

Informationssicherheitsrichtlinie für FinanzCH – CH

Regeln / Policy

Dokumenttyp: Regeln / Policy

Version: V1.2 · Status: Published Version · Datum: 09.08.2026

Owner: Martin Bischoff · 4T2 Solutions GmbH

Public · Publierte Version



Dokumentkontrolle

Feld	Wert
Dokumentname	Informationssicherheitsrichtlinie für FinanzCH – CH
Version	V1.2
Status	Published Version
Vertraulichkeit	Public
Owner	Martin Bischoff
Publikationszweck	Publizierte Version

Inhaltsverzeichnis

1. Zweck, Wirkung und Anwendbarkeit.....	4
2. So steuert das Unternehmen Informationssicherheit.....	4
3. Führung, Verantwortung und unabhängige Prüfung.....	6
4. Vom Schutzbedarf zur Risikoentscheidung.....	7
5. Controls wirksam und nachweisbar steuern.....	8
6. Menschen, Informationen und Zugriffe schützen.....	9
7. Technologie sicher gestalten und betreiben.....	10
8. Standorte und physische Abhängigkeiten schützen.....	12
9. Third Parties und Cloud über den Lifecycle steuern.....	12
10. Security Incidents führen und Geschäftsleistungen erhalten.....	13
11. Reporting, Exceptions und Improvement.....	15
12. Richtlinie umsetzen und nachweisen.....	15
Referenzen und Anwendung.....	16

1. Zweck, Wirkung und Anwendbarkeit

Das Unternehmen kann seine Leistungen nur verlässlich erbringen, wenn es Informationen und Systeme angemessen schützt und auch bei Störungen steuerungsfähig bleibt. Diese Richtlinie bestimmt dafür die Führungsverantwortung, Entscheidungswege und verbindlichen Sicherheitsgrundsätze. Sie schützt Vertraulichkeit, Integrität und Verfügbarkeit. Wo es für Vertrauen und Beweisbarkeit notwendig ist, schliesst der Schutz Authentizität und Nachvollziehbarkeit ein.

Die Richtlinie gilt für alle Personen im Einflussbereich des Unternehmens. Sie erfasst die Informationen, Technologien, Standorte und externen Dienste, die für seine Leistungen benötigt werden. Welche gesetzlichen oder sektoralen Sonderpflichten gelten, entscheidet das Unternehmen durch eine dokumentierte Anwendungsprüfung. Unklare Anwendbarkeit bleibt bis zur Klärung als offene Compliance-Frage sichtbar.¹

Das FINMA-Anwendbarkeitsprofil hält pro Rechtsträger, Bewilligung und Tätigkeit fest, welche finanzmarktrechtlichen Erwartungen gelten. Es bezeichnet insbesondere die Anwendbarkeit der FINMA-Rundschreiben 2023/1 und 2018/3 sowie der einschlägigen Cyber-Aufsichtsmitteilungen. Eine Gruppenzugehörigkeit oder die Bezeichnung als Finanzinstitut ersetzt diese dokumentierte Prüfung nicht.²

Abweichungen sind nur über den geregelten Ausnahmeprozess zulässig. Sie benötigen eine befristete Entscheidung und eine nachvollziehbare Risikobehandlung. Stillschweigende oder unbefristete Abweichungen sind unzulässig.

2. So steuert das Unternehmen Informationssicherheit

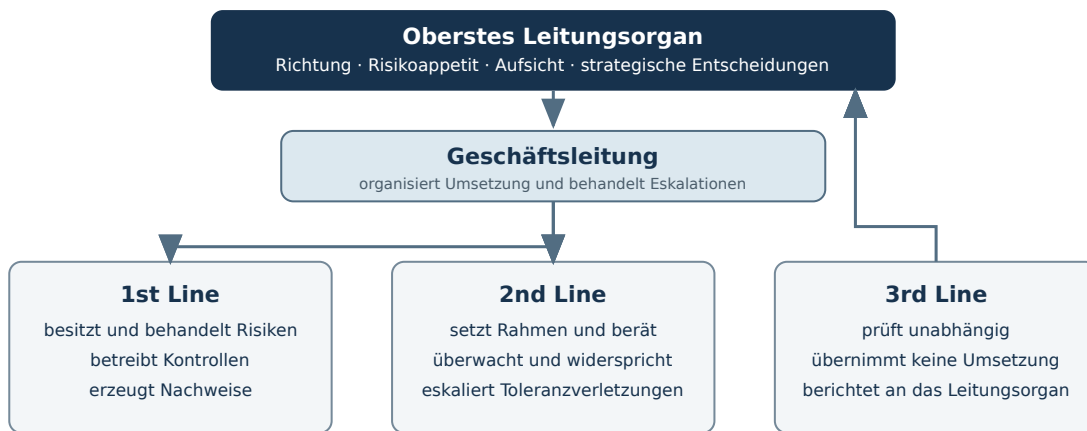
Das oberste Leitungsorgan gibt Sicherheitsambition und Risikoappetit vor. Die Geschäftsleitung übersetzt diese Richtung in Ziele, Zuständigkeiten und Ressourcen. Im Geschäft entstehende Risiken verantwortet die 1st Line. Die 2nd Line setzt den Rahmen und überwacht ihn; die 3rd Line prüft unabhängig.

Jede wesentliche Leistung wird mit ihren Informationen und technischen Abhängigkeiten erfasst. Schutzbedarf und Risikoszenario begründen die Risikoentscheidung. Daraus entstehen Sicherheitsziele und Controls. Ein Control gilt erst als wirksam, wenn sein Betrieb und seine Wirkung belegt sind. Abweichungen führen zurück zu einer befugten Entscheidung; Erkenntnisse aus Security Incidents und Übungen verbessern den Rahmen.

1 Die Anwendungsprüfung berücksichtigt insbesondere das Schweizer DSG, das FINMA-Aufsichtsrecht und die Meldepflicht nach ISG/CSV: <https://www.fedlex.admin.ch/eli/cc/2022/491/de>, <https://www.finma.ch/de/dokumentation/rundschreiben/> und <https://www.ncsc.admin.ch/ncsc/de/home/meldepflicht/meldepflicht-info.html>.

