EIDGENÖSSISCHE FINANZKONTROLLE
CONTRÔLE FÉDÉRAL DES FINANCES
CONTROLLO FEDERALE DELLE FINANZE
SWISS FEDERAL AUDIT OFFICE

Prüfung des Risikomanagements Bund als Führungsinstrument

Eidgenössisches Finanzdepartement, Eidgenössische Finanzverwaltung

EFK-17476 | inkl. Stellungnahmen | 3. Mai 2018 | FinDel D4/2018

Bestelladresse Adresse de commande Indirizzo di ordinazione Ordering address	Eidgenössische Finanzkontrolle (EFK) Monbijoustrasse 45 3003 Bern Schweiz
Bestellnummer Numéro de commande Numero di ordinazione Ordering number	1.17476.600.00183
Zusätzliche Informationen Complément d'informations Informazioni complementari Additional information	www.efk.admin.ch info@efk.admin.ch twitter: @EFK_CDF_SFAO + 41 58 463 11 11
Abdruck Reproduction Riproduzione Reprint	Gestattet (mit Quellenvermerk) Autorisée (merci de mentionner la source) Autorizzata (indicare la fonte) Authorized (please mention source)

Inhaltsverzeichnis

Prüfung des Risikomanagements Bund als Führungsinstrument

Eidgenössisches Finanzdepartement, Eidgenössische Finanzverwaltung

Das Wesentliche in Kürze

Die Risiken der Bundesverwaltung (BVerw) sind vielfältig und können in einzelnen Fällen mit sehr negativen Auswirkungen verbunden sein. Jüngstes Beispiel ist die Zahlung für Bundesbürgschaften von 215 Millionen Franken für die Hochseeflotte der Schweiz[1].

Mit dem Risikomanagement Bund (RM) sollen Risiken des Bundes identifiziert, analysiert und gesteuert werden. Alle Einheiten der BVerw sind verpflichtet, ein RM zu führen. Am Ende des jährlichen Risikoreporting-Prozesses, welcher von der Eidgenössischen Finanzverwaltung (EFV) gesteuert wird, steht die Risikoberichterstattung an den Bundesrat. Nach dem Bundesratsbeschluss wird dieses Reporting auch einer Arbeitsgruppe der Geschäftsprüfungskommission zur Verfügung gestellt.

Risikomanagement: ein unabdingbares Führungsinstrument, das weiterentwickelt werden muss

Insgesamt lässt sich das Fazit ziehen, dass das RM einen guten Entwicklungsstand hat, aber noch zu wenig als Führungsinstrument mit strategischer Ausrichtung genutzt wird. Eine Ursache hierfür ist nach Ansicht der Eidgenössischen Finanzkontrolle (EFK) die ungenügende Integration des RM in die Führungsprozesse. Die Ausgestaltung des RM ist bei den geprüften Verwaltungseinheiten (VE) sehr unterschiedlich.

Es besteht grosser Handlungsspielraum bei der Umsetzung für die Departemente und die VE. Umso wichtiger ist die Rolle der Koordinationsstelle bei der EFV, die trotz geringem Ressourceneinsatz und als Querschnittsamt ohne Weisungsbefugnis wesentlich dazu beiträgt, dass die EFK in allen geprüften VE eine gute Risikokultur feststellen konnte. Das Thema RM ist bei Kadern und Mitarbeitenden präsent. Ein wesentlicher Erfolgsfaktor ist dabei die Nähe der Risikomanager und Risikocoaches zur Departements- bzw. Amtsleitung.

Die Identifikation und Beurteilung der Risiken erfolgen Bottom-Up. Eine Top-Down-Betrachtung, welche die Risiken berücksichtigt, die sich aus der Strategie und beispielsweise den Legislaturzielen einer Einheit bzw. eines Departementes ergeben, lässt sich lediglich bei einer der geprüften Einheiten feststellen. Dadurch ist die Sicht in den VE sehr stark auf operative Risiken beschränkt. Mit wenigen Ausnahmen herrscht eine isolierte Betrachtung der Risiken innerhalb einer VE vor. Der Einbezug von Stakeholdern bzw. die Berücksichtigung von Beziehungen zu anderen (VE- oder departementsüberschreitenden) Risiken konnte nur in wenigen Fällen beobachtet werden.

[1] Medienmitteilung des Bundesrats, Bürgschaften bei Hochseeschiffen: Verkaufsverträge unterschrieben, Botschaft Nachtragskredit verabschiedet, 18.5.2017, https://www.admin.ch/gov/de/start/dokumentation/medienmitteilungen/bundesrat.msg-id-66775.html

Problematische Handhabung der Risiken

Die Bewältigung und das Überwachen von Risiken überzeugt in vielen Teilen nicht. Massnahmen sind griffiger zu formulieren. Ein Massnahmencontrolling lässt sich nicht bzw. nur vereinzelt feststellen. Kenngrössen (z. B. aus dem Controlling), die als Indikatoren für Veränderungen der Risiken dienen und in die Risikobewertung einfliessen könnten, fand die EFK bei den geprüften VE kaum vor.

Die geprüften VE haben keine auf ihre Bedürfnisse abgestimmte Risikostrategie definiert. Die Höhe der für die VE tragbaren Risiken und die risikomindernden Grundstossrichtungen sind dadurch nicht festgelegt. Die Risikoberichterstattung und -kommunikation ist in der heutigen Form überwiegend gut.

Bei der Steuerung von Querschnittsrisiken (Risiken, die in einer ähnlichen Form und Ausprägung bei vielen oder gar allen VE des Bundes vorhanden sind) erkannte die EFK erhebliche systemische Schwachstellen bei der Durchsetzung der risikomindernden Massnahmen und bei der Kommunikation. Die aktuelle Konfiguration der Kommunikation der Querschnittsrisiken stellt nicht sicher, dass die Massnahmen zur Behandlung der Querschnittsrisiken in allen betroffenen VE bekannt oder gar umgesetzt werden. Dies erachtet die EFK als erheblichen Mangel.

Audit de la gestion des risques de la Confédération en tant qu'instrument de pilotage

Département fédéral des finances, Administration fédérale des finances

L'essentiel en bref

L'administration fédérale est exposée à des risques variés dont les conséquences peuvent parfois se révéler très négatives, comme ce fut récemment le cas avec le paiement de cautionnements par la Confédération à hauteur de 215 millions de francs pour la flotte suisse de haute mer[1].

