Informationssicherheit

Monetäre Bewertung von IT-Restrisiken

Auf welcher Grundlage muss eine monetäre Bewertung der IT-Restrisiken durchgeführt werden? Welche Bewertungsansätze sind möglich?

Die aufsichtsrechtlichen Anforderungen in der Informationssicherheit sind in den letzten Jahren immer weiter gestiegen. Vor Veröffentlichung der Bankaufsichtlichen Anforderungen an die IT (BAIT) lag in vielen Banken der Fokus zunächst auf der qualitativen Bewertung der IT-Risiken. Eine quantitative Bewertung wurde hingegen zumeist vernachlässigt bzw. erfolgte in den Banken, ohne nachweisbaren Bezug zu den qualitativ erhobenen IT-Risiken, in Form einer Expertenschätzung. Doch auf welcher Grundlage kann eine nachvollziehbare monetäre Bewertung der IT-Restrisiken erfolgen? Welche Bewertungsansätze sind hierzu möglich?

Erhebung der qualitativen IT-Risiken

In der Informationssicherheit werden den Geschäftsprozessen sogenannte IT-Schutzobjekte (Datenklassen, Anwendungen, Systeme und Infrastrukturkomponenten) zugeordnet und hinsichtlich ihres Schutzbedarfs und Schutzniveaus bewertet. Der Schutzbedarf ergibt sich zumeist aus den Verfügbarkeitsanforderungen der zugeordneten Geschäftsprozesse sowie den hierin verwendeten Datenklassen. Das Schutzniveau hingegen wird aus den umgesetzten und für wirksam befundenen technischen und organisatorischen Maßnahmen (TOM) der jeweiligen Schutzobjekte bestimmt. Die IT-Risiken orientieren sich an dem Bedrohungskatalog und werden bestimmten Bedrohungsfeldern zugeordnet (vgl Abb. 1).

1 ZUORDNUNG ZU BEDROHUNGSFELDERN

Kategorie und Bezeichnung	Schutzziele
B 1 Interne Verfahren	
B1-1 Fehler von Anwendern/Benutzern	A C I N
B1-2 Fehler im Betrieb	A C I N
B1-3 fehlerhafte Prozesse	A C I N
B 2 Menschen	
B2-1 Missbrauch und Diebstahl	A C I N
B2-2 Angriffe auf Verfügbarkeit und Angriffe durch Schadprogramme	A C I N
B2-3 Angriffe auf Menschen (Social Engineering, Erpressung, …)	A C I N
B 3 Infrastruktur/Systeme	
B3-1 Ausfall von Systemen	A
B3-2 Ausfall von Kommunikationsinfrastruktur	A I
B3-3 Ausfall von Infrastrukturkomponenten	A
B 4 Externe Einflüsse	
B4-1 Gebäudeausfall	A
B4-2 Personalausfall	A
B4-3 Urteile, Beschlagnahmung, Reputation	A C I N

A C I N:
A = availability/Verfügbarkeit
C = confidentiality/Vertraulichkeit
I = integrity/Intigrität
N = non-repudiation/Authenzität

Dabei werden die IT-Risiken in Brutto- und Nettorisiken eingeteilt. Die Bruttorisiken weisen meist ein höheres Risiko aus als die Nettorisiken. Um das Risiko zu minimieren, werden Maßnahmen (z. B. Sollberechtigungskonzepte, Zugriffsregelungen) hinterlegt. Das durch die Maßnahmen reduzierte Risiko wird als Nettorisiko bezeichnet.

