Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD

Eidgenössische Finanzverwaltung EFV
Rechtsdienst & Risikomanagement
Risikomanagement und Versicherungspolitik

Handbuch zum Risikomanagement Bund

Version vom 16.09.2024

Änderungskontrolle

Wann	Wer	Beschreibung
21.11.2011	rch	Erstversion (Prüfung durch Kessler und AON)
24.05.2013	rch	Einfügen Risikoaggregation von Querschnittsrisiken (inkl. Anhang «Factsheets Querschnittsrisiken Bund»
24.05.2013	rch	Einfügen Prozess Risiko-Update
10.09.2015	mlu	Überarbeitung Schnittstellen, IKT-Risiken, Definitionen und redaktionelle Korrekturen
28.09.2017	elm/Gre	Überarbeitung Risikoidentifikation (neu: Abschnitte Ressourcen, Flughöhe), Schnittstellen (neu: 6.5 Eventualverbindlichkeiten, Anhang 6; vollständig überarbeitet: 6.2 Notfall- und Krisenmanagement, 6.3 Kontinuitätsmanagement; 6.4 Lage- und Umfeldanalyse).
23.11.2018	elm/Gre	Überarbeitung und Ergänzung Risikostrategie für VE und Dept. (1.2.1), Einbettung RM in Führungsprozesse (2.3), Risiko-Überwachung (3.6.1), Querschnittsrisiken (4.3 und Anhang 10), Klassifizierung (5.3.1), Versicherungsmanagement (6.7), Anhänge 1, 2, 7 und 11 (neu)
29.05.2020	Gre	Korrekturen in Einleitung von Anhang 10
14.09.2020	Gre	Überarbeitung Klassifizierung und Öffentlichkeitsprinzip (neues Kapitel 5.3.1)
24.09.2021	afl	Überarbeitung Kapitel 6.8 Informatiksteuerungsorgan des Bundes (ISB) (neu 6.8 Nationales Zentrum für Cybersicherheit NCSC sowie neu 6.9 Digitale Transformation und IKT-Lenkung DTI)
07.07. bis 02.09.2022	elm / afl	Erläuterung Kernfunktionen RM Bund (Kap. 2.2), Ergänzung Risiko-Update (Kap.3.1.2), Ergänzung Wahl Risikoeigner bei QSR (Kap. 4.3.3), Aktualisierung und Ergänzung Corporate Governance (Kap. 6..6), Ergänzung NCSC (Kap. 6.8), Aktualisierung Glossar Eintrag Risikoeigner (Anhang 1), Ersetzen Mustervorlagen Berichterstattung (Anhang 2), Neufassung Abschnitte «Schutz kritische Infrastrukturen» sowie «Nationale Risikoanalyse» (Anhang 8).
16.09.2024	cmü	Anpassungen im Zusammenhang mit der Weiterentwicklung des RM Bund (Statische / Dynamische Risiken, Schwellenwertanpassung RM Bund). Überprüfung der Gültigkeit sämtlicher Rechtsgrundlagen inkl. Vornahme notwendiger Anpassungen (z.B. Ablösung ISchV und CyRV durch ISV). Abbildung von Veränderungen in der Organisationsstruktur.

Inhaltsverzeichnis

Anhang

Abbildungsverzeichnis

Abkürzungsverzeichnis

BABS	Bundesamt für Bevölkerungsschutz
BACS	Bundesamt für Cybersicherheit
BAG	Bundesamt für Gesundheit
BCM	Business Continuity Management (Kontinuitätsmanagement)
BGA	Bundesgesetz über die Archivierung (SR *152.1*)
BGÖ	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung (SR *152.3*)
BK	Bundeskanzlei
BöB	Bundesgesetz über das öffentliche Beschaffungswesen (SR *172.056.1*)
BR	Bundesrat
BRB	Bundesratsbeschluss
BSTB	Bundesstab Bevölkerungsschutz (vgl. SR *520.17*)
BWL	Bundesamt für wirtschaftliche Landesversorgung
CG	Corporate Governance
DTI	Digitale Transformation und IKT-Lenkung
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EDI	Eidgenössisches Departement des Innern
EDV	Elektronische Datenverarbeitung
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EFD	Eidgenössisches Finanzdepartement
EFV	Eidgenössische Finanzverwaltung
FHG	Finanzhaushaltgesetz (SR *611.0*)
FHV	Finanzhaushaltverordnung (SR *611.01*)
GPK	Geschäftsprüfungskommissionen
GSK	Generalsekretärenkonferenz
IKS	Internes Kontrollsystem
ISDS	Informationssicherheits- und Datenschutzkonzept
ISG	Informationssicherheitsgesetz (SR 128)
ISO	International Organization for Standardization
ISV	Informationssicherheitsverordnung (SR *128.1*)
IT	Informationstechnik (Information Technology)
KNS	Katastrophen und Notlagen Schweiz
KOVE	Koordination des Verkehrswesens im Hinblick auf Ereignisfälle (vgl. SR *520.16*)
NAZ	Nationale Alarmzentrale
NDB	Nachrichtendienst des Bundes
OE	Organisationseinheit
ÖNORM	Regelwerk der österreichischen Organisation für Standardisierung und Innovation («Austrian Standards»)
PC	Personal Computer
RC	Risikocoach/-in
RVOG	Regierungs- und Verwaltungsorganisationsgesetz (SR *172.010*)
R2C_GRC	Risk-to-Chance Governance, Risk & Compliance (IT-Anwendung RM Bund)
SANKO	Sanitätsdienstliches Koordinationsgremium (vgl. SR *501.31*)
SEPOS	Staatssekretariat für Sicherheitspolitik SEPOS
SiA	Sicherheitsausschuss des Bundesrates
SKI	Schutz kritischer Infrastrukturen
SOGE	Sonderstab Geiselnahme und Erpressung (vgl. SR *172.213.80*)
SVS	Sicherheitsverbund Schweiz
UVEK	Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation
VBS	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VE	Verwaltungseinheit
VG	Verantwortlichkeitsgesetz (SR *170.32*)
WBF	Eidgenössisches Departement für Wirtschaft, Bildung und Forschung

0 Zweck dieses Dokuments

Das vorliegende Handbuch zum Risikomanagement des Bundes dient als Ergänzung bzw. Erläuterung der Richtlinie über das Risikomanagement Bund[1]. Es wird von der EFV nach Anhörung der Risikomanagerinnen und Risikomanager der Departemente und der Bundeskanzlei (BK) herausgegeben.

Das Handbuch lehnt sich an die gängigen Normenwerke[2] an. Die im Risikomanagement Bund verwendeten Begriffe werden in Anhang 1 näher erläutert bzw. definiert. Das Handbuch unterstützt die im Risikomanagement tätigen Personen (insbesondere Risikomanagerinnen und Risikomanager, Risikocoach und Risikocoachin, Risikoeignerinnen und Risikoeigner) bei der Erfüllung ihrer Aufgaben und dient den Führungskräften und Mitarbeitenden der Bundesverwaltung als Nachschlagewerk für Fragen im Zusammenhang mit dem Risikomanagement des Bundes.

In grau unterlegten Kästchen werden einerseits verbindliche Vorgaben und andererseits Empfehlungen an die Risikomanagerinnen und Risikomanager und Risikocoaches aufgeführt. Die Vorgaben sind notwendig, um eine einheitliche Umsetzung des Risikomanagements und eine konsolidierte Berichterstattung auf Stufe Bundesrat zu ermöglichen.

Das Handbuch wird aufgrund aktueller Bedürfnisse periodisch angepasst und weiterentwickelt. Die Departemente und die BK können entsprechende Anträge stellen.

1 Grundlagen des Risikomanagements des Bundes

1.1 Risikopolitik

Die Rahmenbedingungen für das Risikomanagement beim Bund werden in den «Weisungen über die Risikopolitik des Bundes» (nachfolgend auch als «Risikopolitik» bezeichnet) verbindlich festgelegt. Die Risikopolitik bildet die Grundlage für die Ausgestaltung, Umsetzung, Leistungsbewertung und Verbesserung des Risikomanagements.

1.1.1 Ziele

Das Risikomanagement ist ein Führungsinstrument auf den Stufen Bundesrat (BR), Departement / BK und Verwaltungseinheiten (VE). Es schafft Transparenz über die aktuelle Risikosituation des Bundes und der einzelnen Organisationseinheiten (OE) und ermöglicht es, rechtzeitig die erforderlichen Massnahmen zur Vermeidung oder Verminderung von Risiken zu treffen. Das Risikomanagement Bund soll insbesondere:

- Die Erfüllung der verfassungs- und gesetzmässigen Aufgaben der Bundesverwaltung und die Erreichung der Ziele des Bundes unterstützen;
- Dem Bundesrat und der Bundesverwaltung ermöglichen, ihre Entscheide unter Berücksichtigung möglicher künftiger Ereignisse und Entwicklungen zu fällen, indem wesentliche negative Auswirkungen auf die Erfüllung der Aufgaben und die Erreichung der Ziele frühzeitig erkannt und analysiert werden;
- Seine eigene Wirksamkeit laufend überprüfen und die stetige Weiterentwicklung und Verbesserung sicherstellen.

[1] Die Richtlinie der EFV wurde gestützt auf Ziff. 7 Abs. 1 der Weisungen des Bundesrates vom 26.06.2024 über die Risikopolitik des Bundes erlassen (vgl. BBl *2024* 1662)

[2] Konkret: ISO 31000, ÖNORM 490x-Reihe.

Ausserdem soll die Sicherheit der Vertreterinnen und Vertreter des Bundes gewährleistet, das Vermögen und die Reputation des Bundes geschützt und die verfügbaren Mittel wirksam und wirtschaftlich eingesetzt werden.[3]

1.1.2 Nutzen

Nach einheitlichen Kriterien umgesetzt, ist das Risikomanagement ein Instrument mit vielfältigem Nutzen für den Bund[4]:

- es trägt zu einer vorausschauenden Erfüllung der Bundesaufgaben bei und fördert eine proaktive Führung;
- es trägt zur Funktionsfähigkeit von Regierung und Verwaltung bei;
- es erhöht die Transparenz und die Übersicht über die Risikosituation und erleichtert damit die Entscheidfindung auf allen Führungsebenen;
- es ermöglicht eine wirksame und wirtschaftliche Zuteilung der erforderlichen Ressourcen für die Minimierung von Risiken;
- es trägt bei, das Vertrauen der verschiedenen Anspruchsgruppen (Bundesversammlung, Bevölkerung usw.) in die Bundesverwaltung und den Bundesrat zu erhöhen;
- es sensibilisiert Mitarbeitende in der Bundesverwaltung im Umgang mit den Risiken in ihrem Bereich.

Nutzen und Ziele, wie soeben erörtert, lassen sich nur erreichen, wenn das Risikomanagement als Teil der Führungs- und Steuerungsprozesse begriffen, implementiert und im praktischen Handeln umgesetzt wird. Dies wird in Ziffer 2.3 näher erläutert.

1.2 Risikostrategie und Risikokultur

1.2.1 Risikostrategie

Mit der Risikostrategie legen Organisationen fest, wie sie mit ihren Risiken umgehen wollen. In einem engeren Sinn beschränkt sich die Risikostrategie auf die Frage, in welchem Verhältnis die Chancen und Risiken stehen sollen bzw. wie hoch die eingegangenen Risiken maximal sein dürfen (Risikotoleranz, Wahl der Bewältigungsoptionen, vgl. dazu Ziff. 3.4).

In einem umfassenderen Sinn zeigt die Risikostrategie auf, wie das Risikomanagement insgesamt geplant, umgesetzt, bewertet und verbessert werden soll. Dies umfasst auch die Verpflichtung der obersten Leitung, d. h. das Committment für das Risikomanagement. Bei grossen Organisationen hat es sich überdies als zweckmässig erwiesen, eine organisationsweite Risikostrategie festzulegen (oft *Risikopolitik* genannt), die dann in einzelnen Risikostrategien für die untergeordneten OE konkretisiert wird.

Risikostrategie Stufe Bund

Die umfassende Risikostrategie des Bundes hat der Bundesrat in seinen *Weisungen über die Risikopolitik des Bundes* festgelegt. Zentrale Punkte sind dabei die Risikodefinition und der Geltungsbereich, die Ziele und Grundsätze sowie die grundlegenden Funktionen im Risikomanagement.

Mit Blick auf die Risikotoleranz und die Risikobewältigung gilt generell, dass sich Risiken aufgrund der Pflicht der Bundesverwaltung, ihre gesetzlichen Aufgaben zu erfüllen, nicht vollständig vermeiden lassen. Der Bund ist bereit, Risiken bewusst und kontrolliert einzugehen,

[3] Ziff. 3 Abs. 1 der Weisungen über die Risikopolitik des Bundes

[4] Vgl. Ziff. 3 der Weisungen über die Risikopolitik des Bundes

sofern dies für die Zielerreichung bzw. die Aufgabenerfüllung unvermeidbar ist. Getreu dem Grundsatz des haushälterischen Umgangs mit Mitteln des Bundes sollen die mit der Erfüllung der Bundesaufgaben einhergehenden Risiken möglichst gering gehalten werden. Der Entscheid über die Umsetzung risikominimierender Massnahmen erfolgt gestützt auf Kosten-/Nutzenüberlegungen (inkl. einer Rechtsgüterabwägung[5]).

Der Bund trägt das Risiko für Schäden an seinen Vermögenswerten und für die haftpflichtrechtlichen Folgen seiner Tätigkeit grundsätzlich selbst[6] (Grundsatz der Eigenversicherung). Einer finanziellen Risikoüberwälzung (z. B. mittels Abschluss eines Versicherungsvertrags, Derivate usw.) stimmt die EFV nur in besonderen Fällen zu[7].

Risikostrategie Stufe Departement und VE

Auf Stufe des einzelnen Departements bzw. der BK sowie der einzelnen VE soll die Risikostrategie aufzeigen, wie die Führung die Risikopolitik des Bundesrates im eigenen Bereich konkret umsetzen will und welche Ziele damit erreicht werden sollen. Eine Risikostrategie sollte sich namentlich zu folgenden Aspekten äussern:[8]

- Verpflichtung bzw. Absicht der obersten Leitung;
- Ziele und angestrebter Nutzen des Risikomanagements für die OE;
- Eckpunkte der Umsetzung eines integrierten Risikomanagements in der OE, d. h. des anzustrebenden Zusammenwirkens von Führungsprozessen und Risikomanagement (vgl. Ziff. 2.3);
- Funktionen, Aufgaben und Erwartungen im Risikomanagement;
- Risikobewältigung (Risikostrategie i. e. S.): Vorgehen bei der Beurteilung der Risikotoleranz (vgl. Ziff. 3.4), Bewältigungsoptionen, Steuerung der Massnahmen zur Risikoreduktion, Festlegung des Reduktionsziels.

Die Risikostrategie soll allen Kadern und Mitarbeitenden der OE bekannt sein. Sie dient ihnen als Grundlage für Führungsentscheide und ist Teil der angestrebten Risikokultur.

1.2.2 Risikokultur

Eine der wichtigsten Voraussetzungen für ein wirksames und vorausschauendes Risikomanagement ist eine gute «Risikokultur»: Alle Mitarbeitenden und jede Führungskraft pflegen einen bewussten Umgang mit Risiken und eine positive Fehlerkultur.

- ***Umgang mit Fehlern****:* Eine positive Fehlerkultur erlaubt die offene Diskussion über Mängel und fördert die Aufdeckung von Risiken innerhalb von Prozessen und Systemen. Lösungen zur Reduktion dieser Risiken können erarbeitet werden. Eine offene Kommunikation über Fehler erlaubt es zudem, aus den Fehlern anderer zu lernen.
- ***Offener Informationsaustausch und Lernkultur****:* Eine offene Kommunikation, unter Berücksichtigung der Sicherheitsvorschriften klassifizierter Informationen (vgl. Ziffer 1.4), und die Bereitschaft, von anderen zu lernen, fördern ein besseres und tieferes Verständnis der eigenen Aufgaben und Prozesse. Insbesondere die Identifikation und die Bewältigung von Risiken an der Schnittstelle zwischen zwei oder mehreren OE werden so erleichtert. Jeder Bereich profitiert von den Erfahrungen der anderen.
- ***Respekt vor fachlichem Wissen und Können****:* Bei der Risikoanalyse und bei der Erarbeitung von Bewältigungsoptionen wird Wert auf die Meinung der Personen mit grossem Know-how gelegt, auch wenn diese keine Entscheidungsbefugnisse haben. Ihre Stellungnahmen und allenfalls davon abweichende Entscheide der Führung

[5] z. B.: Menschenwürde, körperliche Unversehrtheit (Leib und Leben), Eigentum usw.

[6] Art. 50 Abs. 2 FHV

[7] Vgl. Weisungen der EFV vom 11.09.2015 über die Risikotragung und Schadenerledigung im Bund

[8] Vgl. Mustervorlage «Risikostrategie» (Anhang 11)

(«management overruling») sollen dokumentiert werden.

- ***Informationspflicht**:* Die Pflicht jedes Mitarbeitenden, seine Vorgesetzten über relevante Gefahren in seinem Tätigkeitsbereich zu informieren, führt zu erhöhter Aufmerksamkeit und dazu, dass die Risikoverantwortung wahrgenommen wird.

Neben der Förderung von allgemeinen Arbeitsgrundsätzen, welche die Risikokultur verbessern, ist auch ein regelmässiger Austausch zu Themen des Risikomanagements wichtig. Dieser fördert das Risikobewusstsein und die Sensibilität für das Thema Risikomanagement (vgl. auch Ziff. 5.1).

Selbstverständlich kann der Aufbau bzw. die Verbesserung der Risikokultur nicht von einem Tag auf den anderen erfolgen. Das benötigt seine Zeit, denn Arbeitseinstellungen und Denkmuster können oft nur langsam neu ausgerichtet werden. Die EFV schenkt diesem Thema im Rahmen der steten Verbesserung des Risikomanagements Bund grosse Aufmerksamkeit und ergreift nötigenfalls Massnahmen, um weitere Verbesserungen herbeizuführen.

1.3 Geltungsbereich und Risikodefinition

Wichtigster sachlicher Ansatz- und Abgrenzungspunkt des Begriffs Risiko im Risikomanagement Bund sind die Aufgaben und Ziele der Bundesverwaltung. Die genaue Definition lautet:

Definitionstext	**Definierter Aspekt**
Risiken sind Ereignisse und Entwicklungen,	*Art des Eintritts (unmittelbar vs. allmählich)*
die mit einer gewissen Wahrscheinlichkeit eintreten	*Unsicherheit*
und wesentliche negative finanzielle und nichtfinanzielle Auswirkungen haben	*Wesentlichkeit, Schadensdimensionen*
auf die Erreichung der Ziele und die Erfüllung der Aufgaben	*sachliche Eingrenzung*
der Bundesverwaltung.	*institutionelle Eingrenzung*

Das Risikomanagement Bund wird in der zentralen Bundesverwaltung durchgeführt sowie in jenen dezentralen Einheiten, die keine eigene Rechnung führen.[9]

1.4 Umgang mit als «GEHEIM» klassifizierten Informationen

Das Risikomanagement befasst sich mit *allen* Aufgabengebieten des Bundes, somit auch mit sehr sensiblen Bereichen wie z. B. der inneren und äusseren Sicherheit. Auch die Risiken aus diesen Bereichen fliessen in die Risikoberichterstattung an den Bundesrat ein. Als GEHEIM klassifizierte Informationen sind in geeigneter Weise im Risikomanagement zu erfassen. Der Schutz von Informationen des Bundes und der Armee im Interesse des Landes und insbesondere deren Klassifizierung und Bearbeitung ist in der Informationssicherheitsverordnung (ISV)[10] geregelt. Zum Thema Klassifizierung von Informationen des Risikomanagements siehe Ziffer 5.3.1 hiernach.

[9] Risikodefinition und Geltungsbereich sind formell in der «Richtlinie über das Risikomanagement Bund» der EFV aufgeführt.

[10] SR *128.1*

2 Organisation des Risikomanagements Bund

2.1 Aufbau

Das Risikomanagement innerhalb der Bundesverwaltung ist dezentral organisiert. Die Departemente und die BK sind für die Umsetzung in ihrem Bereich verantwortlich. Auf der Stufe Departement / BK und in jeder VE[11] ist je eine Risikomanagement-Funktion vorgesehen, die die verschiedenen Risikomanagement-Tätigkeiten koordiniert und den Risikomanagementprozess steuert. Demgegenüber erfüllt die Koordinationsstelle Risikomanagement in der EFV (Koordinationsstelle EFV) eine departementsübergreifende Funktion. Sie stellt sicher, dass das Risikomanagement in der Bundesverwaltung einheitlich umgesetzt wird.

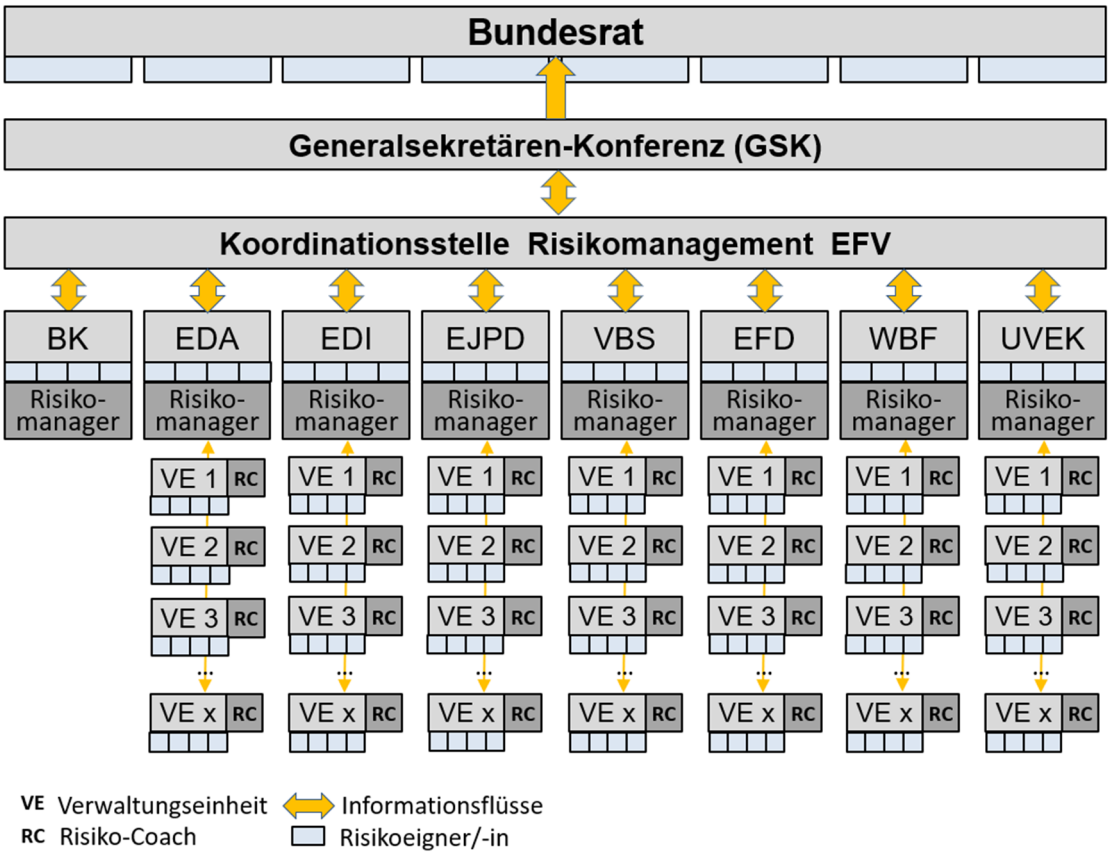


Abbildung 1: Organisation Risikomanagement Bund

2.2 Funktionen und Verantwortlichkeiten

Die Aufgaben und Verantwortlichkeiten der verschiedenen Funktionen im Risikomanagement Bund sind in Ziffer 3 der «Richtlinie über das Risikomanagement Bund» der EFV umschrieben. Zu den Kernfunktionen zählen namentlich:

- **Risikocoach/-in:** Person, welche für die korrekte Anwendung der Methodik RM Bund innerhalb der VE zuständig ist, die den Risikomanagement-Prozess umsetzt und dabei die Geschäftsleitung sowie die Risiko- und Massnahmeneigner berät (s. auch Anhang 4 Pflichtenheft).
- **Risikomanager/-in:** Analoge Funktion zum Risikocoach/-in auf Stufe Departement.

[11] Das Gleiche gilt für die Generalsekretariate. Die Funktion des Risikocoaches Risikocoachin/-coaches des Generalsekretariats kann (muss aber nicht) in Personalunion vom Risikomanager des Departements ausgeübt werden.

Darüber hinaus sorgen die Risikomanager innerhalb ihres Departements für die einheitliche Anwendung der Methodik sowie deren Weiterentwicklung in Zusammenarbeit mit der Koordinationsstelle, für die Umsetzung und Qualität der Berichterstattung und pflegen einen regelmässigen Fachaustausch zwischen den Risikocoaches und verwandten Funktionen wie IKS oder BCM (s. auch Anhang 4 Pflichtenheft).

- **Risikoeigner/-in:** Person, die ein Risiko mit seinen Massnahmen zur Risikominderung steuert und auch für die Berichterstattung über dieses Risiko verantwortlich zeichnet. Sie verfügt über die dafür erforderlichen Entscheidungskompetenzen. Bei Risiken besonderer Tragweite – etwa Querschnittsrisiken – ist auch denkbar, dass die Risikoverantwortung zusätzlich einem strategischen Gremium übertragen wird, das bei zentralen Steuerungfragen informiert wird, mitwirkt oder entscheidet.
- **Massnahmenverantwortliche:** Person, die vom Risikoeigner/-in beauftragt wird, eine spezifische Massnahme zur Risikomminderung zu steuern.

Die Funktionen beim Bund, für deren Ausübung eine Personensicherheitsprüfung durchgeführt werden muss (z. B. Risikomanager), sind in der Verordnung über die Personensicherheitsprüfungen (VPSP; SR *128.31*) aufgeführt.

2.3 Risikomanagement in den Führungsprozessen der Bundesverwaltung

«Das Risikomanagement ist ein Führungsinstrument. Es ist fester Bestandteil der Geschäfts- und Führungsprozesse und gehört zur sorgfältigen und wirtschaftlichen Aufgabenerfüllung und -verantwortung.» Mit diesem ersten Grundsatz der Weisungen über die Risikopolitik[12] verpflichtet der Bundesrat die Geschäftsleitungen auf allen Führungsebenen, dafür zu sorgen, dass das Risikomanagement

1. eng mit den Führungsprozessen verknüpft ist und die Risikodimension in der Führungsarbeit konsequent berücksichtigt wird (funktionale Integration);
2. auf allen Führungsebenen umgesetzt wird und der Informationsfluss zwischen diesen Ebenen, d. h. von der Spitze zur Basis (Topdown) und von der Basis zur Spitze (Bottom-up) gewährleistet ist (vertikale Integration);
3. mit den anderen Prozessen der Führungsunterstützung – z. B. der finanziellen Führung, der IKT-Steuerung oder dem internen Kontrollsystem (IKS) – vernetzt ist und koordiniert betrieben wird (horizontale Integration).

Die praktische Umsetzung dieser drei Merkmale eines *integrierten Risikomanagements* wird nachfolgend erläutert.

2.3.1 Funktionale Integration: Einbettung in Planungs- und Strategieprozesse

Zu den Führungsaufgaben zählt der bewusste und rationale Umgang mit Unsicherheit: mögliche Risiken für die Aufgabenerfüllung und die Zielerreichung sollen frühzeitig erkannt und systematisch gesteuert werden. Das Risikomanagement Bund sieht die dazu geeigneten Instrumente, Methoden und Rollen[13] vor. Für die funktionale Integration des Risikomanagements ist ein optimales Zusammenwirken zwischen den Führungsverantwortlichen und ihren Risikobeauftragten (Risikomanagerinnen und -manager, Risikocoaches) gemäss Ziffer 2.1 essentiell. Dieses wird namentlich an folgenden Merkmalen erkannt:

[12] Ziff. 4 Abs. 1 der «Weisungen über die Risikopolitik des Bundes».

[13] Ausführlich beschrieben in Ziff. 3.1.3 (Informationsflüsse im Risikomanagement Bund) sowie Ziff. 3 der «Richtlinie über das Risikomanagement Bund» der EFV (Funktionen und Verantwortlichkeiten).

- **Die Führungskräfte** nutzen das Risikomanagement für die Führungsarbeit und binden dieses systematisch in ihre Führungsprozesse ein. Insbesondere ziehen sie das Risikomanagement in den ordentlichen Planungs- und Strategieprozessen sowie bei allen wesentlichen inneren oder äusseren Veränderungen ein. In der Regel zweimal pro Jahr analysieren sie die Risikosituation ihrer OE und überprüfen in der Geschäftsleitung die Umsetzung sowie die Wirksamkeit der Massnahmen.
- **Die Risikobeauftragten (Risikocoaches, Risikomanagerinnen und -manager)** beraten die Führungskräfte kompetent und unterstützen die Entscheidungsprozesse in der Geschäftsleitung mit stufengerechter Information und überzeugenden Vorschlägen. Sie halten das Risiko- und Massnahmenportfolio auf aktuellem Stand, koordinieren Risiko-Reportingprozess sowie Risiko-Update und unterbreiten der Geschäftsleitung die periodischen Risikoberichte[14].

Damit die funktionale Integration gelingt, ist also ein *regelmässiger und gezielter Austausch* zwischen Geschäftsleitung und Risikobeauftragten erforderlich. Dieser Austausch soll erstens zu jenen Zeitpunkten erfolgen, an denen die Pläne und Strategien geschmiedet werden. Dies betrifft zunächst die *ordentlichen strategischen Planungen* der VE bzw. der Departemente/BK, aus denen die Legislaturziele hervorgehen (alle vier Jahre) und die jährlich aktualisiert werden. Formal werden diese Planungen in den jährlichen Bundesrats- und Departementszielen festgehalten. Im Rahmen des Budgetprozesses werden diese Ziele und Vorhaben mit Ressourcen ausgestattet (Voranschlag mit Integriertem Aufgaben- und Finanzplan IAFP) und später in der jährlichen *Leistungsvereinbarung zwischen Departement und VE* aktualisiert, konkretisiert und detailliert. Neben diesen Standard-Planungsprozessen können sich *wesentliche Anpassungen von Aufgaben, Strategien und Zielen* im laufenden politischen Prozess grundsätzlich jederzeit ergeben und damit einen Einbezug der Risikobeauftragten nötig machen. Die unmittelbare Berücksichtigung der Risikodimension in den Planungs- und Strategieprozessen ermöglicht tragfähige Entscheide und trägt damit zu einem effizienten Ressourceneinsatz bei (vgl. Ziffer 1.1.2 Nutzen).

Zweitens findet ein Risikodialog zwischen Geschäftsleitung und Risikobeauftragten während des *Risikoreportings* und des *Risiko-Updates* statt. Im Gegensatz zu den Planungsprozessen steht bei diesen Arbeiten die Risikodimension selbst im Zentrum: Während im Rahmen des *Reportings* die Risikoexposition der VE umfassend evaluiert wird, d. h. die bestehenden Risiken aktualisiert, neue potentielle Risiken geprüft und obsolete Risiken erledigt werden, fokussiert das *Risiko-Update* dieselben Schritte auf die Toprisiken zuhanden des Bundesrats.[15] Die Risikoberichte beider Prozesse werden jeweils durch die Geschäftsleitung genehmigt und zuhanden der nächsthöheren Führungsstufe verabschiedet.

Drittens erweist es sich als wertvoll, wenn sich die Geschäftsleitung mindestens einmal pro Legislatur vertieft mit der Risikoexposition und der Risikosteuerung ihrer VE auseinandersetzt. Ziel ist es, aus einer Topdown-Sicht die mittelfristig bedeutenden Risikofelder zu identifizieren und zu beurteilen sowie die Funktionsfähigkeit des eigenen Risikomanagements zu evaluieren.

[14] Die Risikoberichte sind die wichtigsten sichtbaren Outputs des Risikomanagements und ein zentrales Qualitätsmerkmal (vgl. dazu Anhang 2 «Kommentierter Risikoerfassungsbogen»).

[15] Für weiterführende Informationen zum Reporting vgl. Ziffern 3.1 und 4.

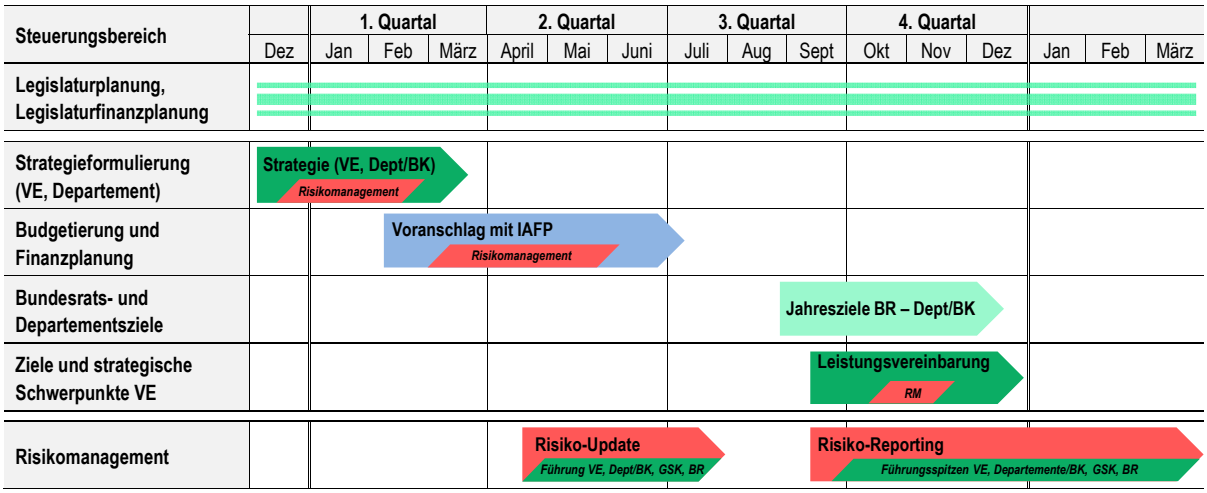


Abbildung 2: Funktionale Integration des Risikomanagements als Führungsprozess

Die funktionale Einbindung des Risikomanagements als Führungsinstrument erfolgt somit idealtypisch über zwei Wege: Im Rahmen der Planungs- und Strategiebildungsprozesse unter Führung der Geschäftsleitung wird das Risikomanagement punktuell einbezogen. Umgekehrt erfolgen Risikoreporting und Update aus der Perspektive und unter Federführung des Risikomanagements selbst. Gemeinsam ist beiden Ansätzen, dass immer die Führungsspitzen der VE, der Departemente/BK und letztlich der Bundesrat für die Risiken ihres Bereichs verantwortlich sind.[16]

2.3.2 Vertikale Integration: Durchgängigkeit zwischen den Führungsebenen

Die Geschäftsleitung muss sicherstellen, dass die Informationen zwischen den verschiedenen Führungsebenen – von der strategischen Führung zum operativen Management bis zu den einzelnen Leistungsprozessen – durchgängig fliessen können: Die Aufträge sollen hierarchieabwärts empfangen und stufengerecht umgesetzt werden können. Umgekehrt müssen die Führungskräfte hierarchieaufwärts über die Umsetzung der Aufträge ins Bild gesetzt werden.

Diese Anforderung gilt auch für das Risikomanagement des Bundes, das die Führungsprozesse auf allen Stufen begleitet (Abbildung 3): Während die bundesweiten Vorgaben, d. h. die Risikopolitik, -methodik und -organisation vom Bundesrat topdown erlassen werden, folgt die Umsetzung – Risikoidentifikation, Bewertung und Bewirtschaftung – einem Bottom-up-Ansatz. Letzteres verlangt eine konsequente Anwendung der gemeinsamen Standards bei Methode und Instrumenten. Nur so ist es möglich, die Risiken der einzelnen VE zu vergleichen und entlang der Führungspyramide sinnvoll zu priorisieren und zu eskalieren.[17]

Die Verbindung von Topdown- und Bottom-up-Ansatz findet nicht nur in der Bundesverwaltung als Ganzes statt, sondern bereits auf Stufe der einzelnen VE. So ist der Risikomanagement-Prozess (Identifikation, Analyse, Bewertung, Bewältigung, vgl. Ziff. 3) zunächst als Bottom-up-Prozess angelegt. Damit wird sichergestellt, dass gestützt auf die Sachkenntnis und praktische Erfahrung an der Basis möglichst alle bedeutenden Risiken erkannt werden. Im Gegenzug fällt der Geschäftsleitung die Aufgabe zu, diese Risiken aus einer Topdown-Sicht abschliessend zu bewerten und zu priorisieren. Dabei wird sie ihr Risikoportfolio auf eine überschaubare Zahl relevanter Risiken begrenzen. Ebenfalls aus einer Topdown-Perspektive soll die Geschäftsleitung periodisch potentielle Risikofelder und Risikoexposition ihrer VE aus einer Gesamtsicht überprüfen (vgl. Ziff. 2.3.1). Analog gilt dieses Prinzip auch auf Stufe des Departements.

[16] Vgl. Ziffer 5 Abs. 3 Bst. a. und Abs. 4 Bst. a. der «Weisungen über die Risikopolitik des Bundes».
[17] Vgl. Kapitel 4.4 über die Auswahl von Risiken im Risikomanagement Bund.

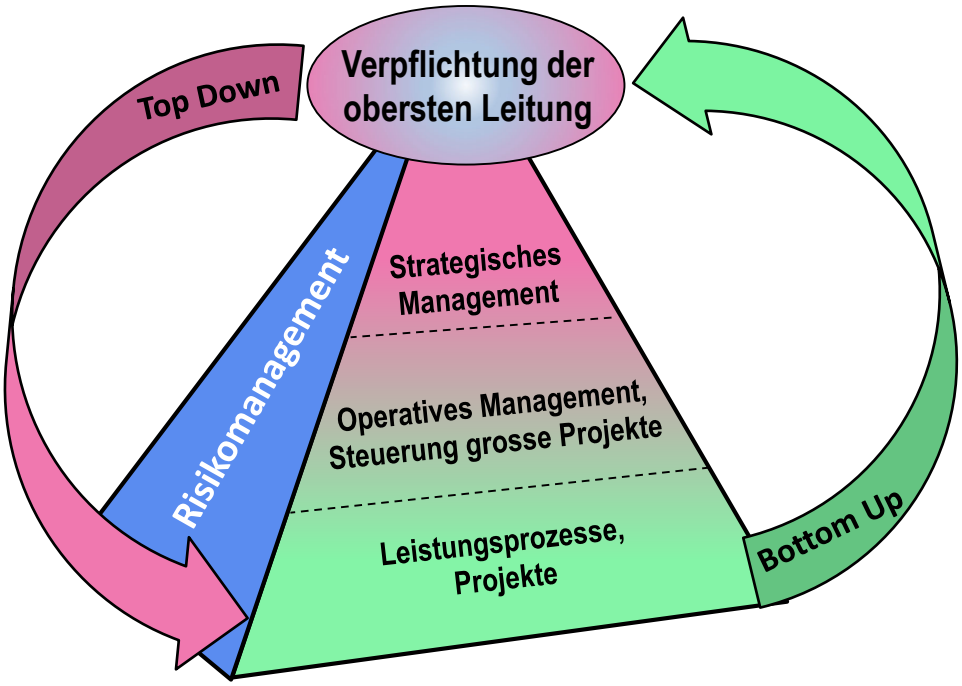


Abbildung 3: Vertikale Integration der Führungsebenen im Risikomanagement

2.3.3 Horizontale Integration: Vernetzung mit weiteren Bereichen der Führungsunterstützung

Neben dem Risikomanagement obliegen der Geschäftsleitung einer VE diverse weitere Führungsaufgaben. Dazu zählen insbesondere der Betrieb des Business Continuity Managements (BCM), des internen Kontrollsystems (IKS) oder des IT-Sicherheitsmanagements; je nach Kernaufgabe führen gewisse VE überdies ein Qualitäts-, ein Compliance- oder ein Arbeitssicherheitsmanagement. Gemeinsam ist diesen Instrumentarien, dass sie die Führungsspitze unterstützen und gleichzeitig entlasten sollen.

Zwischen dem Risikomanagement und diesen Instrumentarien bestehen teils enge Bezüge. Eine gute Vernetzung trägt dazu bei, Synergien zu erschliessen und Silodenken vorzubeugen. So können Erkenntnisse aus benachbarten Bereichen wichtige Hinweise auf latente Risiken geben. Umgekehrt kann das Risikomanagement allfällige Prozesslücken in den anderen Instrumentarien aufdecken und mögliche Massnahmen zur Risikoreduktion aufzeigen. Die Verbindungen zwischen Risikomanagement und den anderen Bereichen bezwecken, die jeweiligen Besonderheiten gegenseitig nutzbar zu machen, um den Gesamtwert der Führungsunterstützung zu erhöhen. Im Sinn nicht abschliessender Beispiele wird sich der Austausch zwischen Risikomanagement und anderen Instrumentarien mit folgenden Fragen befassen:

- **IKS:** Sind die IKS-Prozesse zweckmässig und flächendeckend implementiert oder bestehen Lücken? Gibt es Hinweise auf systemische Mängel, aus denen grössere Risiken für die VE oder das Departement hervorgehen können? (vgl. Ziff. 6.1)
- **BCM:** Wurden die geschäftskritischen Prozesse identifiziert und bei Bedarf aktualisiert? Sind die vorgesehenen Massnahmen ausreichend für die angestrebte Risikoreduktion und greifen sie bei Risikoeintritt, d. h. wurden sie realistisch getestet? (vgl. Ziff. 6.2 und 6.3)
- **IKT:** Werden Projektrisiken systematisch analysiert und gesteuert? Ist das IKT-Controlling auf Projektrisiken gestossen, die sich unter Einwirkung von Umfeldveränderungen akzentuieren könnten? Gibt es aus der ISDS-Analyse (**I**nformations**s**icherheit und **D**aten**s**chutz) Hinweise auf relevante Sicherheitslücken? (vgl. Ziff. **Fehler! Verweisquelle konnte nicht gefunden werden.**)

- **Lage- und Umfeldanalyse:** Gibt es Hinweise auf mittelfristige politische, gesellschaftliche und wirtschaftliche Veränderungen oder auf Megatrends, die neue Risiken oder eine Akzentuierung bestehender Risiken begründen können? (vgl. Ziff. 6.4)

Ein regelmässiger Informationsaustausch stellt die horizontale Integration des Risikomanagements mit den anderen Prozessen der Führungsunterstützung sicher und erlaubt es, ein schärferes Gesamtbild über die Risikoexposition der VE zu gewinnen.