La gestion des risques de la Confédération a pour but d'identifier, d'analyser et de piloter les risques auxquels est exposée l'administration fédérale. Toutes les unités administratives (UA) doivent se doter d'un processus de gestion des risques. En fin d'année, le processus annuel de gestion des risques piloté par l'Administration fédérale des finances (AFF) débouche sur un rapport sur les risques à l'attention du Conseil fédéral. Après son adoption par le Conseil fédéral, ce rapport est également mis à la disposition d'un groupe de travail des Commissions de gestion des Chambres fédérales.

La gestion des risques, un instrument de pilotage indispensable qui doit encore évoluer

Globalement, on peut affirmer que la gestion des risques de la Confédération a atteint un bon niveau de maturité. Mais cet instrument de pilotage est encore trop peu utilisé dans sa dimension stratégique. Selon le Contrôle fédéral des finances (CDF), cela est dû au fait que la gestion des risques n'est pas suffisamment intégrée dans les processus de conduite. Dans les UA examinées, la gestion des risques est mise en œuvre de façon très variable.

Les départements et les UA disposent d'une grande marge de manœuvre. Le rôle de coordination qui incombe à l'AFF est donc d'autant plus important. Malgré les faibles ressources disponibles et le fait qu'elle assume des tâches interdépartementales sans avoir le pouvoir de donner des directives, elle contribue dans une large mesure à ce que le CDF ait pu relever l'existence d'une bonne culture en matière de risque dans toutes les UA examinées. Les cadres et le personnel sont conscients de la problématique de la gestion des risques. La proximité des responsables et conseillers de la gestion des risques avec la direction du département et celle de l'office, est l'un des principaux facteurs de ce bon résultat.

L'identification et l'évaluation des risques se font selon une approche ascendante (bottom up). Une approche descendante (top down), qui prend en compte les risques découlant de la stratégie et, par exemple, des objectifs pour la législature d'une unité ou d'un département, n'a été constatée que dans l'une des unités examinées. Ainsi, la réflexion des UA se limite très fortement aux risques opérationnels. À quelques exceptions près, les

[1] Communiqué de presse du Conseil fédéral, Cautionnement de navires de haute mer: signature des contrats de vente et approbation du message sur le crédit supplémentaire, 18.5.2017, https://www.admin.ch/gov/fr/accueil/documentation/communiques/communiques-conseil-federal.msg-id-66775.html

risques sont envisagés de manière isolée au sein des UA et une prise en compte des différentes parties concernées ou des relations avec les autres risques (touchant plusieurs UA ou départements) n'a pu être observée que dans quelques cas.

Traitement des risques problématique

Sous bien des aspects, la maîtrise et la surveillance des risques sont peu convaincantes. Les mesures doivent être formulées de manière plus précise. Aucun suivi des mesures (controlling) n'a pu être constaté, sauf dans des cas isolés. Dans les UA examinées, le CDF n'a pratiquement pas pu trouver d'indicateurs (issus par exemple du controlling) qui pourraient être utilisés pour mesurer l'évolution des risques et pour les évaluer.

Les UA examinées n'ont pas défini de stratégie en matière de risques adaptée à leurs besoins. Il s'ensuit que ni le niveau des risques qu'elles peuvent supporter, ni leurs axes d'intervention pour atténuer ces risques n'ont été déterminés. Dans leur forme actuelle et dans l'ensemble, le rapport sur les risques et leur communication sont de bonne qualité.

S'agissant du pilotage des risques transversaux (risques de même type et de même intensité qui affectent de nombreuses UA, voire toutes les UA de la Confédération), le CDF a constaté des faiblesses systémiques d'importance dans le cadre de la communication et de la mise en application des mesures visant à atténuer les risques. La structure actuelle de la communication relative aux risques transversaux ne garantit pas que les mesures destinées à remédier à ce type de risques soient connues ou même mises en œuvre dans toutes les UA concernées. Le CDF considère qu'il s'agit là d'une lacune majeure.

Texte original en allemand

Verifica della gestione dei rischi della Confederazione quale strumento di direzione

Dipartimento federale delle finanze, Amministrazione federale delle finanze

L'essenziale in breve

I rischi a cui è esposta l'Amministrazione federale sono molteplici e nel singolo caso possono essere legati a ripercussioni molto negative. L'esempio più recente è costituito dal pagamento di 215 milioni di franchi in fideiussioni federali per la flotta svizzera d'alto mare[1].

La gestione dei rischi mira a identificare, analizzare e gestire i rischi della Confederazione. Le unità dell'Amministrazione federale sono tenute a effettuare una gestione dei rischi. Alla fine della rendicontazione annuale sui rischi, coordinata dall'Amministrazione federale delle finanze (AFF), viene redatto il rapporto sui rischi all'attenzione del Consiglio federale. Dopo la decisione del Consiglio federale, il rapporto viene messo a disposizione anche di un gruppo di lavoro della Commissione della gestione.

Gestione dei rischi: uno strumento di gestione indispensabile da sviluppare ulteriormente

Nel complesso si può concludere che la gestione dei rischi è ben sviluppata ma il suo utilizzo come strumento di gestione con orientamento strategico è inadeguato. Secondo il Controllo federale delle finanze (CDF) una delle cause risiede nella insufficiente integrazione della gestione dei rischi nei processi di direzione. L'impostazione della gestione dei rischi varia molto nelle unità amministrative (UA) esaminate.

I dipartimenti e le UA hanno un ampio margine di manovra di attuazione. Il ruolo del servizio di coordinamento della gestione dei rischi, aggregato all'AFF, riveste pertanto una particolare importanza, perché nonostante un impiego ridotto delle risorse e in veste di ufficio trasversale senza potere impartire istruzioni esso contribuisce in maniera sostanziale al fatto che il CDF abbia potuto constatare una buona cultura del rischio in tutte le UA oggetto di esame. Quadri e collaboratori sono ben a conoscenza dell'argomento della gestione dei rischi. Un importante fattore di successo è la vicinanza dei gestori e dei coach dei rischi alla direzione del dipartimento e dell'ufficio.