2 FINMA stellt Rundschreiben und adressatenbezogene Geltungsbereiche bereit: <https://www.finma.ch/de/dokumentation/rundschreiben/>.

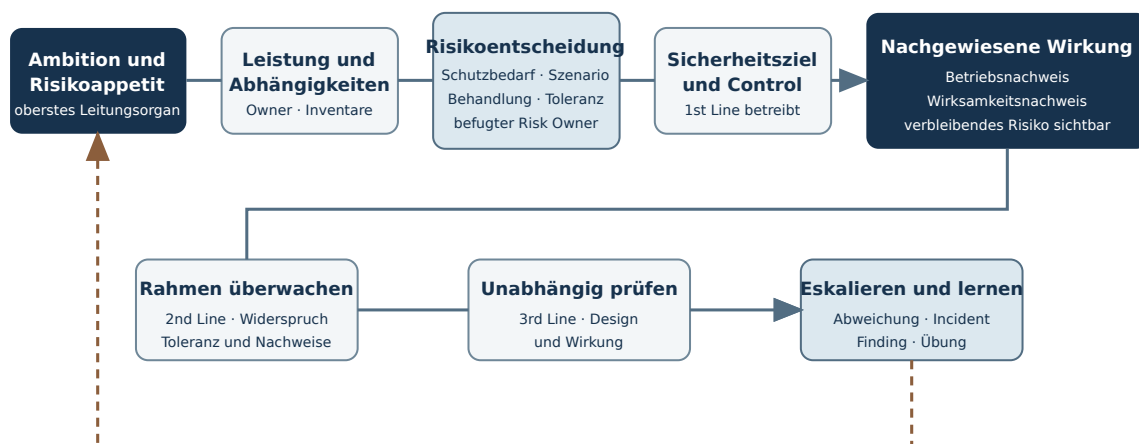
Three Lines: Richtung, Verantwortung und Prüfung



Linien sind Rollen im Steuerungsmodell, nicht zwingend eigene Organisationseinheiten.

VIS-ISP-FINCH-01 – Three Lines verbinden Führungsrichtung mit Ausführungsverantwortung, Rahmenüberwachung und unabhängiger Prüfung.

Informationssicherheit als geschlossener Steuerungskreislauf



Entscheidungen bleiben bei der befugten Geschäftsrolle. Überwachung und Prüfung übernehmen weder Geschäftsrisiko noch operative Controls.

VIS-ISP-FINCH-12 – Die Steuerungskette verbindet Führungsrichtung, Risikoentscheidungen, Controls und Nachweise mit Überwachung, unabhängiger Prüfung und Lernen.

Für Institute im Anwendungsbereich verbindet diese Steuerungskette das Management operationeller Risiken mit der Sicherstellung operationeller Resilienz. Die Geschäftsleitung bestimmt kritische Funktionen, genehmigt Toleranzen für schwere, aber plausible Unterbrechungen und verlangt den Nachweis, dass die Leistung innerhalb dieser Toleranzen erbracht oder wiederhergestellt werden kann.³

3 FINMA-Rundschreiben 2023/1 verbindet das Management operationeller Risiken mit operationeller Resilienz und kritischen Daten: <https://www.finma.ch/de/~media/finma/dokumente/dokumentencenter/myfinma/rundschreiben/finma->

3. Führung, Verantwortung und unabhängige Prüfung

Steuerung, Rahmenüberwachung und unabhängige Prüfung erfordern getrennte Verantwortlichkeiten. Geschäftsrisiken werden dort gesteuert, wo sie entstehen.

Überwachungsfunktionen dürfen sie nicht unbemerkt übernehmen. Das Three-Lines-Modell ordnet diese Aufgaben und schützt die Qualität der Entscheidungen.⁴

Mit der Genehmigung dieser Richtlinie bestimmt das oberste Leitungsorgan die Sicherheitsambition. Es entscheidet über strategische Risiken und wesentliche Toleranzüberschreitungen. Seine Gesamtverantwortung bleibt auch bei Delegation bestehen. Die Geschäftsleitung richtet ein umsetzbares ISMS ein, weist Befugnisse zu und stellt die beschlossenen Ressourcen bereit.

Mindestens jährlich erhält das oberste Leitungsorgan ein entscheidungsorientiertes Lagebild. Wesentliche Ereignisse lösen zusätzliche Berichte aus. Das Lagebild zeigt überschrittene Toleranzen und drohende Folgen. Zugleich wird erkennbar, welche Stelle bis zu welchem Termin entscheiden oder handeln muss.

Die 1st Line erkennt und bewertet die Risiken ihrer Tätigkeit. Sie setzt Controls um, betreibt sie und hält die Nachweise aktuell. Der Risk Owner entscheidet innerhalb seiner Befugnis über die Behandlung. Eine Zustimmung der 2nd Line ersetzt weder diese Entscheidung noch die Verantwortung der 1st Line. Business Owner verantworten die Leistung; Information, System und Service Owner tragen die Ergebnisverantwortung für ihre jeweiligen Schutzobjekte.

Der CISO führt die Gesamtsicht auf Informationsrisiken. Risk Management verbindet sie mit dem unternehmensweiten Risikomanagement. Compliance und Privacy erfüllen ihre eigenständigen Mandate. Die 2nd Line berät und überwacht. Verletzt eine Entscheidung den Rahmen oder fehlt ein Nachweis, widerspricht sie und eskaliert. Sie übernimmt weder Geschäftsrisiko noch operative Controls.

Internal Audit bildet die 3rd Line. Es beurteilt unabhängig, ob Governance und Controls angemessen ausgestaltet sind und in der Praxis wirken. Es übernimmt weder Umsetzung noch operative Freigaben und akzeptiert keine Risiken im Namen der 1st Line.

Eine Eskalation beschreibt Sachverhalt, Geschäftsfolge und verletzte Toleranz. Sie zeigt vertretbare Handlungsoptionen und die benötigte Entscheidung. Erkennt der CISO eine wesentliche Ressourcenunterdeckung, legt er sie der zuständigen Leitungsinstanz vor. Der Mangel überträgt das Geschäftsrisiko nicht auf den CISO.