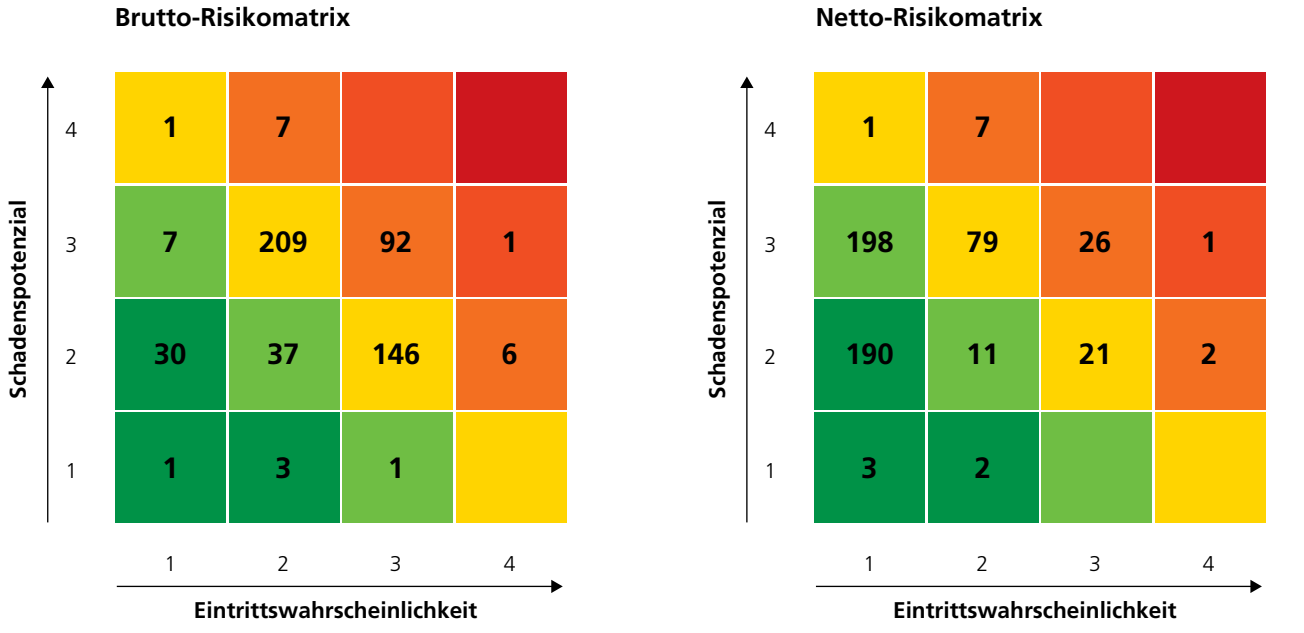
Die hinterlegten Nettorisiken lassen sich je nach Höhe des Risikos wiederum in drei Bereiche kategorisieren:

- Genehmigungspflichtige Risiken
- Meldepflichtige Risiken
- Akzeptable Risiken

Eine Auswertung aller IT-Risiken lässt sich in der Regel über eine Risikomatrix darstellen (vgl. Abb. 2).

Mit der beschriebenen Vorgehensweise werden die qualitativen IT-Risiken erhoben. Doch wie lassen sich die Ergebnisse der qualitativen in eine quantitative Betrachtung überführen? >

2 BEISPIELHAFTE AUSWERTUNG EINER RISIKOMATRIX AUS DER FACHANWENDUNG „ISI KOMPAKT“



Schadenspotenzial
1 = niedrig
2 = mittel
3 = hoch
4 = sehr hoch

Eintrittswahrscheinlichkeit
1 = unwahrscheinlich
2 = möglich
3 = wahrscheinlich
4 = sehr wahrscheinlich

Risikoklassen
- nicht relevant
- vernachlässigbar
- gering
- relevant
- äußerst relevant
- existenzbedrohend

Risikokategorie
- akzeptabel
- akzeptabel
- meldepflichtig
- genehmigungspflichtig
- genehmigungspflichtig
- genehmigungspflichtig

Grundlage zur quantitativen (=monetären) Bewertung der IT-Restrisiken

Zunächst ist zu klären, auf welcher rechtlichen Grundlage eine monetäre IT-Restrisikobewertung durchzuführen ist.

Die Grundlagen finden wir in den BAIT Tz. 13 i. V. m. MaRisk BTR 4: „Die Risikoanalyse auf Basis der festgelegten Risikokriterien hat auf Grundlage eines Vergleichs der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen zu erfolgen. Sonstige risikoreduzierende Maßnahmen aufgrund unvollständig umgesetzter Sollmaßnahmen sind wirksam zu koordinieren, zu dokumentieren, zu überwachen und zu steuern. Die Ergebnisse der Risikoanalyse sind zu genehmigen und in den Prozess des Managements der operationellen Risiken zu überführen." Erläuternd heißt es weiter dazu: „Risikokriterien enthalten bspw. mögliche Bedrohungen, das Schadenspotenzial, die Schadenshäufigkeit sowie den Risikoappetit." (Auszug aus den BAIT 10/2017[1])

In den MaRisk (Fassung vom 27.10.2019[2]) wird der Umgang mit den operationellen Risiken klar definiert (siehe Abb. 3).