L'identificazione e la valutazione dei rischi viene effettuata in base all'approccio dal basso verso l'alto (bottom up). Un'osservazione dei rischi dall'alto verso il basso (top down), che considera i rischi che potrebbero risultare dalla strategia e, ad esempio, dagli obiettivi di legislatura di un'unità o un dipartimento è stata osservata soltanto presso una delle unità oggetto di esame. Quando si analizzano le UE ci si limita pertanto ai rischi operativi. Salvo poche eccezioni, nelle UA vige una considerazione dei rischi isolata. Il coinvolgimento di stakeholder e la considerazione di relazioni con altri rischi (che interessano altre UA o altri dipartimenti) è stato osservato soltanto in alcuni casi.

[1] Comunicato stampa del Consiglio federale del 18.5.2017, Fideiussioni per navi d'alto mare: firmati i contratti di vendita e adottato il messaggio sul credito aggiuntivo, https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-66775.html

Trattamento problematico dei rischi

La gestione e la sorveglianza dei rischi non convince in molti ambiti. Le misure devono essere formulate in maniera più incisiva. Non è stato individuato un controlling delle misure o lo è stato solo in singoli casi. Nelle UA oggetto di esame, il CDF non ha praticamente identificato valori appropriati (ad es. dal controlling) che potrebbero servire da indicatori per le variazioni dei rischi e che potrebbero confluire nella loro valutazione.

Le UA oggetto di esame non hanno definito una strategia dei rischi adeguata alle loro esigenze. Pertanto il livello di rischi sopportabili da un'UA e gli orientamenti di base per la riduzione dei rischi non sono stati stabiliti. Nella loro forma attuale i rapporti e la comunicazione sui rischi sono per lo più buoni.

Per la gestione dei rischi trasversali (rischi di stessa natura e di stessa intensità presenti in molte o forse in tutte le UA della Confederazione) il CDF ha riconosciuto importanti lacune sistemiche nell'attuazione delle misure per ridurre i rischi e nella comunicazione. L'attuale configurazione della comunicazione dei rischi trasversali non garantisce che le misure per il trattamento di questi ultimi siano conosciute o persino attuate in tutte le UA interessate. Il CDF ritiene che ciò sia una grave lacuna.

Testo originale in tedesco

Audit of the Confederation risk management as a management tool

Federal Department of Finance, Federal Finance Administration

Key facts

The risks of the Federal Administration (Fed. Adm.) are diverse and can, in certain cases, be associated with very negative effects. The most recent example is the payment of CHF 215 million for federal sureties for Switzerland's deep-sea fleet[1].

The Confederation risk management's role is to identify, analyse and manage federal risks. All units of the Fed. Adm. are obliged to perform risk management. At the end of the annual risk reporting process, which is managed by the Federal Finance Administration (FFA), the risk disclosure statement is submitted to the Federal Council. Following the Federal Council's decree, this report is also made available to a working group of the Control Committee.

Risk management: an indispensable management tool which needs further development

Overall, the conclusion can be made that risk management is well developed but not used enough as a management tool with strategic orientation. The reason for this is that, in the view of the Swiss Federal Audit Office (SFAO), risk management is insufficiently integrated in management processes. Risk management configuration varies greatly between the administrative units audited.

The administrative departments and units enjoy a lot of flexibility in its implementation. The role of the coordination unit at the FFA which, despite few resources and a lack of power to issue instructions as a cross-divisional office, is all the more important and has significantly contributed to a good risk culture across all the audited administrative units, as the SFAO confirmed. Managers and staff members are aware of risk management. A major success factor is the risk managers' and risk coaches' proximity to department and office management.

Identification and assessment of risk is made on a bottom-up basis. A top-down approach which takes into account the risks arising from a unit's or department's strategy or legal requirements, was only found in one of the audited units. This means the perspective of the administrative units was extremely limited to operative risks. With a few exceptions, the isolated consideration of the risks within each administrative unit prevails. The involvement of stakeholders or the consideration of connections with other (cross-administrative unit or cross-departmental) risks was only observed in a few cases.

[1] Federal Council press release, Guarantees for deep-sea vessels: sales agreements signed, dispatch on supplementary budget issued, 18.5.2017, https://www.admin.ch/gov/en/start/documentation/media-releases/media-releases-federal-council.msg-id-66775.html

Problematic handling of risks

Management and monitoring of risks is insufficient in many sections. Measures should be formulated more firmly. Controlling of measures was only occasionally observed, if at all. In the audited administrative units, the SFAO hardly found any parameters (e.g. from controlling) which serve as indicators for changes in the risks and which could flow into the risk assessment.

The audited administrative units have not defined risk strategies which match their needs. The level of tenable risks for the administrative units and the risk-reducing overall objectives are therefore not defined. The risk disclosure statements and communication are generally good in their current form.

The SFAO found significant systematic weaknesses in the management of intersecting risks (risks which exist in a similar shape and form in many or even all federal administrative units) with regards to the enforcement of risk-reducing measures and in terms of communication. The current configuration of the communication of intersecting risks does not ensure that the measures for managing intersecting risks are known or even implemented in all the administrative units concerned. The SFAO considers this to be a considerable deficiency.

Original text in German

Generelle Stellungnahme der EFV

Die Befunde und Beurteilungen des Prüfberichts decken sich mit den Erfahrungen der EFV in der Koordination des Risikomanagements Bund über weite Strecken. Mit der Topdown-Perspektive, der Integration des Risikomanagements in die (strategischen) Steuerungsprozesse oder auch dem Massnahmencontrolling geht der Bericht auf wesentliche Elemente eines erfolgreichen Risikomanagements ein. In diesem Sinne hält die EFV die Stossrichtungen der EFK-Empfehlungen für folgerichtig und hilfreich auf dem Weg, das RM-System des Bundes kontinuierlich zu verbessern. Die EFV wird sich im Rahmen ihrer Zuständigkeit für die Umsetzung der Empfehlungen einsetzen.

1 Auftrag und Vorgehen

1.1 Ausgangslage

Gestützt auf Artikel 39 des Finanzhaushaltsgesetzes (FHG)[2] betreibt die Bundesverwaltung (BVerw) das Risikomanagement Bund, nachfolgend nur noch Risikomanagement (RM) genannt. Der Bundesrat trägt die Gesamtverantwortung. Das RM wird durch die Eidgenössische Finanzverwaltung (EFV) fachlich betreut. Die Umsetzung obliegt den Departementen und den einzelnen VE.