Kleinere Unternehmen dürfen Rollen kombinieren. Eine kombinierte Rolle darf ihre eigene Umsetzung jedoch nicht abschliessend überwachen oder prüfen; dafür ist eine unabhängige kompensierende Prüfung erforderlich.

Soweit FINMA-Anforderungen gelten, ordnet das Institut die Informationssicherheit in seine unabhängigen Kontrollfunktionen ein und dokumentiert Mandate, Berichtswege und

[rs-2023-01-20221207.pdf](#).

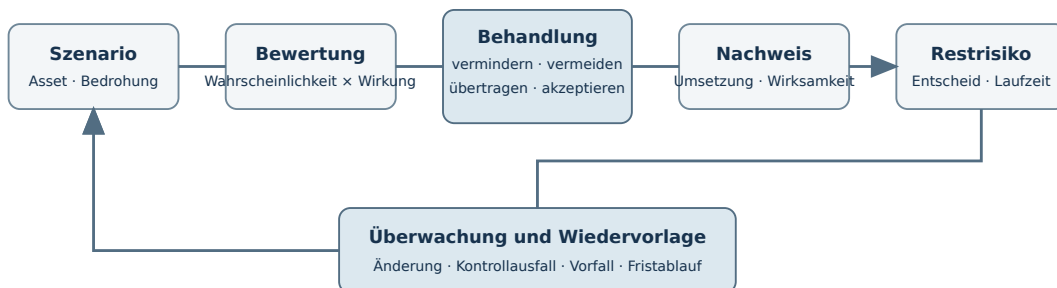
4 Das Three-Lines-Modell folgt der Rollenlogik des Institute of Internal Auditors: <https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf>.

Interessenkonflikte. Eine hybride Sicherheitsfunktion darf operative Aufgaben übernehmen, wenn Überwachung, Eskalation und unabhängige Prüfung ihrer eigenen Arbeit nachweisbar getrennt bleiben.

4. Vom Schutzbedarf zur Risikoentscheidung

Das Unternehmen führt ein aktuelles Inventar der wesentlichen Informationen, Systeme, Services und Abhängigkeiten. Der Schutzbedarf beschreibt die mögliche Auswirkung einer Verletzung der Schutzziele. Neben finanziellen Folgen betrachtet er die Leistungserbringung sowie Pflichten gegenüber Personen, Kunden und Behörden.

Risikobehandlung ist ein wiederkehrender Entscheidungszyklus



Akzeptanz beendet die Überwachung nicht. Wird das Risiko schlagend, beginnt sofort die Incident- und Risikoneubewertung.

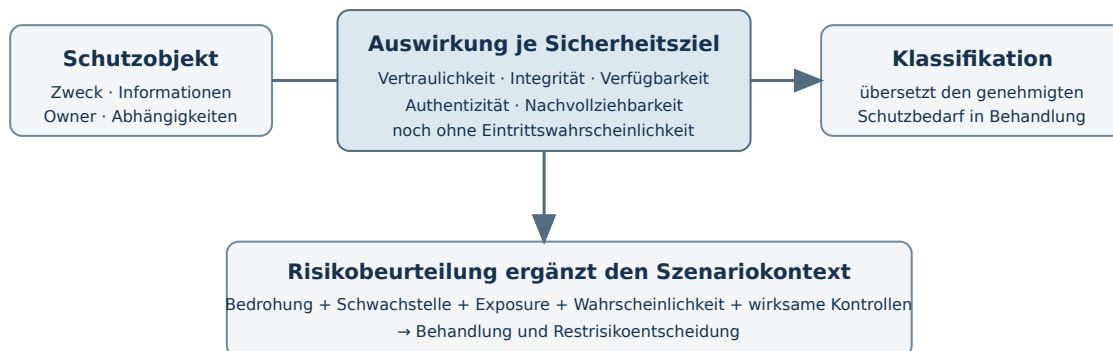
VIS-ISP-FINCH-02 – Risikobehandlung ist ein geschlossener Entscheidungs- und Überwachungszyklus.

Die Risikobeurteilungsmethode ergänzt den Schutzbedarf um ein plausibles Szenario. Sie bewertet Wahrscheinlichkeit und Geschäftsfolge anhand genehmigter Kriterien. Geplante Massnahmen mindern das aktuelle Risiko erst, wenn Umsetzung und Wirkung belegt sind.

Der Risk Owner wählt zwischen Vermeidung, Minderung und Übertragung. Eine Risk Acceptance ist nur innerhalb der genehmigten Toleranz und durch eine befugte Instanz zulässig. Jede Behandlung erhält Termin und Wirksamkeitsnachweis. Exceptions bleiben befristet und benötigen kompensierende Sicherheitskontrollen sowie einen Rückkehrplan. Wesentliche Veränderungen, Kontrollausfälle oder Security Incidents lösen eine Neubewertung aus.

Das Institut identifiziert kritische Funktionen und die für sie notwendigen Personen, Informationen, Technologien, Standorte und Dienstleister. Kritische Daten werden nach ihrer Bedeutung für Geschäftstätigkeit, Risikosteuerung, regulatorische Pflichten und Kundeninteressen bestimmt. Schutzbedarf, Abhängigkeiten und Ausfallfolgen werden gemeinsam beurteilt; reine Systemkritikalität genügt nicht.

Schutzbedarf kommt vor der Risikowahrscheinlichkeit



Eine niedrige Wahrscheinlichkeit senkt nicht den Schutzbedarf eines geschäftskritischen Schutzobjekts.