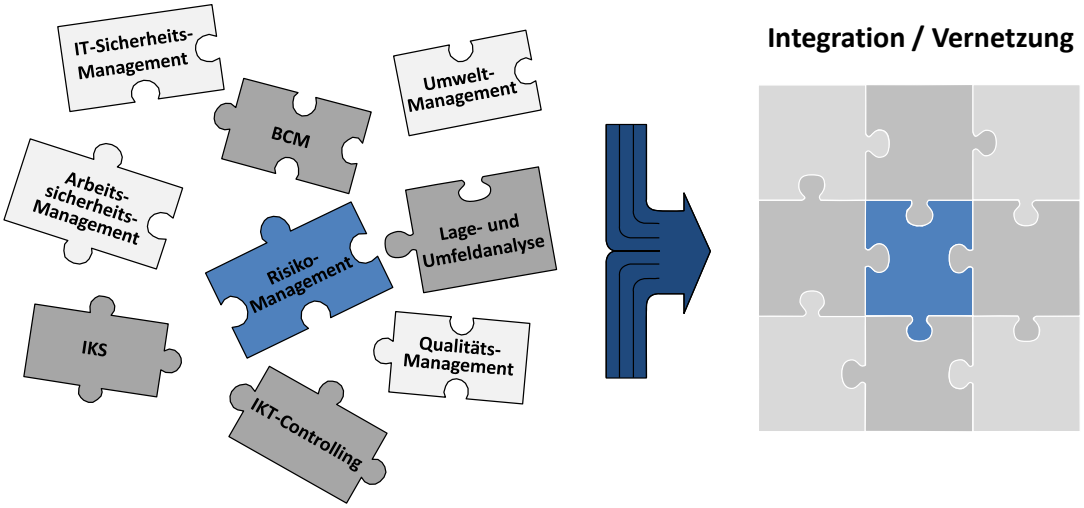


Abbildung 4: Vernetzung von Supportbereichen in der Bundesverwaltung

Definition der Rahmenbedingungen: Integriertes Risikomanagement
Ein integriertes Risikomanagement ist mit den Führungsprozessen und ihren Stabsbereichen auf allen Stufen eng verwoben.

Empfehlung EFV:

- Der Austausch zwischen Geschäftsleitung und Risikomanagement erfolgt einerseits im Rahmen der Planungs-, Strategie- und Zielbildungsprozesse, andererseits im Rahmen des Risikoreportings und des Risiko-Updates. Darüber hinaus soll sich die Führungsspitze mindestens einmal je Legislatur aus einer Gesamtsicht mit der Risikoexposition auf mittlere Sicht sowie mit der Qualität der Risikosteuerung auseinandersetzen (Funktionale Integration).
- Das Risikomanagement soll zwischen den einzelnen Führungsebenen durchgängig betrieben werden können. Es erfolgt deshalb sowohl aus einer Topdown- als auch einer Bottom-up-Richtung, die über die bundesweiten Standards hinsichtlich Methode und Instrumentarium verbunden sind (Vertikale Integration).
- Das Risikomanagement ist vernetzt mit den anderen Bereichen der Führungsunterstützung und erschliesst so Synergien. Namentlich ist mindestens einmal pro Jahr ein strukturierter Austausch mit den Bereichen IKS, BCM, IKT-Controlling und -sicherheit durchzuführen. Abhängig von den Aufgaben und Funktionen einer VE ist auch der Austausch mit weiteren Stabsbereichen zu pflegen (Horizontale Integration).

3 Risikomanagementprozess

Die Konsolidierung der Risiken auf Stufe Departement / BK und Bundesrat setzt voraus, dass die Bewertungen der einzelnen Risiken untereinander vergleichbar sind. Die Identifikation, Analyse und Bewertung, Beurteilung, Bewältigung und Überwachung der Risiken muss deshalb nach einheitlichen Regeln erfolgen. Diese werden mit der «Richtlinie über das Risikomanagement Bund» der EFV verbindlich vorgegeben. Zur Unterstützung einer einheitlichen Umsetzung des Risikomanagementprozesses in der Bundesverwaltung und zur Ermöglichung eines Reportings auf Stufe Bundesrat und Departement / BK wird für die Bewirtschaftung der Risiken und die Risikoberichterstattung eine gemeinsame Informatikanwendung (R2C_GRC) eingesetzt[18]. Diese wird von der EFV zur Verfügung gestellt und betreut.

In dieser und den nachfolgenden Ziffern wird die Umsetzung der Aufgaben innerhalb des Risikomanagementprozesses (vgl. Abbildung 4) in der Bundesverwaltung erläutert.

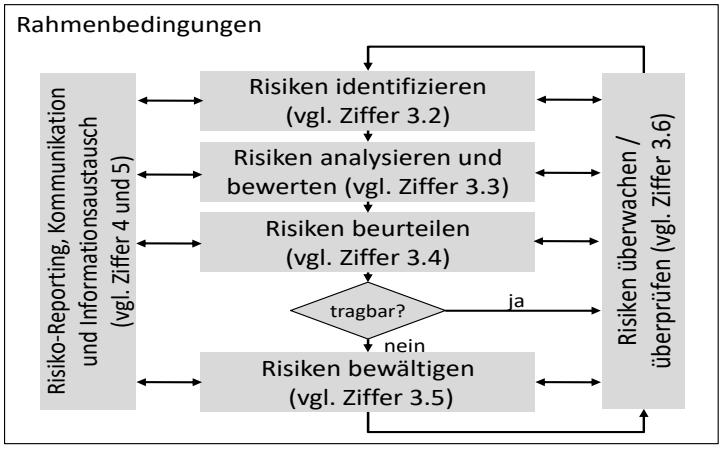


Abbildung 5: Risikomanagementprozess nach gängigen Normen

3.1 Prozessabläufe und Informationsflüsse in der Bundesverwaltung

Die Prozessabläufe können schematisch wie folgt dargestellt werden:

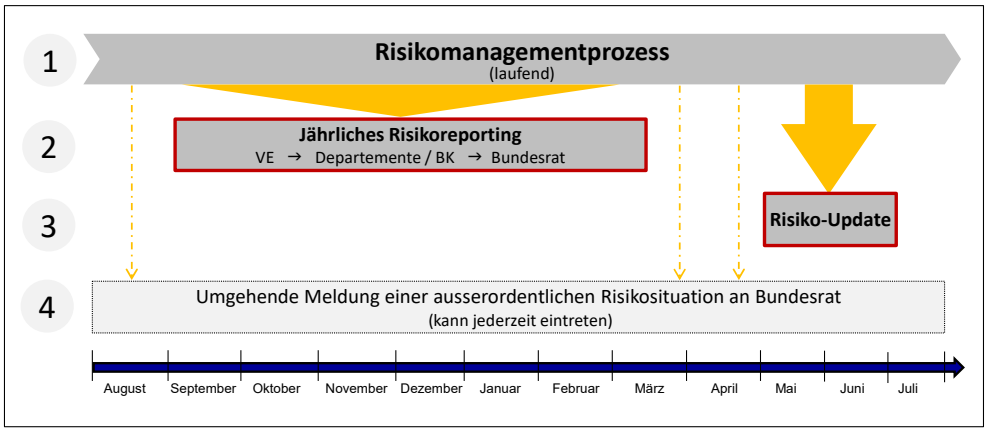


Abbildung 6: Prozessabläufe im Risikomanagement Bund

[18] Ziff. 3 Abs. 1 der Weisungen über die Risikopolitik des Bundes

Die Überwachung der Risikosituation des Bundes durch die Mitarbeitenden und Führungskräfte erfolgt laufend (1). Zusätzlich zum jährlichen bundesweiten Risikoreporting (2) wird für die grössten Risiken des Bundes ein Risiko-Update durchgeführt (3). Bei ausserordentlichen Risikosituationen wird der Bundesrat umgehend informiert (4).[19]

3.1.1 Jährliches Risikoreporting

In der Bundesverwaltung wird einmal jährlich ein *umfassendes* Risikoreporting durchgeführt (vgl. Abbildung 5). Es ist Sache der Risikocoaches und der Risikomanager, für ihre OE die internen Abläufe und Termine im Detail festzulegen. Die Koordinationsstelle EFV gibt nur das Datum für die Abgabe der Departementsreportings verbindlich vor.

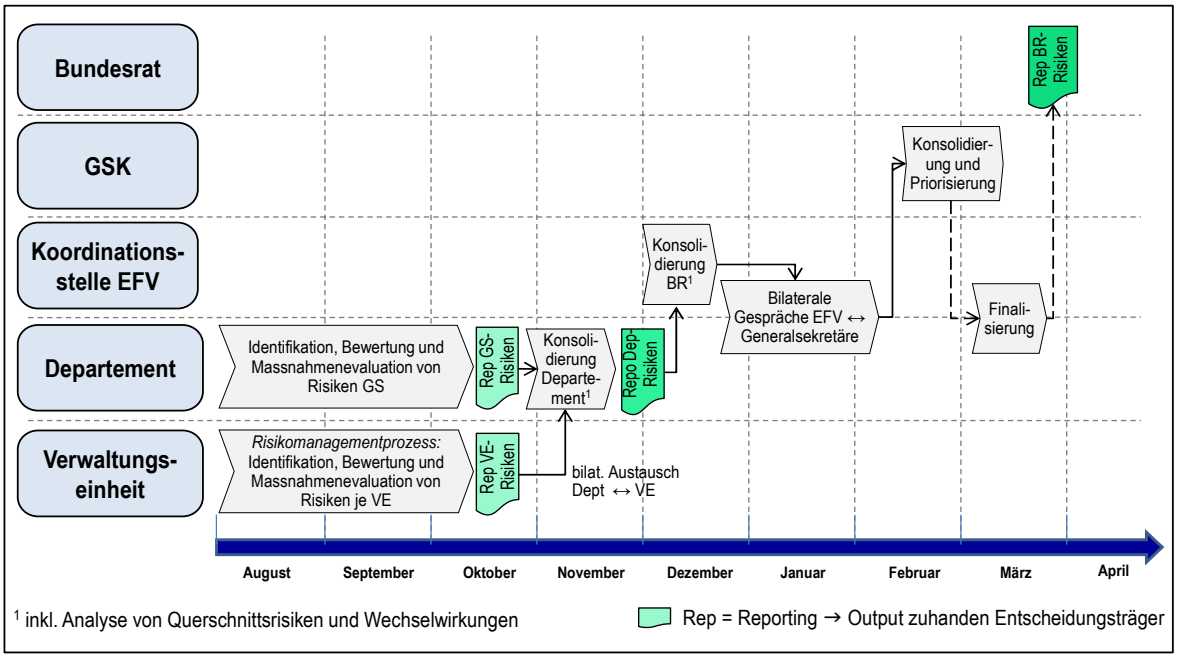


Abbildung 7: Prozessablauf des jährlichen Risikoreportings in der Bundesverwaltung

Die Risikoberichterstattung an den Bundesrat wird von einer Arbeitsgruppe der Geschäftsprüfungskommissionen (GPK) im Rahmen einer Sitzung im April behandelt.

3.1.2 Risiko-Update

Zwecks Dynamisierung und Stärkung des Risikomanagements im Bund wird zusätzlich im Juni ein Risiko-Update durchgeführt. Es handelt sich um einen Topdown-Prozess, der auf die grössten Risiken des Bundes fokussiert. Geprüft und aktualisiert werden folgende Risiken:

- Bundesratsrisiken
- Querschnittsrisiken Bund mit den Quellrisiken der Departemente und der BK (inkl. allfälligen neuen Quellrisiken)
- neue Risiken mit Krisenpotential sowie neue Quellrisiken

Die Vollzugsmeldung an die Koordinationsstelle erfolgt mittels seitens Generalsektretärin oder Generalsekretär digital signiertem Erfassungsblatt. Der Bundesrat wird über die Ergebnisse des Risiko-Updates mittels Informationsnotiz oder Antrag orientiert. Das Risiko-Update wird auch der Arbeitsgruppe «Risikomanagement Bund» beider GPK zur Kenntnis gebracht.

[19] Vgl. Ziff. 5 Abs. 4 der Weisungen über die Risikopolitik des Bundes; flankierend wird die Koordinationsstelle EFV informiert.

3.1.3 Informationsflüsse im Risikomanagement Bund

Die nachfolgende Abbildung verdeutlicht schematisch die wichtigsten Informationsflüsse innerhalb des Risikomanagements bis auf Stufe VE.

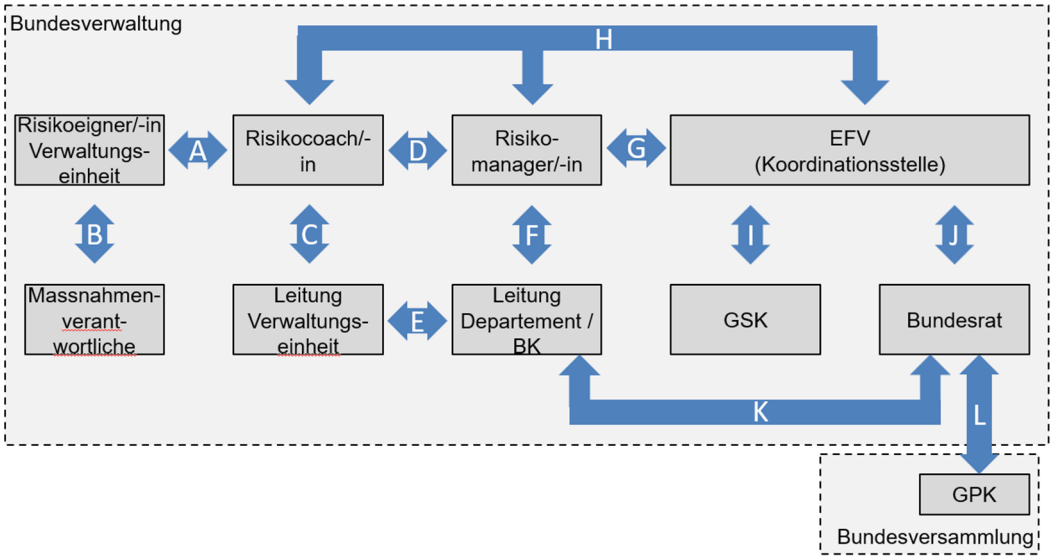


Abbildung 8: Informationsflüsse

Die einzelnen Informationsbeziehungen können wie folgt beschrieben werden:

A Im jährlichen Risikomanagementprozess arbeiten die Risikocoaches mit den unterschiedlichen Risikoeignern der VE zusammen, um neue Risiken zu identifizieren, zu analysieren und zu bewerten, zu bewältigen sowie um bereits identifizierte Risiken zu aktualisieren.

B Die Risikoeigner[20] erteilen den Massnahmenverantwortlichen Aufträge zur Umsetzung von Massnahmen und überwachen deren Umsetzung. Die Massnahmenverantwortlichen berichten den Risikoeignern periodisch über den Stand der Umsetzung und allfällige Probleme und Verzögerungen.

C Die Risikocoaches erstellen zuhanden der Leitung der VE einen Entwurf des Risikoreportings. Diese analysiert und ergänzt die Risiken. Weiter beschliesst sie über die Umsetzung von Massnahmen in ihrem Zuständigkeitsbereich.

D Regelmässiger fachlicher Austausch. Die Risikomanagerinnen und -manager erlassen terminliche und methodische Vorgaben. Die Risikocoaches liefern den entsprechenden Risikomanagerinnen und -managern die Departementsrisiken ihrer VE.

E Information/Diskussion über die Toprisiken der VE, die an das Departement gemeldet werden. Besprechung/Beschlussfassung über Risiko-Massnahmen auf Stufe Departement.

F Die Risikomanagerinnen und -manager konsolidieren die Risiken aller VE und erstellen zuhanden der Leitung des Departementes / der BK einen Entwurf des Risikoreportings. Diese analysiert und ergänzt die Risiken. Weiter verabschiedet sie das Departementsreporting zuhanden des Bundesrats via Koordinationsstelle EFV.

G Regelmässiger fachlicher Erfahrungsaustausch. Die Koordinationsstelle EFV erlässt terminliche und methodische Vorgaben. Die Risikomanagerinnen und -manager liefern der Koordinationsstelle EFV die Kernrisiken ihres Departements / der BK.

[20] Der Risikoeigner/-in kann auch die Leitung der VE oder des Departements / der BK sein.

H Fachliche Schulung der Risikomanagerinnen und -manager und der Risikocoaches sowie Schulung und Unterstützung zur Benützung der gemeinsamen Risiko-Informatikanwendung R2C_GRC (Risk-to-Chance-Governance, Risk & Compliance).

I Die Koordinationsstelle EFV erstellt zuhanden der GSK einen Entwurf des Risikoreportings an den Bundesrat. Die GSK konsolidiert und priorisiert die Risiken aus den Departementen und der BK, analysiert Wechselwirkungen und verabschiedet die Risikoberichterstattung zuhanden des Bundesrats.

J Die Koordinationsstelle EFV finalisiert die Risikoberichterstattung und bringt sie via EFD dem Bundesrat zur Kenntnis.

K Informationsrückfluss aus der Bundesratssitzung an die Leitung des Departments / der BK; allenfalls Auftrag zur Umsetzung von Risiko-Massnahmen auf Stufe Bundesrat.

L Jährliche Besprechung des Bundesrat-Risikoreportings mit einem Ausschuss der GPK.

Definition der Rahmenbedingungen
Vorgaben EFV:

- Innerhalb des Risikomanagementprozesses müssen die Prozesse und Termine der VE mit dem übergeordneten Departements- und dem bundesweiten Prozess abgestimmt werden.
- In der Bundesverwaltung wird einmal jährlich auf Stufe Bundesrat, Departement / BK und VE ein Risikoreporting erstellt.
- Ein zusätzliches Risiko-Update beschränkt sich auf Bundesratsrisiken und Risiken mit Krisenpotenzial.
- Bei einer ausserordentlichen Risikosituation wird der Bundesrat umgehend informiert.

3.2 Identifikation

Der Risikomanagement-Prozess im engeren Sinn beginnt mit der Risikoidentifikation. Dabei geht es darum, die relevanten Risiken einer OE möglichst vollständig zu erkennen, sie zweckmässig abzugrenzen und nachvollziehbar darzustellen. Der Arbeitsschritt ist nicht trivial: Hier entscheidet sich, was auf den Risiko-Schirm der Führungsverantwortlichen gelangt (und was nicht); gleichzeitig wird damit die Basis gelegt für die Qualität und Aussagekraft der anschliessenden Phasen im Risikomanagement-Prozess, namentlich die Analyse und Bewertung sowie die Entwicklung von Massnahmen. Die Risikoidentifikation verlangt daher nicht nur eine gute Kenntnis der Aufgaben, Ziele, Prozesse und Projekte der OE, sondern auch eine gute Balance von methodischer Strenge und pragmatischem Sinn. Die nachfolgenden Ausführungen verstehen sich nicht als Checkliste, die mechanistisch abgearbeitet werden soll, sondern als Wegweiser für ein breiteres Verständnis der Risikoidentifikation.

3.2.1 Ausgangspunkte und Abgrenzung

Gegenstand

Die Risikoidentifikation besteht darin, frühzeitig mögliche Ereignisse und Entwicklungen zu erkennen, welche die Erfüllung der Aufgaben und die Erreichung der Ziele des Bundes beeinträchtigen können. Neben Ereignissen, die kurzfristig eintreten können, sind auch langfristige Entwicklungen zu beachten. Um eine verlässliche, nicht dem Zufall überlassene Risikoidentifikation sicherzustellen, braucht es einen *systematischen*, periodisch durchgeführten Prozess. Dieser ergänzt die stete Aufmerksamkeit der Mitarbeiterinnen und Mitarbeiter des Bundes gegenüber neuen Entwicklungen, die negative Auswirkungen auf die Bundesverwaltung haben können.

Als Ausgangspunkte für die systematische Risikoidentifikation dienen:

- die sich aus den Gesetzen und deren Ausführungsbestimmungen (Verordnungen) ergebenden Ziele und Aufgaben;
- die in den Organisationsverordnungen der Departemente und der BK aufgelisteten Ziele und Funktionen; und
- die Jahresziele des Bundesrates, der Departemente / der BK und der VE.

Nebst den Aufgaben und Zielen des Bundes können ergänzend auch *Prozessdiagramme* herangezogen werden, falls eine VE zwecks Eruierung von Schwachstellen und Einwirkungsorten von Risiken innerhalb eines spezifischen Prozesses solche verwendet. Ebenfalls Gegenstand des Risikomanagementprozesses sind laufende Projekte.

Bezugsrahmen: Risiko für den Bund

Bei der Suche und Identifikation von Risiken, welche die Aufgabenerfüllung oder die Zielerreichung des Bundes negativ beeinflussen können, muss jeweils im Detail analysiert werden, ob und inwiefern *für den Bund* ein Risiko vorliegt. Nachfolgend zwei Beispiele, die die Problematik der Abgrenzung eines Bundesrisikos veranschaulichen sollen.

Pandemie

- Für die volkswirtschaftlichen Schäden, die sich bei einer Pandemie ergeben (Produktivitätsverluste, zusätzliche Gesundheitskosten), ist der Bund grundsätzlich nicht verantwortlich.
- Dem Bundesamt für Gesundheit (BAG) obliegen im Zusammenhang mit der Früherkennung von neuen Bedrohungen für die Gesundheit eine ganze Reihe von Aufgaben[21]. Ein Risiko für das BAG (und somit für den Bund) kann demzufolge darin liegen, dass es dem BAG beispielsweise nicht gelingt, eine Pandemie frühzeitig zu erkennen und die Bevölkerung mit den notwendigen Informationen zu versorgen.
- Von einer Pandemie können Mitarbeiterinnen und Mitarbeiter der gesamten Bundesverwaltung betroffen sein. Fallen diese krankheitshalber in grösserer Zahl aus, ist die Aufgabenerfüllung in mehreren VE möglicherweise in Frage gestellt, was für den Bund ein weiteres Risiko darstellt.

Konkurs einer Grossbank

- Der Konkurs einer Grossbank in der Schweiz und dessen direkte Auswirkungen (z. B. Verluste für Gläubiger und Investoren) sind grundsätzlich kein Risiko des Bundes.

  Die Förderung der Stabilität des schweizerischen Finanzsektors ist eine der Aufgaben des Staatssekretariats für internationale Finanzfragen. Ist ein Institut «systemrelevant» (too big to fail), sodass dessen Ausfall das schweizerische Finanzsystem gefährden oder lahmlegen könnte, so betrifft das Risiko auch den Bund; er müsste gegebenenfalls Rettungsmassnahmen in die Wege leiten.

Knappe Ressourcen begründen (fast) nie ein Risiko

Die finanziellen und personellen Mittel, die einer VE für ihre Aufgaben und Ziele zur Verfügung gestellt werden, sind knapp bemessen und müssen sparsam und effizient eingesetzt werden.[22] Sie werden von den übergeordneten Organen (Direktion VE, Departement/BK, Bundesrat) im Rahmen des Budgetierungs- und Finanzplanungsprozesses festgelegt; die Budgethoheit obliegt der Bundesversammlung.[23] Dabei sind die Kompetenzen und Entscheidungsprozesse gestützt auf die einschlägigen Bundesgesetze detailliert geregelt. Technisch

[21] Art. 9 Organisationsverordnung für das EDI (SR *172.212.1*)

[22] Art. 12 Abs. 4 sowie Art. 57 Abs. 1 FHG

[23] Art. 167 Bundesverfassung (SR *101*), Art. 25 Parlamentsgesetz (SR *171.10*)

gesprochen ist die Ressourcenzuteilung also *systemendogen*[24]: Sie geht aus Politik- und Managemententscheiden hervor, die von den zuständigen Organen des Bundes im Rahmen der Aufgaben- und Haushaltsteuerung getroffen werden. Daraus folgt, dass (Ressourcen-)Beschlüsse der Bundesversammlung, des Bundesrates oder der Departementsleitung *grundsätzlich nie ein Risiko begründen*.[25] Dies gilt auch dann, wenn die Aufgaben und Ziele angesichts enger Budgetvorgaben nur dank besonderer Anstrengungen (z. B. strukturelle Reformen) erfüllt werden können oder grundsätzlich neu festgelegt werden müssen (Gesetzesrevision), wie es etwa im Zuge von Sparprogrammen oft der Fall ist.

Der Entscheid über die Bereitstellung von Ressourcen beeinflusst sowohl das Aufgaben- und Zielverständnis als auch die Form der Aufgabenerfüllung bzw. Zielerreichung. Je mehr Ressourcen für eine Aufgabe zur Verfügung stehen, umso umfassender ist die Aufgabe zu erfüllen. Wenn hingegen weniger Ressourcen bereit stehen, ist allenfalls eine Leistungsreduktion oder ein Aufgabenverzicht angezeigt. Das Risikomanagement darf dabei nicht als Vehikel eingesetzt werden, (1) um zusätzliche Ressourcen zu erwirken, oder (2) zur Absicherung, falls Aufgaben und Ziele mit den zugesprochenen Ressourcen aus Sicht der VE nicht mehr in gewünschter Qualität und Menge erbracht werden können. Das Risikomanagement würde so zweckentfremdet und geschwächt. Für die Erörterung von Ressourcenentscheiden bestehen eigene Gefässe und Prozesse.

In Einzelfällen können ungenügende finanzielle oder personelle Ressourcen allerdings dann ein Risiko begründen, wenn äussere Ereignisse oder Entwicklungen die bereitgestellten Ressourcen und die gesetzlich detailliert festgelegten Aufgaben aus dem Gleichgewicht bringen, sodass die Erfüllung der gesetzlichen Vorgaben in Frage gestellt ist:

- ***Beispiel 1 (Migration):*** Ein wichtiger Parameter für das Budget im Asylbereich ist die erwartete Anzahl an Asylgesuchen. Ein unerwarteter massiver Anstieg der Ankünfte von Flüchtlingen führt zu logistischen Herausforderungen, die mit den verfügbaren Ressourcen kaum mehr bewältigt werden können. Aufgabe des Bundes ist es, in Zusammenarbeit mit weiteren Akteuren alle Vorkehrungen zu treffen, damit möglichst alle Asylsuchenden registriert, sicherheitsüberprüft, den grenzsanitarischen Massnahmen unterzogen, untergebracht und betreut werden können.
- ***Beispiel 2 (Altersvorsorge):*** Strukturelle Veränderungen auf der Leistungsseite (steigende Lebenserwartung, demographischer Altersaufbau) oder auf der Finanzierungsseite (anhaltende Tiefzinsphase) können zu einer Auszehrung der Sozialwerke führen, was die Einhaltung der gesetzlichen Leistungsversprechen und letztlich das Vertrauen in das Vorsorgesystem insgesamt gefährden kann.
- ***Beispiel 3 (Rekrutierung spezialisierter Fachkräfte):*** Das Budget einer VE sieht zwar genügend finanzielle Mittel und Stellen zur Deckung des Personalbedarfs vor. Indes können Schlüsselfunktionen nicht mehr mit geeigneten Fachkräfte besetzt werden, da der Arbeitsmarkt in diesem Berufssegment ausgetrocknet ist. Die Stellen bleiben über längere Zeit vakant, was dazu führen kann, dass Aufgabe und Ziele nicht mehr gesetzeskonform erfüllt werden.

Die Identifikation eines Risikos kann in solchen Fällen sinnvoll sein, wenn zweckmässige Massnahmen in Aussicht genommen werden können. So versprechen beispielsweise die Einrichtung von Frühwarnindikatoren (bevor sich eine Entwicklung zuspitzt) oder die Planung eines Krisendispositivs zur rascheren Bewältigung (nach Eintritt eines Risikos) eine Verbesserung der Aufgabensteuerung.

[24] Von Organen des Systems Bund festgelegt; im Gegensatz zu: exogen = von aussen erzeugt.

[25] Vgl. Richtlinie der EFV über das Risikomanagement Bund, Stand 01.08.2024, Ziff. 2.2.1, S. 4.

3.2.2 Vorgehen und Strukturierung

Sammeln der Risiken

Es existieren diverse Methoden für die Identifikation von Risiken, von spontaner Ideensuche (unzureichend) über Experten- und Mitarbeitendenbefragungen bis zu ausgefeilten System- und Prozessanalysen (aufwendig). Beim Bund hat sich in der Praxis ein *strukturiertes Brainstorming* gut bewährt, bei dem – anlehnend an die Ziele, Aufgaben und Prozesse – nach konkreten Risiken in der OE gesucht wird[26]. Dabei kann das Brainstorming sowohl mit Einzel- als auch mit Gruppeninterviews durchgeführt werden.

Wahl der richtigen Flughöhe: Risiken richtig positionieren und eingrenzen

Sind die Risikofelder oder einzelne Risiken (z. B. mittels Brainstorming) identifiziert, geht es darum, sie zweckmässig einzugrenzen, d. h. sie «greifbar» zu machen (man spricht von «operationalisieren»). Zweckmässig eingrenzen heisst hier, dass das Risiko insbesondere folgende Merkmale aufweist: Es ist

- bedeutend (ohne sich im Generellen zu verlieren);
- spezifisch (ohne im Detail hängen zu bleiben); sowie
- logisch konsistent (ohne wichtige Bedingungen oder Aspekte auszublenden).

Ein zweckmässig operationalisiertes Risiko ist eine zentrale Voraussetzung für die Qualität der weiteren Phasen im Risikomanagement-Prozess (vgl. Kap. 3.3 – 3.5.3). Es bildet ein solides Fundament für eine aussagekräftige Risikobeschreibung (Szenario), für eine plausible Bewertung und für die Entwicklung folgerichtiger Massnahmen zur Risikobewältigung. Diese drei Elemente sind logisch verknüpft; sie müssen gut aufeinander abgestimmt sein, damit sie auch von Personen nachvollzogen werden können, die mit dem Fachgebiet nicht im Detail vertraut sind (Departementsleitung, Bundesrat, parlamentarische Aufsichtsorgane).

Entscheidend ist die ***Wahl der richtigen Flughöhe***, d. h. der Bildausschnitt bzw. der Abstraktionsgrad des identifizierten Risikos. Ist ***die Flughöhe zu gross***, d. h. der betrachtete Ausschnitt zu weit gefasst, verliert sich das Risiko im Allgemeinen. Sein Informationsgehalt beschränkt sich auf Gemeinplätze, weil zu viele Ereignisse und Entwicklungen im Risiko Platz finden. In der Folge tauchen häufig die folgenden Probleme auf:

1. Die Risikobeschreibung bleibt in generellen Aussagen stecken, oder sie stellt verschiedene, kausal unabhängige Ereignisse und Entwicklungen nebeneinander. Für das «Credible worst case»-Szenario wird willkürlich ein einzelnes Ereignis ausgewählt. Dem Risiko fehlt die thematische Geschlossenheit, bisweilen wird es zum «Risiko-Knäuel».
2. Die Risikobewertung (Eintrittswahrscheinlichkeit / Auswirkungen) erfolgt gefühlsmässig und ist kaum objektiv begründbar, da die Risikobeschreibung als Bezugspunkt mehrspurig ist. Weil das Risiko sehr umfassend ist, wird es tendenziell überbewertet, was den Vergleich mit anderen Risiken im Bundesportfolio verzerrt.
3. Die Ableitung von Massnahmen erfolgt oft unsystematisch, das Massnahmen-Set wird übermässig umfangreich und damit unübersichtlich. Ob die Massnahmen richtig gewählt und priorisiert wurden, ist kaum erkennbar. Der Nutzen für die Aufgabensteuerung tendiert gegen Null.

In der Bundesverfassung, im Zweckartikel der Gesetze und den Organisationsverordnungen der Departemente und der BK werden die Aufgaben und Ziele des Bundes sehr allgemein und umfassend beschrieben. Die Konkretisierung ist andernorts geregelt. Bei der Risikoidentifikation können solche Regelungen normalerweise nicht eins zu eins übernommen werden. Es empfiehlt sich, die Themen in einzelne, sachlich zusammenhängende Komponenten aufzugliedern und daraus zwei oder mehrere Einzelrisiken zu bilden.

[26] Gefahrenlisten mit Rückmeldungen, Beobachtungen oder Prognosen aus dem Qualitätsmanagementsystem, der Arbeitssicherheit, IT-Sicherheitsmanagement usw. sollen – sofern vorhanden – beigezogen werden.

Beispiel: Nach Artikel 1 seiner Organisationsverordnung[27] wahrt das EDA «die aussenpolitischen Interessen der Schweiz im Rahmen des verfassungsmässigen Auftrages.» Würde sich die Risikoidentifikation allein auf diese Bestimmung stützen, fände darin ein ganzes Legislaturprogramm mit all seinen Herausforderungen und Unsicherheiten Platz. In einem einzelnen Risiko abgebildet, ergäbe sich daraus ein Risikogebilde, das alles umfasst und nichts mehr aussagt: Die Führungsverantwortlichen erhielten eine Verdoppelung von Programmzielen und -massnahmen, aber keinen Mehrwert.

Umgekehrt ist auch zu vermeiden, ein Risiko auf ***zu tiefer Flughöhe***, d. h. auf Detailstufe zu erfassen, und sich auf einen zu kleinen Bildausschnitt zu konzentrieren. Problematisch ist dabei, dass so eine Vielzahl von Kleinstrisiken auf der Riskmap erscheinen. Das Risikoportfolio wird unübersichtlich, befasst sich zu stark mit Einzelheiten und kann nicht mehr effizient bewirtschaftet werden. Fehlerquelle ist hier in der Regel der alleinige Bezug auf Teilprozesse einer Aufgabe oder auf einzelne Phasen eines Projekts aus einer Bottomup-Analyse[28]. Soweit sich solche Detailrisiken unter einem übergreifenden gemeinsamen Aspekt bewirtschaften lassen, sollen sie aus einer Topdown-Perspektive in ein «Credible worst case»-Szenario zusammengeführt werden (vgl. Kap. 3.3.2 ff.).

Die Wahl der richtigen Flughöhe ist nicht einfach. Ein gutes Augenmass ist gefragt. Bisweilen zeigt sich erst im Lauf der Risikoanalyse und der Bewertung, dass ein Risiko unvorteilhaft eingegrenzt wurde. Ein iteratives Vorgehen zwischen den einzelnen Phasen des Risikomanagement-Prozesses trägt in solchen Fällen dazu bei, das Risiko besser zu verstehen und schliesslich zweckmässig zu erfassen.

Zu beachten ist auch, dass namentlich in grossen Organisationen wie der Bundesverwaltung *Wechselwirkungen* zwischen Risiken bestehen können (vgl. Kapitel 4.5). So können Risiken beispielsweise verkettet sein und sich gegenseitig verstärken, oder ein identifiziertes Risiko kann sich auf mehrere OE zugleich auswirken. Solche Wechselwirkungen sind mit Blick auf eine optimale Bewirtschaftung aus einer Gesamtsicht zu beurteilen. Unter bestimmten Bedingungen ist es vorteilhaft, einzelne Risiken zu einem *Querschnittsrisiko* zu *aggregieren* (vgl. Kap. 4.3). Eine wichtige Voraussetzung für die Risikoaggregation sind auf richtiger Flughöhe identifizierte und eingegrenzte Risiken.

Typisierung der Risiken (Risikokategorien)

Die Risiken in der Bundesverwaltung sind sehr vielfältig. Um eine Unterteilung der Risiken zu ermöglichen und die Identifikation systematisch durchzuführen, werden in der Bundesverwaltung die Risiken *aufgrund ihrer Ursache* in folgende sechs Kategorien unterteilt[29]:

- ***finanzielle und wirtschaftliche Risiken****:* Risiken im Zusammenhang mit dem Finanzmanagement, mit (wirtschaftlichen) Abhängigkeiten des Bundes von Dritten, mit subsidiären Leistungen des Bundes (Darlehen, Bürgschaften, Garantien usw.);
- ***rechtliche Risiken / Compliance****:* Risiken im Zusammenhang mit Schäden anlässlich des Vollzugs von Bundesaufgaben, mit der Einhaltung von rechtlichen Bestimmungen oder Verträgen, mit Aufsichtspflichtverletzungen, mit der Ausfallhaftung nach Art. 19 VG[30];
- ***Sach-, technische und Elementarrisiken****:* Risiko der Zerstörung oder Beschädigung (inklusive Betriebsunterbruch) von bundeseigenen Gebäuden, Einrichtungen, technischen Anlagen, Daten, Kulturgütern;
- ***personenbezogene und organisatorische Risiken****:* Risiken aus den Bereichen Organisation, Führung, Mitarbeitende, Personenschutz, Rekrutierung von Fachkräften, Ausfall von Schlüsselpersonen, Veruntreuung;

---

[27] Organisationsverordnung für das Eidgenössische Departement für auswärtige Angelegenheiten (SR *172.211.1*)

[28] Beispielsweise im Rahmen von Funktionsanalysen wie die FMEA (Kap. 3.3.2).

[29] Weitere Möglichkeiten, mehrere Risiken zu strukturieren oder zu gruppieren, werden im Anhang 3 erläutert.

[30] In Anhang 7 werden einige Risiken des Bundes im Zusammenhang mit Organisationen ausserhalb der Bundesverwaltung aus rechtlicher Perspektive genauer erläutert.

- ***technologische und naturwissenschaftliche Risiken**:* Risiken, die sich aus der Entwicklung und Forschung von technologischen/naturwissenschaftlichen Neuanwendungen (inklusive Spätfolgen) ergeben, wie beispielsweise der Nano- oder der Gentechnologie;
- ***gesellschaftliche und politische Risiken**:* gesellschaftliche Veränderungen (z. B. Demografie), Interessenkonflikte mit dem Ausland usw. In dieser Kategorie finden sich komplexe Risiken, wie z. B.: Ausstieg Atomenergie, Nanotechnologie, Bilaterale Verträge mit der EU.

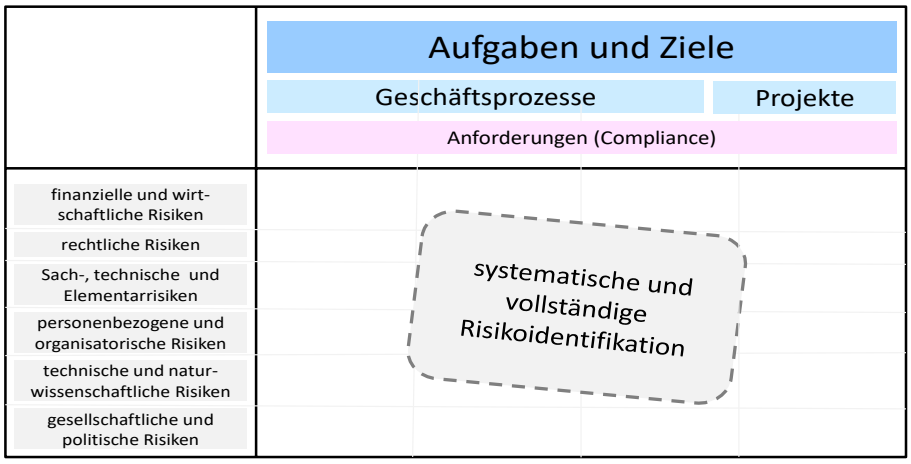


Abbildung 9: Risikoidentifikation

Trotz einer seriösen Risikoidentifikation werden immer sogenannte *Restrisiken* verbleiben, die nicht erkannt und somit nicht bewirtschaftet werden können.[31]

Prozessschritt Risikoidentifikation
Vorgaben EFV:

- Die Identifikation der Risiken ist *ausgehend von den Zielen und Aufgaben der Organisationseinheit* durchzuführen (vgl. Gesetze, Verordnungen, Organisationsverordnung des Departements / der BK, Jahresziele, Geschäftsordnung der VE).
- „Ungenügende" finanzielle oder personelle Ressourcen begründen in der Regel kein Risiko, da sie auf Entscheide von Bundesrat und Parlament zurückgehen und damit systemendogen sind.
- Risiken sollen so eingegrenzt und formuliert werden, dass sie bedeutend, spezifisch und logisch konsistent sind (Wahl der richtigen Flughöhe).
- Die Risiken werden in die sechs (vorgenannten) thematischen Risikokategorien unterteilt. Die Zuordnung zu den Kategorien erfolgt aufgrund der Ursache des Risikos.

Empfehlung EFV:

- Durchführung von Workshops oder Interviews mit Mitgliedern der Leitung sowie Mitarbeitenden, welche für spezielle Bereiche zuständig sind (Wissensträgerinnen und -träger).

[31] Das Nichterkennen von Risiken kann u. a. aufgrund von Betriebsblindheit passieren, aufgrund der Selbstüberschätzung einer Organisation bzw. ihrer verantwortlichen Kader, aufgrund der Unterschätzung einer Entwicklung oder eines Ereignisses oder auch dadurch, dass ganz neue und für die Menschen unerwartete Phänomene auftauchen (sogenannte schwarze Schwäne).

Output Risikoidentifikation: Eine möglichst umfassende Liste von Risiken, welche die Erfüllung der Aufgaben und die Erreichung der Ziele des Bundes negativ beeinflussen können.

Hilfsmittel: Risikoerfassungsbogen (vgl. S. 69 ff.), Prozessbeschriebe.

3.3 Analyse und Bewertung

3.3.1 Allgemeines zum Erfassen von Risiken

Die Risiken des Bundes werden mit Hilfe der Informatikanwendung Risk-to-Chance (R2C_GRC) elektronisch erfasst und dokumentiert. Gestützt darauf wird das Risikoreporting mit seinen beiden Standardformaten – Detailbericht und Kompaktbericht – erstellt (vgl. Ziff. 4.1). Die periodischen Aktualisierungen der Einzelrisiken werden nach jedem Bundesratsgeschäft zur Risikoberichterstattung (Beschluss oder Infonotiz) historisiert, d.h. i.d.R. Mitte März und Mitte September.

Prozessschritt Risikoanalyse und -bewertung
Vorgabe EFV: Jedes Risiko wird mindestens mit folgenden Angaben erfasst

- sprechender Risikotitel: kurz, prägnant, für Dritte verständlich (vgl. Ziff. 3.2)
- Risikoeigner/-in
- Verwaltungseinheit / Departement
- Aufgaben / Ziele der VE, die vom Risiko betroffen sind
- Risikokategorie (vgl. Ziff. 3.2)
- Risikoanalyse, die das Risiko erklärt (vgl. Ziff. 3.3.2)
- allfällige Wechselwirkungen mit anderen Risiken (vgl. Ziff. 3.3.7)
- Risikoursachen
- Worst Case (vgl. Ziff. 3.3.2)
- Bewertung des Risikos (Auswirkungen/Eintrittswahrscheinlichkeit,vgl. Ziff.3.3.4 ff.)
- Erläuterungen und Begründung zur Bewertung des Risikos
- beschlossene oder eingeleitete Massnahmen zur Risikominimierung einschliesslich der Beurteilung und Kommentierung ihres Umsetzungsstands sowie der erwarteten Wirksamkeit (vgl. Ziff. 3.5). Die Wirkung bereits umgesetzter bzw. laufend durchgeführter Massnahmen soll bei Bedarf stichwortartig in der Risikoanalyse berücksichtigt werden.

3.3.2 Methoden zur Analyse und Bewertung von Risiken

Bei der Risikoanalyse geht es vorab darum, das identifizierte Risiko (auch für Aussenstehende) verständlich zu beschreiben, Ursachen und Auswirkungen zu ermitteln und Zusammenhänge zu verstehen (inkl. Wechselwirkungen mit anderen Risiken, vgl. Ziff. 3.3.7 und 4.5). Schliesslich werden die Eintrittswahrscheinlichkeit und die Auswirkungen des Risikos qualitativ oder quantitativ bewertet. Für die Analyse der Risiken soll das beste verfügbare Know-how verwendet werden, bei Bedarf und verhältnismässigem Aufwand soll auch bundesverwaltungsexternes Know-how mit einbezogen werden.