Das RM wurde ab dem Jahr 2003 aufgebaut. Die Rechtsgrundlage im FHG besteht seit dem 1. Mai 2006. In den Weisungen über die Risikopolitik des Bundes vom 24. September 2010 legt der Bundesrat unter anderem Folgendes fest:

Unter Risiko werden Ereignisse und Entwicklungen verstanden, die mit einer gewissen Wahrscheinlichkeit eintreten und wesentliche negative finanzielle und nicht finanzielle Auswirkungen auf die Erreichung der Ziele und die Erfüllung der Aufgaben der BVerw haben.

Das RM hat zum Ziel:

a) mögliche künftige Ereignisse und Entwicklungen vorauszusehen und die Entscheidungsfindung von Bundesrat und BVerw zu unterstützen;

b) die Sicherheit der Vertreterinnen und Vertreter des Bundes zu gewährleisten;

c) das Vermögen und die Reputation des Bundes zu schützen;

d) die verfügbaren Mittel wirksam und wirtschaftlich einzusetzen.

Das RM ist ein Führungsinstrument. Es ist fester Bestandteil der Geschäfts- und Führungsprozesse und gehört zur sorgfältigen und wirtschaftlichen Aufgabenerfüllung.

Erkannte Risiken sind möglichst zu vermeiden oder zu vermindern.

Da es um die Zielerreichung und Aufgabenerfüllung des Bundes geht, sind die relevanten Risiken für das RM eher strategischer Natur.

Die Verantwortlichkeiten werden in den „Richtlinien über das Risikomanagement Bund“ der EFV vom 31. März 2016 festgelegt:

Der Bundesrat trägt die Gesamtverantwortung für die Risiken und das Risikomanagement der BVerw. Die Departementsvorsteherin oder der Departementsvorsteher trägt die Verantwortung für die Risiken des Departements. Die Leiterin oder der Leiter der Verwaltungseinheit (VE) trägt die Verantwortung für die Risiken der VE.

Die nach diesen Regelungen identifizierten und behandelten Risiken durchlaufen je nach Gewichtung von Eintretenswahrscheinlichkeit und Auswirkung die Hierarchiestufen der BVerw.

Für das Erfassen und Verwalten der Risiken steht mit «R2C» (Risk to Chance) eine zentrale IT-Anwendung zur Verfügung.

[2] SR 611.0

1.2 Prüfungsziel und -fragen

Im Fokus der vorliegenden Prüfung stand die Überprüfung der Wirksamkeit des RM.

Die Prüfungsfragen lauten:

1. Wird das RM als Führungsinstrument eingesetzt?
2. Setzen die VE und Departemente die RM-Prozesse so um, dass die wesentlichen Risiken transparent identifiziert und kommuniziert / eskaliert werden?
3. Werden die wesentlichen Risiken ausreichend bewirtschaftet?
4. Gibt es mögliche Effizienzsteigerungen bzw. könnte etwas vereinfacht werden?

Eine inhaltliche Bewertung der jeweiligen Risikokataloge hinsichtlich Vollständigkeit und Korrektheit erfolgte nicht.

1.3 Prüfungsumfang und -grundsätze

Die Prüfung wurde von Petra Kuhn, Daniel Hasler, Stefan Wagner, Philippe Richard und Peter König (Revisionsleitung) mit Unterbrüchen vom 1. Mai bis 10. November 2017 durchgeführt. Das Team arbeitete unter der Supervision von Regula Durrer.

Die Prüfung fand neben der Sektion Risikomanagement und Versicherungspolitik der Eidgenössische Finanzverwaltung (EFV) vor allem bei ausgewählten VE der BVerw statt. Ausschlaggebend für die Wahl waren die Risikolage gemäss Risikolandkarte aus «R2C», aber auch die Grösse und das Aufgabengebiet der VE:

- Bundesamt für Strassen (ASTRA)
- Bundesamt für Meteorologie und Klimatologie (MeteoSchweiz)
- Eidgenössische Zollverwaltung (EZV)
- Bundeskanzlei (BK)
- Generalsekretariat des Eidgenössischen Departements für auswärtige Angelegenheiten (GS-EDA); einbezogen wurden die Direktion für Ressourcen (DR), die Direktion für Völkerrecht (DV) und die Konsularische Direktion (KD)
- Informatiksteuerungsorgan des Bundes (ISB).

1.4 Unterlagen und Auskunftserteilung

Von allen VE wurden die von der EFK verlangten Unterlagen umgehend zur Verfügung gestellt. Die Gesprächspartner standen zur Verfügung und gaben offen Auskunft.

Die EFK dankt allen in dieser Prüfung beteiligten Mitarbeiterinnen und Mitarbeitern der Bundesverwaltung für die gewährte Unterstützung.

1.5 Schlussbesprechung

Die Schlussbesprechung fand am 6. März 2018 statt. Teilgenommen haben:

EFV	Vizedirektorin
	Co-Leiterin und Co-Leiter Sektion Risikomanagement und Versicherungspolitik
GS-EFD	Risikomanager
EFK	Stellvertretende Direktorin
	Fachbereichsleiterin (Verantwortliche für die Prüfung)
	Revisionsleiter

Die EFK dankt für die gewährte Unterstützung und erinnert daran, dass die Überwachung der Empfehlungsumsetzung den Amtsleitungen bzw. den Generalsekretariaten obliegt.

EIDGENÖSSISCHE FINANZKONTROLLE

2 Ein effektives Risikomanagement ist für die Bundesverwaltung und das Parlament essenziell

Jüngste Risikoeintritte wie bei den Bürgschaften für die Hochseeschifffahrt oder die Cyberattacken zeigen, dass Risiken bestehen, welche die BVerw nicht oder nur ungenügend erkannt hat und grosse Schäden angerichtet haben.

Ein funktionierendes RM ist für den Bund ein zentrales Instrument, was man nicht zuletzt daran erkennt, dass der Bundesrat eine Liste der wesentlichsten Risiken, sog. Top-Risiken, auf seiner Ebene führt. Teilweise übernehmen Departementsvorsteher/innen (DV) die Rolle als Risikoeigner und somit die Verantwortung für die Steuerung des Risikos.