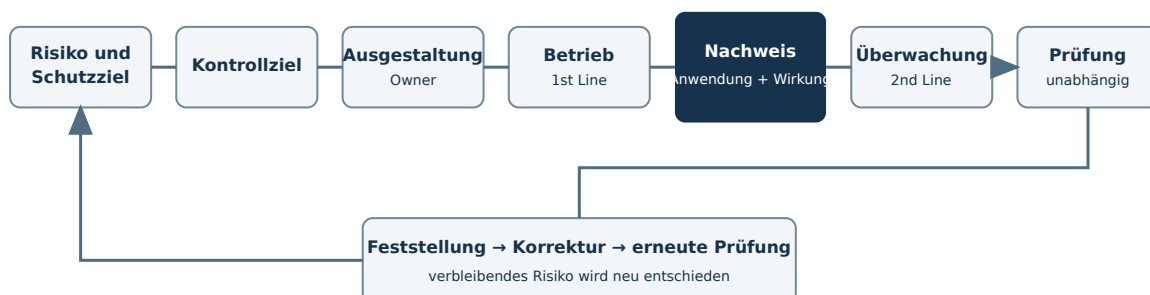
VIS-ISP-FINCH-03 – Schutzbedarf beurteilt die Auswirkung; die Risikobeurteilung ergänzt Szenario und Wahrscheinlichkeit.

5. Controls wirksam und nachweisbar steuern

Sicherheitskontrollen übersetzen Risikoentscheidungen in überprüfbare Schutzwirkung. Schutzbedarf und Risikoszenario bestimmen das Kontrollziel. Die zuständige 1st Line sorgt für Design und Betrieb; die 2nd Line überwacht den Rahmen. Internal Audit kann Design und Wirksamkeit im Betrieb unabhängig prüfen.

Eine installierte Massnahme ist noch kein wirksamer Control. Erst Betriebs- und Wirksamkeitsnachweise zeigen, ob das Ziel erreicht wird. Findings führen zu einer verantworteten Korrektur und erneuten Prüfung. Bleibt ein wesentliches Restrisiko, entscheidet die befugte Instanz über weitere Behandlung oder Acceptance. Der Control Standard regelt die Details; Security Baselines bestimmen technische Parameter.

Vom Risiko zum Wirksamkeitsnachweis



VIS-ISP-FINCH-04 – Ein Control führt vom Schutzziel über Ausgestaltung und Betrieb zum Wirksamkeitsnachweis; Findings lösen Korrektur und erneute Prüfung aus.

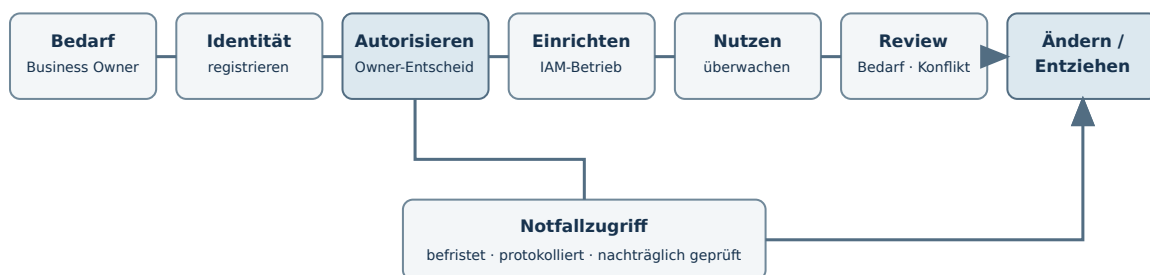
6. Menschen, Informationen und Zugriffe schützen

Informationen bleiben über ihren Lifecycle geschützt. Der Information Owner legt Schutzbedarf und zulässige Nutzung fest. Classification und Handling Rules bestimmen, wer Informationen über welche Kanäle bearbeiten darf. Retention und nachweisbare Löschung folgen geschäftlichen und rechtlichen Anforderungen.

Access beginnt mit einer nachvollziehbaren Identity. Authentication weist die Identität nach; Authorization bestimmt erlaubte Handlungen. Der Business Owner begründet den Bedarf. Information und System Owner genehmigen Access für ihren Bereich. Rollenwechsel oder Austritt führen unverzüglich zur Anpassung.

Privileged Access unterliegt verstärkter Genehmigung und Monitoring. Emergency Access bleibt zeitlich begrenzt und wird nachträglich unabhängig beurteilt. Missbrauchsverdacht führt zur Einschränkung und zur Prüfung eines Security Incidents.

Identität und Berechtigung bleiben über den Lebenszyklus getrennt

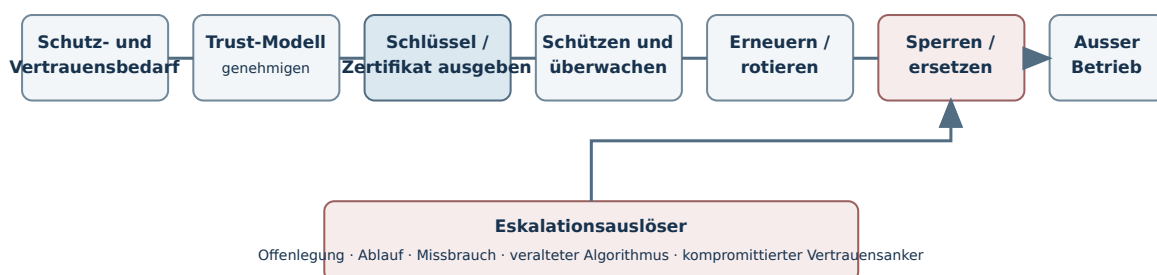


Authentisierung weist Identität nach; sie ersetzt weder Berechtigungsentscheid noch laufende Überwachung.

VIS-ISP-FINCH-08 – Identität, Authorization und Privileged Access werden über den vollständigen Lifecycle gesteuert.

Kryptografie benötigt ein beherrschtes Trust Model. Schlüssel und Zertifikate erhalten eindeutige Verantwortung und einen kontrollierten Lifecycle. Konkrete Verfahren bleiben im Kryptografie- und PKI-Standard.

Kryptografisches Vertrauen braucht einen vollständigen Lebenszyklus



VIS-ISP-FINCH-09 – Schlüssel, Zertifikate und Vertrauensanker benötigen einen kontrollierten Lifecycle.