3 BTR 4 – OPERATIONELLE RISIKEN

1 Das Institut hat den operationellen Risiken durch angemessene Maßnahmen Rechnung zu tragen. Für diese Zwecke ist eine institutsintern einheitliche Festlegung und Abgrenzung der operationellen Risiken vorzunehmen und an die Mitarbeiter zu kommunizieren.	**Definition von operationellen Risiken** Die Festlegung sollte auch eine möglichst klare Abgrenzung zu anderen vom Institut betrachteten Risiken enthalten. **Umgang mit nicht eindeutig zuordenbaren Schadensfällen oder Beinaheverlusten** Die Prozesse zum Management operationeller Risiken sollten auch den Umgang mit nicht eindeutig zuordenbaren Schadensfällen („boundary events"), Beinaheverlusten und zusammenhängenden Ereignissen umfassen. Als sogenannte „boundary events" können Verluste eingestuft werden, die zwar einem Risiko zugerechnet werden oder bereits wurden (z. B. Kreditverluste), die aber ihren Ursprung in Ereignissen wie z. B. mangelhaften Prozessen und Kontrollen haben oder hatten. Als „Beinaheverluste" können durch Fehler oder Mängel ausgelöste Ereignisse bezeichnet werden, die zu keinem Verlust geführt haben (z. B. fehlerhafte Zahlung an falschen Kontrahenten; Rückzahlung durch den Kontrahenten).
2 Es muss gewährleistet sein, dass wesentliche operationelle Risiken zumindest jährlich identifiziert und beurteilt werden.	
3 Das Institut hat eine angemessene Erfassung von Schadensfällen sicherzustellen. Bedeutende Schadensfälle sind unverzüglich hinsichtlich ihrer Ursachen zu analysieren.	**Erfassung von Schadensfällen** Größere Institute haben hierfür eine Ereignisdatenbank für Schadensfälle eingerichtet, bei welcher die vollständige Erfassung aller Schadensereignisse oberhalb angemessener Schwellenwerte sichergestellt ist.
4 Auf Basis der Risikoberichterstattung gemäß BT 3.2 Tz. 6 ist zu entscheiden, ob und welche Maßnahmen zur Beseitigung der Ursachen zu treffen oder welche Risikosteuerungsmaßnahmen (z. B. Versicherungen, Ersatzverfahren, …) zu ergreifen sind.	

ISI kompakt

Mit der Anwendung „ISI kompakt" wird der aufsichtsrechtlich geforderte Informationsverbund zum Informationsrisikomanagement abgebildet:

- Geschäftsprozesse,
- Objekte/Ressourcen,
- Risikoanalysen und
- Maßnahmen der entsprechend verwendeten Standards (SOIT, BSI etc.).

Die Maßnahmen sind selbstverständlich mit den Risiken verknüpft und bilden so das tatsächlich realisierte Schutzniveau am Objekt/an der Ressource ab und sorgen für eine Reduzierung der jeweiligen Risiken. Des Weiteren verfügt die Anwendung über diverse Auswertungsfunktionen zum Informationsrisikomanagement.

Bewertungsansatz der monetären IT-Restrisiken

Bisher gibt es seitens der BAIT und MaRisk keine konkreten Vorgaben, wie die Bewertung durchzuführen ist. Dies eröffnet den Banken die Möglichkeit, ein für sie passendes Verfahren zu nutzen. Als Mehrmandantenanbieter nutzen wir das in unserem Haus entwickelte Tool „ISI kompakt". Es ermöglicht uns eine umfassende Betrachtung und zugleich eine nachvollziehbare Bewertung der IT-Risiken. Die IT-Restrisiken werden übersichtlich dargestellt.

Bei der Bewertung der monetären Restrisiken sollte unabhängig vom eingesetzten Tool immer auch der Risiko-Controller aktiv mit einbezogen werden.

Gleichzeitig sollte jedes Tool die Arbeitsanweisung „100.04.06 RB zum Management operationeller Risiken" – genauer der Anlage 2. – gemäß den Musterarbeitsanweisungen des Genossenschaftsverbands – Verband der Regionen e.V. berücksichtigen. Praktisch heißt das, dass die o. g. Bedrohungen mit der entsprechenden Kategorie „Ereigniskategorie (3. Ebene)" verknüpft werden. Eine Zuordnung sieht dann wie folgt aus (siehe Abb. 4).