Die Koordination des RM-Systems liegt in der Verantwortung der EFV, welche auch die Rolle eines Querschnittsamtes über die gesamte BVerw wahrnimmt. Wie in anderen Querschnittsfunktionen der BVerw verfügt die EFV über keine Weisungsbefugnis gegenüber den anderen VE. Sie erarbeitet und pflegt die methodischen Standards und Referenzdokumente des RM Bund, instruiert die Anwender, koordiniert die Risikoberichterstattung und stellt die Anwendung «R2C» zur Verfügung. In diesem zentralen Tool werden die Risiken erfasst und bewertet, sowie die Massnahmen und deren Umsetzungsstand dokumentiert. Aus dem Tool werden standardisierte Berichte (Reporting) zu den strategischen Risiken erstellt. Dazu gehört ein jährlicher Bericht des Bundesrates an die Geschäftsprüfungskommissionen (GPK) der eidgenössischen Räte (Arbeitsgruppe Risikoreporting), die die Top-Risiken des Bundes analysiert und würdigt.

In ihrem jüngsten Bericht vom 30. Januar 2018[3] weisen die GPK darauf hin, dass sie einige Punkte nicht abschliessend beurteilen konnten. Zu diesen finden sich im vorliegenden Bericht ergänzende Ausführungen. Zu erwähnen sind die mangelhaften Rückmeldungen an die VE (Kapitel 3 des vorliegenden Berichts) und die Behandlung von Querschnittsrisiken (Kapitel 6). Des Weiteren verweisen die GPK bezüglich der Frage der Nutzung des RM als Führungsinstrument auf die Prüfung der EFK. In den Kapiteln 3 und 4 des vorliegenden Berichts wird auf diese Fragestellung näher eingegangen.

In das RM sind alle Verwaltungsstufen des Bundes eingebunden. Die VE und die Generalsekretariate identifizieren, analysieren, bewerten, steuern und kommunizieren die Risiken, die durch das Erfüllen ihrer Aufgaben entstehen. Alle weiteren beteiligten Stellen sind beratend, analysierend, unterstützend und kommunizierend tätig.

Die Hierarchie des RM kann der nachstehenden Abbildung 1 entnommen werden.

[3] https://www.parlament.ch/centers/documents/de/bericht-mm-gpk-n-2018-02-02-d.pdf

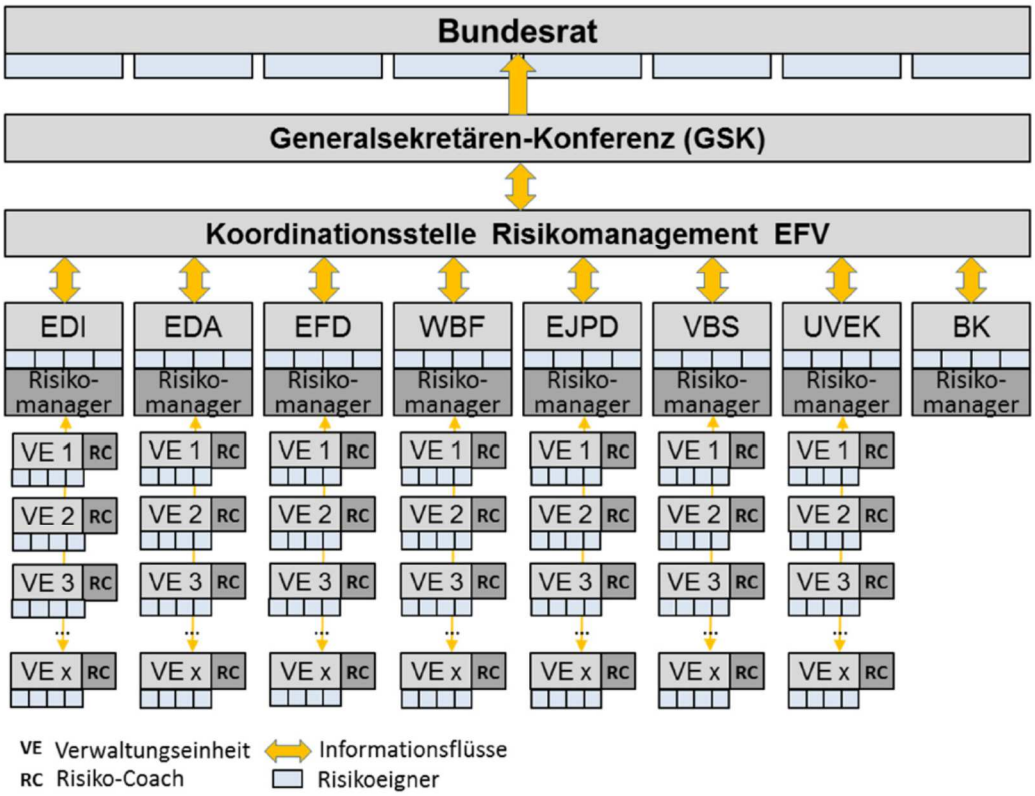


Abbildung 1: Organisation Risikomanagement Bund (Quelle EFV)

Die je nach Hierarchiestufe und Rolle unterschiedlich ausfallenden Aufgaben verlangen nach einer differenzierten Nutzung des RM als Führungsinstrument. In den VE herrscht eine operative Betrachtungsweise der Risiken vor.

3 Die Top-Risiken des Bundesrates werden Bottom-Up identifiziert

Die DV können sich durch die Amtsdirektorinnen und -direktoren oder durch den Risikomanager des Departements über die aktuelle Risikolage informieren lassen. Die Risikomanager der Departemente informieren in der Regel zweimal jährlich (November/Dezember und im Juni), im Rahmen des von der EFV koordinierten Risikoreportings oder Risikoupdates. Nicht geregelt sind Auslöser und Art der Information an die DV durch die Amtsdirektorinnen und -direktoren. Verbindlich ist lediglich, dass bei einer Verschärfung der Risikosituation umgehend zu informieren ist.

In nahezu allen geprüften VE wurden die Risiken stark «Bottom-Up», also überwiegend aus den operativen Tätigkeiten (Tagesgeschäft und Projekte) identifiziert. Die von der EFV im Handbuch geforderte «Top-Down»-Identifizierung entlang des gesetzlichen Auftrags und der Zielsetzungen (z. B. anhand von Strategie und Legislaturzielen) der VE findet bei den meisten geprüften Einheiten noch nicht statt, der Fokus liegt auf den operativen Risiken. Die strategische Risikobetrachtung ist bei den geprüften VE erst teilweise im Aufbau. Formell etabliert ist diese ab Stufe Departement.