Da Risiken sehr unterschiedlich sein können, hat die Praxis für ihre Analyse und Bewertung

mehrere Methoden entwickelt. Einige sollen hier kurz erläutert werden.[32]

- ***Szenarioanalysen**:* Bei den Szenarioanalysen werden Ursachen von identifizierten Risiken ermittelt und die Auswirkungen von einzelnen Szenarien eingeschätzt und dargestellt. Ziel ist es, die Ursache-Wirkungsketten vor und nach dem Eintritt eines Risikos zu verstehen. In den meisten Fällen wird dabei ein sog. «credible worst case»-Szenario zur Darstellung des Risikos verwendet (vgl. Ziff. 3.3.3). Spezifische Formen der Szenarioanalysen sind das «Ursache-Wirkungsdiagramm» (verwendet zur Analyse von eingetretenen Schadenereignissen), und die «Fehlerbaum- und Ablaufanalyse» (verwendet bei komplexen technischen Systemen).
- ***Indikatorenanalysen**:* Bei der Indikatorenanalyse wird versucht, Indikatoren bzw. Vorkommnisse, die beinahe zu einem Schaden geführt hätten, zu erkennen. Sie können auf das mögliche Eintreten eines worst-case-Risikoszenarios hinweisen. Durch die Analyse dieser Vorkommnisse bzw. Indikatoren können Massnahmen zur Risikominimierung gefunden und umgesetzt werden. Eine spezifische Form einer Indikatorenanalyse ist das «Change Based Risk Management», bei dem *Veränderungen* identifiziert, systematisch bewertet und deren Einfluss auf die Organisation analysiert werden.
- ***Funktionsanalysen**:* Bei einer Funktionsanalyse wird das untersuchte Objekt (meist ein technisches System oder ein Prozess) in Teilsysteme/-prozesse zerlegt und deren Funktionen/Aufgaben ermittelt. Danach wird nach möglichen Fehlfunktionen (und deren Ursachen) gesucht, die die Funktionsfähigkeit der Teilsysteme und des Gesamtsystems beeinträchtigen können. Eine häufig verwendete Funktionsanalyse ist die «Failure Mode and Effects Analysis» (FMEA).
- ***Statistische Analysen**:* Bei den statistischen Analysen wird das Risiko als statistisches Mass der Unsicherheit betrachtet. Diese Analysen bedingen eine gute und genügend grosse Datengrundlage. Gebräuchliche Risikokennzahlen sind die Standardabweichung und der Value-at-Risk. Mit einer Monte Carlo-Simulation lassen sich Risiken in einem wiederholten Zufallsprozess simulieren und eine Schadensverteilung eines Risikos oder einer aggregierten Gruppe von Risiken ermitteln.

Während die Szenarioanalyse eine allgemein anwendbare Methode ist, die sich zudem gut für eine Topdown-Analyse eignet, sind einige der anderen hiervor erwähnten Methoden nur sehr spezifisch anwendbar.

Prozessschritt Risikoanalyse und -bewertung
Vorgabe EFV:

- In der Bundesverwaltung werden die Risiken mit Hilfe der Szenarioanalyse dargestellt. Andere Analysemethoden sind fakultativ.

Empfehlung EFV:

- Für die Analyse der Risiken soll das beste verfügbare Know-how verwendet werden, bei Bedarf und verhältnismässigem Aufwand soll auch bundesverwaltungsexternes Know-how mit einbezogen werden.

3.3.3 Schadensverteilung eines Risikos

Die meisten Risiken können sich in unterschiedlichem Ausmass realisieren: Ein Hochwasser kann sich als lokales Ereignis mit moderatem Sachschaden manifestieren, das häufig vorkommen kann, oder als sehr seltenes «Jahrhunderthochwasser» mit gravierenden Auswir-

[32] Vgl. dazu z. B. ÖNORM 4902-2

kungen. Es gibt generell drei Möglichkeiten den unterschiedlichen Ausprägungen eines Risikos Rechnung zu tragen:

- ***Schadensverteilung**:* Bei Vorliegen statistischer Daten oder bei einem genügenden Verständnis des Risikos kann dieses mit einer genauen Schadensverteilung beschrieben werden.
- ***Szenarien**:* Szenarien sind eine gute Annäherung. Häufig werden drei Szenarien dargestellt, die zusammen die ganze Bandbreite des Risikos abbilden.
- ***«Credible worst case»**:* Das Risiko wird in der schlimmst möglichen aber noch realistischen Ausprägung dargestellt. Es wird derjenige Fall abgebildet, welcher der Organisation die grössten Schwierigkeiten bereiten kann.

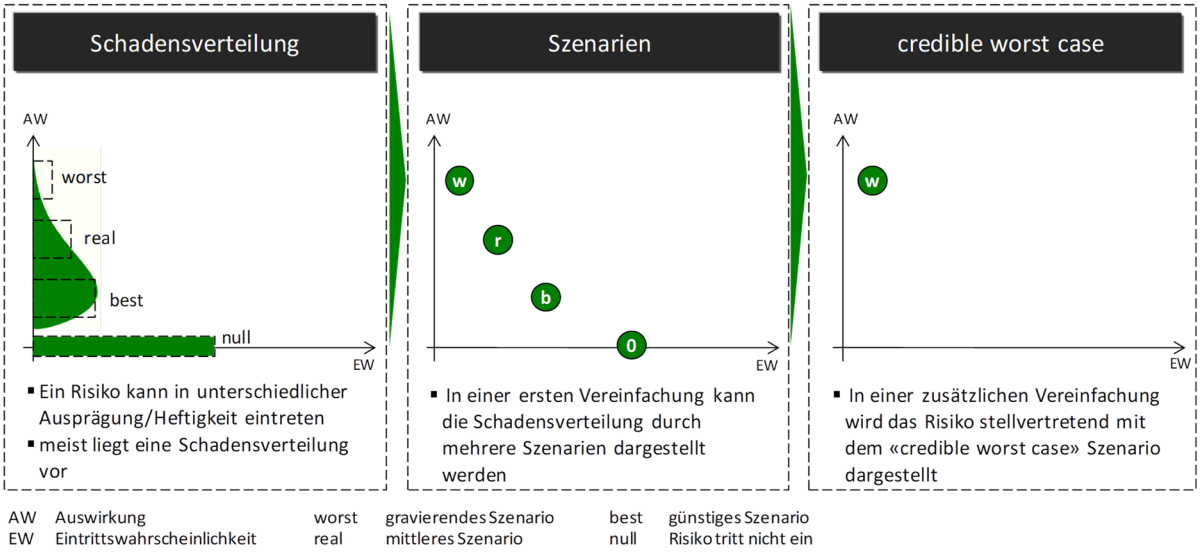


Abbildung 10: Schadensverteilung eines Risikos

Prozessschritt Risikoanalyse und -bewertung
Vorgabe EFV:

- In der Bundesverwaltung wird das Risiko als «credible worst case» dargestellt. Bei Bedarf und für ein besseres Verständnis des Risikos können zusätzlich auch mehrere Szenarien oder eine Schadensverteilung dargestellt werden.

3.3.4 Bewertung der Auswirkungen

Die Auswirkungen eines Risikos können vielfältig und verschiedenartig sein. Aus Sicht Risikomanagement Bund sind oft gleichzeitig verschiedene Auswirkungsdimensionen von Bedeutung. Im Einvernehmen mit den Risikomanagerinnen und Risikomanagern der Departemente und der BK wurde festgelegt, dass die Auswirkungen der Risiken mit den folgenden fünf Dimensionen beschrieben werden sollen:

- finanzielle Auswirkungen
- Personenschäden
- Beeinträchtigung der Reputation
- Beeinträchtigung der Geschäftsprozesse
- Auswirkungen auf die Umwelt

In allen fünf Dimensionen muss das Risiko bezüglich der Höhe der Auswirkungen auf einer

sechsstufigen Skala von «sehr gering» bis «sehr hoch» bewertet werden (vgl. Bewertungsmatrix Risikomanagement Bund), wenn die Auswirkungsdimension für das Risiko relevant ist. Jede Dimension hat im Vergleich zu den anderen Dimensionen das gleiche Gewicht. Wenn mehrere Dimensionen von Bedeutung sind, wird das Risiko in einer ***Gesamtbewertung*** entsprechend der höchsten Auswirkung eingestuft (Maximalprinzip). Im folgenden Beispiel (Gesamteinstufung hoch) wird das Prinzip der Gesamtbewertung verdeutlicht.

Auswirkungen	sehr gering	gering	moderat	wesentlich	hoch	sehr hoch
Finanzielle Auswirkungen				X		
Personenschäden					X	
Beeinträchtigung Reputation				X		
Beeinträchtigung Geschäftsprozesse			X			
Auswirkungen auf Umwelt						

Abbildung 11: Gesamtbewertung der Auswirkung

Bereits umgesetzte Massnahmen zur Verminderung eines Risikos werden bei der Bewertung der Auswirkungen berücksichtigt (Grundsatz der ***Nettobewertung***).

In der Bewertungsmatrix wird nur die Bewertungsskala auf Stufe Bund und Departement / BK festgelegt. In den Mandanten für das operative Risikomanagement können den konkreten Bedürfnissen (Höhe des Budgets, spezielle Charakteristiken der Risiken, usw.) angepasste Skalen verwendet werden.[33] Die EFV befürwortet solche Individualisierungen der Bewertungsskala, da auf diese Weise in den VE das Risikomanagement als Führungs- und Arbeitsinstrument gestärkt wird.

Prozessschritt Risikoanalyse und -bewertung
Vorgaben EFV:

- Zu jedem Risiko müssen alle relevanten Auswirkungsdimensionen bewertet werden. Die Bewertungen sind zu dokumentieren und wo angezeigt kurz zu erläutern. Das Risiko wird gesamthaft entsprechend der höchsten Auswirkung eingestuft.
- Bereits wirksame Risikominimierungsmassnahmen sind bei der Bewertung zu berücksichtigen.

Empfehlung EFV:
Die EFV empfiehlt die Einführung von bedürfnisgerecht angepassten Bewertungsskalen der Auswirkungen pro VE.

3.3.5 Qualitative oder quantitative Bewertung

Bei der qualitativen Bewertung wird das Risiko jeweils einer Klasse für die Eintrittswahrscheinlichkeit und einer Klasse für die Auswirkung zugeordnet. Die Einstufung erfolgt qualitativ aufgrund der Beschreibung der verschiedenen Auswirkungsdimensionen.

[33] Die technische Umsetzung in R2C_GRC erfolgt durch die EFV.

Bei der quantitativen Bewertung wird das Risiko mit einem Zahlenwert für die Eintrittswahrscheinlichkeit in Prozent und einem Frankenbetrag für die Auswirkung bewertet. Die Einschätzung des Risikos erfolgt zahlenmässig mittels Eingabe konkreter Werte. Eine quantitative Bewertung ist in der Regel nur dann zweckmässig, wenn die Datenlage sehr gut ist (z. B. vorhandene statistische Angaben über Schadenfälle) und ausschliesslich mit finanziellen Auswirkungen gerechnet werden muss.

Prozessschritt Risikoanalyse und -bewertung
Empfehlung EFV:

- Die EFV empfiehlt, die *qualitative* Bewertung der zu einem Risiko relevanten Auswirkungsdimensionen.

3.3.6 Bewertung der Eintrittswahrscheinlichkeit

Ein Risiko ist per Definition ein unsicheres Ereignis. Dessen Eintrittswahrscheinlichkeit liegt zwischen 0 und 100 Prozent. Dieser Prozentwert kann auf zwei verschiedene Arten interpretiert werden:

a. Eine Eintrittswahrscheinlichkeit von 10 % kann zum Beispiel bedeuten, dass in einem Jahr das Risiko mit 10 %-iger Eintrittswahrscheinlichkeit eintritt bzw. dass sich das Risiko im Durchschnitt in 10 Jahren einmal realisiert. Wir sprechen von einer Periodenwahrscheinlichkeit bzw. einer *Jahreswahrscheinlichkeit*. In dieser Interpretation kann das Risiko über einen längeren Zeithorizont mehr als einmal auftreten. Beispiele sind die meisten operativen Risiken, die häufig durch Ereignisse ausgelöst werden.

b. Eine Eintrittswahrscheinlichkeit von 10 % kann auch als *Fallwahrscheinlichkeit* interpretiert werden. Ein Beispiel einer Fallwahrscheinlichkeit ist ein Risiko, das entweder eintreten kann oder ausbleibt, aber nicht mehrmals auftreten kann. Dies können zum Beispiel strategisch-politische Risiken sein, die durch eine negative Entwicklung ausgelöst werden. Aufgrund eines dynamischen Umfelds haben solche Risiken häufig einen einmaligen Charakter. Weiter ist auch die Eintrittswahrscheinlichkeit, dass ein spezifisches Projekt scheitert, als Fallwahrscheinlichkeit zu interpretieren.

Diesen unterschiedlichen Interpretationen muss beim Vergleichen von Risiken Rechnung getragen werden, indem beispielsweise in der Beschreibung des Risikos erklärt wird, ob es mehrmals eintreten kann und gegebenenfalls in welchem Zeitraum. Damit die Riskmap bezüglich der Eintrittswahrscheinlichkeit aussagekräftig ist, müsste man streng genommen Risiken mit Periodenwahrscheinlichkeit und solche mit Fallwahrscheinlichkeit trennen. Auf Stufe Bundesrat wird aus Gründen der Praktikabilität auf diese Unterteilung verzichtet. Die Eintrittswahrscheinlichkeit ist als Fallwahrscheinlichkeit *und* als Jahreswahrscheinlichkeit zu verstehen und muss je nach Risiko unterschiedlich interpretiert werden.

Die finanziellen Folgen von bekanntermassen *mehrmals jährlich auftretenden Ereignissen* (sog. Frequenzschäden, z. B. Motorfahrzeugschäden einer Versicherung) sind mit einem Jahresdurchschnittswert zu budgetieren. Das Risiko besteht dann in einer allfälligen Überschreitung des budgetierten Wertes im betreffenden Jahr.

Die in der Bundesverwaltung verwendete Eintrittswahrscheinlichkeitsskala ist in der Bewertungsmatrix Risikomanagement Bund abgebildet (vgl. Kap. 3.3.4 ff. und 3.4). Auf VE-spezifische Eintrittswahrscheinlichkeitsskalen wird aus Gründen der Übersichtlichkeit und Vergleichbarkeit verzichtet.

3.3.7 Wechselwirkungen zwischen Risiken

Jedes Risiko muss daraufhin analysiert werden, ob sich bei dessen Eintritt nebst den primären Folgen weitere Auswirkungen auf andere Risiken entfalten. Der Eintritt eines Risikos

kann z. B. dazu führen, dass der Eintritt eines weiteren Risikos wesentlich wahrscheinlicher wird (positive Korrelation). Auch das Gegenteil gibt es: Die Eintrittswahrscheinlichkeit eines anderen Risikos kann den Eintritt eines anderen unwahrscheinlicher machen (negative Korrelation). Generell ist zu prüfen, ob ein Zusammenhang mit anderen identifizierten Risiken, allenfalls Risiken in einer anderen VE oder einem anderen Departement, besteht. Wechselwirkungen zwischen Risiken müssen erkannt, möglichst gut verstanden und in der Risikobeschreibung erläutert werden. Eine erste Prüfung auf Wechselwirkungen wird bei der Analyse des Einzelrisikos durchgeführt. Wegen der auf den Stufen Departement / BK und Bundesrat vorhandenen grösseren Übersicht über alle identifizierten Risiken erfolgt eine weitere umfassende Prüfung der Wechselwirkungen zwischen den grösseren Risiken in der Bundesverwaltung durch die Risikomanager, die Koordinationsstelle EFV und die GSK (vgl. Ziff. 4.5).

Prozessschritt Risikoanalyse und -bewertung
Vorgabe EFV:

- Bei jedem Risiko ist auf den Stufen VE, Departement / BK und Bundesrat zu prüfen, ob Wechselwirkungen mit anderen Risiken bestehen.

Output Risikoanalyse und -bewertung: Eine verständliche Beschreibung jedes Risikos und eine Bewertung der Eintrittswahrscheinlichkeit und der Auswirkungen des Risikos.

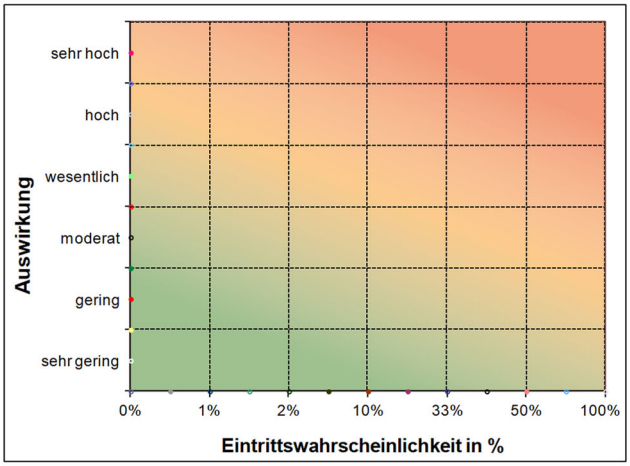
Hilfsmittel: Bewertungsmatrix Risikomanagement Bund.

3.4 Beurteilung

Nachdem die Risiken bewertet worden sind, werden im nächsten Prozessschritt die Bedeutung und die Tragbarkeit der Risiken beurteilt. Einerseits geht es darum herauszufinden, ab welcher Höhe sich das Management mit einem Risiko befassen und Massnahmen ins Auge fassen soll. Andererseits geht es um die Frage, ob die Risiken bei Eintritt mit den eigenen Mitteln getragen werden können.

Risikotoleranz

Mit der Definition der sechs Stufen der Auswirkungen (von «sehr gering» bis «sehr hoch») in der Bewertungsmatrix Bund wird eine grobe Einstufung der Risiken nach ihrer Bedeutung vorgenommen. Die konkrete Bedeutung im Einzelfall hängt u. a. vom Risikokontext und der Grösse der untersuchten Organisationseinheit ab und sollte auf Stufe VE individuell festgelegt werden. Weiter müssen die Leitungen auf den Stufen VE, Departement / BK und Bundesrat definieren, wo ihre Risikotoleranzschwelle liegt. Dabei ist immer unterstellt, dass **alle gesetzlichen und regulatorischen Vorgaben eingehalten** sind. In der nachfolgenden Darstellung wird eine *mögliche* Unterteilung der Risiken in drei Risikotoleranzstufen skizziert.



	Beurteilung
hohes Risiko	Das Risiko stellt eine erhebliche Gefahr dar und muss in der Direktion behandelt werden. Diese setzt sich mit möglichen Massnahmen auseinander und entscheidet bzgl. deren Umsetzung. Das Risiko wird regelmässig verfolgt, solange es sich auf dieser Stufe befindet.
mittleres Risiko	Das Risiko stellt eine ernstzunehmende Gefahr dar. Es muss in der Direktion bekannt sein und von ihr verstanden werden. Die Entwicklung wird verfolgt und wo sinnvoll Massnahmen umgesetzt.
tiefes Risiko	Das Risiko kann akzeptiert werden, es wird innerhalb der Abteilung bewirtschaftet und wo sinnvoll Massnahmen umgesetzt.

Abbildung 12: Beispiel Risikotoleranzstufen

Die Risikotoleranz wird ausserhalb des Risikomanagementprozesses entwickelt. Im Prozess werden lediglich die bewerteten Risiken an diesen Risikotoleranzen gemessen und beurteilt. Selbstverständlich helfen die Toleranzstufen nur, eine *grobe* Idee zu entwickeln, wie mit einem Risiko umgegangen werden soll. Schliesslich muss für jede Bewältigungsmassnahme vor ihrer Umsetzung einzeln beurteilt werden, ob die Kosten der Umsetzung in einem sinnvollen Verhältnis zur Risikoverminderung stehen.

In der Bundesverwaltung wird zur Beurteilung eines Risikos primär die Höhe des Risikos (Auswirkung und Eintrittswahrscheinlichkeit) unter Einbezug der Grösse der VE und deren Aufgaben herangezogen. In Spezialfällen kann das Risiko zusätzlich noch unter Beizug weiterer Dimensionen beurteilt werden:

- Bei Risiken in Finanzmärkten ist eine Rendite-Risiko-Abwägung der Standard, d. h. das getragene Risiko muss in einem sinnvollen Verhältnis zur erwirtschafteten Rendite stehen.
- Im Sicherheitsbereich findet häufig eine Güterabwägung zwischen (Personen-)Risiko und Nutzen statt. Beispielsweise muss bei einem Medikament das Restrisiko (Nebenwirkungen) mit dem Nutzen für die Patienten ins Verhältnis gesetzt werden, um zu einer vernünftigen Beurteilung des Risikos zu gelangen.

Finanzielle Risikotragfähigkeit

Die Bundesverwaltung orientiert sich in ihrer Tätigkeit an ihren Aufgaben und Zielen. Das Gesamtrisiko der Bundesverwaltung ist wesentlich durch die von ihr zu erfüllenden Aufgaben geprägt. Um Risiken zu vermeiden, kann demnach nicht auf bestimmte Aufgabenerfüllungen verzichtet werden. Deshalb ist das Gesamtrisiko der Bundesverwaltung hauptsächlich in der Bewirtschaftung der einzelnen Risiken steuerbar. Auf eine Gesamtaggregation aller Risiken in der Bundesverwaltung und der Gegenüberstellung mit dem vorhandenen Kapital wird aus diesem Grund verzichtet.[34]

Die Sicherstellung der Liquidität und Zahlungsfähigkeit der Bundesverwaltung erfolgt durch die Bundestresorerie in der EFV. Diese kann mit den Tresorerieanlagen monatliche Schwankungen von Einnahmen und Ausgaben von bis zu mehreren Milliarden Franken ausgleichen. Damit kann sie den Eintritt auch von sehr hohen finanziellen Risiken des Risikomanagements (> 10 Mia. CHF) selbst im Fall eines rapiden Geldabflusses decken. Für schweizerische Grossereignisse mit massivem finanziellen Schaden für den Bund (z. B. Kernschmelze

[34] In der Privatwirtschaft orientiert sich die Tragbarkeit von Risiken häufig am vorhandenen (Eigen-) Kapital, d. h. die aggregierten Risiken müssen durch genügend Eigenkapital und liquide Mittel gedeckt und getragen werden können. Ein Gesamtrisiko, das diese Schwelle übersteigt, ist für das Unternehmen existenzgefährdend und somit nicht tragbar. Das Gesamtrisiko kann in diesem Fall gesenkt werden, indem auf bestimmte Tätigkeiten und Geschäfte verzichtet wird oder diese im Umfang wesentlich reduziert werden, oder mittels Aufnahme von zusätzlichem Kapital zur Deckung dieser Risiken.

in einem AKW, Erdbeben) muss die Liquidität und Aufnahme von Kapital durch den Bund gesondert analysiert werden.

3.5 Bewältigung

3.5.1 Bewältigungsoptionen

Die Risikobewältigung umfasst im Wesentlichen die folgenden unterschiedlichen Handlungsoptionen:

- ***Risiko vermeiden**:* In vielen Fällen kann die Bundesverwaltung ein Risiko nicht komplett vermeiden, denn dies wäre nur durch den Verzicht auf ein Geschäft/Aufgabe möglich, was in den allermeisten Fällen nur über eine entsprechende Gesetzesänderung durchzuführen wäre.
- ***Risiko vermindern**:* Bei vielen Risiken können mit diversen Massnahmen die Eintrittswahrscheinlichkeit und/oder die möglichen Auswirkungen bei Eintritt des Risikos reduziert werden. Einerseits können Massnahmen präventiv ergriffen werden, andererseits kann die Vorbereitung und der Einsatz eines Krisen- oder eines Kontinuitätsmanagements (vgl. Ziff. 6.2 und 6.3) als Massnahme angesehen werden um ein eingetretenes Risiko möglichst rasch und mit wenig Kosten zu bewältigen.
- ***Risiko überwälzen**:* Einige Risiken können versichert und so auf Dritte übertragen werden. Dies kann unter gewissen Umständen (insbesondere wirtschaftliche Gründe) Sinn machen (vgl. Ziff. 6.7). Derivative Instrumente, Verträge und Garantien bilden weitere Möglichkeiten der Risikoüberwälzung.
- ***Risiko akzeptieren:*** bedeutet die bewusste Inkaufnahme oder das aktive Eingehen von Risiken im Rahmen von gesetzlichen bzw. regulatorischen Vorgaben.

In der Bundesverwaltung wird auch nach Umsetzung von mitigierenden Massnahmen häufig ein *Nettorisiko* bleiben, das diese selber trägt. Einerseits kann aus wirtschaftlichen Gründen entschieden werden, das Risiko bewusst selber zu tragen. Andererseits existieren Risiken, die vom Bund getragen werden müssen, weil ein gesetzlicher Auftrag besteht und keine Minimierung des Risikos möglich ist.

3.5.2 Definition, Auswahl und Umsetzung von Massnahmen

Von den Ursachen eines Risikos ausgehend muss der Risikoeigner mit Hilfe des Risikocoaches und von Fachexperten nach möglichen Massnahmen suchen, die das Risiko reduzieren können. Ein genaues Verständnis der Ursachen und der Ursache-Wirkungsketten hilft, geeignete Massnahmen zu finden. Massnahmen müssen klar beschrieben sein, wenn notwendig muss eine Unterteilung in Einzelschritte vorgenommen werden.[35] Zudem muss eine massnahmenverantwortliche Person definiert und ein Endtermin für die Umsetzung festgelegt werden, wenn notwendig mit Zwischenmeilensteinen.

Nach der Identifikation und der Beschreibung von möglichen Massnahmen geht es darum, diese zu beurteilen. Dabei sind die *Kosten* zur Umsetzung der Massnahme mit dem Nutzen, konkret der *Verminderung oder Überwälzung des Risikos*, ins Verhältnis zu setzen. Bei rein finanziellen Auswirkungen kann als grober Ansatz die Reduktion des Risiko-Erwartungswertes[36] mit den Kosten der Massnahme verglichen werden. Bei Risiken mit nicht-finanziellen Auswirkungen erfolgt zwangsläufig eine subjektive Einschätzung des Kosten/Nutzen-Verhältnisses. Diese Einschätzung sollte vom Risikoeigner vorgenommen werden, im Idealfall unterstützt durch Fachpersonen mit dem notwendigen Know-how und unter Berücksichtigung

[35] Als Hilfreich erweist sich dabei die SMART-Methode, mit deren Hilfe sich Massnahmen auf ihre klare und konkrete Formulierung hin überprüfen lassen. Die Massnahmen müssen spezifisch, messbar, attraktiv, realistisch und terminiert sein.

[36] Der Erwartungswert eines Risikos ist das Produkt aus finanzieller Auswirkung und Eintrittswahrscheinlichkeit.

der Risikotoleranz.

Danach werden die als sinnvoll beurteilten Massnahmen priorisiert und über die Umsetzung entschieden. Diese Entscheidung trifft der Risikoeigner bzw., je nach Höhe der Kosten, eine übergeordnete Instanz. Die Umsetzung der Massnahme erfolgt durch den Massnahmenverantwortlichen.

Prozessschritt Risikobewältigung
Vorgaben EFV:

- Die Kosten von im Risikomanagement beschlossenen Massnahmen fliessen in das Budget (Voranschlag) des Bundes ein.
- Jede Massnahme muss einer groben Kosten-Nutzen-Analyse unterzogen werden. Darüber hinaus ist jeder Massnahme eine verantwortliche Person zuzuweisen sowie ein Endtermin für deren Umsetzung festzulegen.

Output Risikobewältigung: Massnahmenliste auf Stufe VE, Departement / BK und Bundesrat.

3.5.3 Dynamische und statische Risiken

Ein «dynamisches Risiko» ist im Kontext des RM Bund ein Risiko, zu welchem wir Massnahmen umsetzen, um dessen Auswirkungen oder Eintrittswahrscheinlichkeit in Zukunft zu verringern. Dem Risiko sind Massnahmen mit den Status «beschlossen» und / oder «eingeleitet» zugewiesen.

Ein «statisches Risiko» ist ein Risiko, zu welchem wir keine Massnahmen umsetzen, um dessen Auswirkungen oder Eintrittswahrscheinlichkeit in Zukunft weiter zu verringern. Dem Risiko sind ausschliesslich Massnahmen mit den Status «möglich», «laufend durchgeführt», «umgesetzt» oder «abgelehnt» zugewiesen. Es handelt sich damit um ein akzeptiertes Restrisiko.

Die Zuordnung eines Risikos zu einer Klasse kann sich im Laufe der Zeit ändern. Entscheidend ist dabei die Frage, ob Massnahmen existieren, die aktiv zur Risikominderung beitragen.

3.6 Überwachung

Die Überwachung der Risiken und der eingeleiteten Massnahmen ist ein wichtiger Prozessschritt im Risikomanagement, der die Effektivität des Risikomanagements sicherstellt.

3.6.1 Risiko-Überwachung

Durch die kontinuierliche Überwachung der Risiken stellen wir sicher, dass das Wissen bezüglich der vorhandenen Risiken in der Bundesverwaltung stets auf dem aktuellsten Stand ist. Ziel ist es, einerseits Veränderungen im Umfeld zu erkennen, die eine Neueinschätzung bereits erfasster Risiken erfordern. Andererseits sollen neu entstehende Risiken frühzeitig erkannt werden. In der Bundesverwaltung erfolgt die Überwachung der Risiken in erster Linie durch die Risikoeignerinnen und Risikoeigner, die sich im Rahmen ihres Pflichtenheftes mit den Risiken in ihrem Aufgabenbereich befassen.

Bereits erfasste Risiken

Bereits erfasste Risiken müssen laufend überwacht werden, damit auf Veränderungen mit geeigneten Massnahmen reagiert werden kann. Wenn sich bei einem Risiko über längere

Zeit keine Änderungen abzeichnen, ist zu prüfen, ob es abgeschlossen und aus dem Risikoportfolio entfernt werden kann. Dies kann beispielsweise dann der Fall sein, wenn ein Risiko auf ein Niveau reduziert werden konnte, das als Restrisiko akzeptiert wird. Solche Risiken werden typischerweise über mehrere Perioden hinweg nicht mehr mit neuen Massnahmen bewirtschaftet (Grenzkosten für Massnahmen sind höher als der Grenznutzen einer Risikoreduktion). In folgenden Fällen ist es jedoch sinnvoll, auch ein eher statisches Risiko auszuweisen:

- Die Risikoexposition ist labil, es besteht Unsicherheit über die Entwicklung innerer und äusserer Einflüsse (z. B. Ursachen, Interdependenzen, Vulnerabilität);
- Das Restrisiko ist hoch. Es muss sichergestellt werden, dass v. a. die Schadenminimierungsmassnahmen laufend überwacht (und wenn möglich) optimiert werden (z. B. bei Stauanlagen, Erdbebenrisiken; Aufrechterhaltung der «Awareness»).

Neue Risiken

Im Bereich der Früherkennung von Risiken ist die Bundesverwaltung auf wachsame Führungskräfte und Mitarbeiter angewiesen. Diese müssen interne und externe Veränderungen verfolgen und deren mögliche Auswirkungen auf die Risikolage des Bundes erkennen. Dazu sind sie mit entsprechenden externen Know-how-Trägern vernetzt.

3.6.2 Massnahmen-Überwachung

Die Umsetzung von Massnahmen zur Risikoreduktion muss überwacht werden. Dies ist Aufgabe des Risikoeigners, der die Verantwortung für das Risiko trägt. Der Massnahmenverantwortliche setzt die beschlossene Massnahme um und rapportiert dem Risikoeigner über den Fortschritt und allfällige Probleme bei der Massnahmenumsetzung. Beschlossene Massnahmen fliessen zudem in die Planungs- und Reporting-Instrumente der Bundesverwaltung ein.

Prozessschritt Risiko- und Massnahmenüberwachung
Vorgabe EFV:

- Die Überwachung der Risiken und der Massnahmen erfolgt durch den Risikoeigner.
- Statische Risiken werden im Reportingprozess auf Stufe GSK/Bundesrat nicht mehr zur Diskussion gestellt, müssen aber im Rahmen der Risiko- und Massnahmenüberwachung weiterhin überwacht und aktuell gehalten werden.

4 Reporting

Das Reporting der analysierten Risiken ist ein wichtiger Output des Risikomanagement-Prozesses. Im Risikoreporting werden die Ergebnisse aus dem Risikomanagement dargestellt. Diese sollen die Entscheidfindung der Führung im Umgang mit den Risiken unterstützen.

4.1 Inhalt des Risikoreportings

Das Risikoreporting muss mindestens die folgenden Elemente enthalten:

- Eine *Riskmap*, welche die Risikolandschaft der OE darstellt und die Risiken einander gegenüberstellt;
- Die *Entwicklung* der Risiken gegenüber dem letzten Risikoreporting;
- Eine *Massnahmenliste*, die den Fortschritt bei der Umsetzung beschlossener Massnahmen darlegt und als Entscheidungsgrundlage für neue Massnahmen dient.;
- wichtige *Wechselwirkungen* zwischen erfassten Risiken (vgl. Ziff. 4.5).

Risikoreporting
Vorgabe EFV:

- Das Risikoreporting wird mithilfe der IT-Anwendung R2C_GRC erstellt. Die Standardformate sind der Detail- sowie der Kompaktbericht. Während der Detailbericht zuhanden der Führung von VE und Departementen/BK sowie der «Arbeitsgruppe Risikomanagement Bund» beider GPK umfassend über das einzelne Risiko informiert, fasst der Kompaktbericht zuhanden des Bundesrats die Kerninformationen zu jedem Risiko zusammen (vgl. kommentierte Mustervorlagen für beide Berichte in Anhang 2).

4.2 Reporting-Grundsätze

Ein verständliches, übersichtliches und aktuelles Risikoreporting hilft den Entscheidungsträgern, die relevanten Informationen schnell zu erkennen und optimale Entscheidungen bezüglich den Risiken zu treffen. Einige Grundsätze dazu:

- Eine geeignete Anzahl Risiken auswählen (Konzentration auf Risiken, die von den Adressaten beeinflusst werden können; vgl. Ziff. 4.4);
- Kurze, prägnante und für Dritte verständliche Beschreibung der Risiken (nicht zu wenig und nicht zu viel Informationen, Fachjargon vermeiden).

4.3 Aggregation von Querschnittsrisiken

In grossen Organisationen wie der Bundesverwaltung kommt es regelmässig vor, dass in verschiedenen Departementen oder VE die *gleichen oder ähnliche* Risiken identifiziert werden oder dass ein identifiziertes Risiko mehrere OE betrifft. Beispielsweise tangiert der Ausfall eines zentralen EDV-Systems oft mehrere VE. Bei solchen sogenannten Querschnittsrisiken kann es Sinn machen, sie (allenfalls nur zum Teil) zentral zu bewirtschaften und im Reporting auf übergeordneter Stufe (Departement bzw. Bundesrat) zu aggregieren. Bei der Aggregation eines Risikos wird dieses auf der übergeordneten Stufe analysiert, Wechselwirkungen werden aufgezeigt. Die Einschätzung der Eintrittswahrscheinlichkeit und der Auswirkungen des «credible-worst-case»-Szenarios erfolgt unter Berücksichtigung der Einschätzungen und Annahmen untergeordneter Stufen.

Die nachfolgenden Grundsätze der Risikoaggregation sollen ein gemeinsames Verständnis und ein möglichst einheitliches Vorgehen bei der Risikoaggregation in der Bundesverwaltung

sicherstellen.[37]

4.3.1 Aggregationsentscheid

Eine Aggregation von Risiken soll nur erfolgen, wenn sich daraus ein Mehrwert ergibt, beispielsweise:

- Die Gesamtbedeutung eines Risikos bzw. ein Handlungsbedarf wird erst bei der Aggregation der Teilrisiken auf übergeordneter Stufe erkennbar.

  Beispiel: Die gesamten negativen Auswirkungen eines IT-Serverausfalls sind erst erkennbar, wenn die Auswirkungen der ausfallenden Anwendungen in den einzelnen VE *summiert* betrachtet werden.

- Das Risiko kann mit zentral gesteuerten Massnahmen effizienter oder kostengünstiger bewirtschaftet werden (Nutzung von Skaleneffekten).

  Beispiel: Es ist weniger teuer, eine Sensibilisierungskampagne zum sicheren Umgang mit Passwörtern bundesweit durchzuführen, als in jeder VE einzeln.

- Die für die Reduktion eines Risikos zur Verfügung stehenden Mittel können durch die Priorisierung der Minimierungsmassnahmen im Rahmen einer Aggregation effizienter zugeteilt werden.

  Beispiel: Die für die Verbesserung der Erdbebensicherheit budgetierten Mittel werden dann am wirkungsvollsten eingesetzt, wenn gestützt auf die Prüfung der Erdbebensicherheit *aller* Bundesgebäude (aggregierte Sichtweise) eine Priorisierung vorgenommen wird.

- Die Aggregation auf übergeordneter Stufe fördert die Identifikation und das Verständnis von Wechselwirkungen und Schnittstellen.

  Beispiel: Die Wechselwirkungen zwischen der Unternehmenssteuerreform III/Steuervorlage 2017 (ESTV), deren Auswirkungen auf den Bundeshaushalt (EFV) und den Beziehungen mit der EU (SIF) können auf Stufe Departement (EFD) analysiert und bewirtschaftet werden.

Es muss hier davor gewarnt werden, dass eine Aggregation unter Umständen zu einer Trivialisierung der Risiken führen kann. Eine Aggregation sollte nicht durchgeführt werden, nur um auf übergeordneter Hierarchiestufe eine bessere, thematisch gruppierte Übersicht zu erreichen. Es besteht dabei nämlich die Gefahr, dass bei der Aggregation relevante Risikoinformationen verloren gehen und dass das zusammengefasste Risiko so allgemein formuliert werden muss, dass die Gefährdung und der Handlungsbedarf nicht mehr ersichtlich sind.

- *Negativbeispiele:* Zusammenfassung eines Flugzeugabsturzes, einer Zugsentgleisung und eines Tunnelbrandes als «Grossunfälle»; Know-How-Verluste, Korruption, fehlende Arbeitsmotivation und Veruntreuung als «Personalrisiken»; Zeitverzögerungen in mehreren, voneinander unabhängigen Projekten als «Zeitverzögerung Projekte».

4.3.2 Zuständigkeit für die Aggregation

Die Verantwortung bzw. Federführung *für die Aggregation* eines Querschnittsrisikos muss im Rahmen des Risikomanagementprozesses geklärt werden. Davon unabhängig ist die Verantwortung *für die Bewirtschaftung* des Querschnittsrisikos (vgl. Ziff. 4.3.3).

Auf der Stufe Bundesrat wird die Federführung für die Aggregation eines Querschnittsrisikos von der GSK[38] festgelegt[39]. Grundsätzlich gibt es zwei Zuordnungsmöglichkeiten:

[37] Vgl. auch Anhang 10, wo für einige potenzielle Risikofelder die Zusammenhänge und die bundesweiten Strukturen aufgezeigt werden.
[38] Ziff. 5 Abs. 1 Bst. b der Weisungen über die Risikopolitik des Bundes
[39] Auf der Stufe Departement bzw. VE ist in der Regel die Geschäftsleitung zuständig.

- Eine VE, eine interdepartementale Arbeitsgruppe (oder allenfalls eine Projektleitung) hat bereits einen konkreten ***Auftrag zur zentralen Steuerung und Bewirtschaftung*** eines Querschnittsrisikos für die gesamte Bundesverwaltung (Gesetz, Organisationsverordnung, Beauftragung z. B. durch den Bundesrat etc.). Sie übernimmt die Federführung für eine aggregierte Risikobetrachtung und beschafft die benötigten Informationen aus den betroffenen VE. Die Koordinationsstelle Risikomanagement Bund bzw. die Risikomanager unterstützen sie in methodischer Hinsicht.
- Wenn die Aggregation eines Querschnittsrisikos angezeigt ist (vgl. Ziff. 4.3.1), zurzeit aber ***keine zentrale Steuerung*** existiert, erfolgt die Risikoaggregation durch die betroffenen Risikomanager bzw. durch die Koordinationsstelle Risikomanagement Bund. Diese ziehen die notwendigen Fachexperten und die für die Risikobewirtschaftung zuständigen OE bei. Gestützt darauf entscheiden die GSK bzw. die zuständige Geschäftsleitung über die Zuteilung der Federführung.

4.3.3 Klärung der Verantwortlichkeiten bei der Bewirtschaftung

Die Bezeichnung des Risikoeigners eines Querschnittsrisikos folgt grundsätzlich den gleichen Kriterien wie bei einem Einzelrisiko (Grundregel: AKV – Übereinstimmung von Aufgabe, Kompetenz und Verantwortung, d.h. die verantwortliche Person kann das Risiko beeinflussen und verändern).

Bei der Bewirtschaftung von Querschnittsrisiken, insbesondere bei der Umsetzung von Risikominimierungsmassnahmen, sind meistens mehrere VE zu beteiligen (z. B. Abwehrmassnahmen gegen Cyberattacken). Aus den Aufgaben der betroffenen VE lässt sich in der Regel ableiten, bei welcher OE die Verantwortung für einen Teilaspekt der Risikobewirtschaftung am sinnvollsten anzusiedeln ist (Identifikation, Bewertung, Massnahmen (Evaluation, Entscheid, Umsetzung), Überwachung). Die Schnittstellen in der Zusammenarbeit müssen geklärt und die Verantwortlichkeiten festgelegt werden. Nur so lassen sich Doppelspurigkeiten oder Lücken in der Bewirtschaftung von Querschnittsrisiken vermeiden.

Die Steuerung von Querschnittsrisiken ist komplex[40]. Das hängt u. a. damit zusammen, dass der Risikoeigner des Querschnittsrisikos gegenüber den Eignern der Quellrisiken und den Massnahmenverantwortlichen in vielen Fällen nicht weisungsberechtigt ist (dezentrales Verwaltungsprinzip). Auf Stufe Bundesrat wird diesem Umstand dadurch Rechnung getragen, dass halbjährlich (im Rahmen der Reportingprozesse) zu jedem Querschnittsrisiko eine Koordinationssitzung mit dem Eigner des Querschnittsrisikos und den Eignern der Quellrisiken durchgeführt wird. In diesem Rahmen werden der Risikobeschrieb, das Worst Case-Szenario, die Bewertung des Querschnittsrisikos und der Quellrisiken sowie die umzusetzenden Massnahmen im Einvernehmen festgelegt. Grosse Bedeutung kommt dem zentralen Massnahmencontrolling durch den Eigner des Querschnittsrisikos zu. Allfällige wesentliche Differenzen sind durch die Koordinationsstelle Risikomanagement Bund in einer ersten Stufe an die GSK und nötigenfalls an den Bundesrat zu eskalieren.

Die Aggregation von Querschnittsrisiken ist überwiegend ein Topdown-Prozess, weshalb die Quellrisiken i. d. R. im Rahmen der erwähnten Koordinationssitzung bzw. vom Eigner des Querschnittsrisikos festgelegt werden. In letzter Instanz entscheidet die GSK (bzw. die Geschäftsleitung Departement/VE).

4.3.4 Reporting

Querschnittsrisiken sollen grundsätzlich sowohl auf der Stufe VE (falls für die VE relevant) als auch (aggregiert) auf übergeordneter Stufe in die Risikoberichterstattung einfliessen.[41]

[40] Vgl. dazu auch Ziff. 6 des EFK-Berichts 17476 «Prüfung des Risikomanagements Bund als Führungsinstrument» vom 03.05.2018

[41] Bei einer Aggregation von Risiken auf übergeordneter Stufe erscheinen die aggregierten Quellrisiken nicht auf der Riskmap, wenn im R2C_GRC die Aggregation mit der Funktion «aggregiertes Risiko» durchgeführt wird.

4.3.5 Informationsaustausch

Für die erfolgreiche Steuerung eines Querschnittsrisikos ist ein steter Informationsaustausch zwischen dem Eigner des Querschnittsrisikos und den Eignern der Quellrisiken unerlässlich. Letzteren muss insbesondere die Stossrichtung der Risikominimierungsmassnahmen bekannt sein.

Generell ist ein Informationsaustausch zwischen Risikomanagern, Risikocoaches und Risikoeignern, die sich mit Querschnittsrisiken befassen, unerlässlich.[42] Erfahrungen können ausgetauscht und neue Ideen im Umgang mit Querschnittsrisiken entwickelt werden.

