Risikobewertungs-Template

Systematische Risikobewertung für Finanzunternehmen

1. Risiko-Identifikation

Risikoregister

Risiko-ID	Risikobeschreibung	Risikokategorie	Identifikationsdatum	Verantwortlich
R001	Ausfall kritischer IT-Systeme	Operationell	2024-01-15	CTO
R002	Cybersecurity-Angriff auf Kundendaten	Operationell	2024-01-20	CISO
R003	Regulatorische Änderungen (Basel IV)	Compliance	2024-02-10	Compliance Officer
R004	Kreditausfälle Großkunden	Kreditrisiko	2024-02-15	CRO
R005	Zinsänderungsrisiko	Marktrisiko	2024-02-20	Treasurer

2. Risikobewertung Matrix

Bewertungsschema

Eintrittswahrscheinlichkeit:

- 1 = Sehr niedrig (< 5%)
- 2 = Niedrig (5-15%)
- 3 = Mittel (15-40%)
- 4 = Hoch (40-70%)
- 5 = Sehr hoch (> 70%)

Auswirkung:

- 1 = Minimal (< 100k EUR)
- 2 = Gering (100k-500k EUR)
- 3 = Mittel (500k-2M EUR)
- 4 = Hoch (2M-10M EUR)
- 5 = Kritisch (> 10M EUR)

Risikobewertungs-Matrix

Risiko-ID	Beschreibung	Eintrittswahrscheinlichkeit	Auswirkung	Risikoscore	Risikoklasse

Risiko-ID	Beschreibung	Eintrittswahrscheinlichkeit	Auswirkung	Risikoscore	Risikoklasse
R001	IT-System Ausfall	2	4	8	Hoch
R002	Cybersecurity-Angriff	3	5	15	Kritisch
R003	Regulatorische Änderungen	4	3	12	Hoch
R004	Kreditausfälle	2	4	8	Hoch
R005	Zinsänderungsrisiko	3	3	9	Hoch

3. Detaillierte Risikobeschreibungen

R001: Ausfall kritischer IT-Systeme

Risikobeschreibung: Kompletter oder teilweiser Ausfall der Kernbankensysteme, wodurch operative Geschäftstätigkeiten beeinträchtigt werden.

Potenzielle Ursachen:

- Hardware-Versagen
- Software-Bugs
- Stromausfälle
- Menschliche Fehler
- Wartungsarbeiten

Auswirkungen:

- Unterbrechung des Kundenservice
- Verlust von Transaktionsdaten
- Reputationsschäden
- Regulatorische Strafen
- Umsatzverluste: 2-5M EUR pro Tag

Aktuelle Maßnahmen:

- Redundante Systeme
- 24/7 Monitoring
- Disaster Recovery Plan
- Regelmäßige Backups

R002: Cybersecurity-Angriff auf Kundendaten

Risikobeschreibung: Erfolgreicher Cyberangriff, der zu Datenschutzverletzungen und Diebstahl von Kundendaten führt.

Potenzielle Ursachen:

- Phishing-Angriffe
- Malware/Ransomware
- Insider-Bedrohungen
- DDoS-Attacken
- Social Engineering

Auswirkungen:

- GDPR-Strafen bis 20M EUR
- Reputationsschäden
- Kundenabwanderung
- Rechtsstreitigkeiten
- Operative Unterbrechungen

Aktuelle Maßnahmen:

- Multi-Faktor-Authentifizierung
- Endpoint Protection
- Security Awareness Training
- Penetration Testing
- Incident Response Plan

R003: Regulatorische Änderungen (Basel IV)

Risikobeschreibung: Neue regulatorische Anforderungen führen zu erhöhten Kapitalanforderungen und Compliance-Kosten.

Potenzielle Ursachen:

- Basel IV Implementierung
- ESG-Regulierung
- Open Banking Richtlinien
- AML/KYC Verschärfungen

Auswirkungen:

- Erhöhte Kapitalanforderungen: +15-25%
- Compliance-Kosten: +2-3M EUR jährlich
- Geschäftsmodell-Anpassungen
- Wettbewerbsnachteile

Aktuelle Maßnahmen:

- Regulatory Watch Programm
- Frühwarnsystem
- Compliance-Team Aufstockung
- Szenario-Planung

---

4. Risikominderungsstrategien

Strategie-Matrix

Risiko-ID	Minderungsstrategie	Verantwortlich	Umsetzungsfrist	Kosten (EUR)	Erwartete Risikoreduktion
R001	Cloud-Migration	CTO	Q2 2025	2,5M	60%
R002	Zero-Trust-Architektur	CISO	Q4 2024	1,8M	70%
R003	Regulatory Compliance Platform	CCO	Q1 2025	800k	50%
R004	Kreditportfolio-Diversifikation	CRO	Q3 2025	500k	40%
R005	Zinssicherungsgeschäfte	CFO	Q1 2025	200k	80%