Im Rahmen der periodischen Aktualisierung (Start jeweils im Sommer, Abschluss im November) werden von jedem Amt die Top-Risiken an den Risikomanager des Departements gemeldet. Dabei greifen departementsspezifische Vorgaben. Aus den Meldungen aller VE und des Generalsekretariats bestimmt die oder der DV die Top-Risiken des Departements, basierend auf den von der EFV definierten Schwellenwerten für die Bundesratsrisiken. Diese Top-Risiken werden durch die Sektion Risikomanagement und Versicherungspolitik der EFV (in Abb. 1 als Koordinationsstelle bezeichnet) durch einen Vergleich mit den bisherigen Meldungen und Rückfragen plausibilisiert. Beigezogen werden dabei die Abteilung Ausgabenpolitik der EFV und der Bereich Lageanalyse und Krisenfrüherkennung der BK. Nach dieser Plausibilisierung und methodologischen Prüfung der Risikobeschreibung findet eine bilaterale Besprechung zwischen der EFV und dem Generalsekretär des jeweiligen Departements statt.

In einem nächsten Schritt werden diese Top-Risiken des Bundes in der Generalsekretärenkonferenz (GSK) behandelt. Nebst einer Prüfung von Vollständigkeit und Plausibilisierung geht es in dieser um das Festlegen der Querschnittsrisiken, also Risiken, die mehrere VE betreffen. Für solche wird eine verantwortliche VE festgelegt, welche mangels Weisungsbefugnis allerdings eine eher koordinierende Rolle einnimmt (siehe Kapitel 6). Das Ergebnis ergibt dann die Liste der Top-Risiken des Bundes.

Nach der Behandlung in der GSK bereitet die Koordinationsstelle das Risikoreporting für das betreffende Geschäftsjahr in seiner finalen Version auf. Danach erfolgt der Beschluss durch den Bundesrat.

Das RM wird im Bundesrat als ordentliches Geschäft behandelt. Allfällige Rückfragen fliessen über die ordentlichen Prozesse an die als verantwortlich bezeichneten Stellen. Die Überwachung der risikomindernden Massnahmen erfolgt über die normale Geschäftskontrolle und das nächste Risikoreporting. Die Kommunikation des Bundratsbeschlusses zum Risikoreporting an die VE erfolgt nach Ermessen der Departemente. Vereinzelt hatten die VE keine Kenntnis davon, insbesondere nicht über sie betreffende Querschnittsrisiken.

Beurteilung

Das RM ist ab Departementsstufe bis hin zur Behandlung im Bundesrat in die ordentliche Geschäftsabwicklung integriert. Die Prüfung der Risiken erfolgt über mehrere Stufen hinweg. Zusätzlich ergibt ein Abgleich zwischen den Top-Risiken und den Einschätzungen des Bereichs Lageanalyse und Krisenfrüherkennung der Bundeskanzlei weitere Sicherheit für die Vollständigkeit und korrekte Bewertung der Risiken auf Stufe Bundesrat.

4 Die Verwaltungseinheiten setzen das Risikomanagement zu wenig als Führungsinstrument ein

In allen geprüften VE konnte die EFK feststellen, dass das Thema RM an sich einen hohen Stellenwert geniesst. Die Amtsleitungen und die weiteren befragten Führungskräfte beziehen klare Positionen für das RM und verlangen dies auch von ihren Mitarbeitenden. Mit Letzteren wurden Interviews geführt, aus denen hervorgeht, dass durchwegs ein gutes Bewusstsein für das Thema vorhanden ist.

4.1 Das Risikomanagement ist trotz der klaren Positionierung kaum mit Führungsprozessen verbunden

Die EFV empfiehlt im Handbuch zum RM, «den Strategie- und den Controlling-Prozess (Finanzplanung und Voranschlag) mit dem Risikomanagementprozess der VE zu vernetzen».

Eine systematische, im RM-Prozess der VE festgehaltene Schnittstelle zum Controlling-Prozess wurde nur bei MeteoSchweiz festgestellt. Sofern Massnahmen aus dem RM wesentliche finanzielle und/oder personelle Ressourcen benötigen, fliesst dieser Bedarf bei allen geprüften VE in die entsprechenden Planungen ein. Das Beantragen und die allfällige Genehmigung dieser Mittel erfolgen mit dem ordentlichen Voranschlagsprozess. Die EFK fand keine Hinweise dafür, dass Risiken aufgrund nicht genehmigter Mittel zur Massnahmenumsetzung wieder vom Risikokatalog entfernt wurden.

Einige VE lassen die Massnahmen aus dem RM in die Zielvereinbarungen der verantwortlichen Mitarbeitenden einfliessen. Systematisch wird dies beispielsweise beim ASTRA und bei MeteoSchweiz gemacht.

Die Integration der (Top-)Risiken in ein Management-Informationssystem (MIS) wurde nur bei MeteoSchweiz festgestellt.

4.2 Das Risikomanagement ist selten auf die Geschäftsstrategie abgestimmt

Bei den VE werden die Geschäftsstrategie und das RM überwiegend isoliert betrachtet und nicht in Bezug zueinander gebracht. Zu erwarten wäre einerseits, dass die mit der Umsetzung der Geschäftsstrategie verbundenen Risiken erkannt werden. Andererseits müsste, sofern überhaupt definiert, die Risikostrategie mit der Geschäftsstrategie abgestimmt sein.

Die meisten der geprüften VE verfügen über keine eigene Risikostrategie und basieren auf den allgemeinen Aussagen in Kapitel 1.2 des Handbuchs zum RM (der Bund ist bereit, nicht vermeidbare Risiken bewusst und kontrolliert einzugehen, Grundsatz der Eigenversicherung). Dadurch fehlen VE-spezifische Grundsätze zu Risikotoleranz (wie viel Risiko sind wir bereit zu tragen), aber auch vor allem zur Risikosteuerung (wie führen wir die Risiken an die definierte Toleranzschwelle). Die EFK stellt fest, dass bei den meisten getroffenen Massnahmen das Vermindern der Risiken ohne definierten Zielzustand bzw. ohne Abwägen von

Aufwand und Nutzen der Massnahmen im Vordergrund steht. Der im Handbuch zum RM festgehaltene Grundsatz «Der Bund ist bereit, Risiken kontrolliert und bewusst einzugehen, sofern dies für die Zielerreichung bzw. die Aufgabenerfüllung unvermeidbar ist», weicht einer deutlich feststellbaren Risikoaversion.