Grundsätze Risikoaggregation
Vorgaben EFV:

- Bei Querschnittsrisiken ist jeweils zu prüfen, ob und auf welcher Stufe (VE, Departement, Bund) eine Aggregation sinnvoll oder gar notwendig ist.
- Die Zuständigkeit bzw. Federführung für die Risikoaggregation ist festzulegen.
- Die Aufgaben und Verantwortlichkeiten der Akteure (Identifikation, Analyse, Bewertung, Massnahmen, Überwachung) sind zu klären bzw. festzulegen. Fehlende Informationen für eine aggregierte Risikobetrachtung sind zu beschaffen.
- Für die Risikoberichterstattung ist das aggregierte Risiko übersichtlich, verständlich und möglichst umfassend darzustellen.
- Der Informationsaustausch zwischen allen Akteuren ist aktiv zu fördern.

4.4 Auswahl von Risiken

Bei Vorhandensein vieler Risiken ist es im Rahmen des Reportings sinnvoll, sich auf wenige und für die Entscheidungsträger relevante Risiken zu konzentrieren. Die Konzentration auf diese Risiken erleichtert die Lesbarkeit einer Riskmap und ermöglicht es den Führungskräften, sich auf die Bewirtschaftung der für sie wichtigsten Risiken zu konzentrieren. Informationsdichte: Je höher die Hierarchiestufe, desto verdichteter muss die Information dargestellt werden.

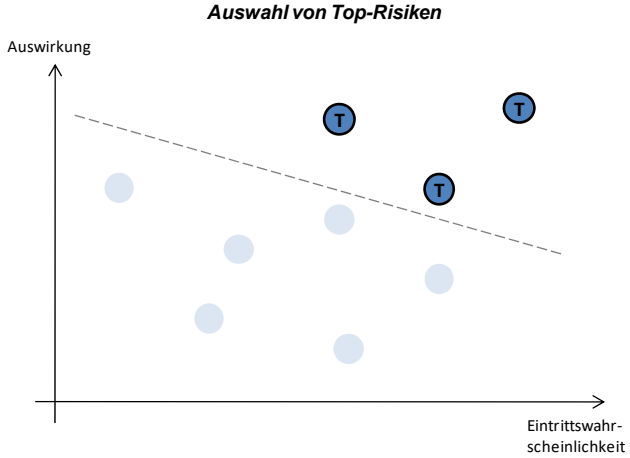


Abbildung 13: Auswahl von Top-Risiken

In der Bundesverwaltung wird mit den folgenden Regeln ein stufengerechtes Reporting sichergestellt:

[42] Die Koordinationsstelle Risikomanagement Bund unterstützt den Informations- und Erfahrungsaustausch zwischen den VE und Departementen mit Veranstaltungen, Informationsnotizen etc.

Auf Stufe der VE werden im Risikomanagementprozess die vorhandenen Risiken erfasst, analysiert und bewertet. Gleichzeitig erfolgt der gleiche Prozess auch im Generalsekretariat der Departemente, das sich mit Risiken auf Stufe Departement (Top-Down-Sicht) auseinandersetzt. Eine Auswahl dieser Risiken wird an die Leitung der VE rapportiert. In der Richtlinie werden keine Vorgaben gemacht, wie innerhalb einer VE die Risiken für die Leitung konsolidiert werden. Die Koordinationsstelle EFV empfiehlt aber, dass in Absprache mit dem Leiter der VE eine Reportingschwelle VE und/oder eine grobe Anzahl Toprisiken festgelegt werden.

Jede VE meldet danach ihre drei grössten Risiken an den Risikomanager des Departements. Falls mehr als drei Risiken die Reportingschwelle des Departements überschreiten, werden auch diese weitergemeldet. Die Reportingschwelle auf Stufe Departement wird durch die Leitung des Departements definiert und muss mit den Vorgaben auf Stufe Bundesrat abgestimmt sein. Risiken, die nicht an das Departement gemeldet werden, gelten als sogenannte *Bereichsrisiken*. Die aus den VE an das Departement gemeldeten Risiken sind *Departementsrisiken*.

Für das Bundesratsreporting meldet jedes Departement und die BK der Koordinationsstelle EFV seine/ihre grössten drei Risiken. Die Leitung des Departements / der BK definiert die drei Toprisiken ihrer OE. Zusätzlich müssen weitere Risiken gemeldet werden, wenn diese eine hohe bzw. sehr hohe Auswirkung haben (ungeachtet derer Eintrittswahrscheinlichkeit). Die von jedem Departement und der BK gemeldeten Risiken werden *Kernrisiken* genannt. Diese Risiken werden durch die Koordinationsstelle EFV geprüft: Es findet eine erste Plausibilisierung, ein Quervergleich und eine erste Harmonisierung der Risiken statt. In einem Gespräch mit dem Generalsekretär je Departement können Rückfragen gestellt werden und die Risiken allenfalls angepasst werden. Die überarbeiteten Risiken werden danach der GSK vorgelegt. Diese prüft die Risiken auf ihre Vollständigkeit und aggregiert allfällige Querschnittsrisiken. Danach werden die wichtigsten Risiken für das Reporting zuhanden des Bundesrates ausgewählt. Als Richtgrösse gelten 10–15 Risiken, die dem Bundesrat unterbreitet werden sollen. Diese gelten als sogenannte *Bundesratsrisiken.*

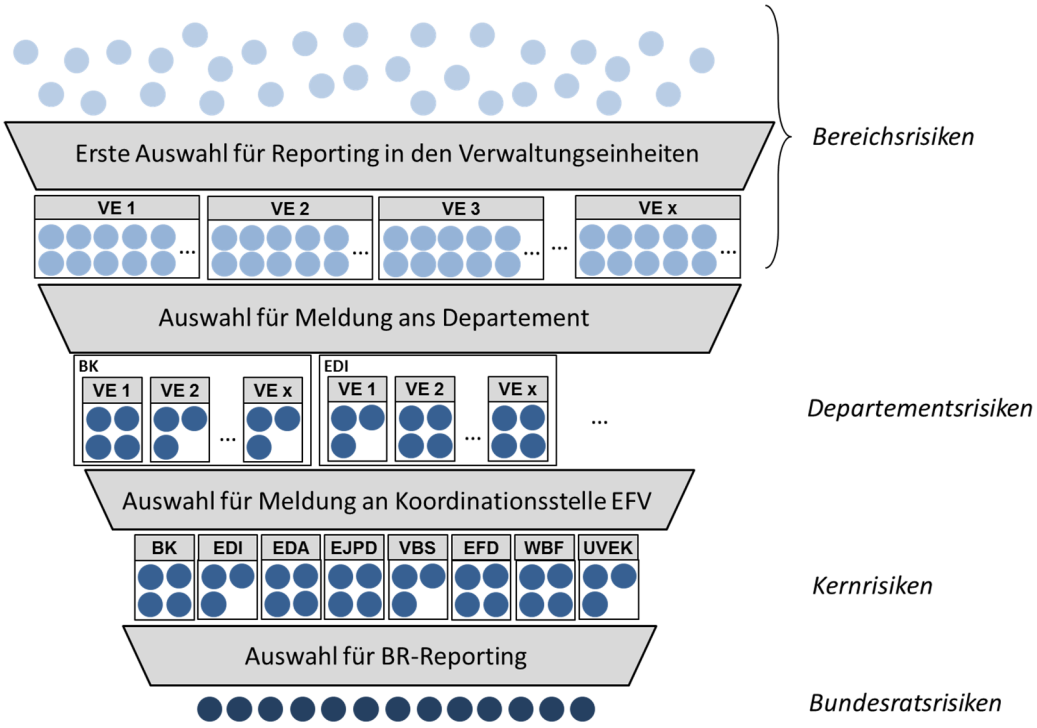


Abbildung 14: Auswahl von Risiken in der Bundesverwaltung

4.5 Wechselwirkungen

4.5.1 Organisatorischer Umgang mit Wechselwirkungen

Auf *Stufe Bundesrat* übernimmt die Generalsekretärenkonferenz die Aufgabe, die aus den Departementen und der BK gemeldeten Risiken auf Wechselwirkungen hin zu prüfen. Die Koordinationsstelle EFV initiiert und begleitet die dazu notwendigen interdepartementalen Abstimmungen.

Auf *Stufe Departement* koordiniert der Risikomanager die notwendigen Abstimmungen zur Analyse und Bewirtschaftung von verwaltungseinheitsübergreifenden Wechselwirkungen innerhalb des Departements.

Wenn in einer VE ein Risiko Wechselwirkungen mit einem Risiko einer VE aus einem *anderen* Departement / der BK aufweist, initiiert und begleitet die Koordinationsstelle EFV die Abstimmung zwischen diesen zwei VE.

4.5.2 Abbildung von Wechselwirkungen

Für eine quantifizierte Aggregation aller Risiken ist die genaue Definition des Wirkungsmechanismus erforderlich. Aber auch bei einer qualitativen Betrachtung (wie sie in der Bundesverwaltung auf Stufe Departement / BK und Bundesrat stattfindet) ist die Analyse und das Verständnis von allfälligen Wechselwirkungen wichtig, um:

- das Gefahrenpotential von verketteten Risiken zu erkennen.
- Ansätze zu erarbeiten, um diese Verkettungen allenfalls aufzubrechen.

Wechselwirkungen mit anderen Risiken werden in der Risikobeschreibung *verbal* erfasst und erläutert. Allenfalls können sie grafisch dargestellt werden.

Risikoreporting
Vorgaben EFV:

- Die VE melden dem Departement alle Risiken, die über dem vom Departement definierten Schwellenwert eingestuft sind, mindestens aber ihre drei grössten.
- Die Departemente und die BK melden der Koordinationsstelle EFV alle Risiken, die über dem Schwellenwert Bund eingestuft sind (Risiken mit hoher bzw. sehr hoher Auswirkung ungeachtet derer Eintrittswahrscheinlichkeit.), mindestens aber ihre drei grössten.
- Wechselwirkungen zwischen Risiken werden analysiert und im Risikoreporting verbal oder grafisch erläutert.
- Querschnittsrisiken werden bei Bedarf auf den übergeordneten Hierarchiestufen aggregiert.

5 Kommunikation

Die Informationsflüsse und die Kommunikation zwischen den verschiedenen Akteuren im Risikomanagement sind wichtig und müssen, je nach Bedarf, in jeder Phase des Risikomanagementprozesses erfolgen (vgl. Ziff. 3.1). Eine gut aufgestellte interne und externe Kommunikation ist notwendig und nützlich, um

- die Risiken unter Berücksichtigung mehrerer Aspekte (aus verschiedenen Bereichen) und mit dem besten vorhandenen Fachwissen zu analysieren;
- sicherzustellen, dass die Interessen, Informationsbedürfnisse und Wahrnehmungen aller Anspruchsgruppen berücksichtigt werden und dadurch das Vertrauen in das Risikomanagement gestärkt wird;
- sicherzustellen, dass angemessen und zeitgerecht auf Veränderungen der Risikosituation reagiert werden kann.

Die Risikokommunikation in ausserordentlichen Lagen (Notfall- und Krisensituationen) wird durch die Bundeskanzlei organisiert und gesteuert und somit im folgenden Abschnitt nicht beschrieben.

Bereits in Ziffer 3.1 werden die Informationsflüsse zwischen den einzelnen Akteuren im Risikomanagementprozess detailliert erläutert. In Ziffer 5.1 werden weitere Elemente der internen Risikokommunikation beschrieben. Ziffer 5.2 befasst sich mit der Risikokommunikation der Bundesverwaltung nach aussen. In Ziffer 5.3 wird auf das Öffentlichkeitsprinzip, der Klassifizierung und der Archivierung von Informationen im Risikomanagement eingegangen.

5.1 Interne Kommunikation und Schulungen

Mittels Schulungen, Veranstaltungen und internen Informationskanälen wird sichergestellt, dass die Mitarbeitenden der Bundesverwaltung bezüglich dem Thema Risikomanagement ausgebildet und sensibilisiert werden. Dadurch soll die vorhandene Risikokultur verbessert, ein Austausch von Wissen im Bereich Risikomanagement ermöglicht und das Wissen zum Risikomanagement erhöht werden.

5.1.1 Schulungen

Folgende Kurse im Bereich Risikomanagement werden in der Bundesverwaltung regelmässig angeboten:

Schulung	Dauer	Häufigkeit	Zielgruppe
Risikomanagement für Topkader	½ Tag	nach Bedarf	Risikoeigner
«Grundlagen Risikomanagement»	1Tag	ca. 2 Mal im Jahr	Interessierte Personen (BCM-Beauftragte, Juristen, Projektmanager etc.)
«Umsetzung Risikomanagement»	3 Tage	ca. 2 Mal im Jahr	Risikomanager und Risikocoaches (obligatorisch für RMg und RC)
Grundschulung R2C_GRC	½ Tag	ca. 2-3 Mal im Jahr	Risikomanager und Risikocoaches (obligatorisch für RMg und RC)

5.1.1.1 Kurs «Umsetzung Risikomanagement»

In diesem Kurs werden die Kernelemente des Risikomanagements in der Bundesverwaltung vermittelt und deren praktische Anwendung geübt. Die Teilnehmer lernen den Aufbau eines Risikomanagement-Systemskennen, die Methoden zur Risikobewertung sowie den Risikomanagement-Prozess und werden befähigt, dies in ihrer Organisationseinheit umzusetzen.

Die wichtigsten Elemente des vorliegenden Handbuchs werden im Kurs behandelt und erläutert. Der Kurs ist für Risikomanager und Risikocoaches obligatorisch.

5.1.1.2 Grundschulung R2C_GRC

Die in der Bundesverwaltung verwendete Software zur Bewirtschaftung der Risiken heisst Risk-to-Chance (R2C_GRC) und wird von der Firma Schleupen AG aus Deutschland angeboten[43]. In einem Leitfaden werden alle für die Risikomanager und Risikocoaches relevanten Funktionalitäten der Software erläutert. Innerhalb der Bundesverwaltung betreut die Koordinationsstelle EFV die Anwendung R2C_GRC und ist erste Ansprechpartnerin bei Fragen, Problemen und bei der Erteilung von Berechtigungen. Grundsätzlich werden die Risiken im System durch die jeweiligen Risikocoaches der VE und Risikomanager der Departemente / der BK bewirtschaftet. Diese haben jeweils nur Zugriff auf die Risiken der eigenen Organisationseinheit. Zudem besteht die Möglichkeit, für einzelne Mitarbeiter Einsichtsberechtigungen zu erteilen.

In einem halbtägigen Kurs werden der Aufbau, die Navigation und die wichtigsten Funktionen der Software Risk-to-Chance (R2C_GRC) vorgestellt. Die Teilnehmer können im Kurs an einem eigenen PC die Benützung der Software üben und direkt Fragen stellen.
Der Kurs wird von der Koordinationsstelle EFV durchgeführt. Der Kurs ist für Risikomanager und Risikocoaches obligatorisch.

5.1.1.3 Ausbildungskurs für Kader (Risikoeigner)

Mit diesem Kurs sollen Risikoeigner in der Bundesverwaltung bzgl. ihrer Verantwortung im Umgang mit Risiken geschult und sensibilisiert werden.

Vorgabe EFV:

- Die Kurse «Grundschulung R2C_GRC» und «Umsetzung Risikomanagement» sind für alle Risikomanager und Risikocoaches obligatorisch.

5.1.2 Veranstaltungen

Netzwerk Risikomanagement

Der Verein Netzwerk Risikomanagement schafft für die im Risikomanagementprozess involvierten Personen eine Plattform für berufliche Kontakte, Erfahrungsaustausch und Weiterbildung. Angeboten werden praxisbezogene Veranstaltungen und Publikationen. Es ist geplant, jährlich eine bis zwei Veranstaltungen zu einem konkreten Risikomanagement-Thema durchzuführen. Der Teilnehmerkreis umfasst primär alle in der Bundesverwaltung interessierte Personen, die einen Bezug zum Risikomanagement haben und weitere am Risikomanagement interessierte Personen.

Innerhalb der Departemente / der BK und der VE finden zudem weitere, meist spezifischere Veranstaltungen zu konkreten Risikothemen statt.

Ein Austausch des Risikomanagementwissens innerhalb der Bundesverwaltung ist erwünscht und wird durch die Koordinationsstelle EFV gesteuert und unterstützt.

5.1.3 Interne Informationskanäle

Eine speziell für die Risikomanager und Risikocoaches erstellte und geschützte Acta Nova-Ablage ermöglicht den unkomplizierten fachlichen Austausch unter den Risikomanagern und

[43] Diese bietet auch einen technischen Support an.

-coaches. Hier werden die Weisungen, Richtlinien und das Handbuch zum Risikomanagement Bund, fachlich-methodische Unterlagen zum Risikomanagement und spezifische Hilfsmittel und Instrumente zur Umsetzung des Risikomanagementprozesses abgelegt.

5.2 Externe Kommunikation

Der Bundesrat nimmt zuhanden der Öffentlichkeit zum Thema Risikomanagement Bund Stellung.

5.2.1 Geschäftsbericht

Der Bundesrat erstattet der Bundesversammlung jährlich einen Bericht über seine Geschäftsführung. Dieser Bericht ist öffentlich und auf der Homepage der Bundeskanzlei aufgeschaltet. Im Band I «Schwerpunkte der Geschäftsführung des Bundesrates» findet sich jeweils ein Beitrag zum Thema Risikomanagement Bund. Darin werden in erster Linie konzeptionell-organisatorische Neuerungen im Risikomanagement des Bundes dargelegt. Auf einzelne Risiken des Bundes wird nur in sehr allgemeiner Form eingegangen.

5.2.2 Staatsrechnung und Voranschlag (Budget)

Auch die Staatsrechnungen und die Voranschläge sind öffentlich zugängliche Dokumente. Sie enthalten verschiedene Informationen aus dem Risikomanagement.

1. Im «Anhang zur Jahresrechnung» (Staatsrechnung Band 1) und im Voranschlag findet sich jeweils ein *allgemeines Kapitel* «Risikomanagement und Risikosituation». Dieses enthält Informationen zum Umgang mit Risiken, zu den Instrumenten und den Massnahmen des Risikomanagements, zur allgemeinen Risikosituation des Bundes und zur Offenlegung der Risiken. Aus Gründen der Vertraulichkeit wird auf eine genaue Bezeichnung und Detailangaben zu einzelnen Risiken verzichtet, soweit sie nicht bilanziert sind oder in den Eventualverbindlichkeiten offen gelegt werden.
2. Die Umsetzungskosten der im Rahmen des Risikomanagements beschlossenen und durchzuführenden *Massnahmen* sind im Budgetierungsprozess zu berücksichtigen.
3. Die rechtlichen Voraussetzungen für die Behandlung von Risiken im Voranschlag und in der Rechnung sind im Finanzhaushaltsgesetz[44] und in der Finanzhaushaltsverordnung[45] festgelegt (siehe Kapitel 6.5 und Übersicht in Anhang 6). Dabei sind die einschlägigen Bestimmungen gemäss den «Richtlinien und Weisungen zur Haushalt- und Rechnungsführung Bund» zu beachten.[46]

Der allgemeine Abschnitt zum Risikomanagement im Anhang der Jahresrechnung wird von der Koordinationsstelle EFV erstellt. Für die Aufnahme von beschlossenen Massnahmen und den aus dem Gesetz vorgeschriebenen Verpflichtungen (Rückstellungen und Eventualverbindlichkeiten) in den Voranschlag und der Staatsrechnung ist in erster Linie der entsprechende Risikoeigner bzw. die zuständige VE verantwortlich.

5.2.3 Stellungnahme des Bundesrates zu parlamentarischen Berichten bezüglich Risikomanagement

Die Geschäftsprüfungskommissionen (GPK) und die Finanzdelegation der eidgenössischen Räte begleiten das Risikomanagement Bund seit Jahren sehr eng. Sie berichten über ihre Tätigkeit im Bereich Risikomanagement Bund im Rahmen ihrer Jahresberichte oder in separaten Berichten. Diese werden jeweils im Bundesblatt publiziert, meistens zusammen mit der entsprechenden Stellungnahme des Bundesrates. Es geht darin jeweils um Grundsatzfragen

[44] Art 49 Abs. 3 FHG

[45] Art. 3 Bst. b und d; Art. 56 Abs. 2 FHV

[46] http://intranet.accounting.admin.ch/ ; zu beachten sind insbesondere die Handbuchkapitel *5.3.4 Rückstellungen* und *10.2 Eventualforderungen und -verbindlichkeiten*.

im Zusammenhang mit der Umsetzung des Risikomanagements Bund, nicht um einzelne Risiken des Bundes.[47]

5.3 Klassifizierung, Öffentlichkeitsprinzip und Archivierung

5.3.1 Schutz von Informationen im Risikomanagement Bund, Öffentlichkeitsprinzip

Klassifizierung

Die Klassifizierung und die Bearbeitung von Informationen des Bundes sind in der Informationssicherheitsverordnung (ISV)[48] geregelt. Entsprechend dem Grad ihrer Schutzwürdigkeit werden die Informationen klassifiziert oder einer der Klassifizierungsstufen INTERN, VERTRAULICH oder GEHEIM zugewiesen (Art. 18 ff. ISV).

Die Erstellung, die Bekanntgabe und das Zugänglichmachen klassifizierter Informationen sind grundsätzlich auf ein Minimum zu beschränken; klassifizierte Informationen dürfen nur jenen Personen bekannt gegeben oder zugänglich gemacht werden, die davon Kenntnis haben müssen (Art. 16 Abs. 1 ISV). Gemäss den Bearbeitungsvorschriften für klassifizierte Informationen sind VERTRAULICH klassifizierte Informationen in elektronischer Form verschlüsselt zu speichern, physisch in Sicherheitsbehältnissen aufzubewahren. Der Versand solcher Informationen per E-Mail erfolgt verschlüsselt.

Ein Teil der Informationen, die auf einem Risikoblatt aufgeführt werden, sind allgemein bekannt, z. B. die gesetzliche Bundesaufgabe, mögliche Beeinträchtigungen bei der Aufgabenerfüllung durch die Bundesverwaltung, Risikoursachen. Schutzwürdig nach Artikel 18 ff. ISV können Informationen über die Einschätzung der Eintrittswahrscheinlichkeit und der möglichen Auswirkungen eines Risikos durch die zuständigen Fachleute sein. Das Gleiche kann für die Beschreibungen der vorgesehenen Risikoreduktionsmassnahmen gelten.

Ein Einzelrisikoblatt und erst recht ein Risikoreporting auf Stufe Verwaltungseinheit, Departement oder Bundesrat ist als «Sammelwerk» im Sinne von Artikel 16 Absatz 2 ISV anzusehen. Es werden darin diverse, mehr oder weniger schutzwürdige Informationen in einem Dokument zusammengetragen. Bei Sammelwerken ist zu prüfen, ob und auf welcher Stufe das Dokument *in seiner Gesamtheit* zu klassifizieren ist.

Beim Entscheid, ob eine Information zu klassifizieren ist, muss beachtet werden, dass eine übermässig restriktive Handhabung des Informationsschutzes die verwaltungsinterne Kommunikation über Risiken und damit den Risikodialog massiv erschweren kann. Auch soll der Verteiler von klassifizierten Information nicht unnötig eingeschränkt sein. Die Vertraulichkeit von tatsächlich schutzwürdigen Informationen ist andererseits strikte sicherzustellen, andernfalls sie dem Risikomanagement nicht zur Verfügung gestellt werden können.

Umgang mit Klassifizierung
Empfehlung EFV:

Aus Sicht der Koordinationsstelle Risikomanagement Bund wäre es – zumindest auf Stufe Bund und Departement – kaum praktikabel, bei jeder Risikoinformation einzelfallweise zu entscheiden, ob eine Klassifizierung gerechtfertigt ist oder nicht. Gestützt auf Artikel 16 Absatz 2 ISV («Sammelwerk») erachtet sie es als zweckmässig, alle Informationen/Dokumente, die sich auf konkrete Risiken beziehen (Einzelrisikoblätter, Risikoberichte, Daten innerhalb der im Bund eingesetzten Risikomanagement-Software) als VERTRAULICH zu klassifizieren und nur aus begründetem Anlass – z. B. anlässlich eines Zugangsgesuchs nach Öffentlichkeitsgesetz – zu überprüfen, ob die Klassifizierung im konkreten Fall ganz

[47] Die Risikoberichterstattung an den Bundesrat wird in der Regel im April von einer Arbeitsgruppe der GPK behandelt.
[48] ISV; SR *128.1*

oder teilweise aufgehoben werden kann.

Öffentlichkeitsprinzip

Das BGÖ soll die Transparenz über den Auftrag, die Organisation und die Tätigkeit der Verwaltung fördern, indem es den Zugang zu amtlichen Dokumenten gewährleistet (Art. 1 BGÖ). Ein amtliches Dokument ist jede Information, die «auf einem beliebigen Informationsträger aufgezeichnet ist» oder «durch einen einfachen elektronischen Vorgang aus aufgezeichneten Informationen erstellt werden» kann, sich im Besitz einer Behörde befindet und die Erfüllung einer öffentlichen Aufgabe betrifft (Art. 5 Abs. 1 und 2 BGÖ). Das Öffentlichkeitsprinzip gilt auch für amtliche Dokumente des Risikomanagements des Bundes (Art. 2 bis 4 BGÖ).

Nicht «fertig gestellte» Dokumente gelten nicht als «amtliche Dokumente» im Sinne des BGÖ (Art. 5 Abs. 3 Bst. b BGÖ). Ein Zugangsrecht besteht nur für Dokumente, die vom Ersteller finalisiert und «dem Adressaten definitiv übergeben» wurden, «namentlich zur Kenntnis- oder Stellungnahme oder als Entscheidgrundlage» (Art. 1 Abs. 2 Öffentlichkeitsverordnung[49]). Dokumente betreffend das Risikomanagement Bund sind vom BGÖ somit erst ab Beginn der Reportingphase betroffen.

Der Zugang zu amtlichen Dokumenten kann eingeschränkt, aufgeschoben oder verweigert werden, u. a. wenn durch seine Gewährung:

- die freie Meinungs- und Willensbildung einer Bundesbehörde, der Bundesversammlung oder des Bundesrates;
- die zielkonforme Durchführung konkreter behördlicher Massnahmen;
- die innere oder äussere Sicherheit der Schweiz;
- die aussenpolitischen Interessen oder die internationalen Beziehungen der Schweiz;
- die Beziehung zwischen dem Bund und den Kantonen oder zwischen Kantonen;
- die wirtschafts-, geld- und währungspolitischen Interessen der Schweiz

beeinträchtigt oder gefährdet werden können (Art. 7 Abs. 1 BGÖ). Weitere Ausnahmebestimmungen finden sich in Artikel 8 BGÖ.

Die Zuständigkeit für die Stellungnahme zu einem Gesuch um Zugang zu einem Dokument liegt grundsätzlich bei der Behörde, die das Dokument erarbeitet hat. In Artikel 11 VBGÖ sind diverse Spezialfälle geregelt. Gemäss Ziffer 2 des Bundesratsbeschlusses zur «Evaluation de la loi sur la transparence» vom 1. April 2015[50] sind ähnliche Gesuche, die bei verschiedenen Verwaltungseinheiten gestellt werden, durch die BK (KID, Rechtsdienst) und das EJPD (BJ) zu koordinieren. Bei Dokumenten betreffend das Risikomanagement Bund hängt die Zuständigkeit in der Regel von der Art des Dokuments bzw. davon ab, welche Behörde es erstellt hat:

- Einzelrisikoblatt: Zuständig ist die Verwaltungseinheit, die das Risiko erfasst hat.
- Reporting der Verwaltungseinheit: Die Verwaltungseinheit
- Departementsreporting: Das Departement
- Querschnittsrisiken Stufe Departement (inkl. Quellrisiken): Das Departement
- Bundesratsreporting zuhanden GSK, Bundesrat und GPK-Arbeitsgruppe: Koordinationsstelle Risikomanagement Bund (EFV)
- Querschnittsrisiken Stufe Bundesrat (inkl. Quellrisiken) zuhanden GSK, Bundesrat und GPK-Arbeitsgruppe: Koordinationsstelle Risikomanagement Bund (EFV)

[49] VBGÖ, SR *152.31*
[50] EXE 2015.0216

Vorgehen bei einem Gesuch um Zugang zu einem klassifizierten Dokument
Empfehlung EFV:

1. Klärung der Zuständigkeit betreffend Klassifizierung: Zuständig ist die Verfasserin / der Verfasser des klassifizierten Dokuments (Art. 11 Abs. 5 VBGÖ).
2. Die Verfasserin / der Verfasser prüft, ob die Klassifizierung nach den Kriterien von Artikel 18 ff. ISV noch gerechtfertigt ist; allenfalls wird das Dokument entklassifiziert (als Ganzes oder in Anwendung des Verhältnismässigkeitsprinzips in Teilen; Art. 11 Abs. 5 VBGÖ).
3. Die für das BGÖ zuständige Person prüft, ob das nachgesuchte Dokument in den Geltungsbereich des BGÖ fällt, insbesondere ob es «fertig gestellt» ist (Art. 5 Abs. 3 Bst. b BGÖ; Art. 1 Abs. 2 VBGÖ).
3. Die für das BGÖ zuständige Person beurteilt «unabhängig von einem allfälligen Klassifizierungsvermerk», ob der Zugang nach BGÖ zu gewähren, zu beschränken, aufzuschieben oder zu verweigern ist (Art. 4 Abs. 1 ISG).

Falls die Anfrage an die Verfasserin / den Verfasser nicht bereits über die für Fragen zum BGÖ zuständigen Person erfolgt, empfiehlt sich in jedem Fall eine entsprechende Kontaktaufnahme.

5.3.2 Archivierung

Die Unterlagen, die im Rahmen des Risikomanagements Bund erstellt (oder empfangen) worden sind, unterstehen den Bestimmungen des Bundesgesetzes über die Archivierung (BGA)[51]. Die Departemente, die BK und die VE sind selber für die Archivierung ihrer Unterlagen verantwortlich.

Zudem werden die einzelnen Risiken innerhalb der Risikomanagement-Applikation Risk-to-Chance (R2C_GRC) *elektronisch* gespeichert und archiviert. Die Risiken werden mindestens einmal jährlich erfasst bzw. aktualisiert und danach innerhalb des R2C_GRC historisiert. Bei *eingetretenen* Risiken werden zusätzlich die erlittenen Schäden und die dazugewonnenen Erkenntnisse im R2C_GRC festgehalten. *Erledigte* Risiken werden aus Gründen der Nachvollziehbarkeit im R2C_GRC nicht gelöscht; ihr Status ist auf «erledigt» zu setzen.

[51] SR *152.1*

6 Schnittstellen

Im Folgenden werden Organisationseinheiten, Projekte und Funktionen innerhalb der Bundesverwaltung beschrieben, die eine Schnittstelle zum Risikomanagement aufweisen. Das Ziel ist, die Aufgaben der jeweiligen Funktion oder Organisation kurz zu erläutern, von den Aufgaben im Risikomanagement abzugrenzen und die Schnittstellen und Informationsflüsse festzulegen. Dies soll zu einem effizienten Risikomanagement ohne Doppelspurigkeiten und Reibungsverlusten beitragen.

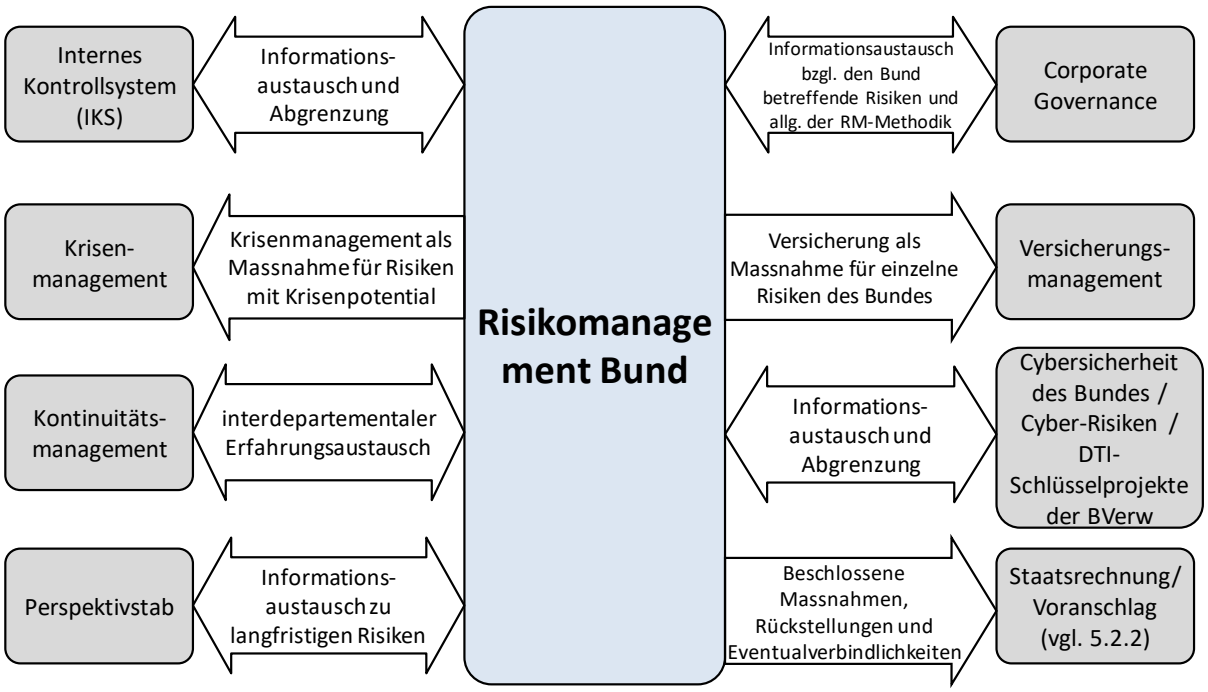


Abbildung 15: Schnittstellen zum Risikomanagement (nicht abschliessend)

6.1 Internes Kontrollsystem (IKS)

Das Interne Kontrollsystem (Art. 39 FHG, Art. 36 FHV) identifiziert operative finanzbezogene Risiken. Es beschreibt und bewertet die identifizierten Risiken und legt risikominimierende regulatorische, organisatorische und technische Kontrollmassnahmen fest. Es erfolgt eine periodische Überprüfung sowohl der identifizierten und bewerteten Risiken als auch der Wirksamkeit der risikominimierenden Kontrollen. Das IKS unterscheidet zwischen automatisierten (beispielsweise Berechtigungen und Validierungen) und manuellen (beispielsweise Verifizierung/Plausibilisierung, Vier-Augen-Prinzip) Kontrollen, wobei wenn möglich automatisierte Kontrollen einzuführen sind.

Im Gegensatz zum breit angelegten Risikomanagement konzentriert sich das IKS auf die Identifikation von operativen Risiken der finanzrelevanten Geschäftsprozesse und auf die Beschreibung und Umsetzung geeigneter Kontrollmassnahmen zur Minimierung dieser Risiken. Das IKS ist demnach Teil des Risikomanagements der Bundesverwaltung.

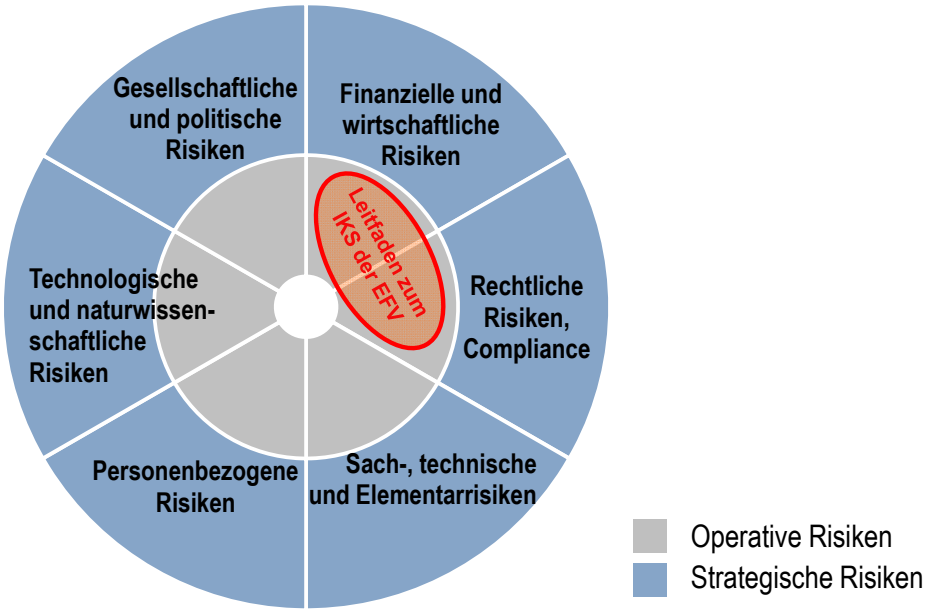


Abbildung 16: IKS und Risikomanagement

Schnittstellen zum Risikomanagement

Die Identifikation und Bewertung von operativen Risiken der finanzrelevanten Geschäftsprozesse und die Erarbeitung von Kontrollmassnahmen fällt theoretisch in den Aufgabenbereich sowohl des Risikocoaches als auch des IKS-Beauftragten. Im Sinne einer optimalen Arbeitsteilung konzentriert sich der Risikocoach im Risikomanagement-Prozess auf die Identifikation aller anderen Risiken der VE, ergänzt seine Risikoliste aber mit den relevanten im IKS-Prozess identifizierten Risiken.

Notwendiger Informationsaustausch

Auf Stufe VE soll ein regelmässiger Austausch zwischen dem Risikocoach und dem IKS-Beauftragten stattfinden. Dabei wird analysiert,

- ob die identifizierten Risiken aus dem Risikomanagement Anpassungen im IKS bzw. neue Massnahmen im Sinne von Kontrollen erfordern.
- ob im IKS-Prozess erkannte Risiken im Risikomanagement zu erfassen sind und einer Berichterstattung bedürfen.

6.2 Notfall- und Krisenmanagement (Früherkennung, Bewältigung)

Ein zweckmässiges Notfall- und Krisenmanagement ist Teil des Risikomanagements[52] und zuständig für die Bewältigung von gravierenden Risiken bei deren Eintritt. Bei Risiken mit hohen Auswirkungen ist es wichtig, über Organe, Einrichtungen und Prozesse zu verfügen, die einen Schadenplatz so schnell als möglich beheben (Notfallmanagement) oder die Reputation, den Handlungsspielraum oder die Existenz der betroffenen Organisation verteidigen (Krisenmanagement) [53]. Zusätzlich müssen, je nach Dauer der Wiederherstellungsphase, die

[52] Ziff. 4 Abs. 6 der Weisungen über die Risikopolitik des Bundes

[53] Vgl. Definitionen «Notfall» und «Krise» in Anhang 1

Kernprozesse der betroffenen Organisation aufrecht erhalten werden (Kontinuitätsmanagement[54]). In diesem Sinn sind Notfall-, Krisen- und Kontinuitätsmanagement für Massnahmen zuständig, die zur Bewältigung von Schäden und zur Linderung der Konsequenzen bei eingetroffenen Risiken beitragen. Dabei liegt die Verantwortung grundsätzlich bei der Linie. Das Risikomanagement gibt zwar den Anstoss für den Aufbau von Vorkehrungen zum Notfall-, Krisen- und Kontinuitätsmanagement und ist verantwortlich für die aktuelle Erfassung entsprechender Massnahmen, befasst sich aber nicht selber mit den Vorbereitungen und mit der Krisenbewältigung.

Überwachung von Risiken bedeutet auch Erkennen und Einschätzen möglicher Entwicklungen unter Beachtung des gegebenen Umfeldes. Die Früherkennung von möglichen Notfällen oder Krisen ist somit Teil des Risikomanagements. Dieses stellt auch sicher, dass zeitgerecht ein adäquates Notfall- und Krisenmanagement bereitgestellt werden kann (vorsorglicher Aufbau einer Krisenorganisation, Üben möglicher Notfall- und Krisenszenarien usw.).

Die in der BK (Sektion Strategische Führungsunterstützung) angesiedelte Krisenfrüherkennung[55] operiert auf einer kurzfristigen strategischen Ebene (bis max. 1,5 Jahre). Sie ergänzt die bestehenden Instrumente durch eine zusätzliche Aussensicht auf die aktuelle Situation und arbeitet dabei mit dem Risikomanagement Bund zusammen. Gestützt auf eine kontinuierliche Analyse von hauptsächlich verwaltungsexternen Quellen identifiziert die Krisenfrüherkennung BK neu aufkommende Risiken bzw. sich abzeichnende Krisen und überprüft die im Risikoreporting des Bundes erfassten Risiken auf Lageveränderungen. Neue Erkenntnisse oder abweichende Einschätzungen werden dem zuständigen Departement über die Koordinationsstelle Risikomanagement Bund gemeldet. Das Zusammenwirken der Krisenfrüherkennung der BK mit dem Risikomanagement Bund ist in einem Detailkonzept geregelt. Bei unterschiedlichen Einschätzungen zwischen den Quellen der Krisenfrüherkennung BK und dem Departement (resp. Risikoeigner) kann die BK den Bundesrat nach Absprache mit dem betroffenen Departement in geeigneter Form informieren.

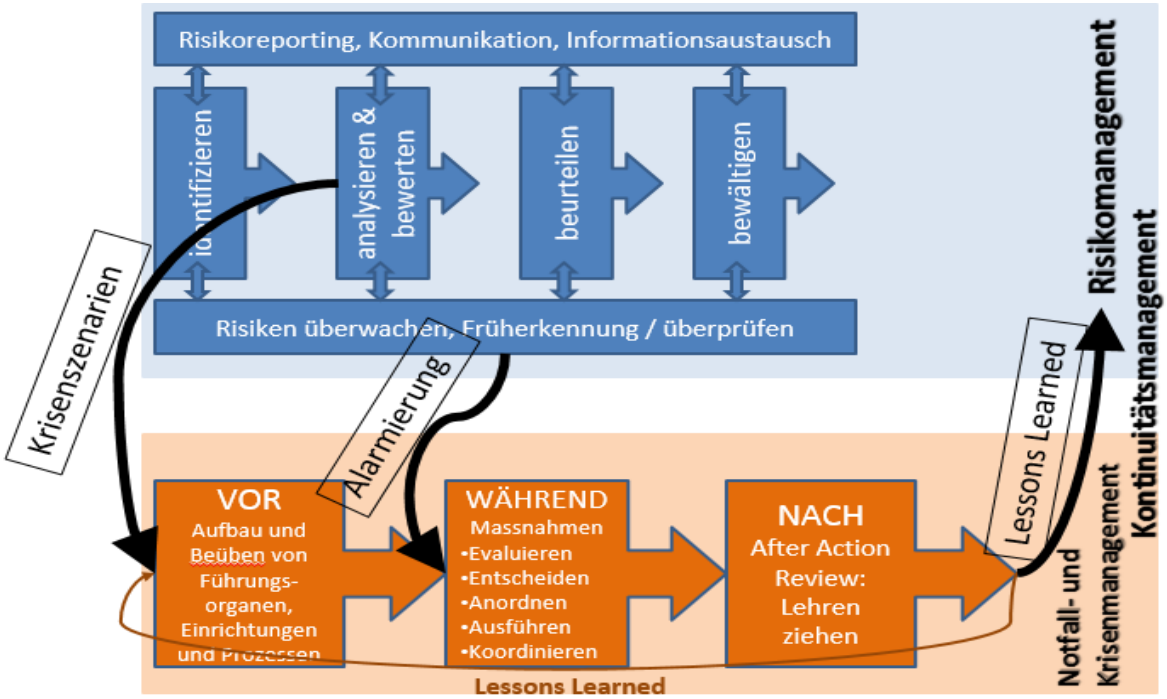


Abbildung 17: Schnittstelle Risikomanagement und Krisenmanagement

[54] Vorkehrungen zum Kontinuitätsmanagement werden auch im Vorfeld erarbeitet und sind in diesem Sinn auch Bewältigungsoptionen des Risikomanagements (vgl. Ziff. 6.3).

