtet wird. Die Excel-Arbeitsmappe enthält diese Angaben für die acht Kennzahlen aus A5. Passen Sie die Schwellen an Ihre Risikotoleranz an und lassen Sie sie vom Verwaltungsrat genehmigen.

ID	Frage, die die Kennzahl beantwortet	Typische Fehlerquelle
K1	Können Angreifer bekannte, kritische Lücken auf erreichbaren Systemen ausnutzen?	Zählt alle Schwachstellen statt nur exponierte und kritische
K2	Sind die wichtigsten Zugänge gegen Phishing geschützt?	Zählt SMS- oder App-Codes als phishing-resistent
K3	Kommen wir nach einem Angriff rechtzeitig zurück?	Berichtet erfolgreiche Backups statt getesteter Wiederherstellungen
K4	Erfüllen wir unsere Meldepflichten?	Erfasst Kenntnis- und Meldezeitpunkt nicht getrennt

ID	Frage, die die Kennzahl beantwortet	Typische Fehlerquelle
K5	Kennen wir die Sicherheitslage unserer kritischen Dienstleister?	Fragebogen ohne Bezug zur Kritikalität
K6	Sind akzeptierte Risiken noch bewusst akzeptiert?	Ausnahmen ohne Ablaufdatum
K7	Wie schnell begrenzen wir Schaden?	Misst Zeit bis Ticketabschluss statt bis Eindämmung
K8	Liefert das Sicherheitsprogramm, was beschlossen wurde?	Meilensteine ohne Wirkungsnachweis

B4 Rhythmus und Gremien

- Verwaltungsrat: mindestens halbjährlich, zusätzlich ad hoc bei wesentlichen Vorfällen.
- Prüfungs- und Risikoausschuss sowie Geschäftsleitung: quartalsweise.
- Ad-hoc-Bericht: bei einem Vorfall, der eine Meldepflicht auslöst oder kritische Geschäftsleistungen unterbricht.

B5 Häufige Fehler

1. Technische Fülle statt entscheidungsrelevanter Klarheit.
2. Ampeln ohne festgelegte Schwellen: Die Farbe wird verhandelt statt gemessen.
3. Keine Verbindung zur Risikotoleranz: Der Verwaltungsrat kann nicht erkennen, ob er handeln muss.
4. Erbetene Entscheide fehlen oder sind als Kenntnisnahme getarnt.
5. Restrisiken werden ohne Befristung und ohne benannte Person akzeptiert.

B6 Hinweise für FinanzCH und Deutschland

FinanzCH (Banken und Wertpapierhäuser): Nach FINMA-Rundschreiben 2023/1 genehmigt das Oberleitungsorgan die Grundzüge des Managements der operationellen Risiken einschliesslich der IKT- und Cyberrisiken und mindestens jährlich die Risikotoleranz für operationelle Risiken. Es genehmigt regelmässig die Strategien für IKT, Cyberrisiken, kritische Daten und BCM sowie mindestens jährlich die kritischen Funktionen und deren Unterbrechungstoleranzen. Zur operationellen Resilienz ist mindestens jährlich sowie bei wesentlichen Kontrollschwächen oder Vorfällen zu berichten. Wesentliche Cyberangriffe sind der FINMA nach Art. 29 Abs. 2 FINMAG zu melden (Aufsichtsmitteilung 05/2020: Information innerhalb von 24 Stunden, Meldung innerhalb von 72 Stunden). Ergänzen Sie A5 um Kennzahlen zu den Unterbrechungstoleranzen und A6 um FINMA.

Deutschland: Für besonders wichtige und wichtige Einrichtungen verpflichtet § 38 BSIG die Geschäftsleitung, die Risikomanagementmassnahmen umzusetzen, ihre Umsetzung zu überwachen und regelmässig an Schulungen teilzunehmen. Die Haftung richtet sich nach Gesellschaftsrecht. Für Finanzunternehmen im Anwendungsbereich von DORA trägt das Leitungsorgan die Verantwortung für das IKT-Risikomanagement (Art. 5 DORA). Für eine deutsche Gesellschaft ersetzen Vorstand oder Geschäftsführung und Aufsichtsrat die Rolle des Verwaltungsrats; Art. 716a und 754 OR gelten dort nicht.

B7 Quellen

- Obligationenrecht, Art. 716a und 754: fedlex.admin.ch/eli/cc/27/317_321_377/de
- FINMA-Rundschreiben 2023/1 «Operationelle Risiken und Resilienz – Banken», in Kraft seit 1. Januar 2024: finma.ch

- FINMA-Aufsichtsmitteilung 05/2020 «Meldepflicht von Cyber-Attacken gemäss Art. 29 Abs. 2 FINMAG»: [finma.ch](https://www.finma.ch)
- Informationssicherheitsgesetz (ISG), Meldepflicht seit 1. April 2025: bacs.admin.ch/de/meldepflicht
- BSI-Gesetz vom 2. Dezember 2025, § 38: gesetze-im-internet.de/bsig_2025/___38.html
- Verordnung (EU) 2022/2554 (DORA), Art. 5: eur-lex.europa.eu/eli/reg/2022/2554/oj
- Bundesgericht, Urteil 4A_306/2009 vom 8. Februar 2010, E. 7.2.4 (Business Judgment Rule)
- Fristenkalender DCH und Glossar: stop.li/werkzeuge/fristenkalender-dch/ · stop.li/werkzeuge/security-glossar/