4.3 Überlegungen, wie nach einem Risikoeintritt vorzugehen ist, fehlen oft

Massnahmen bei Risikoeintritt, zum Beispiel beim Übergang in ein Krisenmanagement oder ein Business Continuity Management (BCM), sind nur vereinzelt, etwa bei der KD des EDA, definiert worden.

Hingegen wurden Risikoeintritte der Vergangenheit durch einige VE analysiert. Zu erwähnen ist hier das ASTRA. Es wurden nicht nur Massnahmen zur Verbesserung der betroffenen Projekte ergriffen. Das ASTRA nutzte die Chance und verbesserte auch das RM an sich.

Beurteilung

Die in den «Weisungen zur Risikopolitik des Bundes» vom Bundesrat vorgegebene Anforderung einer Einbettung des RM in die Geschäfts- und Führungsprozesse ist nach Ansicht der EFK noch nicht erreicht. Die wenigen derzeit im Handbuch vorhandenen Ausführungen zur Verknüpfung dieser Prozesse sind noch nicht zielführend. Einerseits weisen diese nicht auf die entsprechende Verantwortung der Departemente und der VE hin, andererseits zeigen sie als Lösungsansatz lediglich die Integration von Finanzplanung und Budgetierung auf.

Die Top-Risiken des Bundes werden durch die Departementsleitungen, Generalsekretärenkonferenz und den Bundesrat im Dezember sowie im Sommer mit dem Risiko-Update behandelt. Nach Ansicht der EFK drängt sich kein engerer Reporting-Rhythmus auf. Bedingung ist allerdings, dass die umgehende Informationspflicht bei einer wesentlichen Veränderung der Risikosituation eingehalten wird.

Auf Stufe VE ist die Integration des RM in die Führungsprozesse zu verstärken. Insbesondere die Schnittstellen von und zu Planungs- und Steuerungsprozessen sollten definiert werden. Der Stand der Top-Risiken des Amtes muss in der gleichen Periodizität wie wichtige Projekte oder Leistungsdaten zu Kernaufgaben den Direktionen vorgelegt werden.

Empfehlung 1 (Priorität 1)

Die EFK empfiehlt der EFV, konkrete Massnahmen zu einer stärkeren Integration des Risikomanagements in die Führungsprozesse zu definieren und die Umsetzung einzuleiten.

Stellungnahme der EFV

Die EFV ist mit der Analyse und der Beurteilung der EFK einverstanden. Nach Massgabe ihrer Kompetenzen wird die EFV die Kader und RM-Stäbe im Rahmen von Workshops und Schulungen verstärkt bei der Integration des RM in die Führungsprozesse unterstützen.

Beurteilung

Die in vielen VE fehlenden Risikostrategien sind eine der Ursachen dafür, dass das RM noch zu wenig als Führungsinstrument genutzt wird. Die Definition einer Risikostrategie verlangt von den Geschäftsleitungen unter anderem die Klärung der Fragen, in welchem Umfang sie

bereit und in der Lage sind, Risiken zu tragen (Risikotoleranz) und wie und mit welchen Instrumenten die Risiken auf das tolerierbare Mass reduziert werden sollen.

Empfehlung 2 (Priorität 1)

Die EFK empfiehlt der EFV, Vorgaben zu den Departements- bzw. VE-spezifischen Risikostrategien zu etablieren. Im Vordergrund sollte dabei die inhaltliche Auseinandersetzung mit diesem Thema und ein gemeinsames Verständnis stehen. Die schriftlich festgehaltene Risikostrategie soll hingegen kurzgehalten werden. Elemente wie Risikotoleranz der VE, Stossrichtung der risikominimierenden Massnahmen und eine Aussage zum angestrebten Kosten-Nutzen-Verhältnis der angeordneten Massnahmen müssen jedoch darin enthalten sein. Eine methodische Unterstützung der VE durch die EFV ist nötig.

Stellungnahme der EFV

Die EFV ist mit der Empfehlung grundsätzlich einverstanden. Sie wird das Handbuch RM Bund um eine kommentierte Mustervorlage für Risikostrategien ergänzen und ihre Schulungen des RM-Personals entsprechend erweitern. Im Hinblick auf gewisse inhaltliche Elemente bestehen hingegen Vorbehalte: Risikotoleranz und Massnahmentiefe können in aller Regel nur auf das einzelne Risiko bezogen werden, da es sich bei den meisten Risiken des Bundes – zumal bei den strategischen Risiken – um singuläre Fälle handelt. Soweit homogene Risikotypen eruierbar sind (selten), können Toleranz und Massnahmen auch auf diese bezogen werden. Eine globale Festlegung für die gesamte VE wäre aber aus Sicht der EFV jedenfalls zu summarisch und nicht zielführend.

Beurteilung

Zu wenig in die Führungsprozesse integriert sind Massnahmen, welche nach einem Risikoeintritt zum Tragen kommen. Ein BCM oder ein Krisenmanagement können nicht losgelöst von Geschäftsprozessen und RM betrachtet werden. Die zum Prüfungszeitpunkt bei den VE vorhandenen Bedenken über den administrativen Aufwand für das Einrichten dieser Instrumente können ausgeräumt werden, wenn die Zusammenhänge und das Potenzial dargelegt und erkannt werden. Die EFK ist der Meinung, dass hier durch eine tiefere methodische Unterstützung der EFV aufgezeigt werden sollte, wie sich RM, BCM und Krisenmanagement gegenseitig ergänzen und unterstützen. Der EFK ist bewusst, dass dies im aktuellen Umfeld ohne eine Prioritätenänderung im Aufgabenportfolio der Koordinationsstelle RM nicht möglich ist. Mit Bedauern nimmt die EFK zur Kenntnis, dass sich die GSK im Januar 2017 für eine Koordinationsstelle BCM bei der EFV ausgesprochen hat, dieser jedoch keine zusätzlichen Ressourcen zustand und im Gegenzug auf eine vertiefte Begleitung und Schulungen der Ämter verzichtete.

5 Der dezentrale Ansatz führt zu unterschiedlichen Risikomanagement-Reifegraden in den Verwaltungseinheiten

Die Prüfung bei den einzelnen VE zeigte, dass für diese ein grosser Handlungsspielraum in der Umsetzung besteht. Die EFK fand unterschiedliche Lösungen und Reifegrade vor.

Das RM basiert auf der Norm ISO 31000. Diese sieht folgende Elemente vor:

- Risikomanagement-Organisation
- Risikomanagement-Strategie
- Risiko-Identifikation und -Erfassung
- Risiko-Analyse und -Bewertung
- Risiko-Steuerung und -Überwachung
- Risikokommunikation.