[55] Gesetzlicher Auftrag gemäss Art. 32 Bst. g und Art. 33 Abs. 1[bis] RVOG (in Kraft seit 1. Januar 2015).

Die nachfolgende Abbildung gibt einen Überblick über die Instrumente und Organisationseinheiten, die sich in der Bundesverwaltung mit Notfällen und Krisen befassen. Bei den einen läuft permanent ein Prozess der Früherkennung (linke Tabellenhälfte), sie haben aber einen unterschiedlichen Fokus und einen unterschiedlichen Zeithorizont. Sie ergänzen sich und ermöglichen den übergeordneten Hierarchiestufen einen breiteren Überblick. In der rechten Tabellenhälfte sind die Organe aufgeführt, die beim Eintritt einer Krise punktuell aktiv werden (Bewältigung von besonderen und ausserordentlichen Lagen).

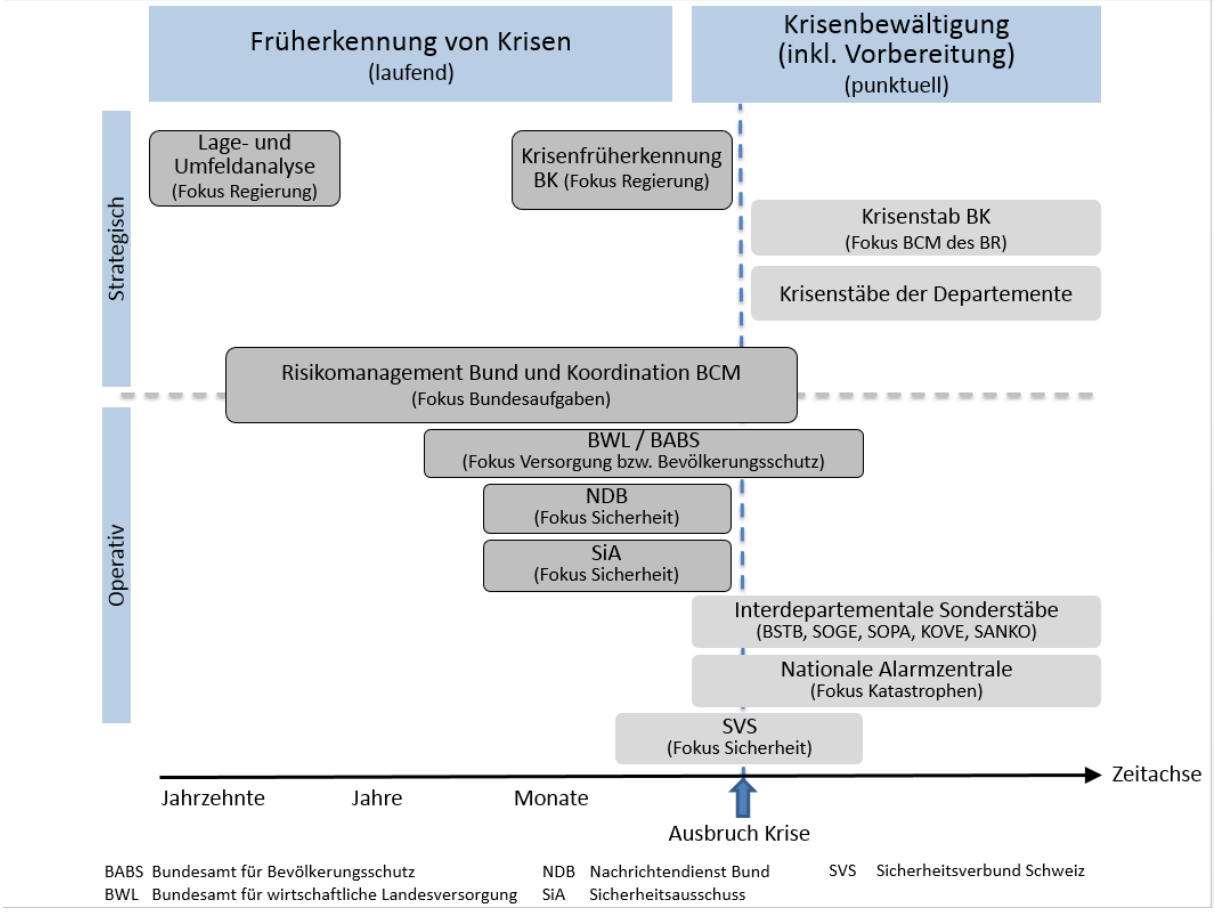


Abbildung 18: Überblick Krisenmanagement-Organisationen

Schnittstellen zum Risikomanagement

Ein zweckmässiges Notfall- und Krisenmanagement ist Teil des Risikomanagements. Das Risikomanagement stellt sicher, dass das Notfall- und Krisenmanagement zeitgerecht aktiviert werden kann.

Notwendiger Informationsaustausch

1. Periodischer Abgleich mit den anderen Organen der Krisenfrüherkennung.
2. Bei Risiken mit potenziell grossen Auswirkungen wird die Linie auf ihre Verantwortung für die Vorbereitung des Notfall- und Krisenmanagements hingewiesen. Der Eintritt solcher Risiken dient als Übungsszenario.
3. Die Früherkennung von Krisen dient der zeitgerechten Alarmierung des Notfall- und Krisenmanagements.
4. Die relevanten Lehren aus der Bewältigung von Notfällen und Krisen werden im Risikomanagement berücksichtigt.

6.3 Kontinuitätsmanagement (BCM)

Das BCM (Business Continuity Management) ist Bestandteil eines integrierten Risikomanagement-Systems. Während das Risikomanagement sich vorausschauend mit den Gefahren für die Aufgabenerfüllung und Zielerreichung auseinandersetzt und Massnahmen zur Risikominimierung vorsieht, fokussiert das BCM auf den Ereignisfall. Sein Zweck ist es, die *Auswirkungen* eines Risikos auf kritische Leistungen und Geschäftsprozesse zu minimieren. Aus Sicht des Risikomanagements ist das BCM somit als Massnahme auf der Auswirkungsseite zu betrachten.

Im Kontinuitätsmanagement werden die notwendigen Vorkehrungen getroffen, damit Bundesrat und Bundesverwaltung ihre Kernaufgaben selbst in ausserordentlichen Situationen erfüllen können. Der Aufbau eines BCM erfolgt für jede VE in vier Phasen:[56]

- ***Phase 1 – BIA erstellen:*** Mit der Business Impact Analyse (BIA) werden die sogenannt «kritischen» Leistungen und Geschäftsprozesse identifiziert, deren Störung oder Ausfall zu empfindlichen materiellen oder immateriellen Schäden führen würde. Die BIA wird in vier Schritten durchgeführt: (1) Erfassen der Leistungen und Prozesse der VE, (2) Festlegen der Kriterien zur Bestimmung der Kritikalität von Leistungen und Prozessen, (3) Bewerten aller Leistungen und Prozesse mit Blick auf ihre Kritikalität und (4) Ermitteln der Ressourcen, die für die kritischen Leistungen und Prozesse benötigt werden.[57]
- ***Phase 2 – Strategie definieren:*** Die Strategie hält das Ziel und die Grundsätze der Umsetzung des BCM fest. Sie definiert namentlich die Zuständigkeiten im BCM der VE, die Bedrohungsszenarien, die Massnahmen, die Berichterstattung und Kommunikation, die Schulung sowie die Durchführung von Testläufen.
- ***Phase 3 – Massnahmen erarbeiten und implementieren****:* Im Business Continuity Plan (BCP) werden die Massnahmen und Pläne entwickelt, damit die kritischen Leistungen und Prozesse möglichst lange aufrechterhalten bzw. die Funktionsfähigkeit der VE möglichst rasch wiederhergestellt werden können. Ziel ist es, die negativen Auswirkungen einer Störung oder eines Ausfalls, d. h. die Schwere und Dauer der Beeinträchtigung zu minimieren. Zu den wichtigen Elementen eines BCP zählen Ersatzarbeitsplätze und -infrastruktur für unerlässliches Personal, Einsatzpläne bei personellen Engpässen oder auch die Gewährleistung der Versorgung mit kritischen Ressourcen (z. B. Lagerhaltung, vertragliche Absicherung für kurzfristigen Abruf, Vereinbarungen mit Lieferanten). Die Kosten für die Sicherstellung der Kontinuität von Geschäftsprozessen (z. B. Redundanzen) müssen dem Nutzen gegenübergestellt werden.
- ***Phase 4 – Einsatzbereitschaft sicherstellen:*** Damit der BCP im Ereignisfall einsatzfähig ist, sind *Testläufe* nötig, mit denen die Massnahmen und deren Zusammenwirken erprobt werden. Ebenso müssen die Verantwortungsträger *geschult* und deren Zusammenspiel *geübt* werden. Da Aufgaben und Rahmenbedingungen einer VE sich im Lauf der Zeit ändern können, sind BIA und BCP periodisch auf ihre Aktualität und Wirksamkeit zu *überprüfen* und bei Bedarf anzupassen.

Die Funktionen und Verantwortlichkeiten für das BCM in der Bundesverwaltung sind in der *Richtlinie über das Kontinuitätsmanagement Bund* festgehalten. Demgemäss trägt die *Leitung der einzelnen VE* die Verantwortung für den Aufbau und die periodische Überprüfung des BCM. Analog zur Organisation des Risikomanagements Bund werden auf Stufe Departement und VE *BCM-Beauftragte* ernannt. Die *Koordinationsstelle Risikomanagement Bund (EFV)* ist beauftragt, zentrale BCM-Fragen zu koordinieren, die Umsetzung des BCM in der Bundesverwaltung zu fördern sowie der GSK im Rahmen des Risikoreportings einmal jährlich Bericht über den Stand der Umsetzung des BCM zu erstatten.

---

[56] Vgl. ISO 22301.

[57] Es ist möglich, dass eine OE keine – im Sinne des BCM – kritischen Leistungen und Prozesse aufweist. In diesem Fall gelten die nachfolgenden Phasen 2 bis 4 nur eingeschränkt.

Schnittstellen zum Risikomanagement

Das BCM stellt Massnahmen und Pläne zur Bewältigung von spezifischen Risikoauswirkungen bereit. Die Existenz und Wirksamkeit dieser Dispositive sind summarisch in den entsprechenden Risikoblättern zu erfassen.

Notwendiger Informationsaustausch

Soweit Departemente und BK ihr BCM entlang der Risikomanagement-Organisation des Bundes aufbauen, besteht kein spezieller Bedarf für Informationsaustausch. Andernfalls ist namentlich in den Reportingphasen ein Austausch zwischen Risikomanagern bzw. Risikocoaches und den BCM-Beauftragten durchzuführen. Die Risikocoaches stellen sicher, dass die Massnahmen aus dem BCM im RM-System (R2C_GRC) angemessen erfasst und aktualisiert sind.

6.4 Lage- und Umfeldanalyse

Gemäss Artikel 32 Buchstabe c^{ter} RVOG sorgt die Bundeskanzlei für eine langfristige und kontinuierliche Lage- und Umfeldanalyse und erstattet dem Bundesrat darüber laufend Bericht. Nach der Aufhebung des Perspektivstabes der Bundesverwaltung[58] hat der Bundesrat das Vorgehen wie folgt festgelegt:

Erstens wird alle vier Jahre ein Expertenbericht mit einer Auslegeordnung über wichtige Trends und Themen erarbeitet, welche die Schweiz in den kommenden 10 bis 15 Jahren beeinflussen und prägen dürften. Zur Ermittlung künftiger Herausforderungen und Perspektiven soll Expertenwissen, z. B. aus den Bereichen Wissenschaft, Wirtschaft, Kultur, Politik und Verwaltung zusammengetragen werden. Dieser Bericht wird dem Bundesrat erstmals Ende 2018 als Grundlage für die Festlegung der politischen Prioritäten (Legislaturplanung) vorgelegt.

Zweitens und ergänzend zu diesem Expertenbericht analysiert die Bundeskanzlei ab 2017 verwaltungsinterne und -externe Informationsquellen. Sie informiert den Bundesrat im Jahresrhythmus über neue Entwicklungen, Ereignisse und Trends, die aufgrund ihrer Relevanz in die Jahresziele des Bundesrates im Folgejahr aufgenommen werden sollten.

Im Vergleich zum Risikomanagement fokussiert die langfristige und kontinuierliche Lage- und Umfeldanalyse v. a. auf strategisch-politische Themen mit einem direkten Bezug zur Regierungstätigkeit und einem mittel- bis langfristigen Zeithorizont (vgl. Abbildung 17). Aus den erkannten mittel- bis langfristigen Herausforderungen können sich im Verlaufe der Zeit Hinweise auf konkrete Risiken für den Bund sowie auf Krisen ergeben. Deshalb ist ein Informationsaustausch zwischen der Bundeskanzlei und dem Risikomanagement Bund unabdingbar.

Schnittstellen zum Risikomanagement

Die im Rahmen der langfristigen und kontinuierlichen Lage- und Umfeldanalyse identifizierten Herausforderungen stellen aus Sicht Risikomanagement zum Zeitpunkt der Identifikation noch abstrakte Gefahren dar. Im Verlauf der Zeit können daraus konkrete Risiken entstehen, die im Risikoreporting der Bundesverwaltung aufgenommen werden müssen.

Notwendiger Informationsaustausch

Der Informationsaustausch ist dadurch sichergestellt, dass die BK nach Bedarf das Risikomanagement Bund einbezieht und die Koordinationsstelle Risikomanagement Bund über ihre Erkenntnisse informiert.

[58] Vgl. BRB vom 07.09.2017

6.5 Rechnungslegung (Eventualverbindlichkeiten)

Eine Schnittstelle zwischen Risikomanagement und Rechnungslegung besteht im Bereich der sogenannten *Eventualverbindlichkeiten*. Höhere Rechnungslegungsstandards (z. B. IFRS, IPSAS[59]) verlangen von privaten Unternehmen und öffentlichen Gemeinwesen, dass sie im Rahmen der Jahresrechnung ihre Eventualverbindlichkeiten ausweisen.[60] Eventualverbindlichkeiten sind Verpflichtungen aus vergangenen Ereignissen, die in der Zukunft unter bestimmten Bedingungen zu einem Mittelabfluss führen können, wobei die Eintrittswahrscheinlichkeit auf unter 50% veranschlagt wird. Dabei sind zwei Fälle zu unterscheiden:

> ***Fall 1:*** Es *besteht bereits* eine rechtliche oder faktische Verpflichtung. Ein Mittelabfluss aus dieser Verpflichtung kann zwar nicht ausgeschlossen werden, wird zum Zeitpunkt der Erfassung jedoch als wenig wahrscheinlich, d. h. unter 50%, erachtet.[61] Beispiele sind Bürgschaften oder Garantien.
>
> ***Fall 2:*** Eine Verpflichtung kann in der Zukunft *eventuell* entstehen. Das zugrunde liegende Ereignis hat zwar bereits stattgefunden, ob daraus eine Verpflichtung entsteht, liegt aber ausserhalb der Kontrolle der Firma bzw. des Gemeinwesens. Die Wahrscheinlichkeit liegt unter 50% und/oder der eventuelle Mittelabfluss kann nicht zuverlässig geschätzt werden. Beispiele sind hängige Rechtsfälle oder verborgener Sanierungsbedarf in einem Immobilienportfolio, etwa aufgrund kontaminierter Böden oder Asbestverseuchung.

Der Sinn der Veröffentlichung von Eventualverbindlichkeiten besteht darin, Anspruchsgruppen und interessierte Kreise (Investoren, Gläubiger bzw. Steuerzahlende) in transparenter Form über mögliche künftige Belastungen der Firma bzw. des Gemeinwesens zu informieren.

Der Bund unterscheidet vier Arten von Eventualverbindlichkeiten[62]:

- *Bürgschaften und Garantien* (z. B. Bürgschaften an Organisationen des gemeinnützigen Wohnungsbaus);
- *Kapitalzusagen* für Entwicklungsbanken (nicht einbezahlte, aber verbindlich zugesagte Garantiekapitalien);
- *Rechtsfälle* (hängige Rechtsverfahren, aus denen ein Urteil mit Kostenfolgen für den Bund hervorgehen kann);
- *übrige* Eventualverbindlichkeiten (z. B. aus der Altlastensanierung von Liegenschaften).

Eventualverbindlichkeiten haben mit Risiken gemeinsam, dass sie mit einer gewissen Wahrscheinlichkeit negative finanzielle Auswirkungen auf den Bund haben können. Sie unterscheiden sich aber grundlegend darin, dass Eventualverbindlichkeiten und Risiken je eigenen Systemen mit unterschiedlichen Zwecken dienen: Während der Ausweis von Eventualverbindlichkeiten als Element der *Rechnungslegung* dazu beiträgt, die Vermögenslage wirklichkeitsgetreu darzustellen, zielt das *Risikomanagement* darauf ab, die Risiken systematisch zu bewirtschaften und damit die Aufgabensteuerung einer OE zu verbessern. Rechnungslegung und Risikomanagement richten sich somit auch an *andere Adressaten* mit *anderen Interessen* (Investoren bzw. Parlament und Steuerzahlende einerseits, Führungsverantwortliche andererseits). Aufgrund dieser Unterschiede wäre eine deckungsgleiche Abbildung in beiden Systemen nicht nur unnötig, sondern auch fachlich falsch.[63] In welchen Fällen eine

---

[59] International Financial Reporting Standards; International Public Sector Accounting Standards.

[60] Der Bund legt seine Eventualverbindlichkeiten gestützt auf IPSAS 19 dar, vgl. Staatsrechnung 2016, Band 1, Ziffer 63, S. 121f. Der Rechnungslegungsgrundsatz ist im *Handbuch für die Haushalt- und Rechnungsführung in der Bundesverwaltung* dargestellt (Kap. 10.2; http://intranet.accounting.admin.ch/handbuch_hh/anhang_rechnung/00137/00185/index.html?lang=de).

[61] Wird der Mittelabfluss als wahrscheinlich beurteilt (>50%), ist in der Bilanz eine *Rückstellung* zu verbuchen.

[62] Der Bund wies 2016 Eventualverbindlichkeiten von rund 23 Mrd. Franken aus (ohne Vorsorgeverpflichtungen und Leistungen an Angestellte), wobei über 90% auf Bürgschaften und Garantien entfallen (vgl. Staatsrechnung 2016, Bd. 1, Kap. 63, S. 121).

[63] Der umgekehrte Fall, wonach ein Risiko eine Eventualverbindlichkeit begründen könnte, ist in der Praxis in aller Regel nicht von Bedeutung, da die Rechnungslegung für die Erfassung von Eventualverbindlichkeiten deutlich engere Kriterien anwendet.

Eventualverbindlichkeit im Risikomanagement übernommen und gesteuert werden soll, ist fallweise zu entscheiden.[64]

Die Erfassung einer Eventualverbindlichkeit als Risiko ist insbesondere dann angezeigt, wenn dies der Aufgabensteuerung einer OE nützt, konkret wenn

- die Aufgabenerfüllung und Zielerreichung einer OE gefährdet ist (Risiko) *und*
- Eintrittswahrscheinlichkeit und Auswirkungen hoch bewertet sind (Wesentlichkeit) *und*
- das Risiko gesteuert werden kann, d. h. wenn Massnahmen zur Reduktion der Eintrittswahrscheinlichkeit bzw. zur Bewältigung der Auswirkungen ergriffen werden können (Steuerbarkeit).

Schnittstellen zum Risikomanagement

Eine Eventualverbindlichkeit kann unter bestimmten Bedingungen ein Risiko begründen (negativer Einfluss auf Aufgaben und Ziele, Wesentlichkeit, Steuerbarkeit).

Notwendiger Informationsaustausch

Risikomanager und Risikocoaches kennen die Eventualverpflichtungen ihrer Einheit(en) und entscheiden aufgrund der dargelegten Grundsätze zusammen mit der verantwortlichen Linie, ob neben der Eventualverbindlichkeit auch ein Risiko ausgewiesen werden soll und begründen dies im Einzelfall.

6.6 Corporate Governance[65]

Gewisse Bundesaufgaben werden von rechtlich, organisatorisch und finanziell verselbständigte Einheiten wahrgenommen, die teilweise oder vollständig im Besitz des Bundes sind und von diesem beherrscht werden (Unternehmen und Anstalten des Bundes). Damit der Bundesrat seine Eigner- und Gewährleistungsfunktion[66] gegenüber diesen Einheiten wahrnehmen kann, legt er als Teil der Corporate Governance des Bundes[67] strategische Ziele[68] fest, die im Regelfall für einen Zeitraum von vier Jahren gelten.

Im Rahmen dieser strategischen Ziele wird das oberste Leitungsorgan (Verwaltungsrat) mit einer spezifischen Vorgabe verpflichtet, ein Risikomanagement (Enterprise Risk Management ERM) und ein Compliancemanagement (CMS) einzurichten und wirksam zu betreiben. Die Standardfomrulierung lautet:

> Ziel XY: «Die <Unternehmung> verfügt über ein Unternehmensrisikomanagement-System (ERM), das sich an der ISO-Norm 31000 orientiert, und ein Compliancemanagement-System (CMS), das sich an der ISO-Norm 37301 orientiert. Sie informiert den Eigner über die wichtigsten Unternehmensrisiken und die Schwerpunkte im CMS.»[69]

---

[64] Die Abgrenzungen zwischen Eventualverbindlichkeiten und Risiken gelten erst recht für sogenannte Rückstellungen. Rückstellungen werden gebildet und in der Bilanz ausgewiesen, wenn sich ein gut quantifizierbarer Mittelabfluss aufgrund eines konkreten Sachverhalts mit grosser Wahrscheinlichkeit (>50%) realisieren wird. Eine Erfassung und Steuerung im Rahmen des Risikomanagements ist aufgrund der wahrscheinlichen Realisierung nicht mehr angezeigt.

[65] Zur Corporate Governance des Bundes: Vgl. Bericht des Bundesrates vom 13. September 2006 zur Auslagerung und Steuerung von Bundesaufgaben (Corporate-Governance-Bericht, BBl *2006* 8233); Zusatzbericht des Bundesrates vom 25. März 2009 zum Corporate-Governance-Bericht – Umsetzung der Beratungsergebnisse des Nationalrats (Zusatzbericht, BBl *2009* 2659); Erläuternder Bericht der Eidgenössischen Finanzverwaltung vom 13. September 2006 zum Corporate-Governance-Bericht des Bundesrates (Erläuternder CG-Bericht EFV).; Bericht des Bundesrates vom 26. Mai 2021 in Erfüllung des Postulates Abate 18.4274 (Eignerstrategie des Bundesrates für die verselbständigten Einheiten des Bundes).

[66] Zusatzbericht, Ziff. 6.2, Leitsatz 16.

[67] Zum Begriff: Erläuternder CG-Bericht EFV, Ziff. II/2.

[68] Art. 8 Abs. 5 RVOG

[69] Mit dieser elastischen Formulierung («…orientiert…») lässt das Ziel bewusst gewisse Spielräume, so dass auch andere international anerkannte Normen – namentlich die US-amerikanische Norm COSO (Committee of Sponsoring Organizations of the Treadway Commission) – angewendet werden können. Solche Ausnahmefälle sind gemäss der «comply or explain»-Regel zu begründen.

Die Zielerreichung beurteilt der Bundesrat anhand eines Audits, das (1) einmal pro Strategieperiode durch eine fachkompetente externe Prüfgesellschaft durchzuführen ist, (2) vom obersten Leitungsorgan des Unternehmens in Auftrag gegeben wird und (3) dessen Bericht das oberste Leitungsorgan dem Bundesrat zur Kenntnis vorlegt. Die Eckpunkte zur Durchführung des Audits – namentlich Prüfumfang, Prüfziele und Prüfkriterien – hält der Eigner in einem «Referenzdokument» zu Handen des obersten Leitungsorgans fest. Zu den zentralen Prüfzielen zählt zum einen die Bestätigung, dass Risiko- und Compliancemanagement nach der angewendeten Norm angemessen implementiert sind (design effectiveness), sowie die Beurteilung, ob diese Systeme auch in der Praxis wirksam funktionieren (operating effectiveness). Stand, Umsetzung und aktuelle Fragen zu ERM und CMS werden an den Eignergesprächen zwischen den zuständigen Departementen/EFV und Führunsspitze des Unternehmens in der Regel am ersten Gesprächstermin in der Jahresagenda behandelt.

Übernimmt der Bund gegenüber einzelnen verselbständigten Einheiten spezifische Haftungen, Garantien, Bürgschaften und Eventualverpflichtungen, müssen eingehendere risikopolitische Vorgaben (z. B. Vorgaben zur Vermeidung oder Verminderung bestehender Risiken, Versicherungspflicht, Reservenbildung) gemacht und deren Einhaltung regelmässig überprüft werden[70].

Das Risikomanagement des Bundes steht den Unternehmen und Anstalten des Bundes bei methodischen Fragen und Themen rund ums Risiko- und Compliancemanagement zur Verfügung. Der regelmässige Erfahrungsaustausch trägt dazu bei,dass diese Managementsysteme sowohl bei den Bundesunternehmen als auch in der Bundesverwaltung verbessert werden.

Schnittstellen zum Risikomanagement

Organisatorisch bestehen keine Schnittstellen zwischen dem Risikomanagement des Bundes und den Managementsystemen der Bundesunternehmen und Anstalten; Zuständigkeiten und Verantwortung sind klar getrennt. Inhaltlich können aber Überschneidungen bestehen:

- Bestehen spezifische Haftungen, Garantien und Bürgschaften des Bundes (z. B. in Bezug auf die Ausfallhaftung gemäss Art. 19 VG) für die verselbständigten Einheiten, so sind sie zwingend Gegenstand des Risikomanagements des Bundes.
- Auch wenn keine spezifischen Haftungen, Garantien und Bürgschaften des Bundes bestehen, kann sich dieser im Einzelfall veranlasst sehen, bei einer Veränderung der Risikosituation bei verselbständigten Einheiten, deren Risikofähigkeit zu stärken (z. B. Rekapitalisierung).
- Durch die Eigner- und Gewährleistungsfunktion des Bundesrates und die damit verbundenen Steuerungs- und Kontrollaufgaben bleibt letztlich die Verantwortung für die wirtschaftliche Leistungsfähigkeit und die Erfüllung der übertragenen Aufgaben beim Bundesrat, der auch nach einer Verselbständigung die politische Gesamtverantwortung und die damit verbundenen Eignerrisiken trägt[71].

Notwendiger Informationsaustausch

Ein Austausch ist sinnvoll mit Blick auf

- methodische Themen rund um das Risiko- und Compliancemanagement (auf fachlicher Ebene);
- Umsetzungsstand der Zielerreichung ERM und CMS sowie Risiken des Bundes, die sich direkt aus der Eigner- und Gewährleistungsfunktion sowie der politischen Gesamtverantwortung des Bundesrates ergeben (Eignergespräche).

[70] Corporate-Governance-Bericht, Ziff. 4.2.4 a. E., Leitsatz 12; Erläuternder CG-Bericht EFV, Ziff. I/5.4. Diese umfassendere Überprüfung kann allenfalls im Rahmen eines entsprechenden Auftrages durch die Revisionsstelle erfolgen.

[71] Art. 8 Abs. 4 RVOG

6.7 Versicherungsmanagement

Der Bund trägt als sog. Eigenversicherer das Risiko für Schäden an seinen Vermögenswerten und für die haftpflichtrechtlichen Folgen seiner Tätigkeit grundsätzlich selbst[72]. Ausnahmsweise kann ein Risiko durch den Abschluss eines Versicherungs- oder Schadenerledigungsvertrages mit einem Dritten bewirtschaftet werden, insb. wenn das Risiko ein hohes Schadenpotenzial aufweist, das Fachwissen für die Schadenerledigung in der Bundesverwaltung fehlt oder wenn die Risikoüberwälzung wirtschaftlich ist.[73] Beim Abschluss von Versicherungen ist zu beachten, dass die Vertragskonditionen ein optimales Preis-Leistungs-Verhältnis aufweisen und den Marktverhältnissen entsprechen. Die Koordinationsstelle Risikomanagement in der EFV ist in der Bundesverwaltung gleichzeitig die zentrale Versicherungsstelle. Die Risikominimierungsmassnahme «Risikotransfer» liegt damit in ihrer ausschliesslichen Zuständigkeit. Anträge von OE auf Abschluss eines Versicherungsvertrages geben der Koordinationsstelle zudem nützliche Hinweise auf Risikoexponierungen in der Bundesverwaltung.

Schnittstellen zum Risikomanagement:
Die Koordinationsstelle Risikomanagement in der EFV ist in der Bundesverwaltung gleichzeitig die zentrale Versicherungsstelle.

6.8 Bundesamt für Cybersicherheit (BACS)

Das *Bundesamt für Cybersicherheit* (BACS) ist das Kompetenzzentrum für Cyberbedrohungen in der Schweiz und für die Cybersicherheit des Bundes verantwortlich. Es erarbeitet Informatik-Sicherheitsvorgaben, berät die Verwaltungseinheiten bei deren Umsetzung und erhebt den Stand der Informatiksicherheit in den Departementen und der Bundeskanzlei.

Namentlich verantwortet das BACS auch die bundesweite Koordination der Steuerung von Cyberrisiken: Im Rahmen dieser Aufgabe führt das BACS das strategische Cyberrisiko des Bundes; dabei werden die Erkenntnisse aus den einzelnen Cyberrisiken, die von den verschiedenen IKT-Leistungserbringern geführt werden, ebenso berücksichtigt wie die Risikomassnahmen aus der nationalen Cyberstrategie (NCS).

Risikoeigner des strategischen Cyberrisikos ist der Direktor des Bundesamtes für Cybersicherheit. In seiner Funktion ist er verantwortlich, dass die wesentlichen Cyberbedrohungen in der Kerngruppe Cyber[74] (KG-Cy) adressiert werden, wo sie departementsübergreifend auf strategischer Ebene angegangen werden. Er sorgt gleichsam für eine hohe Visibilität der Bundesaktivitäten im Bereich Cyberrisiken.

Schnittstelle Cybersicherheit des Bundes

Die Anforderungen an die Cybersicherheit, um für die IT-Schutzobjekte der Bundesverwaltung einen angemessenen Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit zu gewährleisten, sind in der Informationssicherheitsverordnung (ISV) über die Informationssicherheit in der Bundesverwaltung und der Armee[75] und in den darauf basierenden Vorgaben des BACS zum Sicherheitsverfahren festgelegt. Die Sicherheitsmassnahmen orientieren sich an den jeweils aktuellen ISO-Standards betreffend die IT-Sicherheitsverfahren. Die Zuständigkeit für die Umsetzung der IT-Sicherheitsanforderungen liegt bei den einzelnen VE. Die Risiken aus IT-Projekten und aus dem IT-Betrieb werden identifiziert, bewertet und durch angemessene Massnahmen im Rahmen des Sicherheitsverfahrens reduziert

[72] Art. 50 Abs. 2 FHV
[73] Vgl. Weisungen der EFV vom 11.09.2015 über die Risikotragung und Schadenerledigung im Bund, Ziff. 1.2.
[74] In der Kerngruppe Cyber sind vertreten: NCSC (Vorsitz), fedpol, NDB sowie GS-VBS.
[75] SR 128.1

bzw. eliminiert. Restrisiken müssen der Leitung der VE bekannt sein und von ihr bewusst in Kauf genommen werden. Basierend auf einer strukturierten Umfrage bei den Informatiksicherheitsbeauftragten auf Stufe Departement (ISBD) und Bundeskanzlei deklarieren diese den Stand der Informatiksicherheit ihrer jeweiligen Departemente sowie der Bundeskanzlei. Diese Selbstdeklarationen werden durch das BACS plausibilisiert und anschliessend verfasst das BACS zuhanden des Bundesrates jährlich den Bericht zum Stand der Informatiksicherheit in der Bundesverwaltung. Es muss sichergestellt werden, dass in diesem Bericht aufgeführte wesentliche Risiken im Rahmen des Risikomanagements analysiert werden.

Schnittstellen zum Risikomanagement

Abweichungen zu den IT-Sicherheitsvorgaben können die Aufgabenerfüllung oder Zielerreichung der Bundesverwaltung gefährden. Der periodische Bericht des BACS zum Stand der Informatiksicherheit in der Bundesverwaltung kann für das Risikomanagement Bund wertvolle Informationen enthalten. Umgekehrt ist es auch möglich, dass aufgrund der Risikoberichterstattung der Bericht des BACS komplementiert werden kann.

Notwendiger Informationsaustausch

Periodischer Abgleich zwischen der Koordinationsstelle Risikomanagement Bund, dem Risikomanager des Departementes und dem RM-Coach BACS (Stand der Informatiksicherheit in der Bundesverwaltung), gegenseitige Orientierung bei besonderen Vorkommnissen, Sicherstellung des Wissensaustausches und departementsübergreifende Behandlung von wesentlichen Cyberrisiken durch die Kerngruppe Cyber (KG-Cy).

6.9 Digitale Transformation und IKT-Lenkung (DTI)

Der Bereich DTI der Bundeskanzlei erlässt als Kompetenzzentrum für Fragen der Digitalisierung Vorgaben, initiiert eigene Digitalisierungsprojekte oder unterstützt Vorhaben von Departementen und Ämtern. Er sorgt für eine departementsübergreifende Sicht auf die Vorhaben, Mittel und Verwaltungsleistungen der digitalen Transformation und der IKT in der Bundesverwaltung.

Schnittstelle DTI-Schlüsselprojekte der Bundesverwaltung

Sogenannte DTI-Schlüsselprojekte der Bundesverwaltung sind IKT-Projekte oder IKT-Programme, die aufgrund ihres Ressourcenbedarfs, ihrer strategischen Bedeutung, ihrer Komplexität, ihrer Auswirkungen oder ihrer Risiken eine verstärkte übergeordnete Führung, Steuerung, Koordination und Kontrolle erfordern. Die Aufgaben und Verantwortlichkeiten im Zusammenhang mit den IKT-Schlüsselprojekten sind in den Weisungen des Bundesrates vom 16. März 2018 zu den IKT-Projekten in der Bundesverwaltung und zum IKT-Portfolio des Bundes geregelt. Zuständig für die Festlegung von Schlüsselprojekten ist der Bundeskanzler, nach Konsultation der GSK.

Die Verantwortlichen der Schlüsselprojekte erstatten zuhanden des Bereichs DTI halbjährlich einen Statusbericht, welcher die für die Oberaufsicht relevanten Informationen umfasst. Der Bereich DTI erstellt daraus einen konsolidierten Bericht über den Stand aller Schlüsselprojekte, der von der GSK zur Kenntnis genommen wird und anschliessend an die Geschäftsprüfungskommissionen und die Finanzdelegation der eidgenössischen Räte weitergeleitet wird. Der Bereich DTI kann Massnahmen vorschlagen. Der Bundeskanzler entscheidet nach Anhörung der GSK, ob er diese Massnahmen dem Bundesrat zum Beschluss unterbreiten möchte.

Nach Ziffer 4.4 Weisungen des Bundesrates vom 16. März 2018 zu den IKT-Projekten in der Bundesverwaltung und zum IKT-Portfolio des Bundes ist es Aufgabe der zuständigen VE,

die Risiken ihrer Schlüsselprojekte nach den Vorgaben des Risikomanagements Bund zu identifizieren, zu analysieren und zu bewerten. Sie melden und überwachen jene Risiken, die wesentliche negative Auswirkungen auf die Erreichung der Ziele und die Erfüllung der Aufgaben der Bundesverwaltung haben können. Damit sichergestellt ist, dass schwerwiegenden Problemen bei Schlüsselprojekten auch aus Sicht des Risikomanagements Bund nachgegangen wird, meldet die Koordinationsstelle Risikomanagement Bund in der EFV den Risikomanagern der betroffenen Departemente raschmöglichst alle «roten» Projekte auf dem Controlling-Bericht des Bereichs DTI. Der Risikomanager klärt ab, ob das rote Schlüsselprojekt als Risiko erfasst, korrekt analysiert und wie es zu bewerten ist. Er informiert anschliessend die Koordinationsstelle Risikomanagement Bund über den Stand aus Sicht Risikomanagement Bund.

Schnittstellen zum Risikomanagement

Probleme im Zusammenhang mit grösseren Digitalisierungs- und IKT-Projekten können die Aufgabenerfüllung oder Zielerreichung der Bundesverwaltung gefährden. Die halbjährliche Statusübersicht über die DTI-Schlüsselprojkete kann für das Risikomanagement Bund wertvolle Informationen enthalten, da sie sich auf die umfangreichsten und potentiell risikoreichsten IKT-Vorhaben konzentriert. Umgekehrt ist es auch möglich, dass aufgrund der Risikoberichterstattung Lücken in der Statusübersicht des Bereichs DTI festgestellt werden.

Notwendiger Informationsaustausch

Periodischer Abgleich zwischen der Koordinationsstelle Risikomanagement Bund, den Risikomanagern der betroffenen Departemente und der DTI-Berichterstattung (Statusübersicht über die DTI-Schlüsselprojekte der Bundesverwaltung), gegenseitige Orientierung bei besonderen Vorkommnissen, Sicherstellung des Wissensaustausches.

6.10 Eidgenössische Finanzkontrolle (EFK)

Die Eidgenössische Finanzkontrolle (EFK) ist das oberste Finanzaufsichtsorgan des Bundes. Sie unterstützt das Parlament und den Bundesrat, ist unabhängig und nur Verfassung und Gesetz verpflichtet. Der Aufgabenbereich ist im Finanzkontrollgesetz (FKG) geregelt. Die EFK prüft das Finanzgebaren der Bundesverwaltung und zahlreicher halbstaatlicher und internationaler Organisationen. Massgebend bei ihren Prüfungen sind die Kriterien der Wirtschaftlichkeit und Wirksamkeit, der Ordnungs- und Rechtmässigkeit.

In ihrem Bericht zum Informatikprojekt «INSIEME» haben die Finanz- und Geschäftsprüfungskommissionen dem Bundesrat empfohlen, dass die jährliche Berichterstattung der EFK über wichtige Umsetzungspendenzen («Revisionspendenzen») – d. h. alle offenen Empfehlungen der höchsten Wichtigkeitsstufe – angemessen in das Risikomanagement des Bundes sowie in das jährliche Risikoreporting des Bundesrates an die GPK einfliessen sollen. Der BR wies in seiner Stellungnahme[76] daraufhin, dass Umsetzungspendenzen Hinweise über eine ungenügende Aufgabenerfüllung oder Zielerreichung der Bundesverwaltung beinhalten können. Er hat die Empfehlung deshalb angenommen. Sie wird seit 2015 entsprechend umgesetzt.

Jede VE bzw. jedes Departement ist im Rahmen des Risikomanagementprozesses dafür verantwortlich, dass die (wichtigsten) Revisionspendenzen im Risikomanagement berücksichtigt werden (normaler Prozess). Als zusätzliches Controllinginstrument werden die Umsetzungspendenzen einmal jährlich zwischen der EFK und der Koordinationsstelle Risikomanagement Bund besprochen. Resultate aus diesem Validierungsgespräch fliessen anschliessend mittels

[76] Vgl. BBl *2015* 6745

Rückfragen der EFV zurück an die entsprechenden VE resp. das entsprechende Departemente. Dadurch ist sichergestellt, dass der Austausch sowohl über den ordentlichen Prozess, als auch durch Rückfragen der Koordinationsstelle Risikomanagement Bund optimiert wird.

Schnittstellen zum Risikomanagement

Revisionspendenzen der EFK können Hinweise auf eine ungenügende Aufgabenerfüllung oder Zielerreichung der VE und Departemente enthalten und sind daher im Rahmen des Risikomanagement-Prozesses zu berücksichtigen.

Notwendiger Informationsaustausch

Abgleich mit dem jährlichen Bericht der EFK über die wichtigsten Umsetzungspendenzen («Revisionspendenzen Prio. A»).

6.11 Weitere Schnittstellen

In der Bundesverwaltung existieren auch Projekte, die sich mit besonderen Themen des Risikomanagements beschäftigen. Der Informationsaustausch und die Abgrenzung werden im Anhang 8 erläutert. Dieser Anhang wird regelmässig aktualisiert.

7 Verbesserung des Risikomanagements Bund

Das Risikomanagement in der Bundesverwaltung wird stetig weiterentwickelt und verbessert.[77] Die Risikocoaches, die Risikomanager und die Koordinationsstelle EFV nutzen Erkenntnisse aus ihrer Risikomanagementtätigkeit in der Bundesverwaltung um Verbesserungen des Risikomanagements vorzuschlagen und allenfalls umzusetzen. Auf Stufe Bundesrat ist die Koordinationsstelle EFV zuständig für den Entscheid und die Umsetzung von Verbesserungsmassnahmen des Risikomanagements. Auch bundesverwaltungsexterne Inputs (z. B. Risikomanagementveranstaltungen) tragen dazu bei, Verbesserungspotential des bundesweiten Risikomanagements zu erkennen. Die Richtlinie und das vorliegende Handbuch werden nach Bedarf regelmässig angepasst.

7.1 Leistungsbewertung

Um das Risikomanagement in der Bundesverwaltung laufend zu verbessern, muss dessen Leistung regelmässig bewertet werden. Es können dabei zwei Dimensionen unterschieden werden: die inhaltliche Verbesserung, d. h. die Veränderung des Risikoprofils (der Gesamtheit der Risiken) der Bundesverwaltung und die organisatorische Verbesserung, d. h. inwiefern ein effektives Risikomanagement-System aufgebaut wurde und umgesetzt wird.

Bei der *inhaltlichen* Verbesserung können entweder auf risikoindividueller oder aggregierter Stufe Aussagen erarbeitet werden, wie stark das Risiko bzw. das aggregierte Risikopotential der Bundesverwaltung vermindert werden konnte. Da in der Bundesverwaltung auf eine quantitative Aggregation verzichtet wird, konzentriert sich das Risikomanagement Bund auf die grössten Einzelrisiken und darauf inwiefern diese reduziert werden konnten. Die Veränderungen der Risiken werden in den Berichterstattungen auf Stufe Bund, Departement / BK und VE dargestellt.

Bei der *organisatorischen* Verbesserung geht es um die Prüfung, wie weit der Aufbau eines effektiven Risikomanagement-Systems erfolgt ist und ob dieses in der Praxis umgesetzt wird. Diese Prüfung erfolgt meistens mit Hilfe eines Audits/Reviews. Zusätzlich sollte regelmässig untersucht werden, ob in einer Organisation allgemeine Strukturen und Eigenheiten vorliegen, welche die Effektivität des Risikomanagementprozesses beeinträchtigen und eine allmähliche Entwicklung von Risiken begünstigen können (vgl. Anhang 9).