Mitarbeitende erhalten rollenbezogene Regeln und Training. Wirksamkeit zeigt sich auch im Meldeverhalten und in Übungen. Mobile Work und externe Kommunikation ändern den Schutzbedarf nicht. Nicht freigegebene Cloud-, Software- oder AI-Services dürfen keine geschützten Unternehmensinformationen erhalten.

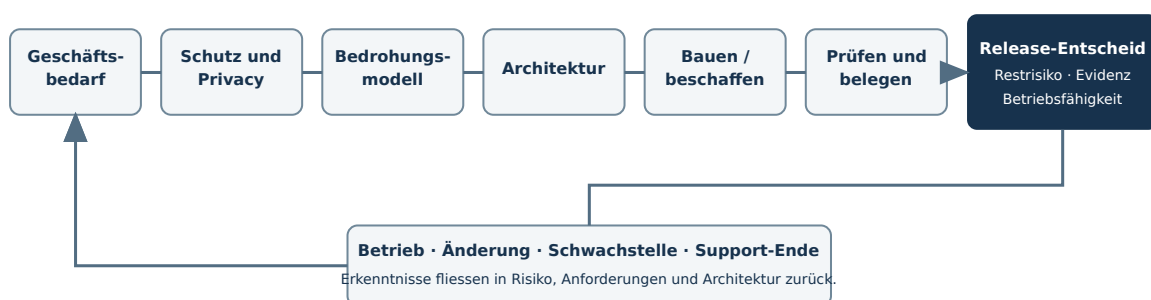
Der Business Owner beantragt die Nutzung eines AI-Service und beschreibt Zweck, Informationsumfang und erwarteten Nutzen. Security, Privacy und Legal prüfen Risiken, Datenschutz sowie Rechte an Eingaben und Ergebnissen. Procurement klärt die vertraglichen Bedingungen. Erst die bezeichnete Instanz genehmigt den Einsatz und legt seine Grenzen fest. Entdeckt das Unternehmen Shadow AI, schützt es die betroffenen Informationen und führt den Dienst einer dokumentierten Risikoentscheidung zu.⁵

Wiederkehrende risikoarme Nutzungen dürfen innerhalb eines genehmigten Nutzungsprofils freigegeben werden; neue Zwecke, geschützte Informationen, wesentliche Änderungen oder erhöhte Risiken lösen eine individuelle Prüfung durch die betroffenen Funktionen aus.

7. Technologie sicher gestalten und betreiben

Security by Design verankert Anforderungen vor Architektur- und Beschaffungsentscheidungen. Der Business Owner verantwortet Zweck und Geschäftsrisiko. Security Architecture setzt Prinzipien; Entwicklung, Technik und Beschaffung setzen sie um und erzeugen Nachweise. Privacy by Design ergänzt dies für personenbezogene Daten.⁶

Security by Design ist ein Lebenszyklus, kein einzelnes Freigabegate



VIS-ISP-FINCH-10 – Security by Design verbindet Geschäftsbedarf, Architektur, Freigabe und Betrieb.

⁵ Der NIST AI RMF behandelt AI Governance als durchgängige Lifecycle-Aufgabe und schliesst Risiken aus Drittparteien, Daten und Rechten ein: <https://airc.nist.gov/airmf-resources/airmf/5-sec-core/>.

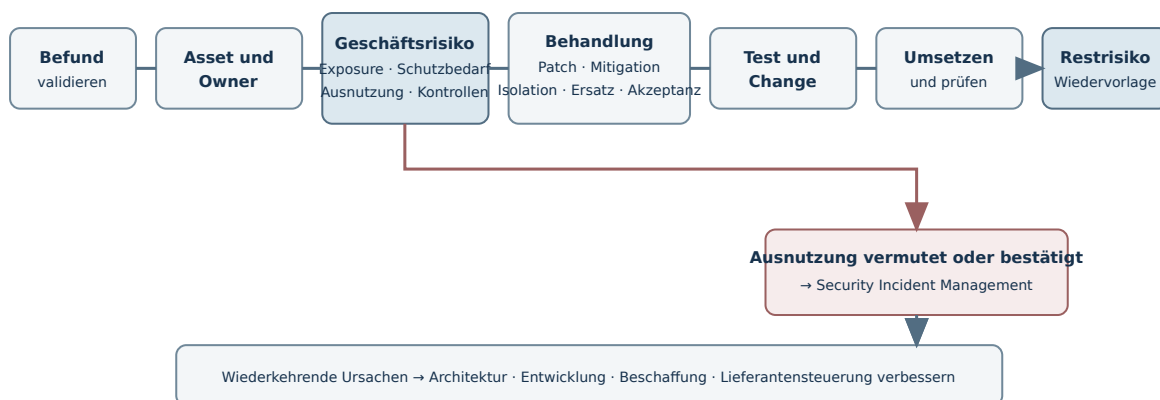
⁶ Privacy by Design ist im Schweizer DSG und in der DSGVO verankert: <https://www.fedlex.admin.ch/eli/cc/2022/491/de> und <https://eur-lex.europa.eu/eli/reg/2016/679/oj>.

Der sichere Lifecycle reicht von Sicherheitsanforderungen und Threat Modelling bis zur dokumentierten Freigabe. Offene Vulnerabilities und Restrisiken müssen sichtbar sein. Eine wesentliche Designschwäche verhindert die Freigabe, sofern keine befugte Instanz eine befristete Exception genehmigt.

AI-generierter Code und vorgeschlagene Komponenten durchlaufen denselben Secure SDLC wie andere Beiträge. Der Entwicklungsverantwortliche stellt Herkunft und Lizenzlage fest und veranlasst eine fachliche Prüfung. Security Tests und die Software Bill of Materials machen Abhängigkeiten sichtbar. Erst die Release Authority darf den geprüften Stand freigeben; ein AI-Output gilt nicht als Sicherheitsnachweis.⁷

Vulnerability Management behandelt Findings als Risikoinformation. Severity unterstützt die Priorisierung, ersetzt aber nicht die Geschäftsbeurteilung. Exposure und aktive Ausnutzung bestimmen die Dringlichkeit; Ausnutzung führt in den Security-Incident- Prozess.