4 ZUORDNUNGSTABELLE

Bedrohung aus SOIT	Ereigniskategorie der Anlage 2
B1-1 Fehler von Anwendern/ Benutzern	7.1.2 Fehler bei der Dateneingabe, -pflege oder -speicherung
B1-2 Fehler im Betrieb	7.1.4 fehlerhafte Anwendung von Modellen/Systemen
B1-3 fehlerhafte Prozesse	7.1.5 Buchführungsfehler/ falsche Prozesszuordnung
B2-1 Missbrauch und Diebstahl	2.2.2 Diebstahl von Informationen (mit finanziellem Schaden)
B2-2 Angriffe auf Verfügbarkeit und Angriffe durch Schadprogramme	2.2.1 Schäden durch Hackeraktivitäten
B2-3 Angriffe auf Menschen (Social Engineering, Erpressung, …)	2.1.1 Diebstahl/Raub
B3-1 Ausfall von Systemen	6.1.1 Hardware
B3-2 Ausfall von Kommunikations-infrastruktur	6.1.3 Telekommunikation
B3-3 Ausfall von Infrastruktur-komponenten	6.1.4 Versorgungsausfall/ -störung
B4-1 Gebäudeausfall	6.1.2 Software
B4-2 Personalausfall	3.1.1 Ausgleichszahlungen, Zuwendungen, Abfindungen
B4-3 Urteile, Beschlagnahmung, Reputation	4.2.2 unzulässige Geschäfts-/ Marktpraktiken

>

AUTOREN UND ANSPRECHPARTNER

Björn Scherer
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: bjoern.scherer@dz-cp.de

Benjamin Wellnitz
Beauftragter Informationssicherheit & Datenschutz,
E-Mail: benjamin.wellnitz@dz-cp.de

Diese Zuordnung soll als Beispiel für die weitere Bearbeitung der Risiken dienen.

Nach entsprechender Auswertung aus dem Informationssicherheitsmanagementsystem werden die gebildeten Mittelwerte zur Eintrittswahrscheinlichkeit (EW) und zum Schadenspotenzial (SP) über alle im jeweiligen Bedrohungsbereich liegenden Einzelrisiken an das Self-Assessment/die Risikoinventur übergeben (vgl. Abb. 5).

Bereits getroffene Aussagen der Fachbereiche zu den Eintrittswahrscheinlichkeiten und den Schadenspotenzialen können abgeglichen werden. Hier empfehlen wir das Maximalwertprinzip (konservativer Bewertungsansatz): Je nachdem, welcher Wert höher ist, wird dieser übernommen. Ist die getroffene Aussage des Fachbereiches höher als der Wert aus der Informationssicherheit, so ist der Wert des Fachbereichs beizubehalten. Sofern der Fachbereich einen niedrigeren Wert veranschlagt hat, so ist der Wert aus der Informationssicherheit zu verwenden.

Nach Übertragung aller Positionen erfolgt eine Monte-Carlo-Simulation (Verfahrensmethode aus der Stochastik), um den entsprechenden individuellen Schadenswert zu berechnen. Hierzu sollte der Risiko-Controller eingebunden werden, um die Berechnung durchzuführen.

Fazit

Aufsichtsrechtlich ist spätestens mit den BAIT die monetäre Bewertung der IT-Restrisiken – neben der qualitativen Analyse – zwingend erforderlich. Welche Bewertungsmethoden gewählt werden, sollte seitens der Bank gut überlegt werden und nachvollziehbar (für Dritte) dokumentiert werden. Dabei ist der Weg – wie die Bewertung für die Bank erfolgt – gut zu begründen. ▬

5 BEISPIEL EINER RISIKOINVENTUR IN ISI KOMPAKT

B1 Interne Verfahren	150	BE	SW	EW	SP
B1-1 Fehler von Anwendern/Benutzern	**60**	**2**	**1**	**2**	**2**
agree mobile WLAN-V-R2.1.1. Ungeeignete Aufstellung der WLAN-Access-Points		1	1	1	3
agree21Banking-V-R2.1.1: Versehentliche Falscheingaben durch den Bankmitarbeiter		3	3	3	2
agree21Banking-V-R2.1.1: Versehentliche Falscheingaben von Konditionen oder Kreditlimits durch den Bankmitarbeiter, die einen erweiterten Schaden verursachen können		3	3	3	2
agree21Banking-V-R2.1.1: Versehentliche Falscherfassung bei Zahlungsverkehrsdaten durch den Bankmitarbeiter, die einen erweiterten Schaden verursachen können		1	1	1	2

[1] BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht, https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=9 (Stand: 28.10.2019)

[2] BaFin – Bundesanstalt für Finanzdienstleistungsaufsicht https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs0917_marisk_Endfassung_2017_pdf_ba.pdf?__blob=publicationFile&v=5 (Stand: 28.10.2019)