7.2 Audit / Review

Ein wichtiger Ansatzpunkt für die Konsolidierung und Verbesserung des Risikomanagement-Systems ist die Durchführung eines Audits. Als Prüfstellen kommen grundsätzlich die Innenrevision oder die externe Revision in Frage; je nach Ressourcenlage kann auch ein spezialisierter externer Audit-Anbieter in Betracht gezogen werden. Bei der Prüfung des Risikomanagement-Systems stehen – ähnlich einer Beurteilung des Reifegrades – die folgenden Leitfragen im Vordergrund:

- Existiert ein Commitment der obersten Leitung, das Risikomanagement umzusetzen?
- Umfasst das Risikomanagement alle Bereiche der Bundesverwaltung?
- Existiert eine von der Leitung genehmigte Risikopolitik?
- Sind die Risikoeigner, Risikomanager und Risikocoaches benannt und nehmen sie ihre Aufgaben wahr?
- Existiert eine angemessene interne und externe Risikokommunikation?

[77] Ziff. 4 Abs. 8 der Weisungen über die Risikopolitik des Bundes

- Verfügen Risikomanager und Risikocoaches über die passende Eignung, Ausbildung und Erfahrung?
- Ist das Risikomanagement in wichtigen Prozessen der Bundesverwaltung integriert?
- Passen die verwendeten Methoden zu den Anwendungsgebieten?
- Sind die Risikobeurteilungen dokumentiert und von den Risikoeignern freigegeben worden?
- Sind Massnahmen zur Risikobewältigung umgesetzt und werden dies auf ihre Wirksamkeit überprüft?
- Wird die Wirksamkeit des Risikomanagements (inkl. die Aufgabenerfüllung durch die Koordinationsstelle EFV) regelmässig von einer unabhängigen Stelle bewertet?
- Ist das Risikomanagement-System gut dokumentiert, sind die Dokumente auffindbar und aktuell?

7.3 Zertifizierung

Bei ISO 31000:2018 handelt es sich um eine Richtlinie («Guideline»), und nicht um einen zertifizierbaren Standard.

Anhang 1: Begriffsdefinitionen (Glossar)

In diesem Anhang werden in alphabetischer Reihenfolge Begriffe definiert und erläutert, die im Risikomanagement Bund verwendet werden. Für die Funktionen und Verantwortlichkeiten im Risikomanagement Bund wird auf Ziffer 2.2 verwiesen. Die Begriffe werden im Rahmen vom Risikomanagement Bund einheitlich verwendet. Dadurch wird die Kommunikation verbessert und ein gemeinsames Verständnis geschaffen. Die nachfolgenden Definitionen lehnen sich im Allgemeinen an gängige Normen an. Diese enthalten weitere Begriffsdefinitionen, auf die hier verwiesen werden kann.

Akzeptiertes Risiko: Risiko, das z. B. aus technischen, praktischen oder wirtschaftlichen Gründen nicht (weiter) reduziert werden soll und somit getragen wird.

Auswirkung: Folge eines Ereignisses oder einer Entwicklung, die zu einer Beeinträchtigung der Ziele oder der Aufgabenerfüllung der Bundesverwaltung führt (Abweichung von ÖNORM 490x-Reihe). Die verschiedenen Auswirkungsdimensionen werden in Ziffer 3.3.4 näher erläutert.

Bedrohung: Potenzielle Quelle eines Risikos, die zu einer ungünstigen Entwicklung führen kann.

Bereichsrisiken: Alle auf Stufe Verwaltungseinheit identifizierten und bewirtschafteten Risiken.

Bottom-up-Ansatz: Vorgehensweise bei der Risikobeurteilung, bei der die Einzelteile der Organisation auf der untersten Stufe Gegenstand der Risikoidentifikation und der Risikoanalyse sind. Die Risiken werden entlang der Linienorganisation nach oben gemeldet und dort konsolidiert.

Brainstorming: Methode, bei der im Rahmen einer Gruppe eine Vielfalt von Ideen gesammelt, bewertet und geordnet wird. Das Sammeln der Ideen erfolgt ohne Einschränkungen, jegliche Kritik ist verboten. Bei der Bewertung und Ordnung geht es darum, problemferne Ideen auszusortieren und thematisch verwandte Ideen zu gruppieren.

Bundesratsrisiken: Die für den Bundesrat wichtigsten Risiken, die in einem Konsolidierungsprozess aus allen Risiken der Bundesverwaltung und nach Überprüfung durch die GSK an den Bundesrat gemeldet werden.

Bundesverwaltung: Sie untersteht dem Bundesrat und umfasst die Departemente und die Bundeskanzlei. Die einzelnen Departemente gliedern sich in Ämter, die zu Gruppen zusammengefasst werden können und sie verfügen je über ein Generalsekretariat. Zur Bundesverwaltung gehören ferner dezentralisierte VE nach Massgabe ihrer Organisationserlasse.[78]

Departementsrisiken: Alle von den VE an das Departement gemeldeten Risiken. Dies sind die grössten Risiken je VE und alle Risiken, die eine definierte Risikohöhe überschreiten.

Dynamische Risiken: beinhalten Massnahmen, welche die Auswirkung oder die Eintrittswahrscheinlichkeit zukünftig weiter reduzieren (Massnahmenstatus «eingeleitet» oder «beschlossen»).

Entwicklung: Eine allmähliche Veränderung von Umständen.

Ereignis: Plötzlicher Eintritt einer bestimmten Kombination von Umständen.

Gefahr: Potenzielle Quelle eines Risikos, die zu einem plötzlich eintretenden Schadenereignis führen kann.

Internes Kontrollsystem: Das IKS umfasst alle regulatorischen, organisatorischen und

[78] Art. 2 RVOG

technischen Massnahmen, die eingeführt werden, um identifizierte Risiken in der Organisation zu minimieren. Das IKS in der Bundesverwaltung konzentriert sich insbesondere auf die finanzrelevanten Geschäftsprozesse.

Kernrisiken: Alle von den Departementen und der Bundeskanzlei an die Koordinationsstelle EFV gemeldeten Risiken Dies sind die grössten Risiken je Departement / der BK und alle Risiken, die eine definierte Risikohöhe überschreiten.

Kontinuitätsmanagement (Business Continuity Management, BCM): Im Kontinuitätsmanagement werden alle notwendigen Vorkehrungen getroffen, damit die Bundesverwaltung und der Bundesrat ihre Kernaufgaben selbst in ausserordentlichen Situationen termingerecht erfüllen können (Abweichung von ÖNORM 490x-Reihe).

Krise: Situation, die organisationsweit ausserordentliche Massnahmen erfordert. Im Gegensatz zu einem Notfall bezieht sich eine Krise auf eine Organisation: eine Organisation (oder System/Institution) befindet sich in einer Krise, wenn ihre Reputation (Glaubwürdigkeit, Vertrauen), ihr Handlungsspielraum oder ihre Existenz gefährdet ist.

Krisenfrüherkennung: Auseinandersetzung mit Ereignissen und Trends, die bereits sichtbar sind und ein Potenzial besitzen, sich meist in einer Zeitspanne von Monaten bis max. 1,5 Jahren zu Krisen zu entwickeln.

Massnahmenverantwortlicher: Person, die für die konkrete Umsetzung einer Massnahme zur Reduktion eines Risikos verantwortlich ist und vom Risikoeigner einen entsprechenden Auftrag erhält.

Nettorisiko: Der Teil eines Risikos, der nach Umsetzung von Risikobewältigungsmassnahmen verbleibt.

Notfall: Plötzliches und für gewöhnlich unvorhergesehenes Ereignis mit schwerwiegenden negativen Folgen, das ein rasches Eingreifen erfordert. Im Gegensatz zu einer Krise bezieht sich ein Notfall auf ein Ereignis, das einen Schadenplatz anrichtet (geografisch abgrenzbar), der so schnell als möglich aufzuräumen respektive zu beheben ist.

Organisationseinheit: Gruppe von Personen und Einrichtungen mit einem Gefüge von Verantwortungen, Befugnissen und Beziehungen. Der Begriff OE kann sich auf die Bundesverwaltung als Ganzes, ein Departement / die BK, eine VE oder kleinere Einheiten beziehen.

Quellrisiko: Einzelrisiko, das mit anderen Risiken auf übergeordneter Ebene zu einem Querschnittsrisiko aggregiert wird.

Querschnittsrisiken*:* Ereignisse oder Entwicklungen, die sich beim Eintritt in mehreren VE gleichzeitig negativ auswirken oder unabhängig voneinander in mehreren VE gleiche oder ähnliche negative Auswirkungen auf die Aufgabenerfüllung und Zielerreichung haben können. *Beispiele:* Grossflächiger IKT-Ausfall, Pandemie, Erdbeben, Korruption etc.

Restrisiko[79]***:*** Im Risikomanagement Bund werden in den drei gängigen Anwendungsfällen präzisere Begriffe verwendet (Abweichung von ÖNORM 490x-Reihe): -> Akzeptiertes Risiko -> Nettorisiko -> Unerkanntes Risiko

Riskmap: Darstellung, in der Risiken entsprechend ihren Auswirkungen und der Eintrittswahrscheinlichkeit graphisch eingeordnet werden.

Risiko: Ereignisse und Entwicklungen, die mit einer gewissen Wahrscheinlichkeit eintreten

[79] Vgl. Brühwiler, Bruno (2011). *Risikomanagement als Führungsaufgabe*. (3., überarbeitete und aktualisierte Auflage). Bern: Haupt Verlag.

und wesentliche negative finanzielle und nichtfinanzielle Auswirkungen auf die Erreichung der Ziele und die Erfüllung der Aufgaben der Bundesverwaltung haben (Abweichung von ÖNORM 490x-Reihe).[80]

***Risikoaggregation**:* Verfahren, das mehrere Risiken auf übergeordneter Ebene zusammenfasst. Die Berichterstattung und zum Teil die Bewirtschaftung des aggregierten Risikos (übergreifende Massnahmen) erfolgen dann auch auf übergeordneter Ebene. *Beispiel:* Ein IKT-Ausfall in der EFV und einer in der ESTV können aggregiert werden, wenn bei beiden Risiken die Ursache dieselbe ist, z. B. ein Stromunterbruch im Gebäude, in welchem beide Systeme betrieben werden.

Risikoaggregation (quantitativ) [81]***:*** Verfahren, welches das Zusammenwirken mehrerer, voneinander evtl. abhängiger Einzelrisiken zu einem Gesamtrisiko (VaR) ermittelt und aufzeigt.

Risikoakzeptanz: Entscheidung, ein spezifisches Risiko zu tragen (s. auch → *Risikotoleranz*).

Risikoakzeptanzschwelle: Pro OE definierte Risikohöhe, ab der Bewältigungsmassnahmen ins Auge gefasst werden sollen.

Risikoart: Unterteilung von Risiken nach unterschiedlichen Kriterien.

Risikobeauftragte: Sammelbezeichnung für Risikomanager und Risikocoaches in der Bundesverwaltung.

Risikobeurteilung: Prozess, der die Ergebnisse der Risikobewertung mit der Risikotoleranz vergleicht, um zu bestimmen, ob die Risikohöhe akzeptierbar bzw. tolerierbar ist (Abweichung von ÖNORM 490x-Reihe).

Risikobewältigung: Auswahl und Umsetzung von Massnahmen, um ein Risiko zu vermeiden oder zu vermindern. Das Notfall-, Krisen- und Kontinuitätsmanagement sind auch Bestandteile der Risikobewältigung.

Risikobewertung: Systematische Ermittlung und Gebrauch von Informationen, um ein Risiko zu verstehen und nach Eintrittswahrscheinlichkeit und Auswirkungen auf die Bundesverwaltung einzuschätzen (Abweichung von ÖNORM 490x-Reihe).

Risikocoach: Person, die den Risikomanagement-Prozess auf Stufe VE anwendet und umsetzt und für die Einbettung des Risikomanagements in der VE zuständig ist.

Risikoeigner: Person mit der Entscheidungskompetenz und Verantwortung, das Risiko zu steuern. Soweit diese Voraussetzung erfüllt ist, kann der Risikoeigner hierarchisch auf allen (Kader-)Stufen innerhalb der Bundesverwaltung angesiedelt sein.

Risikohöhe: Ausmass des Risikos, geschätzt oder gemessen, als bestimmte Kombination von Auswirkungen und Eintrittswahrscheinlichkeit.

Risikoidentifikation: Prozess, um Risiken zu finden und mit ihren Ursachen und Auswirkungen zu beschreiben.

Risikokategorie: Eine Unterteilung der Risiken in thematische Gruppen.

Risikokommunikation: Andauernder oder wiederkehrender Prozess, um Informationen bezüglich des Umgangs mit Risiken mit den interessierten Parteien auszutauschen.

[80] Ziff. 2 Abs. 1 der Weisungen über die Risikopolitik des Bundes

[81] Beispielsweise mit einer Monte Carlo-Simulation.

Risikokonsolidierung: Verfahren, das mehrere, unabhängig voneinander identifizierte Einzelrisiken aufgrund ihrer Art oder Bedeutung aggregiert, gruppiert oder selektioniert.

Risikokultur: Betriebsklima, in welchem alle Mitarbeitenden und jede Führungskraft einen bewussten Umgang mit Risiken und eine positive Fehlerkultur pflegen.

Risikomanagement-Prozess: Systematische Anwendung von Grundsätzen, Verfahren und Tätigkeiten, um über Risiken zu kommunizieren, Informationen auszutauschen, Zusammenhänge zu erstellen, Risiken zu identifizieren, zu analysieren, zu bewerten, zu bewältigen und zu überwachen.

Risikomanager: Person, die den Risikomanagement-Prozess auf Stufe Departement / BK anwendet und umsetzt sowie für die Einbettung des Risikomanagements im Departement / BK zuständig ist.

Risikopolitik: Absichten und Ziele des Bundesrates betreffend den Umgang mit Risiken. Die Risikopolitik wurde vom Bundesrat in der Form von verbindlichen Weisungen erlassen.

Risikorichtlinie: Verbindliche Vorgabe der EFV, wie das Risikomanagement in der Bundesverwaltung umzusetzen und laufend zu verbessern ist.

Risikotoleranz: Annahme eines Risikos im Rahmen der gesetzlichen bzw. regulatorischen Vorgaben.

Risikoverminderung: Entscheidung über und Umsetzung von Massnahmen, um die Eintrittswahrscheinlichkeit oder die Auswirkungen eines Risikos günstig zu beeinflussen.

Statische Risiken; sind Restrisiken, welche in der aktuellen Ausprägung mit bestehenden flankierenden Vorkehrungen (mögliche, laufend durchgeführte, umgesetzte oder abgelehnte Massnahmen) akzeptiert sind. Diese werden in der Regel im Rahmen des Tagesgeschäfts noch überwacht, eine weitere Risikoreduktion ist jedoch nicht beabsichtigt.

SMART: Die SMART-Regel ist eine Methode, mit deren Hilfe sich Ziele auf ihre klare und konkrete Formulierung hin überprüfen lassen. Die Ziele müssen **S**pezifisch, **M**essbar, **A**ttraktiv, **R**ealistisch und **T**erminiert sein.

Szenario: Konkrete und bildhafte Darstellung eines Risikos mit Annahmen über mögliche Zusammenhänge von Ursachen und Abfolgen von Ereignissen oder Entwicklungen, die aufzeigt, wie sich Bedrohungen/Gefahren in der Bundesverwaltung verwirklichen können.

Topdown-Ansatz: Vorgehensweise bei der Risikobeurteilung, bei der die Gesamtheit der Organisation oder des Systems Gegenstand der Risikoidentifikation und -analyse ist.

Unerkanntes Risiko: Risiko einer Organisation, das trotz einer adäquaten Risikoidentifikation unerkannt bleibt und deshalb nicht bewirtschaftet werden kann.

Unsicherheit: Zustand fehlender Information bezüglich des Eintritts zukünftiger Ereignisse oder Entwicklungen, ihrer Auswirkungen und ihrer Wahrscheinlichkeit.

Value-at-Risk: Schadenhöhe, die bei einer bestimmten, genügend hohen Wahrscheinlichkeit (z. B. 95% oder 99%) nicht überschritten wird.

Verwaltungseinheit: Ämter der Bundesverwaltung. Sie besorgen die Verwaltungsgeschäfte.[82]

Wahrscheinlichkeit: Relative Häufigkeit des Eintritts zukünftiger Ereignisse oder Entwicklungen (objektive Definition). Unsicherheit von Aussagen bzw. Grad an persönlicher Über-

[82] Art. 43 Abs. 1 RVOG

zeugung betreffend den Eintritt eines Ereignisses oder einer Entwicklung (subjektives Verständnis). Die Wahrscheinlichkeit eines Risikos kann sich auf eine Periode (z. B. Jahreswahrscheinlichkeit) oder auf eine Anzahl von Fällen (Fall-Wahrscheinlichkeit) beziehen.

Wechselwirkungen: Gegenseitige Abhängigkeiten oder Beeinflussungen zwischen einzelnen Risiken.

Anhang 2-1: Mustervorlage Detailbericht

R3	<Risikotitel> Prägnanter, sprechender Risikotitel	<Risikoeigner> Person, die Aufgabe/Risiko steuert	<VE>	<Dept>
<Risikotyp> (z.B. Kernrisiko, Bundesratsrisiko → automatisch)			Stand:	<Datum>

Allgemeine Hinweise

Methodisch: Aufgaben und Ziele des Bundes sind massgebend (Risikodefinition), Risiko **mit Blick auf Steuerung** angemessen eingrenzen (Flughöhe), Risikokontext und -faktoren präzis analysieren und begreifen. Detaillierte Infos in Handbuch Kapitel 3.2.

Formal: Texte kurz, aussagekräftig; Fachjargon vermeiden, Abkürzungen bei erster Verwendung ausschreiben. **Der Text soll von Aussenstehenden rasch und klar verstanden werden können.** Wichtigste Adressaten sind Amtschefs/innen, Generalsekretäre/innen, Departementschef/innen, Eidg. Räte.

Aufgabe / Ziel — max. 700 Zeichen

- Übergeordnete Aufgabe/Ziel(e) kurz umreissen, die vom Risiko betroffen sind (Fundstelle Gesetz, Verordnung, BRB angeben)

→ **Zweck:** Zuständigkeit feststellen (AKV).

Worst Case — max. 1100 Zeichen

- Knappe Schilderung des schlimmst möglichen Falls, der sich bei Risikoeintritt zutragen könnte. **Verständlichkeit und Plausibilität sind besonders wichtig.**

→ **Zweck:** Gegenstand der Risikobewertung.

Ursachen

- Die wichtigsten Ursachen, die in der Risikoanalyse im Regelfall bereits aufgeführt sind, werden hier nochmals stichwortartig genannt und allenfalls kurz beschrieben.
- Form: <Risikoursache 1 (evtl. knappe Beschreibung)>

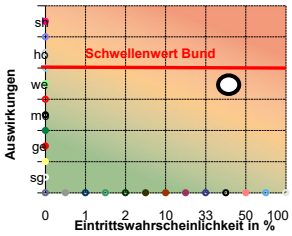
→ **Zweck:** Die Ursachen sind Ansatzpunkte für Massnahmen zur Senkung der Eintrittswahrscheinlichkeit. Die stichwortartige Auflistung gibt einen raschen Überblick.

Analyse — max. 2500 Zeichen

- Knappe Erläuterung, worin das Risiko besteht, d.h. das Risiko mit seinen Ursachen, Auswirkungen, Einflussfaktoren erklären.
- Mögliche Leitfragen: Welches Ereignis oder welche Entwicklung kann sich aus welchen Gründen zutragen? Was sind die zentralen Ursachen? Welche Faktoren und Bedingungen sind wichtig? Welche finanziellen und/oder nicht-finanziellen Auswirkungen sind bei Risikoeintritt zu erwarten, inwiefern und mit welchen Folgen können die Aufgaben bzw. Ziele nicht mehr erfüllt werden?

→ **Zweck:** Risiko verstehen.

Bewertung Worst Case



- ***Generelle Hinweise:*** *Bewertet wird das Worst Case Szenario unter Berücksichtigung aller aktiver Massnahmen (Nettorisiko!) → gegebene reale Bedingungen sind massgebend.*
- *Falls dem Risiko ein Primärereignis zugrunde liegt (z.B. Naturereignis wie Hochwasser), wird nur das Risiko bewertet, das **für den Bund** daraus entsteht. Die Auswirkungen beziehen sich auf Bund (Ausnahmen: Personenschäden, Umwelt).*

→ ***Zweck Erläuterungen:*** *Bewertung nachvollziehbar machen.*

Erläuterung Eintrittswahrscheinlichkeit EW — max. 700 Zeichen

- *Knappe Erläuterung der Grundlagen, Annahmen oder Vergleiche, welche der EW zugrunde gelegt werden.*

Erläuterung Auswirkungen AW — max. 600 Zeichen je Dimension

[Dimensionen: finanziell, Personenschäden, Reputation/Vertrauen, Unterbruch Geschäftsprozesse, Umwelt]

- *Knappe Erläuterung der Grundlagen, Annahmen oder Vergleiche, welche der AW zugrunde gelegt werden.*
- *Jede relevante AW-Dimension ist zu bewerten / zu erläutern. Massgebend für die AW-Bewertung des Risikos ist die AW-Dimension mit der höchsten Bewertung (Maximalprinzip).*
- *Finanzielle AW sowie mindestens eine nicht-finanzielle AW-Dimension sind Pflicht.*

Erläuterung Bewertungsänderung — max. 700 Zeichen

- *Soweit die EW und/oder die finanzielle AW und/oder eine nichtfinanzielle AW geändert wurde: kurze Begründung.*

Aktive Massnahmen

- **Generelle Hinweise:** Massnahmen werden ergriffen, um das Risiko hinsichtlich EW (Prävention Ursachen) und/oder mit Blick auf das Schadenausmass (Verkürzung und Milderung AW) zu senken. Analyse, Worst Case, Bewertung und Massnahmen bilden ein logisches Ganzes.
- **Status aktive Massnahmen: eingeleitet** = in Gang; **beschlossen** = grünes Licht, noch nicht gestartet; **Inaktive Massnahmen: umgesetzt** = abgeschlossen; **abgelehnt** = geprüft und verworfen **möglich** = Entwurf liegt vor, nicht beschlossen; **laufend durchgeführt** = wiederkehrend..
- **Beurteilung und Kommentar: Umsetzung** = Vergleich zu Plan; **Wirksamkeit** = realistische, transparente Einschätzung der erwarteten Wirkung.

1.	<Massnahmentitel> prägnanter, sprechender Titel	<Massnahmeneigner/in> verantwortliche Person	<Termin>	<Status>

- **Kurzbeschreibung:** Worin besteht die Massnahme, Fokus auf Eckpunkte, keine Details/Diskussionen/Projektpläne. ermöglicht den Lesenden, die Massnahme rasch zu verstehen und einzuordnen.

Beurteilung	1	2	3	4	Kommentar Massnahmenverantwortliche/r
Umsetzung 1 = plangemäss; 2 = leicht verzögert 3 = erheblich verzögert.; 4 = stark verzögert	☒	☐	☐	☐	▪ Knappe Erläuterung der Beurteilung. Gründe für (kritische) Beurteilung, Verbesserungsvorschläge, Handlungsempfehlungen (in Stichworten). ▪ Wichtig: möglichst faktenbasiert, ungeschönt und transparent.
Wirksamkeit 1 = hoch; 2 = eher hoch; 3 = eher schwach; 4 = schwach	☐	☐	☒	☐	

Anhang 2-2: Mustervorlage Kompaktbericht

1

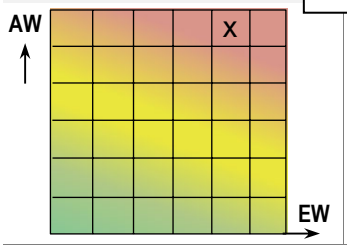
R4	<sprechender Kurztitel Risiko>	<Name Risikoeigner/in>	<VE>	<Dept>

2 **Risiko**

Worst Case **2a**

- ***Zweck:*** *Eckpunkte des Risikos verstehen.*
- ***Inhalt:*** *Schilderung des Risikoeintritts im Worst Case.*
- ***Form:*** *Knapp und verständlich, Fokus auf das Wesentliche.*
- ***Zeichenbegrenzung:*** *1100 Zeichen.*

Bewertung **2b**



Auswirkung AW
sehr hoch
Vorperiode → aktuell →

Wahrscheinlichkeit EW
wahrscheinlich
Vorperiode → aktuell →

Kommentar Risikoeigner/in **2c**

- ***Zweck:*** *Kommentar durch Risikoeigner/in.*
- ***Inhalt:*** *Kommentar zur Entwicklung des Risikos,*
  weitere wichtige Sachverhalte für das Verständnis des Risikos, Besonderheiten etc.
- ***Form:*** *Knapp, verständlich, wesentlich;*
  mit Aufzählungszeichen arbeiten.
- ***Zeichenbegrenzung:*** *1100 Zeichen.*

3 **Massnahmen**

Beurteilung Risikoeigner/in (1 = trifft vollständig zu; 4 = trifft nicht zu) **3a**

	1	2	3	4
Umsetzung verläuft nach Plan	☒	☐	☐	☐
Massnahmen sind wirksam und ausreichend	☐	☒	☐	☐

Würdigung/Kommentar Risikoeigner/in **3b**

- ***Zweck:*** *Kommentar durch Risikoeigner/in*
- ***Inhalt:*** *Würdigung, Kommentierung der Beurteilung in 3a (Umsetzung, Wirksamkeit)*
- ***Form:*** *Knapp, verständlich, wesentlich;*
  mit Aufzählungszeichen arbeiten.
- ***Zeichenbegrenzung:*** *1100 Zeichen.*

Erläuterungen

Die vorliegende Darstellung zeigt das Format für die Risikoberichterstattung an den Bundesrat. Der Bericht fokussiert auf die Kerninformationen des Risikos und seiner Massnahmen. Stufengerechte, d.h. knappe und konzise Texte erlauben es dem Bundesrat und den Mitgliedern der GSK, rasch das Wesentliche zu erfassen und zu verstehen. Dazu gehört eine Titelseite, die mit Risikomatrix und Risikoliste eine Übersicht über das gesamte Risikoportfolio gibt.

Hinweise zu den einzelnen Feldern:

1 **Titelblock** mit Risikonummer, Risikotitel, Risikoeigner/in sowie Verwaltungseinheit und Departement.

2 **Block Risiko**

2a **Worst Case:** Knappe Schilderung des Szenarios bei einem Risikoeintritt (Ereignis oder Entwicklung). Auch soll das Risiko hier in seinen Kernpunkten verständlich werden – GSK und Bundesrat sollen nachvollziehen können, worin das Risiko besteht, worum es geht und was geschieht. (max.1100 Z.)

2b **Bewertung:** Die Bewertungsinfos werden von der Software aufgrund der Bewertungseingaben automatisch erzeugt.

2c **Kommentar Risikoeigner/in:** Hier kommentiert und erläutert der/die Risikoeigner/in wichtige Sachverhalte und Besonderheiten des Risikos (z.B. zu Risikoentwicklung und Dynamik. Falls es sich um ein Querschnittsrisiko mit x Quellrisiken handelt → eingangs Kommentar erwähnen. (max.1100 Zeichen)

3 **Block Massnahmen**

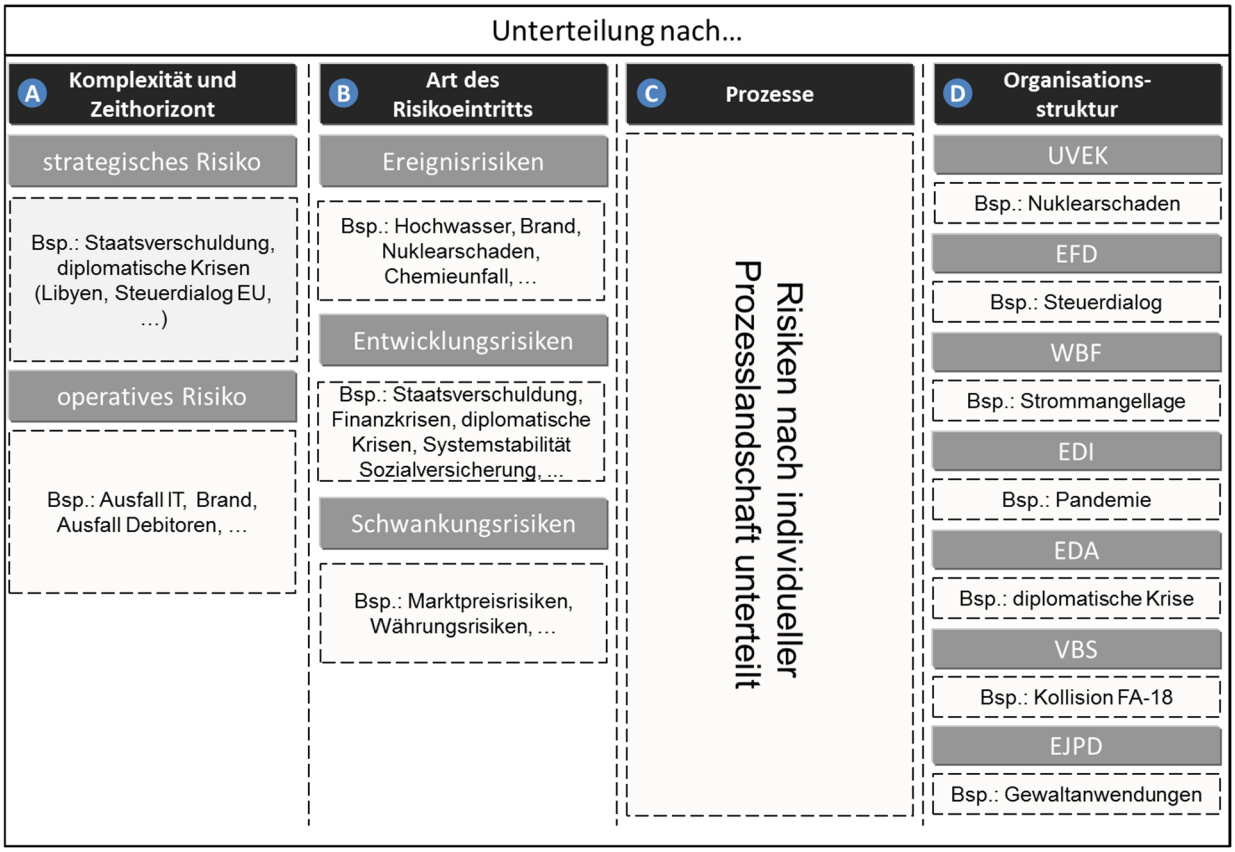
Hier beurteilt und kommentiert der/die Risikoeigner/in das gesamte aktive Massnahmen-Set.

3a **Beurteilung Massnahmen:** Auf einer Vierer-Skala werden die Massnahmen insgesamt beurteilt mit Blick auf die Umsetzung (plangemäss vs. Planabweichung) sowie Wirksamkeit (wirken die Massnahmen gemäss deren erwarteter Wirkung?).

3b **Kommentar Risikoeigner/in:** In diesem Feld wird die Beurteilung der Massnahmen (3a) kommentiert und erläutert (Besonderheiten, Schwierigkeiten, Lücken, Bedarf für Intensivierung u.ä.). (max.1100 Z.)

Anhang 3: Strukturierung von Risiken

Die folgenden Unterteilungen können neben den Risikokategorien zusätzlich hilfreich sein, um sich einen Überblick zu verschaffen und die Vielzahl an Risiken zu systematisieren. Dieser Abschnitt soll das gemeinsame Verständnis fördern und einen Anhaltspunkt geben, mit welchen Methoden das Risiko analysiert und bewertet werden kann.



a. ***Komplexität und Zeithorizont***: Eine Unterscheidung zwischen strategischen und operativen Risiken ist in der Theorie und Praxis vieler Organisationen üblich. Strategische und operative Risiken unterscheiden sich in mehrfacher Hinsicht: Strategische Risiken sind im Vergleich zu operativen Risiken meist komplexer (viele Zusammenhänge mit anderen Faktoren), längerfristiger Natur, abstrakter (weniger fassbar) und auf oberer Hierarchiestufe einer Organisation angesiedelt. Als weiteres Kriterium gilt manchmal auch die Höhe bzw. Bedeutung eines Risikos: grosse Risiken werden eher als strategisch bezeichnet und in die Verantwortung der obersten Hierarchiestufe angesiedelt. Zudem unterscheiden sich strategische Risiken häufig auch in der Art des Risikoeintritts von den operativen Risiken, indem sie häufig die Charakteristiken eines Entwicklungsrisikos aufweisen.

   Die Unterscheidung von strategischen und operativen Risiken erfolgt manchmal auch, um ein stufengerechtes Reporting zu erstellen: Während der Fokus der obersten Hierarchiestufe eher auf den strategischen Risiken der Organisation liegt, sind die tieferen Hierarchiestufen in ihrem Bereich für das Management der operativen Risiken verantwortlich.

   Je nach Risikoart sind unterschiedliche Methoden für die Analyse und Bewertung zu verwenden: Bei strategischen Risiken bieten sich v.a. Indikator- und Szenarioanalysen an, bei operativen Risiken können je nach Risiko alle Methoden der Analyse Sinn

machen. Die Methoden zur Analyse und Bewertung von Risiken werden in Ziffer 3.3.2 beschrieben.

b. ***Art des Risikoeintritts***: Risiken können in der Art unterschieden werden, wie sie auftreten. Bei einem *Ereignisrisiko* tritt dieses relativ schnell und plötzlich auf, meistens unerwartet. Ein *Entwicklungsrisiko* hingegen stellt eine Situation dar, die sich nach und nach verschärft und die negativen Auswirkungen im Zeitverlauf immer grösser werden, das Risiko ist also zeitlich nicht gut eingrenzbar und hat häufig einen längerfristigen Charakter. Ein solches Risiko kommt meistens auch nicht ganz unerwartet, weil es sich erst im Zeitverlauf entwickelt und durch Indikatoren schon vorher entdeckt werden kann. Die typische Eigenschaft eines *Schwankungsrisikos* ist, dass dieses eigentlich immer eintritt, wobei die Höhe und die Richtung des Ausschlags (Chance oder Risiko) vorher unbekannt sind. Finanzmarktrisiken sind typische Schwankungsrisiken.

   Je nach Art des Risikos sind unterschiedliche Methoden für die Analyse und Bewertung zu verwenden: bei Schwankungsrisiken sind v.a. statistische Analysen sinnvoll, bei Ereignisrisiken am ehesten Szenarioanalysen und bei Entwicklungsrisiken machen Indikatoranalysen am meisten Sinn (vgl. Ziffer 3.3.2).

c. ***Prozesse***: Eine Unterteilung der Risiken nach Prozessen macht Sinn, wenn beispielsweise eine Verwaltungseinheit ein Qualitätsmanagement umsetzt und die Erfüllung ihrer Aufgaben mit Hilfe von klar definierten Prozessen steuert.

d. ***Organisationsstruktur***: Eine Unterteilung der Risiken nach Organisationsstruktur wird in der Praxis häufig umgesetzt. Eine solche Unterteilung unterstützt die klare Zuordnung eines Risikos zu einer Organisation und dessen Leitung.

Anhang 4: Pflichtenhefte für Risikomanager und Risikocoaches

Pflichtenheft Risikomanager

Umsetzen des Risikomanagementprozesses auf Stufe Departement / BK ▪ Zeitliche und organisatorische Planung und Kommunikation des Risikomanagementprozesses auf Stufe Departement / BK in Abstimmung mit den Terminen der Koordinationsstelle EFV. ▪ Durchführen des Risikomanagementprozesses in der Funktion als Risikocoach im Generalsekretariat (Fokus auf Aufgaben des Departements / der BK).
Einheitliches Implementieren des Risikomanagements innerhalb des Departements/der BK ▪ Abklären des Bedarfs nach einer departementsweiten Risikorichtlinie, welche die Vorgaben aus der Richtlinie über das Risikomanagement Bund berücksichtigt und allfälliges Erstellen einer Richtlinie auf Stufe Departement / BK.
Koordination und Steuerung der Risikocoaches der VE des Departements. ▪ Organisiert den fachlichen Austausch der Risikocoaches innerhalb des Departements mit regelmässigen Sitzungen. ▪ Organisiert und führt die Abstimmung bezüglich Querschnittsrisiken innerhalb des Departements.
Erstellen des Risikoreportings auf Stufe Departement / BK ▪ Zusammenführen der aus den VE (inkl. Generalsekretariat) gemeldeten Departementsrisiken, Prüfung von Wechselwirkungen zwischen den Risiken. ▪ Analyse und Führen der Diskussionen, Abklärungen und des Quervergleichs der Departementsrisiken innerhalb des Departements / der BK und zwischen den VE. ▪ Erstellen eines Reportings für den Departementsvorsteher und die Leitung des Departements / der BK. ▪ Zustellen des Reportings an die Koordinationsstelle EFV für das Bundesratsreporting. ▪ Vorschlag bezüglich Auswahl der Kernrisiken des Departements / der BK (Entscheid beim Vorsteher).
Koordinieren die Abstimmungen zur Analyse von Wechselwirkungen zwischen Risiken aus unterschiedlichen VE Fachliche Unterstützung der Risikoeigner auf Stufe Departement / BK und der Risikocoaches ▪ Antworten auf Fragen zur Methodik des Risikomanagements der Risikoeigner auf Stufe Departement / BK. ▪ Antworten auf Fragen zum System R2C_GRC und fachlichen Fragen der Risikocoaches.
Schnittstelle zur und Ansprechperson für die Koordinationsstelle EFV ▪ Teilnahme an den regelmässigen Risikomanagement-Workshops auf Stufe Bund (organisiert durch die Koordinationsstelle EFV). ▪ Zusammenarbeit mit Koordinationsstelle EFV bei der Diskussion der Bundesratsrisiken des Departements / der BK.
Entscheide des BR, der GSK und der Koordinationsstelle EFV den Risikocoaches und den Risikoeigner stufengerecht kommunizieren.
Vernetzung des Risikomanagements mit anderen Führungsprozessen im Departement / in der BK. ▪ Vernetzen des Risikomanagements mit weiteren Führungsprozessen, insb. mit dem IKS, mit dem Qualitätsmanagement, dem IT-Sicherheitsmanagement usw.

Verbesserung des Risikomanagements im Departement / in der BK und in der BVerw
▪ Aus den Erfahrungen im Risikomanagement Ideen generieren, um das Risikomanagement in der Bundesverwaltung zu verbessern und weiterzuentwickeln. ▪ Teilnahme an Risikomanagement-Veranstaltungen, insb. bei Veranstaltungen mit thematischem Bezug zum Departement / zur BK. ▪ Fördern des Risikobewusstseins auf Stufe Departement / BK und im Generalsekretariat.

Pflichtenheft Risikocoach

Umsetzung Risikomanagementprozess auf Stufe VE
▪ Zeitliche und organisatorische Planung und Kommunikation des Risikomanagementprozesses innerhalb der VE in Abstimmung mit den Terminen auf Stufe Departement (Vorgabe des Risikomanagers). ▪ Durchführung des Risikomanagementprozesses in der VE: Gruppen-Workshops mit Leitung der VE bzw. geeigneten Wissensträgern, Einzeldiskussionen usw.
Einheitliche Implementierung des Risikomanagements innerhalb der VE
▪ Abklärung des Bedarfs nach einer VE-spezifischen Risikorichtlinie, welche die Vorgaben aus der Richtlinie über das Risikomanagement Bund bzw. Departement berücksichtigt.
Erstellen eines adäquaten Risikoreportings auf Stufe VE
▪ Zusammenführen der in den Abteilungen und Sektionen erfassten und analysierten Risiken inkl. der vorgeschlagenen Massnahmen. ▪ Führen der Diskussionen, Abklärungen und des Quervergleichs zwischen den Risiken der unterschiedlichen Abteilungen. ▪ Erstellen eines Reportings für den Leiter der VE. ▪ Erstellen eines Reportings für den Risikomanager des Departements.
Fachliche Unterstützung der Risikoeigner auf Stufe VE
▪ Antworten auf Fragen zur Methodik des Risikomanagements und Strukturierung von Risiken der Risikoeigner und der Direktion der VE.
Schnittstelle zur und Ansprechperson für den Risikomanager des Departements
▪ Teilnahme an Risikomanagementsitzungen im Departement (vom Risikomanager organisiert). ▪ Zusammenarbeit und Austausch bezüglich Auswahl der Departementsrisiken der VE.
Entscheide des BR, der GSK, der Koordinationsstelle EFV und des Risikomanagers der Direktion der VE und den Risikoeigner der VE stufengerecht kommunizieren.
Vernetzung des Risikomanagements mit anderen Führungsprozessen in der VE
▪ Vernetzen des Risikomanagements mit weiteren bestehenden Führungsprozessen in der VE, insb. mit dem IKS, aber auch mit dem Qualitätsmanagement, dem IT-Sicherheitsmanagement usw.
Verbesserung des Risikomanagements in der VE und in der Bundesverwaltung
▪ Aus den Erfahrungen im Risikomanagement Ideen generieren, um das Risikomanagement in de VE und in der Bundesverwaltung zu verbessern und weiterzuentwickeln. ▪ Teilnahme an Risikomanagement-Veranstaltungen, insb. bei Veranstaltungen mit thematischem Bezug zur VE. ▪ Fördern des Risikobewusstseins innerhalb der VE.

Anhang 5: Beispiel einer Einsichtsverweigerung in das Risikomanagement Bund (Risikodatenbank R2C_GRC)

Einschreiben
xxx
xxx
xxx

Bern, xxx

Ihr Einsichtsgesuch vom xxx

Sehr geehrter Herr xxx

Mit E-Mail vom xxx verlangten Sie von der EFV gestützt auf das Öffentlichkeitsgesetz (BGÖ; SR *152.3*) Einsicht in die «Datenbank R2C_GRC (Risikomanagement-System zur Erfassung der bundesweiten Risiken)».

Nach Prüfung der Sachlage gelangen wir zu folgender ***Stellungnahme***:

1. Der Zugang wird verweigert.
2. Eine Gebühr wird nicht erhoben (Art. 17 Abs. 1 BGÖ).

Begründung:
Die EFV stellt den Departementen / der BK für die Bewirtschaftung ihrer Risiken und die Risikoberichterstattung eine gemeinsame Informatikanwendung zur Verfügung. Die Kurzbezeichnung der Anwendung lautet «R2C_GRC». Die wesentlichen Risiken des Bundes werden darin im Detail identifiziert, analysiert und bewertet. Ausserdem werden Massnahmenpläne inklusive deren Stand der Umsetzung dargelegt. Die Risikoberichterstattung erfolgt (mindestens) einmal jährlich und wird auf allen Stufen (VE, Departement / BK, Generalsekretärenkonferenz, Bundesrat) als VERTRAULICH klassifiziertes Geschäft behandelt. Zwecks Wahrung der Vertraulichkeit der Informationen haben auch die Geschäftsprüfungskommissionen für die Behandlung der Risikoberichterstattung an den Bundesrat besondere Massnahmen getroffen.

Die Klassifizierungsstufe wurde aufgrund des vorliegenden Gesuchs überprüft (Art. 11 Abs. 5 Öffentlichkeitsverordnung (SR *152.31*)); sie ist gerechtfertigt.

Das Interesse des Bundes an der Wahrung der Vertraulichkeit der in der Applikation R2C_GRC aufgeführten Informationen ist gross. Eine Einsichtnahme könnte insbesondere die freie Meinungs- und Willensbildung in Bezug auf die Bewirtschaftung der Risiken und die zu treffenden Massnahmen beeinträchtigen. Ausserdem besteht die Gefahr der Vereitelung der zielkonformen Durchführung von konkreten behördlichen Massnahmen und auch die innere und äussere Sicherheit der Schweiz könnte unter Umständen erheblich gefährdet sein.

Ein höher zu gewichtendes Interesse an der Einsichtnahme ist vorliegend nicht ersichtlich.

Aus diesen Gründen wird der Zugang zu den in R2C_GRC enthaltenen Informationen insbesondere gestützt auf Art. 7 Abs. 1 Bst. a–c BGÖ nicht gewährt.