Schwachstelle, Patch, Änderung und Incident bilden eine Risikokette



VIS-ISP-FINCH-11 – Vulnerabilities, Patches und Changes bilden eine Risikobehandlung; Ausnutzung führt in das Incident Management.

Patches stammen aus vertrauenswürdiger Quelle und werden angemessen getestet. Die Change Authority genehmigt die Verteilung. Erst erfolgreiche Installation und nutzbare Geschäftsleistung belegen die Behandlung. Emergency Changes verkürzen den Vorlauf, heben Verantwortung und Review aber nicht auf.

Security Baselines beschreiben sichere Konfigurationen. Netzwerkzonen begrenzen Angriffsflächen. Operational Technology erhält eigene risikogerechte Baselines. Logging und Monitoring beantworten definierte Detection Questions; Alarmer erhalten eine verantwortliche Triage. Fehlende Sichtbarkeit gilt als Control Failure oder möglicher Security Incident.

Das Institut plant risikobasierte Cyberübungen und Szenariotests für kritische Funktionen. Ziele, Szenario, Teilnehmer, Toleranzen, Beobachtungen und Verbesserungsmaßnahmen werden

⁷ NIST SP 800-218 beschreibt Secure-Software-Development-Practices einschliesslich der Kontrolle externer Komponenten: <https://csrc.nist.gov/pubs/sp/800/218/final>.

dokumentiert. Ein Test besteht nicht allein deshalb, weil Technik wieder verfügbar ist; die kritische Leistung muss innerhalb der genehmigten Toleranz erbracht werden können.⁸

8. Standorte und physische Abhängigkeiten schützen

Physische Sicherheit schützt Informationen und Leistungen vor unberechtigtem Zutritt, Diebstahl, Manipulation und Umwelteinwirkungen. Das Unternehmen legt risikogerechte Sicherheitszonen fest. Zutritt wird begründet vergeben und bei Rollenwechsel entzogen.

Standortverantwortliche setzen lokale Anforderungen um. Facility Management, IT und Arbeitssicherheit koordinieren ihre Beiträge, ohne Fachverantwortungen zu vermischen. Betriebsmittel und Datenträger bleiben auch bei Transport, Wartung und Entsorgung geschützt. Versorgungsausfälle werden mit Security Incident Management und Business Continuity verbunden.

9. Third Parties und Cloud über den Lifecycle steuern

Der Bezug externer Leistungen überträgt die Durchführung, nicht die Verantwortung des Unternehmens. Der Business Owner verantwortet Nutzen und Risiko. Due Diligence muss Kritikalität, Konzentrationsrisiko und Exit-Fähigkeit erkennen lassen.

Verträge bestimmen Sicherheitsanforderungen und Meldewege. Sie sichern angemessene Prüfrechte und regeln Security Incidents sowie Rückgabe oder Löschung von Informationen. Bei kritischen Services werden Anforderungen entlang wesentlicher Subcontractors weitergegeben.

Gegenüber wesentlichen Providern sichert sich das Unternehmen die für seine Steuerung notwendigen Weisungs-, Informations- und Prüfungsrechte. Sie erstrecken sich risikogerecht auf materielle Subcontractors und die erforderlichen Nachweise. Kann ein Provider keine ausreichenden Rechte gewähren, entscheidet die befugte Risikoinstanz vor der Beauftragung über Vermeidung, zusätzliche Behandlung oder Risikoakzeptanz.⁹

Für Cloud Services dokumentiert das Unternehmen das Shared Responsibility Model. Unklare Zuständigkeit ist ein Risiko. Vor Go-live weist der Service Owner nach, dass Zugriffe und Datenflüsse kontrolliert und Recovery vorbereitet sind. Wesentliche Änderungen lösen eine erneute Beurteilung aus. Beim Exit bestätigt der Owner, dass Zugriffe entzogen und Informationen zurückgegeben oder gelöscht wurden.

8 FINMA präzisiert Cyberrisiken und szenariobezogene Cyberübungen in ihrer Aufsichtsdokumentation: <https://www.finma.ch/de/dokumentation/dossier/dossier-cyberrisiken/auf-einen-blick-cyberrisiken/>.

9 Die Lieferanten- und Supply-Chain-Steuerung ist Teil des NIST CSF 2.0; konkrete Vertragsrechte bleiben eine risikobasierte Unternehmensentscheidung: <https://www.nist.gov/cyberframework>.

Drittparteienrisiko: Verantwortung vom Bedarf bis zum Exit



VIS-ISP-FINCH-05 – Drittparteienrisiko wird vom Bedarf bis zum nachgewiesenen Exit gesteuert.

Das Auslagerungsinventar verbindet die bezogene Leistung mit kritischen Funktionen, Daten, Standorten, wesentlichen Subcontractors, vertraglichen Rechten und Exit- Vorkehrungen. Wesentliche Änderungen, Konzentrationen oder Einschränkungen von Prüfrechten werden der befugten Instanz vor einer Fortführung zur Entscheidung vorgelegt.¹⁰

Kritische Services benötigen eine praktisch durchführbare Ausweichoption: Substitution, Fallback oder einen getesteten Exit. Fehlt sie, macht der Business Owner Konzentration und Folgen transparent. Die zuständige Leitungsinstanz entscheidet über zusätzliche Resilienz oder eine befristete Risikoakzeptanz.

10. Security Incidents führen und Geschäftsleistungen erhalten

Das Unternehmen führt Security Incidents mit einem gemeinsamen Lagebild. Der Incident Lead koordiniert die fachliche Reaktion. Ausserordentliche Unternehmensentscheidungen trifft die Krisenorganisation, während Business Continuity priorisierte Leistungen erhält oder wiederherstellt. Je nach Lage arbeiten diese Führungsstränge gleichzeitig.

Ein Security Event muss beurteilt werden. Bestätigt sich eine relevante Beeinträchtigung oder ist sie hinreichend wahrscheinlich, beginnt die Behandlung als Security Incident. Ein Notfall liegt bei gefährdeten wesentlichen Leistungen vor. Eine Krise entsteht, wenn normale Organisation und Mittel nicht ausreichen.