5. Risiko-Monitoring und KPIs

Key Risk Indicators (KRIs)

KRI	Beschreibung	Zielwert	Schwellenwert	Aktuelle Werte	Trend
System Availability	IT-System Verfügbarkeit	> 99,9%	< 99,5%	99,7%	↗
Security Incidents	Anzahl Sicherheitsvorfälle/Monat	< 5	> 10	7	↘
Compliance Score	Regulatory Compliance Index	> 95%	< 90%	93%	→
Credit Loss Rate	Kreditausfallrate	< 1,5%	> 3%	1,8%	↗
Duration Gap	Zinsbindungsrisiko	< 2 Jahre	> 4 Jahre	2,3 Jahre	↘

Eskalationsmatrix

Grün (Risikoscore 1-6):

- Routinemäßige Überwachung
- Quartalsweise Berichterstattung
- Verantwortlich: Risikomanager

Gelb (Risikoscore 7-12):

- Verstärkte Überwachung
- Monatliche Berichterstattung
- Eskalation an: Risikomanagement-Komitee

Rot (Risikoscore 13-25):

- Sofortige Maßnahmen erforderlich
- Wöchentliche Berichterstattung
- Eskalation an: Vorstand/Geschäftsführung

---

6. Risiko-Reporting Template

Monatlicher Risikobericht

Berichtszeitraum: [Monat/Jahr] **Erstellt von:** [Risikomanager] **Berichtsdatum:** [Datum]

Executive Summary

- Anzahl neuer Risiken: [X]
- Risiken mit gestiegener Bewertung: [X]
- Risiken mit gesunkener Bewertung: [X]
- Kritische Risiken (Score >12): [X]

Top 5 Risiken

1. [Risiko-ID]: [Beschreibung] - Score: [X]
2. [Risiko-ID]: [Beschreibung] - Score: [X]
3. [Risiko-ID]: [Beschreibung] - Score: [X]
4. [Risiko-ID]: [Beschreibung] - Score: [X]
5. [Risiko-ID]: [Beschreibung] - Score: [X]

Maßnahmen-Status

- Geplante Maßnahmen: [X]
- Laufende Maßnahmen: [X]
- Abgeschlossene Maßnahmen: [X]
- Überfällige Maßnahmen: [X]

Empfehlungen

- [Empfehlung 1]
- [Empfehlung 2]
- [Empfehlung 3]

---

7. ESG-Risikobewertung

ESG-Risikokategorien

Environmental Risks:

- Klimawandel-Risiken
- Regulatorische Umweltauflagen
- Transition Risks (Energiewende)
- Physical Risks (Extremwetter)

Social Risks:

- Reputationsrisiken
- Arbeitssicherheit
- Diversität & Inklusion
- Kundenzufriedenheit

Governance Risks:

- Korruption & Bestechung
- Datenschutz & Privatsphäre
- Vorstand & Aufsichtsrat
- Stakeholder-Management

ESG-Bewertungsschema

ESG-Risiko	Impact	Likelihood	ESG-Score	Priorität
Klimawandel Transition	4	4	16	Hoch
Datenschutz-Verletzungen	5	3	15	Hoch
Reputationsschäden	4	3	12	Mittel
Diversität Compliance	2	3	6	Niedrig

8. Stresstests und Szenario-Analysen

Standard-Szenarien

Szenario 1: Wirtschaftsrezession

- BIP-Rückgang: -3%
- Arbeitslosigkeit: +2pp
- Kreditausfälle: +150%
- Erwarteter Verlust: 15-25M EUR

Szenario 2: Cyber-Attacke

- System-Ausfall: 48-72h
- Betroffene Kunden: 50.000
- Direkter Schaden: 5-10M EUR
- Reputationsschäden: 10-20M EUR

Szenario 3: Regulatorische Verschärfung

- Kapitalanforderungen: +20%
- Compliance-Kosten: +3M EUR/Jahr
- Geschäftsmodell-Anpassung: 6-12 Monate

Szenario-Auswirkungen

Szenario	Probability	Financial Impact	Recovery Time	Mitigation Available
Rezession	25%	15-25M EUR	18-24 Monate	Ja
Cyber-Attacke	15%	15-30M EUR	3-6 Monate	Teilweise
Regulatorik	60%	5-15M EUR	12-18 Monate	Ja

Genehmigung:

- Risikomanager: [Name, Datum]
- CRO: [Name, Datum]
- CEO: [Name, Datum]

Dieses Template ist für Trainingszwecke entwickelt und sollte an spezifische Unternehmensanforderungen angepasst werden.