Freundliche Grüsse

xxx
Öffentlichkeitsverantwortliche EFV

Hinweis auf das Schlichtungsverfahren (vgl. Art. 13 BGÖ)

[1] Einen Schlichtungsantrag stellen kann eine Person:

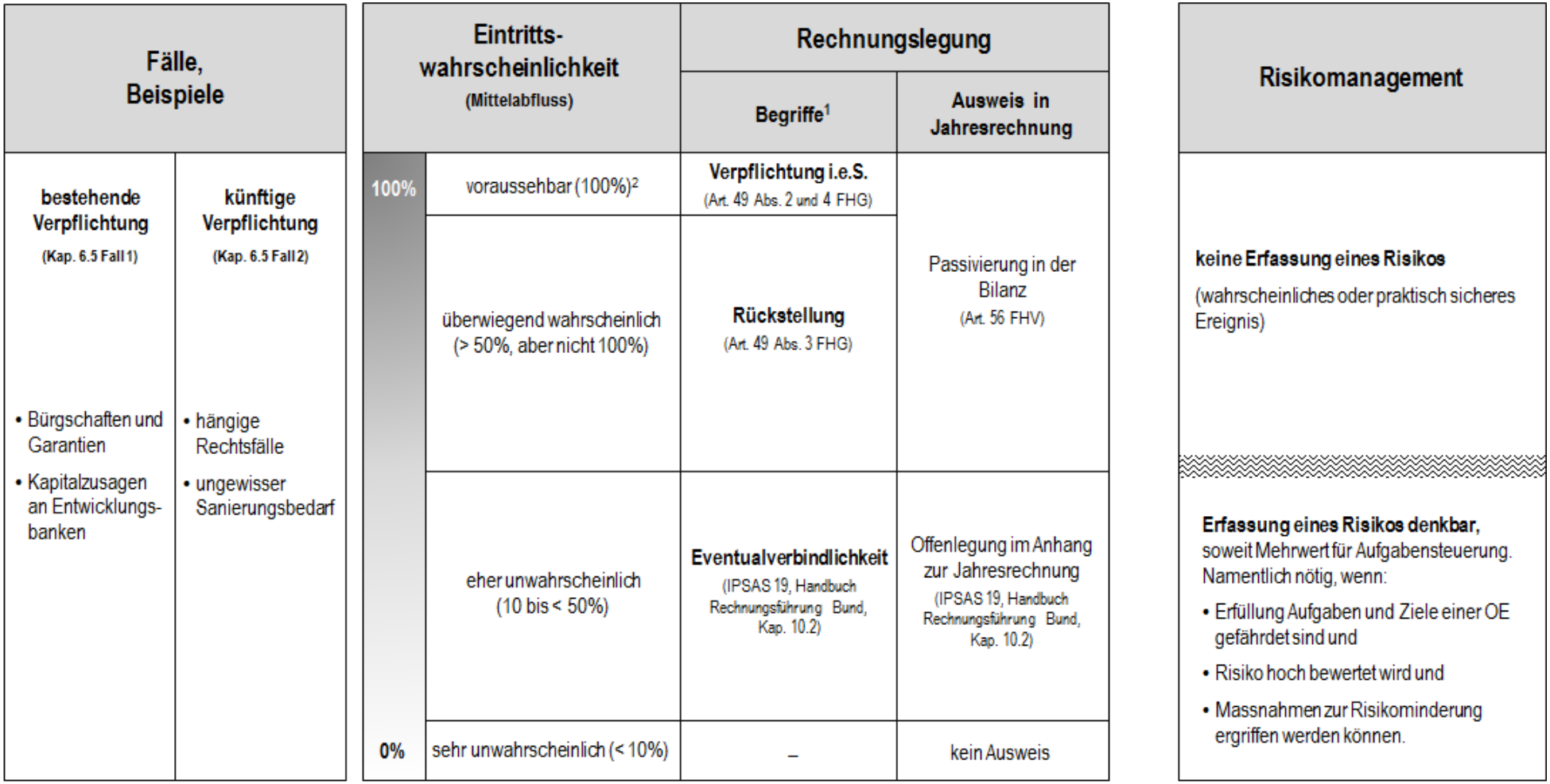
a. deren Zugang zu amtlichen Dokumenten eingeschränkt, aufgeschoben oder verweigert wird;

b. zu deren Gesuch die Behörde nicht fristgerecht Stellung genommen hat; oder

c. die nach Artikel 11 angehört worden ist, wenn die Behörde gegen ihren Willen den Zugang gewähren will.

[2] Der Schlichtungsantrag ist der oder dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten innert 20 Tagen nach Empfang der Stellungnahme oder nach Ablauf der der Behörde für die Stellungnahme zur Verfügung stehenden Frist schriftlich zu stellen.

Anhang 6: Schnittstelle «Risikomanagement – Rechnungslegung Bund»



[1] vgl. Botschaft vom 24. November 2004 zur Totalrevision des Bundesgesetzes über den eidgenössischen Finanzhaushalt (BBl *2005* 5, S. 15, 57, 61 f., 85 f., 104 f. und 107).

[2] Ein Mittelabfluss ist *voraussehbar* nach Art. 49 Abs. 2 FHG (Kurzformel: Wahrscheinlichkeit = 100%), wenn sein Eintritt *praktisch sicher* ist. Hingegen kann es keine *absolute Gewissheit* für ein in der Zukunft liegendes Ereignis geben.

Anhang 7: Organisationen ausserhalb der Bundesverwaltung

Aus den Beziehungen des Bundes zu Organisationen ausserhalb der Bundesverwaltung können sich aus Sicht Risikomanagement Bund sehr unterschiedliche Risiken ergeben. In diesem Anhang sollen folgende Konstellationen näher betrachtet werden:

1. Der Bund gewährt einer Organisation Darlehen, Bürgschaften, Garantien usw.;
2. Eine Stelle im Bund übt bezüglich einer Organisation eine Aufsichtsfunktion aus oder amtet als Revisionsstelle;
3. Ausfallhaftung des Bundes nach Artikel 19 Verantwortlichkeitsgesetz (VG)[83] und weitere Finanzierungsrisiken;
4. Haftung des Bundes für Bundesvertreter in Leitungs- oder Verwaltungsorganen einer Organisation;
5. Risiken bei verselbstständigten Einheiten, die auf den Bund als Eigner «durchschlagen» können.

1. Darlehen, Bürgschaften, Garantien usw.[84]

Die Gewährung von Darlehen, Bürgschaften, Garantien oder ähnlichen Absicherungen durch den Bund zugunsten von Dritten setzt eine formalgesetzliche Grundlage voraus. Das Gesetz legt fest, an wen, unter welchen Umständen, zu welchem Zweck, in welchem Umfang und unter welchen Konditionen derartige Leistungen erbracht werden können (oder müssen). Mit solchen Leistungen an Dritte will der Bund in aller Regel die Erfüllung von Aufgaben im Bundesinteresse fördern, indem diese kostengünstiger finanziert werden können.

Aus Sicht Risikomanagement Bund kann ein Risiko z. B. darin bestehen, dass

- die Leistungen des Bundes durch den Dritten zweckentfremdet werden,
- die vorgesehene Rückerstattung oder Verzinsung nicht erfolgt oder
- der Bund nicht geplante zusätzliche Leistungen erbringen muss, um die gewünschte Aufgabenerfüllung sicherstellen zu können (beispielsweise bei einem Ausfall des Begünstigten infolge Konkurs).

Die Auswirkungen dieser Risiken sind in den meisten Fällen finanzieller Art, aber auch die Reputation des Bundes kann stark betroffen sein. Es ist unerlässlich, dass die Aufgabenerfüllung durch die Begünstigten sowie deren Geschäftsführung und finanzielle Lage durch die zuständige Bundesstelle in geeigneter Weise stetig überwacht werden. Nötigenfalls muss mittels geeigneten Massnahmen rechtzeitig die Aufgabenerfüllung sichergestellt und allenfalls eine Sanierung verlangt werden. Zum Risikomanagement gehört es auch, von Zeit zu Zeit die Grundsatzfrage zu prüfen, ob die Bundesförderung mit den bisher verwendeten Instrumenten noch notwendig und effektiv ist.

2. Aufsichts- und Revisionstätigkeiten des Bundes

Für Schäden, die Bundesangestellte in Ausübung ihrer amtlichen Tätigkeit Dritten widerrechtlich zufügen, haftet der Bund nach Artikel 3 ff. VG ohne Rücksicht auf das Verschulden

[83] SR *170.32*
[84] Zur Abbildung dieser Tatbestände nach den Regeln der Rechnungslegung vgl. Ziff. 6.5 und Anhang 6

des Angestellten. Diese Staatshaftung erstreckt sich auch auf Fälle, wo ein Dritter einen Schaden geltend macht, der auf eine von der zuständigen Bundesstelle ungenügend wahrgenommene Aufsichtspflicht oder auf eine unsorgfältige Revision durch die EFK zurückzuführen ist.[85] Aus Sicht Risikomanagement Bund handelt es sich hier um mögliche Haftungsrisiken mit vorwiegend finanziellen Auswirkungen. Wegen der für die Geschädigten in der Regel relativ schwierigen Rechts- und Beweislage kann die Eintrittswahrscheinlichkeit des Risikos aus Sicht Bund oft als relativ klein eingestuft werden. Ob ein Risiko zu erfassen ist, ist im Einzelfall zu entscheiden.

3. Ausfallhaftung des Bundes nach Artikel 19 VG und weitere Finanzierungsrisiken

Bei der Ausfallhaftung des Bundes nach Artikel 19 VG müssen folgende Merkmale erfüllt sein:

- Eine Organisation steht *ausserhalb der ordentlichen Bundesverwaltung*; sie hat eigene Rechtspersönlichkeit und eine eigene Rechnung.
- In einem Gesetz wurde diese Organisation *mit öffentlich-rechtlichen Aufgaben des Bundes* (Bundesverwaltungsaufgaben) *betraut*.
- Bei Tätigkeiten *im Zusammenhang mit der Erfüllung dieser delegierten Aufgaben* fügen Organe oder Angestellte der Organisation einem Dritten widerrechtlich einen Schaden zu.
- Für diesen Schaden haftet in erster Linie die Organisation selber. Nur soweit sie die geschuldete Entschädigung nicht zu leisten vermag, haftet der Bund dem Geschädigten für den ungedeckten Betrag (sog. Ausfallhaftung).

Dieser Haftungssituation im Risikomanagement Bund adäquat Rechnung zu tragen, ist eine sehr komplexe Aufgabe. Ein nicht versicherter Haftungsfall nach Artikel 19 VG ist einer der vielen möglichen Gründe für finanzielle Schwierigkeiten bei einer beauftragten Organisation. Unabhängig von deren Ursachen können solche Schwierigkeiten (drohende Illiquidität oder Überschuldung) die Erfüllung der übertragenen Aufgabe gefährden. Der Bund ist jedoch daran interessiert, dass die delegierte öffentlich-rechtliche Bundesaufgabe weiterhin erfüllt wird. Eine rasche Substitutionsmöglichkeit für die beauftragte Organisation besteht aber meist nicht. Es kann deshalb für den Bund gegenüber der Organisation ein faktisches (kein rechtliches) Refinanzierungsrisiko in dem Sinne bestehen, dass der Bund zwecks Sicherstellung der Erfüllung der delegierten Bundesaufgabe z. B. finanziell zur Sanierung der beauftragten Organisation beitragen muss. Das Risiko «Ausfallhaftung nach Artikel 19 VG» ist demzufolge nur ein Finanzierungsrisiko. Bei dessen Beurteilung müssen auch die vorhandenen Versicherungsdeckungen der Organisation beachtet werden.

4. Haftung des Bundes für Bundesvertreter in Leitungs- oder Verwaltungsorganen einer Organisation

Die Statuten von Aktiengesellschaften können vorsehen, dass der Bund einen Vertreter in den Verwaltungsrat entsenden kann. In solchen Ausnahmefällen haftet der Bund gegenüber der Gesellschaft, den Aktionären und den Gläubigern, wenn der Vertreter durch absichtliche oder fahrlässige Verletzung seiner Pflichten einen Schaden verursacht.[86] Bei Bundesvertretern, die aufgrund einer Beteiligung des Bundes an einer Gesellschaft in einen Verwaltungsrat gewählt und nicht entsendet werden, liegen häufig spezifische gesetzliche oder vertragli-

[85] Sollten in Ausnahmefällen die Aufsichtsfunktion oder die Revisionstätigkeit des Bundes auf einer privatrechtlichen Grundlage beruhen, wären allfällige Haftpflichtansprüche eines Dritten aufgrund der entsprechenden privatrechtlichen Haftungsnorm zu beurteilen.

[86] Art. 762 Abs. 4 in Verbindung mit Art. 754 OR. Eine analoge Regelung gilt bei Genossenschaften (vgl. Art. 926 Abs. 3 OR)

che Grundlagen für eine Haftung des Bundes vor (bei Bundesangestellten im Anstellungsverhältnis; bei beauftragten Dritten im Auftragsverhältnis bzw. in den erteilten Instruktionen). Diese sind im Einzelfall zu regeln (schriftliches Mandat und Instruktionen) bzw. im Schadenfall zu prüfen. Ebenfalls zu prüfen ist der Abschluss bzw. das Bestehen von Organhaftpflichtversicherungen.

5. Risiken bei verselbstständigten Einheiten

Der Bund besitzt als alleiniger oder mehrheitlicher Eigentümer Unternehmen, denen er die Erfüllung von Bundesaufgaben übertragen hat[87] (Post, SBB, Swisscom, Skyguide und RUAG, aber auch die Anstalten des ETH-Bereichs, Swissmedic usw.). Der Bundesrat nimmt die eignerstrategische Steuerung dieser Unternehmen wahr. Gerät ein Bundesunternehmen in finanzielle Schwierigkeiten (z. B. infolge von Managementfehlern, riskanten Investitionen im In- und Ausland, nicht rechtzeitig erkannten Marktveränderungen), kann das schwerwiegende Auswirkungen auf den Bund haben: Ausfall von Gewinnausschüttungen, Wertverlust auf Beteiligungen in der Bilanz des Bundes, finanzielle Unterstützung durch den Bund, damit die Erbringung der übertragenen Bundesaufgabe bzw. im Extremfall die Existenz des Unternehmens sichergestellt werden kann usw. Die eignerstrategische Steuerung der Bundesunternehmen ist aus Sicht Risikomanagement Bund eine komplexe Bundesaufgabe, die mit zahlreichen Herausforderungen verbunden ist. Sie erfordert eine intensive Zusammenarbeit zwischen dem Risikomanagement und den Eignerstellen.

[87] Vgl. Art. 8 Abs. 5 RVOG

Anhang 8: Weitere Tätigkeiten mit Bezug zum Risikomanagement

Folgende Tätigkeiten weisen teilweise enge Berührungspunkte und Schnittstellen mit dem Risikomanagement Bund auf und werden deshalb kurz umrissen.

I. Schutz kritischer Infrastrukturen (SKI)

Als kritische Infrastrukturen (KI) werden Prozesse, Systeme und Einrichtungen bezeichnet, die essenziell für das Funktionieren der Wirtschaft oder das Wohlergehen der Bevölkerung sind. Dazu zählen etwa die Energieversorgung, der Schienenverkehr oder die medizinische Versorgung. Als kritische Infrastrukturen bezeichnet werden nicht nur Bauten und Anlagen, sondern Versorgungssysteme und Dienstleistungen im weitesten Sinne. Schwerwiegende Ausfälle, beispielsweise ein landesweiter Stromausfall, können gravierende volkswirtschaftliche Schäden verursachen und die Bevölkerung massiv beeinträchtigen. Der Schutz kritischer Infrastrukturen umfasst unter anderem bauliche, technische, organisatorische oder rechtliche Massnahmen, die zum Ziel haben, solche Ausfälle nach Möglichkeit zu vermieden oder im Ereignisfall die Funktionsfähigkeit möglichst rasch wieder zu erlangen.

Im Juni 2012 hat der Bundesrat erstmals eine nationale Strategie zum Schutz kritischer Infrastrukturen (SKI) verabschiedet, um die Resilienz (Widerstands-, Anpassungs- und Regenerationsfähigkeit) der Schweiz im Hinblick auf KI zu verbessern. Ende 2017 hat er die Strategie aktualisiert und dabei an der übergeordneten Zielsetzung und Stossrichtung der Strategie von 2012 festgehalten. Ende 2022 wird er erneut über eine aktualisierte Strategie befinden.

Der Schutz kritischer Infrastrukturen ist eine Verbunds- und Querschnittsaufgabe mit Nahtstellen zu verschiedenen Politik- und Aufgabenbereichen (Energiepolitik, Sicherheitspolitik, Schutz vor Naturgefahren usw.). Dementsprechend erfolgt auch die Umsetzung der nationalen SKI-Strategie massgeblich im Rahmen von dezentralen Strukturen und Zuständigkeiten. Die Kompetenzen der beteiligten Bundesstellen, der Kantone und Gemeinden sowie der KI-Betreiber bleiben vorbehalten. Das Bundesgesetz über den Bevölkerungsschutz und den Zivilschutz (BZG) vom 20. Dezember 2019 verlangt[88], dass der Bund Grundlagen im Bereich SKI erstellt und dass das BABS ein Inventar der Objekte kritischer Infrastrukturen betreibt sowie die Planungs- und Schutzmassnahmen der Betreiberinnen kritischer Infrastrukturen – in enger Zusammenarbeit mit diesen – koordiniert. [89]

Während das Risikomanagement Bund auf die Risiken für die Aufgabenerfüllung der Bundesverwaltung fokussiert, geht es bei SKI um die Risiken bzw. um die Stärkung der Resilienz kritischer Infrastrukturen. Schnittstellen können sich unter anderem dadurch ergeben, dass die Bundesverwaltung selber ebenfalls Teil der kritischen Infrastrukturen ist (Teilsektor Parlament, Regierung, Justiz, Verwaltung), ein Ausfall bestimmter kritischer Infrastrukturen (etwa Strom, Telekommunikation) auch schwerwiegende Auswirkungen auf die Aufgabenerfüllung der Bundesverwaltung haben kann oder auch dadurch, dass gewisse Unternehmen, die zu den kritischen Infrastrukturen zählen, teilweise oder vollständig in Bundebesitz sind.

II. Nationale Risikoanalyse

Die nationale Risikoanalyse «Katastrophen und Notlagen Schweiz» (KNS) untersucht die Auswirkungen von verschiedenen Gefährdungen aus den Bereichen Natur, Technik und Gesellschaft auf die Bevölkerung und ihre Lebensgrundlagen in der Schweiz. Übergeordnetes Ziel ist es, eine gemeinsame Grundlage zur Vorbereitung der Gesellschaft auf die Bewältigung von bestimmten Schadensereignissen zu schaffen. Ein gemeinsames Verständnis über

[88] Art. 8 BZG (SR 520.1)

[89] Für genauere Informationen sei auf die SKI-Strategie 2018-2022 verwiesen (BBl 2018 503, Webseite Schutz Kritischer Infrastrukturen (admin.ch)

die verschiedenen Auswirkungen, den Ablauf und die Dynamik von Gefährdungen ist dabei zentral, weil (die Vorbereitung auf) deren Bewältigung eine immer engere Zusammenarbeit verschiedener Stellen bei Bund und Kantonen, der Wirtschaft, Wissenschaft und Bevölkerung erfordert. KNS stützt sich auf das Bevölkerungsschutz- und Zivilschutzgesetz (BZG) und wird im Bundesamt für Bevölkerungsschutz koordiniert. Im Rahmen der Arbeiten zur nationalen Gefährdungsanalyse wurden mehrere Produkte entwickelt, die periodisch aktualisiert werden, dazu zählen[90]:

- *Der Risikobericht und die Risikobroschüre* zeigen die Resultate der Analysen von 44 untersuchten Katastrophenereignissen und Notlagen und wie diese zueinander in Beziehung stehen.
- *Der Methodenbericht* dokumentiert das Vorgehen und die angewandte Metrik.
- *Gefährdungskatalog:* Zusammenstellung möglicher Gefährdungen. Der Katalog stellt eine systematische und mit Beispielen dokumentierte Übersicht denkbarer Ereignisse und Entwicklungen dar, ohne diese zu priorisieren.
- *Gefährdungsdossiers:* zu den identifizierten Gefährdungen werden vorhandene Informationen aufgearbeitet, systematisch aufgebaute Szenarien entwickelt und in einem sogenannten Gefährdungsdossier zusammengestellt. Die Szenarien in den Gefährdungsdossiers sind die Grundlage für die Risikoanalyse bzw. den Risikobericht.

Während sich Risikomanagement Bund auf die Bundesverwaltung konzentriert, fokussieren sich die Arbeiten im Rahmen der nationalen Risikoanalyse auf Katastrophen und Notlagen mit Auswirkungen auf die Bevölkerung und ihre Lebensgrundlagen.

[90] Vgl. auch www.risk-ch.ch

Anhang 9: Stolpersteine im Risikomanagement

Einige allgemeine Stolpersteine, die eine effektive Umsetzung des Risikomanagements insbesondere bei komplexen und schwer fassbaren Risiken beeinträchtigen können und eine allmähliche Entwicklung von Risiken begünstigen können, werden nachfolgend kurz erläutert. Es ist Aufgabe der Risikoeigner, der Risikomanager und Risikocoaches, solche Probleme in ihrem Bereich zu identifizieren und zu minimieren.

- ***Bürokratie:*** Eine proaktive Umsetzung des Risikomanagementprozesses ist für den Erfolg entscheidend. Nachdem der Prozess einige Jahre immer gleich durchgespielt und umgesetzt wurde, steigt die Gefahr, dass er danach immer mehr zu einer bürokratischen Routinearbeit verkommt. Dies führt dazu, dass nicht mehr proaktiv nach neuen Risiken und Änderungen der bestehenden Risiken gesucht, der Prozess möglichst rasch und ohne ein entsprechendes Engagement durchgeführt und so wichtige Risiken nicht erkannt und keine entsprechenden Gegenmassnahmen getroffen werden.

- ***Fehlender Einbezug von Anspruchsgruppen:*** Der Einbezug aller relevanten Personen im Risikomanagementprozess ist von grosser Bedeutung. Erstens stellt er sicher, dass die bestmögliche und möglichst vollständige Information zur objektiven Beurteilung eines Risikos vorliegt. Zweitens hilft er, das Vertrauen (intern und extern) in das Risikomanagement und dessen Resultate wesentlich zu erhöhen. Ein fehlender Anspruchsgruppeneinbezug kann schliesslich zu erheblichen Verzögerungen in der Analyse und Bewältigung von Risiken führen.

  Beispiel: grosse Kraftwerksprojekte (breit angelegter Einbezug von Anspruchsgruppen ermöglicht erst deren Umsetzung)

- ***Interessenkonflikte und absichtliche Fehldarstellung von Risiken***: Sowohl bei der Analyse von Risiken als auch bei der Umsetzung von Bewältigungsmassnahmen können vorhandene Interessenkonflikte den Risikomanagementprozess behindern. Spezifische Interessen von Anspruchsgruppen können einerseits zu einer absichtlichen oder unabsichtlichen Fehldarstellung und -analyse von Risiken führen. Andererseits können sie auch notwendige Massnahmenumsetzungsentscheide blockieren. Interessenkonflikte müssen aufgedeckt und wenn möglich gelöst werden.

  Beispiel: von der Tabakindustrie finanzierte Studien über gesundheitliche Risiken des Rauchens

- ***Verstreute bzw. nicht klar geregelte Verantwortlichkeiten***: Besonders in komplexen Organisationen, in denen verschiedene Akteure gemeinsam Verantwortung tragen oder die Verantwortung nicht klar geregelt ist, kann dies in Kombination mit einer schlechten Kommunikation dazu führen, dass notwendige Massnahmenentscheide nicht oder zu spät gefällt und umgesetzt werden, weil niemand voll in der Verantwortung steht.

  Beispiel: Strom-Blackout Italien

- ***Abwägung zwischen Transparenz und Vertraulichkeit:*** Die Vertraulichkeit (und damit die fehlende Kommunikation) von Risikoinformationen ist in einigen Fällen zum Schutz der nationalen Sicherheit oder zur Vermeidung von öffentlicher Panik gerechtfertigt. Fehlende Transparenz bezüglich Risiken kann andererseits das Vertrauen in das Risikomanagement vermindern und aufgrund fehlender Informationen dazu führen, dass einige Risiken deswegen nicht die nötige Dringlichkeit zu ihrer Bewältigung erhalten.

  Beispiel: Bilanzfälschung Enron

- ***Informationsasymmetrien:*** In einigen Fällen dient die Aufrechterhaltung von Informationsasymmetrien den Zielen des Risikomanagements, beispielsweise kann die

Geheimhaltung von Informationen zur Terrorismusbekämpfung die nationale Sicherheit erhöhen. In vielen Fällen ist die Aufrechterhaltung und das Bestehen von Informationsasymmetrien aber schädlich, weil dadurch beispielsweise Risikomanager und Entscheidungsträger nicht alle notwendigen Informationen zur Analyse und Bewertung eines Risikos erhalten und deswegen notwendige Bewältigungsmassnahmen vernachlässigen.

Beispiel: Subprime-Krise USA (Investoren und Hausbesitzer bezüglich Risiken zu wenig informiert)

- ***Öffentliches Verständnis und Toleranz von Risiken:*** Neben der wissenschaftlichen und objektiven Analyse von Risiken werden grosse Risiken in der Gesellschaft immer auch von der breiten Öffentlichkeit bewertet, wobei diese Einschätzung von der objektiven Bewertung abweichen kann. Neben der Einschätzung der Eintrittswahrscheinlichkeit und der Höhe der Auswirkungen spielen für das öffentliche Verständnis und für die öffentliche Toleranz der Risiken folgende Faktoren eine wesentliche Rolle: kulturelle Werte, persönliche Kontrollierbarkeit des Risikos, Verteilung der Auswirkungen auf die Bevölkerung, Familiarität des Risikos, menschliches Verschulden des Risikos, bewusstes Tragen des Risikos durch die Bevölkerung usw. Um die Akzeptanz von Entscheiden im Umgang mit solchen Risiken zu erhöhen müssen solche Überlegungen im Risikomanagement mit einbezogen werden.

  Beispiel: Gentechnik (unterschiedliche Risikowahrnehmung in USA und EU), Problematik radioaktiver Abfall, Klimawandel, …

- ***Erkennen von und Handeln in unerwarteten Situationen***: Einerseits existieren bei der Identifikation von neuen Risiken häufig kognitive Barrieren. Das heisst viele Menschen haben Mühe, Ereignisse ausserhalb von akzeptierten Paradigmen zu erkennen. Um dem entgegenzuwirken ist es wichtig, bei der Identifikation von Risiken einen Fokus auf Kreativität zu legen und beispielsweise auch Querdenker in der Risikoidentifikation mit einzubeziehen. Andererseits kann manchmal eine Organisation auf schnelle Änderungen nicht situationsgerecht reagieren. In diesen Fällen ist eine Haltung und Kultur anzustreben, die Entscheidungen unter Unsicherheit und die Fähigkeit, von vorhandenen und nicht mehr geeigneten Abläufen und Strukturen Abschied zu nehmen, fördert.

  Beispiel: 9/11-Terroristenangriff auf Twin-Towers (unerwartete Angriffsmethode)

Anhang 10: Factsheets zu potenziellen Risikofeldern im Bund

In diesem Anhang werden einige potenzielle Risikofelder in der Bundesverwaltung analysiert und erläutert. Ein klares und gemeinsames Verständnis soll den bundesweiten Umgang damit verbessern.

Die Ausführungen zu den einzelnen Themen sind wie folgt strukturiert:

- *Risikoanalyse:* Terminologie, allfällige Unterteilung in Unterrisiken, Wechselwirkungen etc.;
- Involvierte *Akteure* und ihre Aufgaben im Risikomanagementprozess;
- *Zusammenarbeit* der Akteure;
- *Zentrale Kompetenzstellen* im Risikofeld, weitere Informationen;
- *Massnahmenoptionen und Best Practices*;
- *Empfehlungen* der Koordinationsstelle Risikomanagement Bund.

Folgende potenzielle Risikofelder werden in diesem Anhang analysiert:

A) IKT-Risiken

B) Infrastrukturrisiken (ohne IKT-Risiken)

C) Vermögensdelikte

D) Personalrisiken

E) Ungenügendes IKS zur Sicherstellung der Ordnungsmässigkeit der Staatsrechnung

A) IKT-Risiken

Risikoanalyse

Informations- und Kommunikationstechnologien (IKT) werden heute vielseitig eingesetzt. Sie unterstützen in den Departementen und VE die Geschäftsprozesse zur Erfüllung der Aufgaben. Alle Ereignisse und Entwicklungen im IKT-Umfeld, die negative Auswirkungen auf die Erfüllung der Aufgaben oder auf die Zielerreichung des Bundes haben, sind als IKT-Risiken der Bundesverwaltung zu betrachten. Für einen IKT-Leistungserbringer (LE) ist der Ausfall bzw. die Störung der IKT-Infrastruktur *per se* ein Risiko, da der Betrieb der IKT-Systeme zugunsten seiner Leistungsbezüger (LB) seine Hauptaufgabe darstellt. Um den sicheren Betrieb der IKT-Leistungen gewährleisten zu können, ist der LE auf verlässliche Lieferanten angewiesen. IKT-Risiken treten häufig verwaltungseinheits- und departementsübergreifend auf, was ihre Bewirtschaftung komplex macht.

Grundsätzlich werden vier Arten von Beeinträchtigungen der IKT-Systeme unterschieden. Je nach konkretem Szenario können mehrere Beeinträchtigungen gleichzeitig auftreten. Alle unterbrechen oder stören wichtige Geschäftsprozesse und können zu finanziellen Folgen und Reputationsschäden führen:

a. Ausfall von Anwendungen oder/und Nichtverfügbarkeit von Daten (Verfügbarkeitsrisiko)
b. Abfluss von sensiblen Daten (Vertraulichkeitsrisiko)
c. Manipulation von Daten (Integritätsrisiko)
d. Daten können unbemerkt verändert werden (Nachvollziehbarkeit und Integrität)

Diese Beeinträchtigungen können zahlreiche Ursachen haben, die ihrerseits als Risiken angesehen werden können. Nachfolgend eine nicht abschliessende Aufzählung solcher Risiken:

- Spionagetätigkeiten
- Cyberattacken
- Malware (Viren, Trojaner etc.)
- Elementarereignisse (Brand, Wasser etc.)
- Archivierungs- und Speicherungsprobleme
- Nicht-Kompatibilität von IT-Systemen
- ungenügende Leistungsfähigkeit von Systemen
- fehlendes IT-Know-How
- Fahrlässigkeit von Mitarbeitenden im Umgang mit Daten und Anwendungen
- IT-Insellösungen und Schnittstellenrisiken (insbes. auch bei Outsourcing von IKT-Dienstleistungen)
- zu weit gefasste Zugriffsberechtigungen
- alternde bzw. nicht mehr gewartete Technologien/Plattformen
- Projektverzögerungen bei Entwicklung von neuen IKT-Systemen
- Abhängigkeitsrisiken beim Einsatz von externen Leistungserbringern bzw. Beratern

Normalerweise wird für jede IKT-Anwendung bzw. die darin enthaltenen Daten der erforderliche Schutzbedarf eruiert. Hierzu erstellt der Datenherr eine Schutzbedarfsanalyse. Besteht für Daten ein höherer Schutzbedarf, muss ein Informationssicherheits- und Datenschutzkonzept (ISDS-Konzept) erstellt werden. Darauf aufbauend wird i. d. R. zwischen dem IKT-LE und dem IKT-LB ein Service Level Agreement (SLA) abgeschlossen.

Beispiele von Wechselwirkungen bei IKT-Risiken:

- IKT-Infrastrukturrisiken am Standort des LE (Brand, Überschwemmung, Stromausfall etc.) können zu Ausfällen von IKT-Systemen und Anwendungen beim LB führen.[91]
- Mit IKT-Massnahmen kann auch ein Veruntreuungsrisiko reduziert werden.

[91] In der Regel wird die erforderliche Gebäudeinfrastruktur-Sicherheit zwischen dem IKT-LE und dem BBL bzw. armasuisse in einem SLA festgelegt.

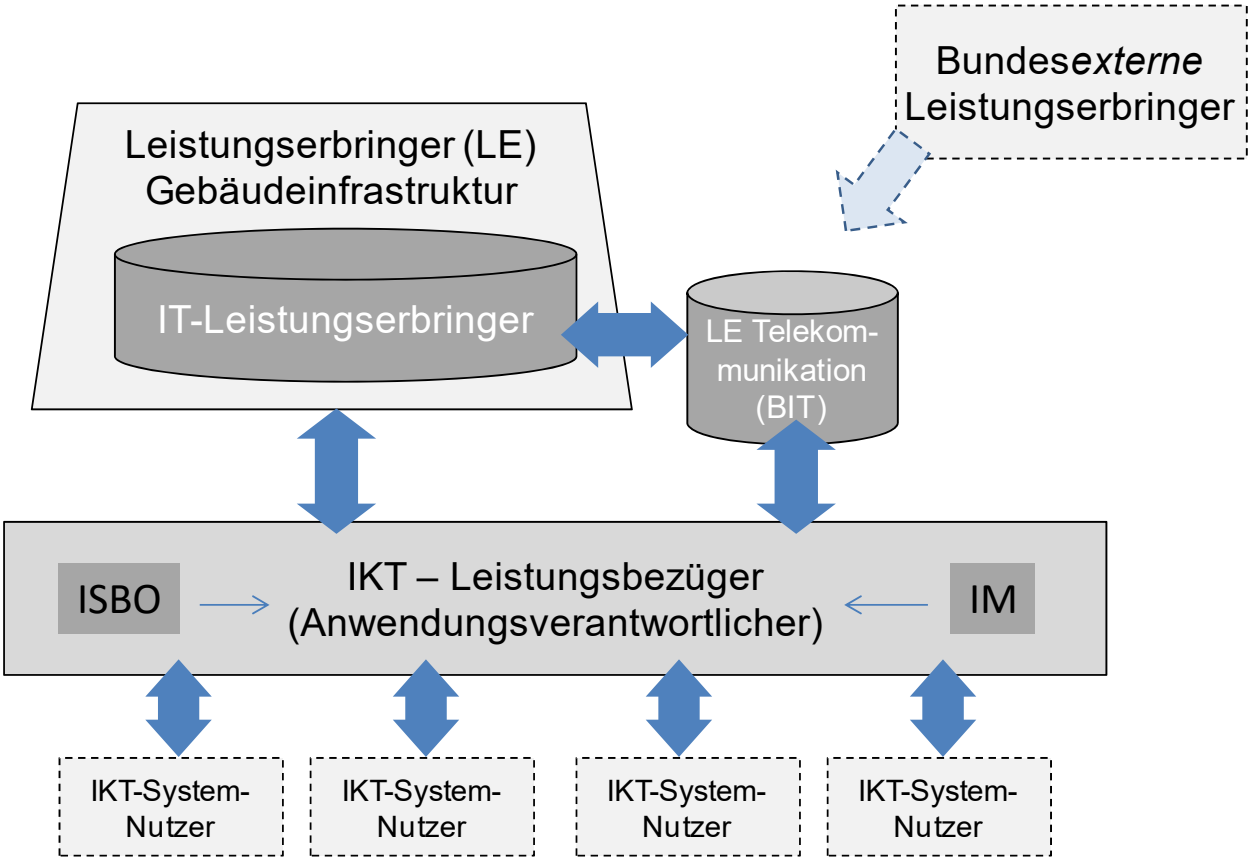
Akteure und ihre Aufgaben im Risikomanagementprozess	
IKT-LE/Bereitsteller (BIT[92], FUB, ISC-EJPD, ISCeco, Informatik EDA, ZAS)	*Risikoidentifikation:* insb. Infrastrukturrisiken für den IKT-Betrieb; *Risikobewertung:* insb. Einschätzung der Eintrittswahrscheinlichkeit und der Auswirkungen auf der Bereitstellungsebene; *Risikobewältigung:* Massnahmenevaluation (zusammen mit dem LB) und Massnahmenumsetzung auf LE-Ebene; *Überwachung:* insb. der technischen Massnahmen und von Änderungen im technischen Umfeld.
IKT-LB/Anwender[93]	*Risikoidentifikation:* insb. auf personeller und organisatorischer Ebene; *Risikobewertung:* insb. die Auswirkungen auf die Aufgabenerfüllung bzw. die Geschäftsprozesse der VE; *Risikobewältigung:* Das BCM des LB umfasst die Evaluation von und den Entscheid über Massnahmen zur Schadenminimierung und zur Wiederherstellung der Prozesse (inkl. Definition der Risikotoleranz bzw. der Sicherheitsanforderungen); Umsetzung der Massnahmen auf Anwenderseite; *Überwachung:* insb. auch der IKT-Nutzer
LE Gebäudeinfrastruktur für IKT (BBL, ar)	*Risikoidentifikation:* insb. in Bezug auf den Einfluss von Infrastrukturrisiken (z. B. Stromunterbrüche) auf IKT-Risiken; *Risikobewertung*: insb. die Auswirkungen auf die Aufgabenerfüllung der IKT-LE *Risikobewältigung:* Evaluation und Umsetzung von baulichen und gebäudetechnischen Massnahmen; *Überwachung:* insb. von baulichen und gebäudetechnischen Massnahmen.
IKT-Nutzer[94]	*Risikoidentifikation: –* *Risikobewertung: –* *Risikobewältigung:* Umsetzung von personellen und organisatorischen Massnahmen (Passwörter etc.); *Überwachung: –*
Bundesexterne LE (Swisscom, EWB, Software-Anbieter etc.)	Es ist wichtig, beim Abschluss von Verträgen mit bundesexternen LE auf deren Einfluss auf die Systeme des Bundes und die damit verbundenen Risiken zu achten und diese wo möglich zu reduzieren (BCM mit Lieferanten abstimmen).

[92] Das BIT ist nicht nur Informationstechnik-LE für mehrere Departemente, es ist auch Hauptleistungserbringer im Bereich der bundesweiten Telekommunikation (Netze) und zudem bundesweit verantwortlich für die Generierung der digitalen Zertifikate (PKI = Public Key Infrastruktur).

[93] Beratend zum Thema IKT-Sicherheit bzw. IKT-Anwendungen stehen den LB/Anwendern in den Departementen und Ämtern die sog. Informatiksicherheitsbeauftragten (ISBD bzw. ISBO) und der Integrationsmanager (IM) zur Verfügung.

[94] IKT-Systemnutzer können auch bundesverwaltungsexterne Benutzer wie Firmen/Bevölkerung/Kantone sein, die auf die IKT des Bundes zugreifen können. Diese sollen in das RM mit einbezogen werden (insb. wegen der Sicherheit).

Zusammenarbeit der Akteure



Zentrale Kompetenzstellen; weitere Informationen

Zentrale Kompetenzstellen:

- ***Bereich DTI der Bundeskanzlei****:* Vorgeben und Überwachen der IKT-Strategie Bund;Digitale Transformation der Bundesverwaltung; Führung der Standarddienste[95].
- ***Bundesamt für Cybersicherheit BACS:*** Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Es ist verantwortlich für die koordinierte Umsetzung der Nationalen Cyberstrategie (NCS).
- ***Bundesamt für Bauten und Logistik (BBL)****:* Verantwortlich für die Unterbringung der zivilen Bundesverwaltung, inkl. IKT-Infrastruktur.
- ***Armasuisse (ar)****:* Verantwortlich für alle Immobilien des VBS, inkl. IKT-Infrastruktur.
- ***Bundesamt für wirtschaftliche Landesversorgung (BWL)****:* Unter anderem strategische Beobachtung der IKT-Entwicklungen und Ergreifen entsprechender Massnahmen.[96]

[95] Bspw. Büroautomation, Datenkommunikation

[96] Vom Erdbeben und dem nachfolgenden Tsunami in Japan waren u. a. auch diverse Hersteller von Computerfestplatten betroffen, was weltweit zu Versorgungsengpässen führte. Das BWL trifft für Ereignisse dieser Art Vorsorgemassnahmen (z. B. Einrichten von Lagerbeständen).

Weitere Informationen und Unterlagen:

- IKT-Strategie des Bundes
- Verordnung über die digitale Transformation und die Informatik (VDTI)
- Verordnung über die Informationssicherheit in der Bundesverwaltung und der Armee (ISV)

Massnahmenoptionen und Best Practices

In einem umfassenden Konzept (i. d. R. ISDS-Konzept) sollen der benötigte Schutzbedarf festgehalten und die notwendigen Massnahmen definiert werden. Regelmässige Aktualisierungen (z. B. bei einem neuen Release der Anwendung) sind durchzuführen. Nachfolgend eine Aufzählung möglicher Massnahmen zur Reduktion von IKT-Risiken:

Organisatorische und personelle Massnahmen:

- Restriktive Zugriffsbeschränkungen für Anwendungen und Daten
- Restriktive Zugangsbeschränkungen zur IKT-Infrastruktur
- 4-Augen-Prinzip pflegen
- Sicherer Umgang mit und Verwendung von starken Passwörtern
- IT-Governance[97] (u. a. auch Nutzungsregeln für Internet und Software)
- Vorbereitung und Einübung eines Business Continuity-Plans für den Fall des Eintritts eines unvorhergesehenen Ereignisses

Technische Massnahmen:

- Einsetzen von Firewall und Antivirenprogramm
- Regelmässiges Back-Up von Daten
- Technische Aufzeichnung der Änderungen an Daten (Erhöhung der Nachvollziehbarkeit)
- Datenverschlüsselung
- Führen von IT-Ereignisprotokollen (sog. Log-Files; sie erhöhen die Nachvollziehbarkeit von Ereignissen)
- Einrichten von automatischen Kontrollen in den Systemen (Plausibilitätskontrolle)

Empfehlungen der EFV an Risikomanager und Risikocoaches

1. ***Prüfen, ob eine Aggregierung notwendig oder sinnvoll ist:***
   - Bei departements- oder verwaltungseinheitsübergreifenden Wechselwirkungen und Auswirkungen sollen IKT-Risiken i. d. R. aggregiert werden, vor allem wenn wichtige Geschäftsprozesse betroffen sind. Das stellt sicher, dass die Wechselwirkungen verstanden, die Gesamtbedeutung erkannt und gemeinsame Massnahmen abgestimmt umgesetzt werden können. Die Koordinationsstelle empfiehlt, auf Stufe Leistungserbringer, Departement und/oder Bund eine Aggregation durchzuführen.
2. ***Prüfen, ob bereits eine zentrale Steuerung existiert:***
   - Auf Stufe Bund hat das ISB in diversen Bereichen eine Steuerungsfunktion bei den IKT-Risiken. Wo das nicht der Fall ist, muss eine Aggregation unter Federführung der Risikocoaches der Leistungserbringer, der Risikomanager der Departemente und/oder der Koordinationsstelle Bund durchgeführt werden.
3. ***Informationen beschaffen und Aufgaben bzw. Verantwortlichkeiten klären:***
   - Sicherstellen, dass alle betroffenen VE bzw. Abteilungen das zu aggregierte IKT-Risiko in ihrem Bereich analysiert und bewertet haben.
   - Prüfen bzw. sicherstellen, dass Aufgaben, Verantwortlichkeiten, Schnittstellen etc. in Bezug auf die Risikobewirtschaftung geklärt sind, z. B. in Service Level Agreements (SLA).