Die Geschäftsleitung bezeichnet vorab die Rolle, die einen Notfall erklären und die Notfallorganisation aktivieren darf. Sie handelt nach genehmigten Kriterien und sorgt für eine dokumentierte Übergabe. Die Notfallorganisation setzt vorbereitete Kontinuitäts- und Wiederherstellungspläne um; sie ist weder der Incident Lead noch automatisch das Crisis Management Team.¹¹

¹⁰ FINMA-Rundschreiben 2018/3 regelt die aufsichtsrechtliche Behandlung von Outsourcing innerhalb seines Anwendungsbereichs: <https://www.finma.ch/de/dokumentation/rundschreiben/>.

¹¹ BSI Standard 200-4 trennt und koordiniert Notfall-, BCM- und Krisenstrukturen: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8.

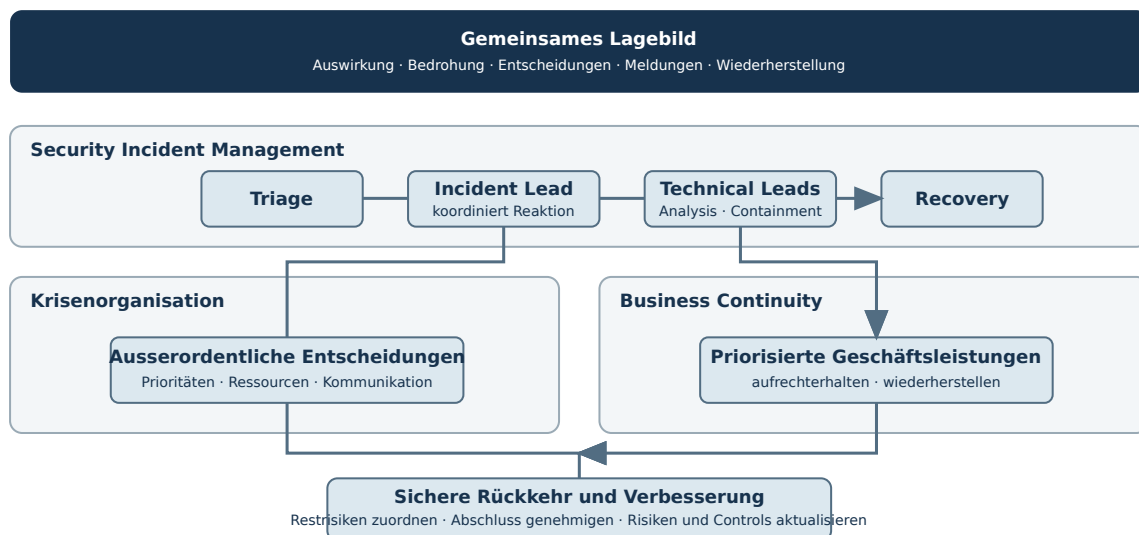
Die Triage entscheidet, ob ein Event geschlossen, beobachtet oder als Security Incident behandelt wird. Unsicherheit darf notwendiges Containment nicht verhindern. Eine Matrix ordnet Priorität und Führungsebene zu und legt fest, welche Meldungen zu prüfen sind.

Für jeden bestätigten Security Incident benennt das Unternehmen eine einzelne Person als Incident Lead. Diese Rolle führt das Lagebild und bereitet Entscheidungen vor. Sie ist weder ein lokales Einsatzgremium noch das Crisis Management Team. Technical Leads begrenzen den Angriff; Business-, Information- und System Owner beurteilen die Folgen.

Meldepflichten werden bereits während der Triage geprüft. Interne Klassifikation oder Formularabschluss dürfen den Fristbeginn nicht verschieben. Das Meldepflichtenprofil bestimmt Auslöser, Entscheidungsinstanz und Adressat.¹²

Der Incident Lead eskaliert ausserhalb seiner Befugnis. Das Crisis Management priorisiert Unternehmensziele und Ressourcen. Business Continuity hält Leistungen aufrecht oder stellt sie wieder her. Alle Beteiligten nutzen dasselbe Lagebild.

Getrennte Führung, gemeinsames Lagebild



VIS-ISP-FINCH-13 – Incident Lead, Krisenorganisation und Business Continuity bleiben getrennte Führungsstränge und arbeiten mit einem gemeinsamen Lagebild.

Das FINMA-Meldepflichtenprofil wird parallel zur Behandlung aktiviert. Es bestimmt nach Rechtsträger und Ereignis, welche Stelle die Aufsicht informiert, welche Frist läuft und welche Aktualisierungen erforderlich sind. Die interne Klassifikation darf eine notwendige erste Meldung nicht verzögern; die Mitteilung ersetzt weder Behandlung noch andere gesetzliche Meldungen.¹³

12 Das Meldepflichtenprofil hält insbesondere FINMA-Aufsichtserwartungen, ISG/CSV und Art. 24 DSGVO aktuell: <https://www.finma.ch/de/dokumentation/dossier/dossier-cyberisiken/auf-einen-blick-cyberisiken/>, <https://www.ncsc.admin.ch/ncsc/de/home/meldepflicht/meldepflicht-info.html> und <https://www.fedlex.admin.ch/eli/cc/2022/491/de>.

13 Die FINMA-Dokumentation zu Cyberisiken hält aktuelle aufsichtsrechtliche Melde- und Übungserwartungen zusammen: <https://www.finma.ch/de/dokumentation/dossier/dossier-cyberisiken/>

Ein technischer Ausfall kann einen Notfall auslösen, ohne ein Security Incident zu sein. Umgekehrt kann ein Security Incident behandelt werden, ohne dass ein Notfall erklärt wird. Überschreitet die Lage die vorbereiteten Pläne oder verlangt sie ausserordentliche Unternehmensentscheidungen, aktiviert die bezeichnete Instanz das Crisis Management. Zuständigkeiten und Übergänge werden regelmässig geübt.