[97] Vgl. ISACA, www.isaca.ch

- IKT-Risiken nötigenfalls in Teilrisiken aufsplitten, damit klare Verantwortlichkeiten zugeteilt werden können.
- Zurückhaltung beim Zusammenfassen von sehr unterschiedlichen IKT-Risiken. Z. B. ist eine Aggregation unter dem umfassenden Titel «IKT-Risiken» nicht sinnvoll (relevante Risikoinformationen gehen verloren; Handlungsbedarf nicht mehr ersichtlich).

4. ***Reporting des aggregierten Risikos:***
   - Die betroffenen IKT-Anwendungen sind aufgrund der zu erwartenden Auswirkungen bei Eintritt des Risikos zu priorisieren. Daraus ergibt sich der «credible worst case» und auch die Priorisierung der Massnahmen.
   - Sicherstellen, dass Wechselwirkungen aufgezeigt werden und in die Analyse mit einbezogen wurden.

5. ***Informationsaustausch:***
   - Die Zusammenarbeit der Informatiksicherheitsbeauftragten der Verwaltungseinheiten (ISBO's) mit den Risikocoaches ist unerlässlich.
   - Einheitliches Vorgehen bei Analyse und Bewertung des zu aggregierenden IKT-Risikos sicherstellen. Nötigenfalls Workshops mit allen Beteiligten. Koordination von Massnahmen unterstützen.
   - Informationsaustausch allgemein fördern (insb. zwischen LE und LB).

B) Infrastrukturrisiken (ohne IKT-Risiken)

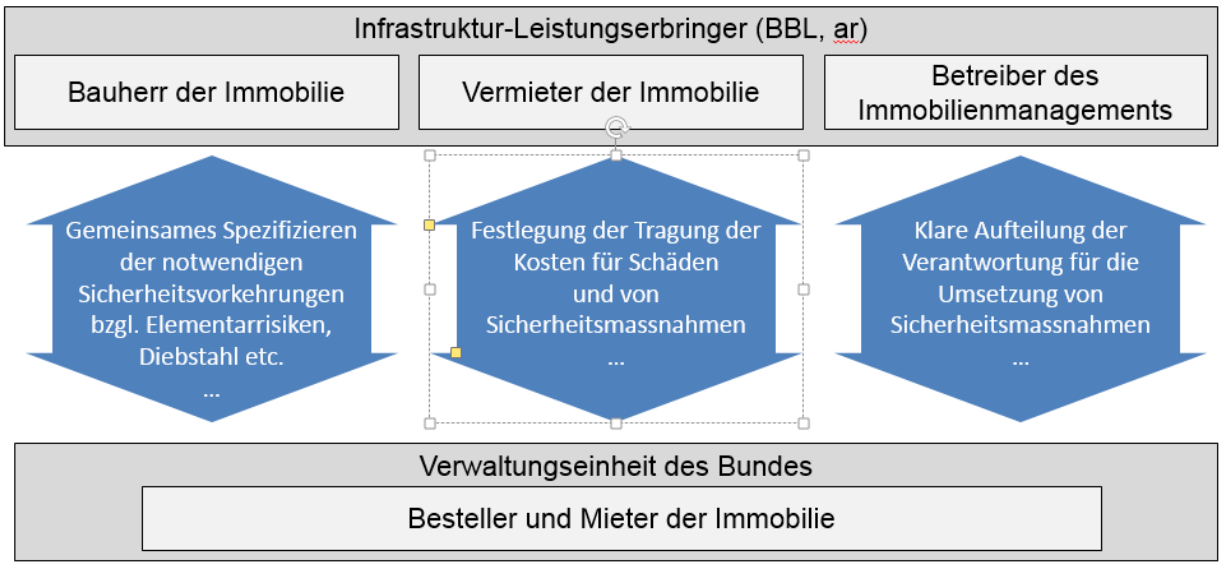
Risikoanalyse
Unter Infrastrukturrisiken werden Risiken verstanden, die negative Auswirkungen auf die Infrastruktur in der Bundesverwaltung haben. Unter Infrastruktur sind in erster Linie die Immobilien der Bundesverwaltung und die für den Betrieb notwendigen Infrastrukturen zu verstehen. Explizit ausgeschlossen sind hier die Informations- und Kommunikationstechnologien[98], die häufig durch andere OE betrieben werden. Folgende Ereignisse (nicht abschliessend) können unter den Begriff «Infrastrukturrisiken» subsummiert werden: a. Elementarereignisse (Hochwasser, Erdbeben, Lawinen) b. Brand c. Stromunterbrüche d. Einbruch und Diebstahl e. Unbefugter Zugang (z. B. in Rechenzentren etc.) f. Vandalismus Sachschäden haben finanzielle Auswirkungen. Zudem sind die Unterbrüche in den Tätigkeiten und Prozessen der VE zu berücksichtigen und zu bewerten. Es kann Verletzte und Tote und auch Reputationsschäden geben. Die Risikoexponierung muss aufgrund der geografischen Lage und der Nutzung der Immobilie im Einzelfall analysiert werden. Schon beim Bau einer Immobilie können Massnahmen zum Schutz gegen Infrastrukturrisiken eingeplant und umgesetzt werden. Dies bedingt ab Projektbeginn eine gute Zusammenarbeit zwischen dem Bauherrn und dem späteren Nutzer des Gebäudes. Bei der Immobilienbewirtschaftung muss klar geregelt werden, wer welche Risiken trägt und wer welche sicherheitstechnischen Massnahmen umsetzt. Beispiele von Wechselwirkungen bei Infrastrukturrisiken: ▪ Infrastrukturschaden (insb. Stromunterbruch) löst IKT-Risiko aus, wenn wichtige IKT-Infrastruktur der Bundesverwaltung im betroffenen Gebäude untergebracht ist.

Akteure und ihre Aufgaben im Risikomanagementprozess	
Infrastruktur-Bereitsteller (BBL, ar)	*Risikoidentifikation*: insb. der bau- und gebäudetechnischen Risiken *Risikobewertung*: insb. Eintrittswahrscheinlichkeiten von technischen Risiken (Brand etc.) *Risikobewältigung*: Vorschläge für technische Massnahmen erarbeiten und Massnahmen umsetzen *Überwachung*: der baulichen (und z. T. organisatorischen) Massnahmen
Bundessicherheitsdienst (BSD; fedpol)	*Risikoidentifikation*: Gefährdungen durch Personen *Risikobewertung*: insb. Bewertung der Eintrittswahrscheinlichkeit aufgrund der aktuellen Lage *Risikobewältigung*: Zutrittskontrollen für Bundesgebäude, Abschrankungen, Personenschutz, Zusammenarbeit mit privaten Sicherheitsdiensten und Kantonspolizei

[98] Ausser die WLAN-Anlagen, welche durch den Gebäudeinfrastruktur-Leistungserbringer bereitgestellt werden.

	Überwachung: stete Überwachung der Sicherheitslage für Personen und Bundesgebäude
VE als Mieterin	*Risikoidentifikation:* – *Risikobewertung:* insb. Auswirkungen auf die Geschäftsprozesse der VE *Risikobewältigung*: Vorschläge für Massnahmen erarbeiten und Umsetzung bzgl. der Gebäude- und Personensicherheit *Überwachung*: v. a. der organisatorischen Massnahmen

Zusammenarbeit der Akteure



Zentrale Kompetenzstelle; weitere Informationen

Bundesamt für Bauten und Logistik (BBL): Wichtige Informationen zu den Dienstleistungen (z. B. Kontroll- und Sicherheitsdienstleistungen) des BBL finden sich auf der bundesinternen BBL-Kundenplattform.

Massnahmenoptionen und Best Practices

- Festlegen von Rettungsausgängen und -wegen
- Vordefinierte Schliesspläne für Immobilien (Gebäudesicherung)
- Installation von Alarmanlagen (inkl. Videoüberwachung)
- Vorbereitung von Notfallprozessen/-abläufen, Evakuierungsübungen[99]
- Gebäudezugangskontrollen
- Notfallorganisation vorbereiten
- Feuerlöscher, Sprinkleranlagen, Gebäudesicherungssysteme usw.
- Versicherungsfragen prüfen (bspw. Sachschäden)[100]

[99] Diese Massnahmen werden durch den Mieter/Nutzer umgesetzt.

[100] Aufgrund des Grundsatzes der Eigenversicherung schliesst der Bund in der Regel keine Versicherungen ab. Die EFV ist für das Versicherungswesen zuständig.

Empfehlungen der EFV an Risikomanager und Risikocoaches

1. ***Prüfen, ob eine Aggregation notwendig oder sinnvoll ist:***
   - Bei departements- oder verwaltungseinheitsübergreifenden Wechselwirkungen sollten Infrastrukturrisiken i. d. R. aggregiert werden. Aufgrund der geografischen Nähe vieler Immobilien im Grossraum Bern empfiehlt die Koordinationsstelle, insb. die Risiken Stromunterbruch[101] und Elementarereignisse aggregiert zu betrachten.
2. ***Prüfen, ob bereits eine zentrale Steuerung existiert:***
   - Die zentrale Steuerung der Infrastrukturen des Bundes erfolgt auf Stufe der Leistungserbringer (BBL, ar). Eine Aggregation der Risiken sollte vorerst auf dieser Stufe umgesetzt werden.
3. ***Informationen beschaffen und Aufgaben bzw. Verantwortlichkeiten klären:***
   - Sicherstellen, dass alle betroffenen VE bzw. Abteilungen das zu aggregierende Infrastrukturrisiko in ihrem Bereich analysiert und bewertet haben.
   - Prüfen bzw. sicherstellen, dass Aufgaben, Verantwortlichkeiten, Schnittstellen etc. in Bezug auf die Risikobewirtschaftung geklärt sind, z. B. in Service Level Agreements (SLA).
4. ***Reporting des aggregierten Risikos:***
   - Die betroffenen Geschäftsprozesse sind aufgrund der Einschätzung der zu erwartenden Auswirkungen bei Eintritt des Risikos zu priorisieren. Daraus ergibt sich der «credible worst case» und auch die Priorisierung der Massnahmen.
5. ***Informationsaustausch:***
   - Informationsaustausch zwischen den Leistungserbringern und den Verwaltungseinheiten als Nutzer fördern.

[101] Für längerfristige Unterbrüche existiert eine interdepartementale Arbeitsgruppe «Priorisierung der Bundesgebäude bei Stromausfall».

C) Vermögensdelikte

Risikoanalyse
Unter ***Korruption*** wird der Missbrauch einer Vertrauensstellung zwecks Erlangung eines ungerechtfertigten materiellen oder immateriellen Vorteils verstanden. Konkrete Formen sind bspw. Bestechung, Vorteilsannahme, Vorteilsgewährung. Bei der ***Veruntreuung*** geht es um die unrechtmässige Aneignung von Vermögenswerten durch Mitarbeitende der Bundesverwaltung. Bei der ***ungetreuen Amtsführung*** werden in einem Rechtsgeschäft die von den Angestellten zu wahrenden öffentlichen Interessen geschädigt, um sich oder einem andern einen unrechtmässigen Vorteil zu verschaffen. Bei ***Insidergeschäften*** werden nicht-öffentliche Informationen von einem Mitarbeitenden zur eigenen Bereicherung ausgenutzt. Neben den finanziellen Auswirkungen, zum Beispiel durch die Bezahlung überhöhter Preise im Beschaffungswesen, sind bei solchen Risiken auch die Reputationsschäden beträchtlich. Nicht alle Verwaltungstätigkeiten sind hinsichtlich Korruption und Veruntreuung gleich stark exponiert. Besonders korruptionsanfällig sind zum Beispiel die Vergabe öffentlicher Aufträge oder Kontakte mit Staaten, die in internationalen Korruptionsratings schlecht abschneiden, aber auch die Steuer-, Revisions-, Aufsichts- und Konzessionserteilungsbereiche, der Grenzkontrollsektor und die Bereiche Justiz und Polizei. Vermögensdelikte treten vor allem in Bereichen auf, in denen Finanzflüsse und Zahlungen gesteuert und ausgelöst werden. Nährboden für solche Risiken sind bspw.: eine unzureichende Bindung oder Loyalität des Arbeitsnehmers gegenüber dem Arbeitgeber, eine erhöhte Anonymität in der Organisation, Arbeitsplatzunzufriedenheit, Frustration, fehlende Motivation, ungenügende Kontrollen, ungenügend geordnete Abläufe und Prozesse. *Wechselwirkungen*: ▪ Aufgedeckte Fälle von Korruption und Veruntreuung können zu Verunsicherung des Personals führen; weitere Mängel in den Organisationsabläufen werden aufdeckt.

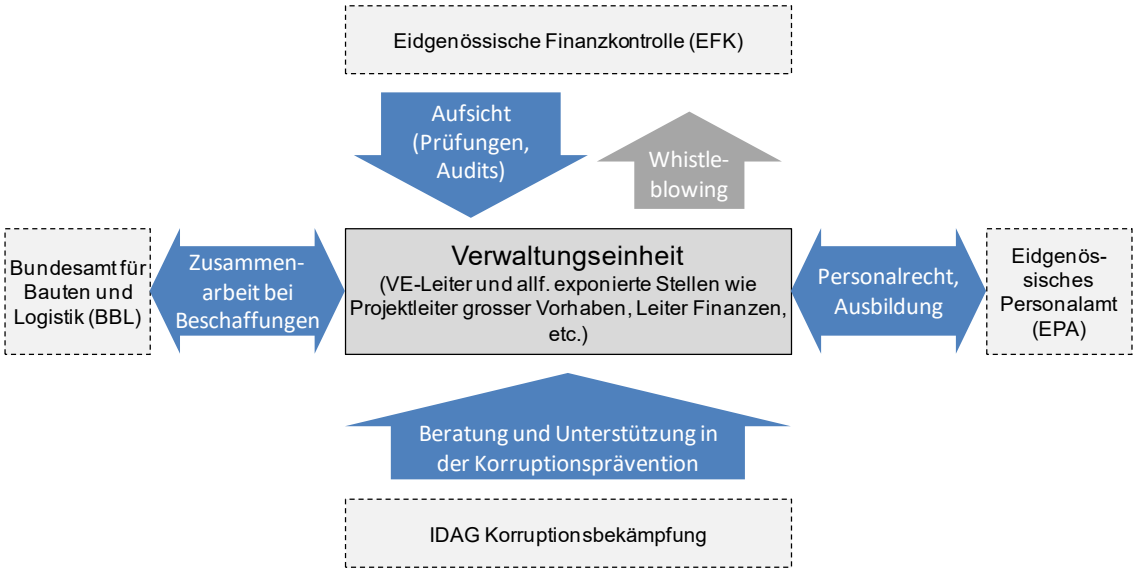
Akteure und ihre Aufgaben im Risikomanagementprozess	
Verwaltungseinheit (insb. Leiter VE; aber auch Grossprojekt-Leiter, Leiter Finanzen, Compliance & Risk Abteilungen etc.)	*Risikoidentifikation*: ja, insb. identifizieren von exponierten Arbeitsstellen *Risikobewertung*: ja *Risikobewältigung*: ja, verantwortlich für die Definition und Umsetzung von Massnahmen *Überwachung*: ja
Eidgenössische Finanzkontrolle (EFK)[102]	*Risikoidentifikation*: ja, z. B. im Rahmen der Rolle als Whistleblowing-Stelle des Bundes *Risikobewertung*: ja *Risikobewältigung*: Empfehlungen zur Reduktion von Korruptions- und Veruntreuungsrisiken *Überwachung*: Audits/Revisionen[103]
IDAG Korruptionsbekämpfung (Federführung EDA)	*Risikoidentifikation: -* *Risikobewertung: -*

[102] Vgl. http://www.efk.admin.ch/index.php?option=com_content&view=article&id=223&Itemid=238&lang=de

[103] Die EFK führt Audits nicht nur im Bereich Korruption durch, sondern in vielen unterschiedlichen Bereichen wie z.B. IT-Sicherheit, IKS etc.

	Risikobewältigung: insb. Vorschläge für Massnahme-*Strategien* erarbeiten[104] *Überwachung*: ja, IDAG Kerngruppe
Bundesamt für Bauten und Logistik (BBL) und armasuisse (ar)	*Risikoidentifikation*: im Bereich Beschaffung *Risikobewertung*: - *Risikobewältigung*: setzt Massnahmen zur Reduktion des Korruptionsrisikos in der Beschaffung um *Überwachung*: -
Eidgenössisches Personalamt (EPA)	*Risikoidentifikation*:- *Risikobewertung*:- *Risikobewältigung*: ja, bundesweite Massnahmen (Vorschriften, Ausbildung etc.) *Überwachung*: -

Zusammenarbeit der Akteure[105]



Zentrale Kompetenzstellen; weitere Informationen

Für Korruption:

- Die ***Interdepartementale Arbeitsgruppe (IDAG) zur Korruptionsbekämpfung*** erarbeitet Strategien zur Korruptionsbekämpfung auf nationaler und internationaler Ebene und lanciert Sensibilisierungs- und Informationskampagnen.
- Das ***Bundesamt für Bauten und Logisitik*** (BBL) ist für das Beschaffungswesen des Bundes zuständig und hat Erfahrung im Bereich der Korruptionsprävention.[106] Es bietet neben Beratungen in der Beschaffung auf seiner Website u. a. ein Faktenblatt zum Thema Korruptionsprävention und Beratung an.

Weitere Informationen:

- ***GIMAP***: Beschaffungswegweiser und interaktiver Führer zum Thema öffentliches Beschaffungswesen

[104] Vgl. Bericht an den Bundesrat März 2011 und Massnahmen für Prävention von Korruption

[105] Das EPA informiert im Rahmen von Personalrechtsausbildungen über die allgemeinen Verhaltensregeln (Verhaltenskodex) der Angestellten und Vorgesetzten. Über die departements- bzw. amtsspezifischen Weisungen z. B. nach Art. 94*d* BPV informieren die Departemente und Ämter intern selber.

[106] Beim BBL sind auch die Beschaffungskommission des Bundes (BKB) und das Kompetenzzentrum Beschaffungswesen Bund (KBB) angegliedert.

- ***Bundespersonalgesetz*** und ***Bundespersonalverordnung*** enthalten Verhaltensvorschriften für Mitarbeitende (bspw. Art. 20, 21 Abs. 3 und 23 BPG; Art. 91 bis 94*d* BPV).
- Weitere Ausführungen finden sich im ***Verhaltenskodex Bundesverwaltung***[107] sowie in den ***Richtlinien zu Nebenbeschäftigungen und öffentlichen Ämtern*** *(EPA)*[108]
- Broschüre Korruptionsprävention und Whistleblowing

Massnahmenoptionen und Best Practices

- Einrichtung und Bekanntmachung der Whistleblowing-Stelle bei der EFK
- Verhaltenskodex Bundesverwaltung und Verhaltensanweisungen der Departemente und Ämter gestützt auf Art. 94*d* BPV (Ausstandsregeln, Annahme von Geschenken etc.)
- regelmässige Information, Sensibilisierungsmassnahmen (insb. durch IDAG Korruptionsbekämpfung) und Schulung der Mitarbeitenden[109]
- Audits und Stichproben
- interne Kontrollen, bspw. das Vier-Augen-Prinzip[110] (hier ist nicht nur die formelle, sondern auch die materielle Prüfung wichtig)
- systemtechnische Kontrollen und Massnahmen (z. B. Zugriffsbeschränkungen und Freigabeerfordernisse, elektronische Visierung)
- materielle Überprüfung der Waren und Dienstleistungen (bei grösseren Zahlungen)
- konsequente Funktionstrennungen
- Personensicherheitsprüfungen bei exponierten Stellen
- Einholen von Referenzen und Prüfung von amtlichen Registern bei Neuanstellungen
- Vorbildfunktion der Vorgesetzten
- Loyalität der Mitarbeitenden erhöhen
- Einführung von Anzeigepflichten und -rechten für Mitarbeitende (Art. 22*a* im BPG)

Spezifische Massnahmen zur Verminderung von Korruption:

- Unbefangenheitserklärungen von exponierten Personen
- Verpflichtung zu schriftlichen Verträgen in der Beschaffung
- zentrales und transparentes Beschaffungsverfahren
- Integritätsklausel in Verträgen mit Lieferanten
- Begründung und Dokumentation von Verfahren und Vergabeentscheiden
- Risikobeurteilung bei der Vergabe von Aufträgen
- konsequente Durchsetzung der Ausstandsregeln

Empfehlungen der EFV an Risikomanager und Risikocoaches

[107] BBl *2012* 7873

[108] In diversen VE wurden spezifischere Verhaltensweisungen erarbeitet (bspw. EFV).

[109] Über Themen der Integrität, bspw. über Anzeigepflichten und Melderecht nach BPG.

[110] Dieses besagt, dass wichtige Entscheidungen nicht von einer einzelnen Person getroffen oder kritische Tätigkeiten nicht von einer einzelnen Person durchgeführt werden sollen oder dürfen, dies um das Risiko von Fehlern oder Missbräuchen zu reduzieren.

1. ***Prüfen, ob eine Aggregation notwendig oder sinnvoll ist*:**
   - Es werden bereits diverse Massnahmen zentral umgesetzt (EPA, EFK, BBL etc.). Verwaltungseinheits- oder departementsübergreifende Wechselwirkungen bestehen keine. Eine Aggregation würde im Wesentlichen nur die Gesamtbedeutung des Risikofeldes aufzeigen. Die Verantwortung für die Bewirtschaftung der Risiken liegt aber bei den VE. Die Koordinationsstelle EFV empfiehlt keine Aggregation.

2. ***Prüfen, ob bereits eine zentrale Steuerung existiert*:**
   - Es gibt diverse zentrale Kompetenzstellen (siehe oben). Diese haben eine beratende Funktion, erarbeiten aber keine aggregierte Risikobetrachtung.

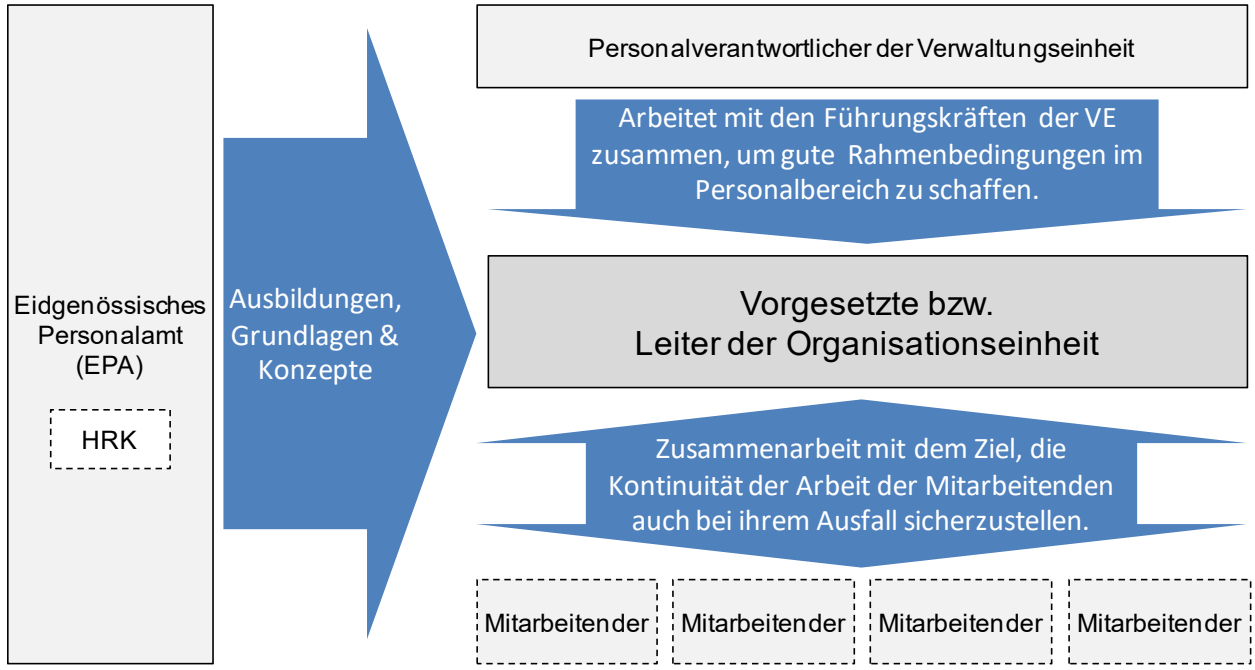
D) Personalrisiken; insbesondere Know-How-Verluste

Risikoanalyse	
Der ***Ausfall von Schlüsselpersonen*** mit speziellem Know-How infolge von Krankheit, Unfall, Kündigung oder aus anderen Gründen kann zu Störungen im Geschäftsablauf der VE, zu Unterbrüchen in wichtigen Prozessen und zu Mehrkosten führen. Ein ***Know-How-Mangel*** in einer VE ist oft auch Ergebnis einer schleichenden Entwicklung: unattraktive Rahmenbedingungen für das Personal, ungenügende Weiterbildungsmöglichkeiten, Fachkräftemangel auf dem Markt usw. Weitere Risiken im Personalbereich können sein: Konzentration von Spezialwissen auf zu wenige Personen, fehlende oder ungenügende Dokumentation von wichtigen Prozessen, fehlendes Wissensmanagement, übermässiger Einsatz von externen Beratern etc. Die Geschwindigkeit, mit der ein Know-How-Ausfall eintritt (unmittelbar bei Todesfall, Ablauf der Kündigungsfrist, planbare Pensionierung) entscheidet massgeblich darüber, wie hoch die negativen Auswirkungen für die VE ausfallen. *Wechselwirkungen*: ▪ Ein Ausfall eines Mitarbeitenden kann zu Schwierigkeiten bei der Arbeitsbewältigung durch die verbliebenen Mitarbeiter und in einem negativen Szenario mittelfristig zu weiteren Abgängen führen.	
Akteure und ihre Aufgaben im Risikomanagementprozess	
Mitarbeitender in einer VE	*Risikoidentifikation*: Erkennen von Prozessen und Know-How, wo eine Dokumentation und eine Stellvertreterregelung notwendig oder sinnvoll ist.[111] *Risikobewertung*: - *Risikobewältigung*: Evaluation von möglichen Massnahmen zusammen mit den Vorgesetzten und Umsetzung von Massnahmen *Überwachung*: -
Führung/Vorgesetzter des Mitarbeitenden	*Risikoidentifikation*: Erkennen von Prozessen und Know-How, wo eine Stellvertreterregelung und eine Dokumentation notwendig oder sinnvoll ist. *Risikobewertung*: ja, Auswirkung eines Ausfalls des Spezialwissens auf die OE einstufen *Risikobewältigung*: Evaluation von möglichen Massnahmen (zusammen mit den Mitarbeitenden) und Massnahmenentscheide treffen (inkl. Definition der Risikotoleranz) *Überwachung*: ja
Personalverantwortlicher der VE	*Risikoidentifikation*: Mängel im Bereich Rekrutierung und Führung in der VE erkennen *Risikobewertung*: - *Risikobewältigung*: Evaluation von möglichen Massnahmen und deren Umsetzung

[111] Dabei muss berücksichtigt werden, dass der betroffene Mitarbeitende einen geringen Anreiz hat, sein Spezialwissen (das einen Teil seiner Qualifikation und seines Marktwertes ausmacht) zu teilen oder zu dokumentieren. Aus diesem Grund stehen vor allem die Führung und die Personalverantwortlichen der OE in der Verantwortung für die Bewirtschaftung dieses Risikos.

	Überwachung: der Wirkung dieser Massnahmen
Eidgenössisches Personalamt (EPA), inkl. Human Resources Konferenz (HRK)[112]	*Risikoidentifikation*: für bundesweite Risiken im Bereich Mitarbeiterrekrutierung und -bindung *Risikobewertung*: - *Risikobewältigung*: Evaluation von möglichen bundesweiten Massnahmen und deren Umsetzung *Überwachung*: -

Zusammenarbeit der Akteure



HRK = Human Resources Konferenz

Zentrale Kompetenzstelle; weitere Informationen

Eidgenössisches Personalamt (EPA): Erarbeitet bundesweite Grundlagen und Konzepte (bspw. zum Thema Mitarbeiterbindung), integriert das Thema Know-How-Verluste in diverse (Kader-)Schulungen etc.

- Grundlagendokumente: Personalstrategie Bundesverwaltung,

Massnahmenoptionen und Best Practices

- Stellvertretungen für die wichtigsten Funktionen/Stellen (Voraussetzung: Identifikation der wichtigsten Funktionen/Stellen bzw. Wissensträger)
- Aufbau eines Wissensmanagements, damit sich das Know-How auf mehrere Personen verteilt
- Personalmarketing für die Rekrutierung von qualifiziertem Personal (zentral im EPA)
- Massnahmen zur Erhöhung der Mitarbeiterbindung (Retention Management): modernes Arbeitsumfeld, konkurrenzfähige Anstellungsbedingungen, Karriereentwicklungsmodelle, Kompetenzmodelle etc. (zentral im EPA)

[112] Die Human Resources Konferenz hat den Lead bei der Koordination und Umsetzung der bundesrätlichen Personalpolitik. Mitglieder sind die Personalchefs der Departemente und der Bundeskanzlei.

- nachvollziehbare Dokumentation von Geschäftsprozessen
- Förderung des informellen Austausches zwischen Mitarbeitenden
- Zurückhaltung bei längerfristigen Einsätzen von externen Beratern
- frühzeitige Nachfolgeplanung bei der Pensionierung von Wissensträgern

Empfehlungen der EFV an Risikomanager und Risikocoaches

1. ***Prüfen, ob eine Aggregation notwendig oder sinnvoll ist:***
   - Es gibt bereits zentral umgesetzte Massnahmen (EPA; HRK). Keine Wechselwirkungen zwischen den VE. Eine Risikoaggregation würde somit v. a. dem Zweck dienen, die Gesamtbedeutung des Risikofeldes auf Stufe Departement und Bund aufzuzeigen. Die Verantwortung für die Bewirtschaftung der Risiken liegt aber bei jeder einzelnen VE. Die Koordinationsstelle EFV empfiehlt keine Aggregation.
2. ***Prüfen, ob bereits eine zentrale Steuerung existiert:***
   - Es gibt eine zentrale Kompetenzstelle (EPA). Diese hat eine rein beratende Funktion und führt keine Risikoaggregation durch.
3. ***Informationsaustausch:***
   - Ein regelmässiger Austausch zwischen den Personalverantwortlichen der VE kann hilfreich sein, um Ansätze und Ideen zur Minderung dieser Risiken auszutauschen und von guten Beispielen innerhalb der Bundesverwaltung zu lernen.

E) Ungenügendes IKS zur Sicherstellung der Ordnungsmässigkeit der Staatsrechnung

Risikoanalyse

Die Buchführung der Bundesverwaltung ist dezentral organisiert. Jede Verwaltungseinheit erfasst die Buchungsvorgänge selber und ist demnach auch selber für die Einhaltung der rechtlichen Vorschriften zur Ordnungsmässigkeit der Staatsrechnung verantwortlich. Die Finanzberichterstattung (Erstellung der Staatsrechnung) hingegen wird zentral in der EFV vorgenommen.

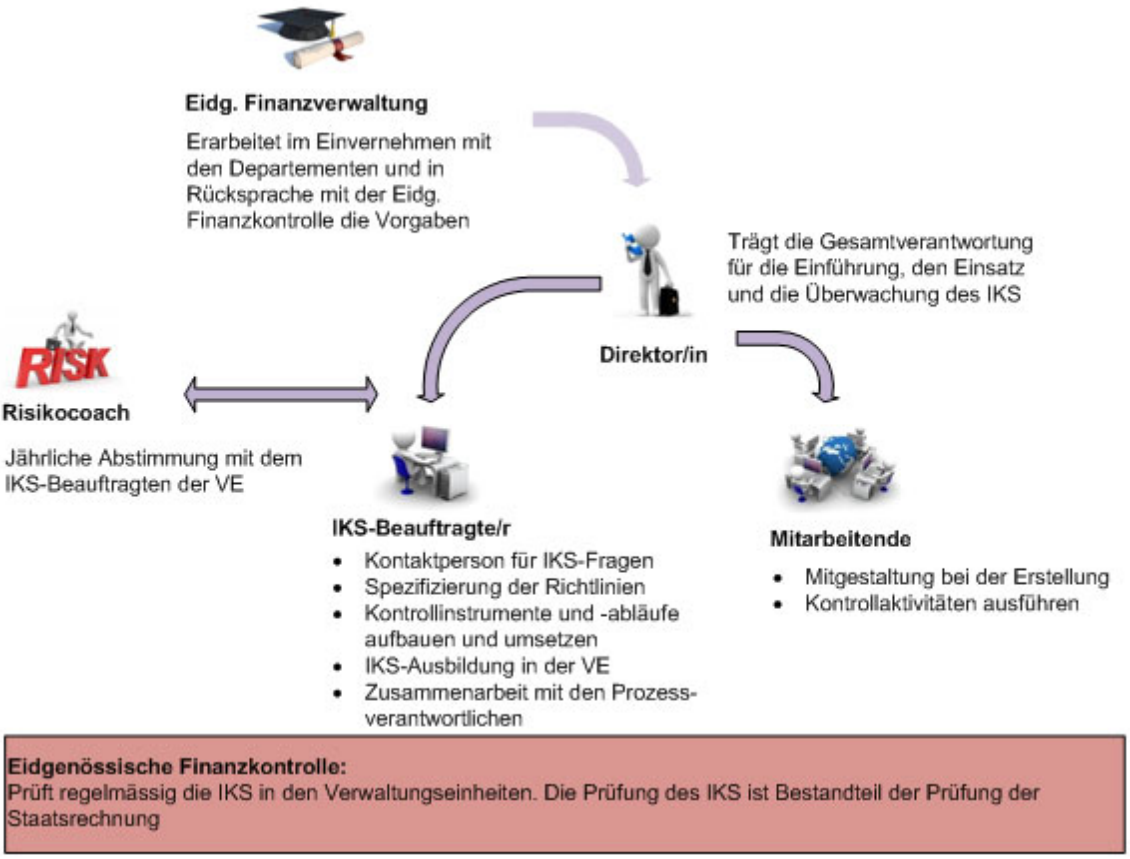
Die Ordnungsmässigkeit der Staatsrechnung umfasst folgende Aspekte:

- Grundsätze ordnungsmässiger Buchführung (Art. 38 FHG und 28 FHV):
  - Vollständigkeit: Alle Finanzvorfälle und Buchungstatbestände sind lückenlos und periodengerecht zu erfassen.
  - Richtigkeit: Die Buchungen müssen den Tatsachen entsprechen und sind nach den Weisungen der EFV vorzunehmen.
  - Rechtzeitigkeit: Die Buchhaltung ist aktuell zu halten und der Geldverkehr tagesaktuell zu erfassen. Die Vorgänge sind chronologisch festzuhalten.
  - Nachprüfbarkeit: Die Vorgänge sind klar und verständlich zu erfassen. Korrekturen sind zu kennzeichnen und Buchungen durch Belege nachzuweisen.
- Grundsätze ordnungsmässiger Rechnungslegung (Art. 47 FHG und 54 FHV):
  - Wesentlichkeit: Es sind sämtliche Informationen offen zu legen, die für eine rasche und umfassende Beurteilung der Vermögens-, Finanz- und Ertragslage notwendig sind.
  - Verständlichkeit: Die Informationen müssen klar und nachvollziehbar sein.
  - Stetigkeit: Die Grundsätze der Budgetierung, Buchführung und Rechnungslegung sollen soweit als möglich über einen längeren Zeitraum unverändert bleiben.
  - Bruttodarstellung: Aufwände und Erträge sowie Investitionsausgaben und -einnahmen sind getrennt voneinander ohne gegenseitige Verrechnung in voller Höhe auszuweisen.

Das Interne Kontrollsystem (IKS) ist ein zentrales und geeignetes Instrument zur Sicherstellung der Ordnungsmässigkeit der Buchführung und Rechnungslegung in den Verwaltungseinheiten. Fehlt ein solches oder ist es in wesentlichen Teilen mangelhaft, besteht das Risiko, dass die veröffentlichte Finanzberichterstattung der Bundesverwaltung wesentliche Fehlaussagen enthält. Die Finanzberichterstattung des Bundes dient der öffentlichen Rechenschaftsablage gegenüber den Bürgern und als Entscheidungsgrundlage für Politiker, Anleger und Rating-Agenturen. Wesentliche Fehlaussagen in der Finanzberichterstattung ziehen deshalb nicht nur einen Reputationsschaden nach sich, sondern können auch die Entscheidungsgrundlagen für Politiker, Anleger und Rating-Agenturen verfälschen.

Akteure und ihre Aufgaben im Risikomanagementprozess	
Oberste Führungsebene (Direktorin / Direktor)	*Risikoidentifikation*: ja *Risikobewertung*: ja *Risikobewältigung*: ja, verantwortlich für das IKS in ihrem / seinem Zuständigkeitsbereich *Überwachung*: ja
IKS-Beauftragte/r	*Risikoidentifikation:* ja *Risikobewertung*: ja, die Risiko-Kontroll-Matrizes werden regelmässig überprüft und erneuert *Risikobewältigung*: nein, höchstens für ihren / seinen Zuständigkeitsbereich als Linienvorgesetzte/r *Überwachung*: ja, koordiniert die Überwachungstätigkeiten in der VE
Prozessverantwortliche/r finanzrelevanter Geschäftsprozesse	*Risikoidentifikation:* ja, in ihrer / seiner Funktion als Linienvorgesetzte/r kennt die/der Prozessverantwortliche die Risiken in ihrem / seinem Prozess *Risikobewertung*: ja, die Risiko-Kontroll-Matrizes werden regelmässig überprüft und erneuert *Risikobewältigung*: ja, mittels Durchsetzung der IKS-Massnahmen in ihrem / seinem Zuständigkeitsbereich als Linienvorgesetzte/r *Überwachung*: ja, überwacht das Risikomanagement in ihrem / seinem Zuständigkeitsbereich
Mitarbeitende in finanzrelevanten Geschäftsprozessen	*Risikoidentifikation*: nein *Risikobewertung*: nein *Risikobewältigung*: ja, bei der Durchführung der Kontrollen in der täglichen Arbeit *Überwachung*: nein
Eidgenössische Finanzverwaltung	*Risikoidentifikation:* nein *Risikobewertung:* nein *Risikobewältigung:* nein *Überwachung:* nein
Eidgenössische Finanzkontrolle	*Risikoidentifikation:* ja *Risikobewertung*: ja *Risikobewältigung*: nein *Überwachung*: nein

Zusammenarbeit der Akteure



Zentrale Kompetenzstelle; weitere Informationen

Eidgenössische Finanzverwaltung (EFV): Erarbeitet bundesweite Grundlagen und Vorgaben zu den Themen Buchführung, Rechnungslegung und IKS und integriert die Themen in Kurse und Ausbildungen.

- Grundlagendokumente: Handbuch für die Haushalt- und Rechnungsführung, Kapitel 4.8

Massnahmenoptionen und Best Practices

- Um die Ordnungsmässigkeit der Buchführung und Rechnungslegung in der Staatsrechnung sicher zu stellen, ist gemäss Art. 39 FHG in den Verwaltungseinheiten der zentralen Bundesverwaltung ein wirksames und zweckmässiges Internes Kontrollsystem einzurichten. Die notwendigen Massnahmen sind im IKS-Leitfaden der EFV beschrieben. Dieser ist im Handbuch für die Haushalt- und Rechnungsführung in Kapitel 4.8 abrufbar.

Empfehlungen der EFV an Risikomanager und Risikocoaches

Die EFV empfiehlt, im Risikomanagement der Verwaltungseinheit das Risiko der fehlenden Ordnungsmässigkeit in der Buchführung und Rechnungslegung regelmässig zu beurteilen und die Existenz und das dauernde Funktionieren des Internen Kontrollsystems in der Verwaltungseinheit zu prüfen.

Anhang 11: Muster «Risikostrategie» für Departemente / BK sowie VE

Generelle Hinweise:

1. *Eine Risikostrategie soll kurz und konzis verfasst sein (max. 2 A4-Seiten). Sie präzisiert, wie die Risikopolitik des Bundesrates in der Organisationseinheit umgesetzt wird und welche Ziele damit erreicht werden sollen.*
2. *Die Weisungen des Bundesrates und die Richtlinie der EFV zum Risikomanagement sollen in der Risikostrategie grundsätzlich nicht wiederholt werden. Ergänzend kann darauf verwiesen werden.*
3. *Das vorliegende «Muster» dient als Gestaltungshilfe. Es ist an die konkreten Bedürfnisse der Organisationseinheit anzupassen.*

1 Gegenstand

Die vorliegende Risikostrategie zeigt, wie die Geschäftsleitung die Weisungen des Bundesrates über die Risikopolitik des Bundes vom 24.09.2010 umsetzen will. Das Risikomanagement unterstützt die Geschäftsleitung bei der Aufgabenerfüllung und Zielerreichung.

2 Ziele des Risikomanagements

Unsere wichtigsten Ziele sind:

– Ziel 1:

– Ziel 2:

– Ziel x:

3 Grundsätze der Umsetzung

Bei der Umsetzung gelten für uns folgende Grundsätze:

– Wir berücksichtigen die Risikodimension bei der Führungsarbeit auf allen Stufen und beziehen das Risikomanagement bei allen Planungs- und Strategieprozessen aktiv ein.

– Mindestens zweimal jährlich führt die Geschäftsleitung im Rahmen der Risikoberichterstattung einen strukturierten Risikodialog zur Risikoexposition, fokussiert auf die wesentlichen Risiken und prüft die Umsetzung und Wirksamkeit der Massnahmen.

– Die Geschäftsleitung setzt sich mindestens alle vier Jahre vertieft mit ihrem Risikomanagement auseinander. Sie überprüft dabei das Risiko- und Massnahmenportfolio von Grund auf, evaluiert mögliche neue Risikofelder auf mittlere Sicht und beurteilt die Zusammenarbeit mit dem Risikomanagement.

– Der Risikocoach tauscht sich periodisch mit den Verantwortlichen der weiteren Bereiche der Führungsunterstützung über die aktuelle Risikolage aus.

4 Risikobewältigung

Mit unseren Risiken gehen wir wie folgt um:

– Für identifizierte Risiken evaluieren wir risikominimierende Massnahmen. Der Aufwand für solche Massnahmen darf nicht höher als der erwartete Nutzen sein. Entscheide obliegen der Linie und werden dokumentiert.

– Der Risikoeigner überwacht die Umsetzung und die Wirksamkeit der beschlossenen Massnahmen.

– Wir legen bei jedem Risiko fest, welches Reduktionsziel mit den Massnahmen erreicht werden soll.
– Über das Massnahmencontrolling wird der Geschäftsleitung im Rahmen des Risikoreportings Bericht erstattet.

5 Funktionen und Verantwortlichkeiten

Die Geschäftsleitung berät und verabschiedet zweimal jährlich eine Risikoberichterstattung. Diese wird vom Risikocoach in Zusammenarbeit mit den Risikoeignern und nach Konsultation der Massnahmenverantwortlichen vorbereitet.

Dem Risikocoach stehen gemäss Pflichtenheft <xx> Stellenprozente für die Erfüllung seiner Aufgaben zur Verfügung. Er hat in dieser Funktion direkten Zugang zur Amtsleitung und zu den Abteilungsleitenden. Im Übrigen gelten für die Aufgaben und Verantwortlichkeiten im Risikomanagement die Beschriebe in Ziffer 3 der Richtlinie EFV über das Risikomanagement Bund.

6 Schlussbestimmungen

Diese Risikostrategie tritt am <Datum> in Kraft. Sie wird spätestens <Jahr> überprüft und der Geschäftsleitung zur neuen Beschlussfassung vorgelegt.

Ort/Datum/Unterschrift Amtsdirektor/in