Die Behandlung kann zwischen Analysis, Containment und Recovery wechseln. Backup ist nur belastbar, wenn die Wiederherstellung von Daten, Systemen und nutzbarer Leistung getestet ist. Der Incident Lead beantragt den Abschluss nach Beherrschung der Bedrohung und Zuordnung aller Restrisiken. Der Business Owner bestätigt die sichere Wiederaufnahme; die befugte Instanz genehmigt die Rückkehr in den Normalbetrieb. Lessons Learned aktualisieren Risiken und Controls.

11. Reporting, Exceptions und Improvement

Reporting dient Entscheidungen. Wesentliche Indikatoren benötigen einen Bezugswert und eine genehmigte Schwelle. Das Lagebild zeigt Risiken ausserhalb der Toleranz sowie überfällige Behandlungen und Kontrollausfälle. Es bezeichnet die benötigte Entscheidung und die verantwortliche Stelle.

Monitoring beobachtet den laufenden Zustand. Assurance beurteilt mit ausreichender Distanz, ob die Steuerung funktioniert. Internal Audit prüft unabhängig. Findings erhalten Verantwortliche und Termin. Security Incidents und Exercises fliessen in denselben Verbesserungskreislauf; die Geschäftsleitung verfolgt Massnahmen bis zum Wirksamkeitsnachweis.

Für den FinanzCH-Scope zeigt das Management-Lagebild zusätzlich Unterbrechungen und Toleranzverletzungen kritischer Funktionen, Risiken kritischer Daten, wesentliche Cyber-Findings, Konzentrationen und Auslagerungsrisiken sowie überfällige Resilienzmassnahmen. Es nennt die benötigte Entscheidung und nicht nur den Status.

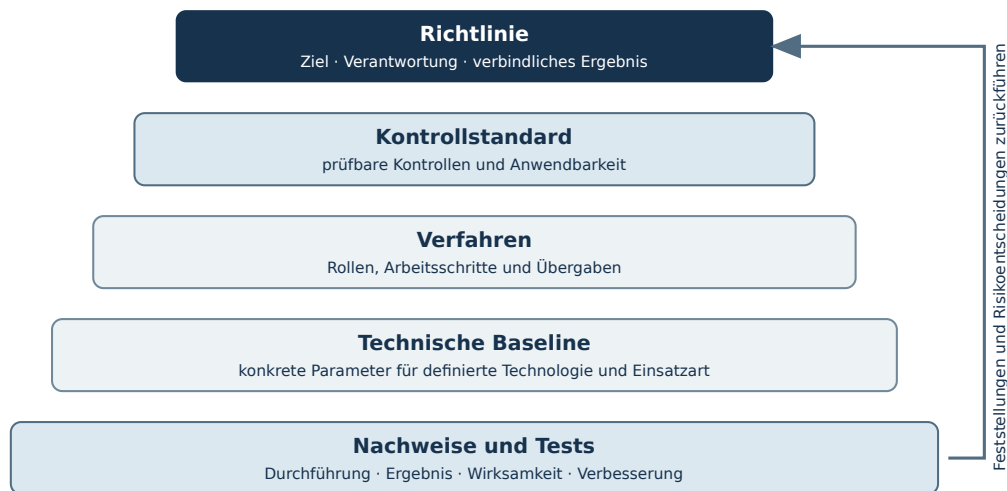
Die bezeichnete Stelle untersucht Verstösse nach Ursache und Auswirkung. Sie schlägt verhältnismässige und rechtmässige Massnahmen vor. Wesentliche oder wiederholte Verstösse legt sie der zuständigen Führungsebene zur Entscheidung vor.

12. Richtlinie umsetzen und nachweisen

Die Richtlinie tritt mit Genehmigung in Kraft. Der Dokumenteigentümer kommuniziert sie und sorgt für Kenntnisnahme. Mindestens jährlich prüft er Aktualität und Anwendbarkeit.

Die Policy bestimmt Ziele und Verantwortungen. Standards übersetzen sie in prüfbare Controls. Procedures und Playbooks beschreiben die Ausführung; Security Baselines legen Parameter fest. Register, Freigaben und Testergebnisse weisen Durchführung und Wirkung nach. Nachgelagerte Dokumente dürfen das Schutzziel nicht abschwächen.

Von der Führungsentscheidung zum Wirksamkeitsnachweis



VIS-ISP-FINCH-07 – Richtlinie, Standard, Verfahren und Baseline führen zu prüfbaren Nachweisen.

Der Dokumenteigentümer sorgt mindestens für Rechts-, Risiko- und Ausnahmeregister sowie für Asset- und Service-Inventare. Die Fachverantwortlichen pflegen Control Standards und Security Baselines. Hinzu kommen IAM, PKI, Secure Development und Vulnerability Management. Incident Response, Crisis Management, Business Continuity und Recovery benötigen eigene Pläne und Nachweise. Ein Assurance Plan und der jährliche Informationssicherheitsbericht schliessen die Kette.

Der FinanzCH-Scope benötigt zusätzlich ein FINMA-Anwendbarkeitsprofil, Inventare der kritischen Funktionen und kritischen Daten, ein kontrolliertes Auslagerungsinventar, Resilienz- und Cyberübungsevidenz sowie ein aktuelles aufsichtsrechtliches Meldepflichtenprofil.

Referenzen und Anwendung

ISO/IEC 27001, BSI 200-1 und NIST CSF 2.0 bilden den methodischen Rahmen. NIST SP 800-53/53A unterstützt Controls und Assurance. Weitere NIST-Standards konkretisieren Identity, Kryptografie, Secure Development, Patch Management und Incident Response. BSI 200-4 unterstützt Business Continuity und Crisis Management. Die Nutzung begründet weder Zertifizierung noch pauschale Rechtskonformität.

Dieses Dokument ist keine Rechtsberatung, aufsichtsrechtliche Zusicherung oder Konformitätsbescheinigung. Das anwendende Institut bleibt für Anwendbarkeit, Genehmigung, Umsetzung und Wirksamkeitskontrolle verantwortlich.

© 2026 4T2 Solutions GmbH. Text und eigene Diagramme stehen unter CC BY 4.0.

Martin Bischoff hat dieses Dokument mit Unterstützung generativer AI erstellt. Auswahl, fachliche Bewertung und Freigabe erfolgen durch Martin Bischoff.