In Anlehnung an den Revisionsstandard Nr. 2 (Prüfung des RM-Systems durch die Interne Revision) des Deutschen Instituts für Interne Revision hat die EFK den Stand des RM-Systems in den jeweiligen Einheiten mit einem Prüfleitfaden (Tabellenkalkulation) beurteilt. Die Beurteilung jedes dieser Elemente erfolgte auf einer Skala von «voll erfüllt» = 3 Punkte, «deutliche Verbesserungspotenziale» = 2 Punkte, «nicht erfüllt» = 1 Punkt. Im Folgenden wird auf jedes der RM-Elemente kurz eingegangen.

In Beilage 3 findet sich eine Illustration der Ergebnisse pro geprüfte Einheit.

Im Folgenden beschränkt sich der Bericht auf exemplarische Aussagen zu den geprüften Einheiten.

5.1 Die Risikomanagement-Organisation ist insgesamt ausreichend

EFV, Sektion Risikomanagement und Versicherungspolitik

Die Organisation der Sektion Risikomanagement und Versicherungspolitik ist definiert, die Dotation beträgt 200 Stellenprozente. Die Mitarbeitenden der Sektion steuern einerseits den Prozess des jährlichen Risikoreportings und sollen andererseits für eine einheitliche Anwendung der RM-Methodik sorgen. Andererseits bilden sie die Verantwortlichen des Bundes im RM aus (ordentliche Fachkurse, massgeschneiderte Workshops), sind benutzerseitig für die RM-Applikation verantwortlich und entwickeln das RM-System weiter. Die Sektion fungiert überdies als Koordinationsstelle für das BCM Bund.

Umsetzung in den geprüften Verwaltungseinheiten, besondere Feststellungen

In der BK wurde das RM organisatorisch in den Bereich «integrale Sicherheit» eingebettet. Die Verantwortlichen des Bereichs haben direkten Zugang zur Geschäftsleitung.

Die EZV hat ein Risikoboard eingerichtet, in dem die bezeichneten Risikoexperten (Vertreter verschiedener Fachrichtungen, z. B. IT-Sicherheit) sitzen. Im Board findet eine Koordination und ein Erfahrungsaustausch statt.

Das ASTRA hat die vorhandenen Grundlagen (Weisungen des Bundesrates, Richtlinien der EFV, Handbuch der EFV) in amtsspezifischen Dokumenten weiter ausgeführt.

MeteoSchweiz verfügt über zertifizierte Prozesse. Dies führt zu einer erweiterten Ausgestaltung des RM, da beispielsweise Schnittstellen zu anderen Prozessen (z. B. Planungsprozesse) eindeutig definiert sein müssen.

In Einzelfällen ist die für das RM verfügbare Kapazität der Risikocoaches zu knapp bemessen oder deren hierarchische Ansiedlung ist zu tief oder die Stellvertretung ist nicht geregelt.

Die Funktionsträger des RM haben grösstenteils die von der EFV angebotenen Schulungen durchlaufen.

Beurteilung

Die RM-Organisation ist in allen geprüften VE etabliert und kann in den meisten Fällen als gut beurteilt werden.

Verbesserungspotenzial besteht in einzelnen Fällen bei Kapazitäten, Stellvertretungen und ungenügender Nähe von Risikocoach, Risikomanager oder Risikoeigner zur Geschäfts- bzw. zur Departementsleitung. Die betreffenden VE wurden durch die EFK auf mögliche Massnahmen zur Verbesserung der Durchschlagskraft des RM aufmerksam gemacht.

Das Erstellen (und periodische Nachführen) von spezifischen, auf die VE zugeschnittenen Grundlagendokumenten zum RM verlangt ein sorgfältiges Abwägen von Nutzen und Aufwand. Die vom ASTRA geführte Dokumentation ist umfangreich. Die Grösse und die Dezentralisierung des Amtes fordern konkrete, direkt anwendbare Regeln. Die Dokumentation ist nach Angaben des ASTRA nun auch vollständig und soll nicht weiter ausgebaut werden.

5.2 Eine Risikomanagement-Strategie fehlt in den meisten Fällen

EFV, Sektion Risikomanagement und Versicherungspolitik

Im «Handbuch zum Risikomanagement Bund» wird die allgemeine Risikostrategie beschrieben. Die Prüfung zeigte, dass sich die meisten VE auf diese Grundlage abstützen. Eine auf die VE bezogene, spezifizierte Risikostrategie wird weder in der Weisung RM, der Richtlinie RM, noch im Handbuch RM verlangt. Die EFV sieht das Erstellen entsprechender Vorgaben und das anschliessende Ausarbeiten der Strategie als Aufgabe der Departemente und der VE an. Einzig der Abschluss von Versicherungen (Strategie der Risikoüberwälzung) ist zwingend mit der EFV abzusprechen.

Verbindlich und eindeutig geregelt sind hingegen die Risikopolitik (durch die entsprechende Weisung des Bundesrates), die Risikodefinition (als Bestandteil dieser Weisung) und die finanzielle Risikotragfähigkeit (Kapitel 3.4 des Handbuches).

Umsetzung in den geprüften Verwaltungseinheiten, besondere Feststellungen

MeteoSchweiz verfügt über keine eigene Risikostrategie. Eine wahrnehmbar gut etablierte Risikokultur und das pragmatische Umsetzen der Vorgaben der EFV ermöglichen es MeteoSchweiz, ein wirkungsvolles und in die Führungsprozesse integriertes RM zu betreiben.

Die EZV realisiert in den nächsten Jahren ein grosses Transformationsvorhaben. Die Risikostrategie wird im Zuge dieses Vorhabens erstellt.

Im ASTRA wird das RM stark von der Direktion getragen und vorgelebt. Risikoeintritte werden analysiert und führen zu einer Verbesserung des Systems RM. Das Prinzip der laufenden Verbesserung wurde auch bei MeteoSchweiz festgestellt.

Beurteilung

Die EFK stellt fest, dass die Sektion Risikomanagement und Versicherungspolitik der EFV durch ihr Engagement und Vorbild zu einer guten Risikokultur beigetragen hat.

Die VE verzichten auf das Erstellen eigenständiger Risikostrategien und beziehen sich auf die entsprechenden Ausführungen im Handbuch. Nach Ansicht der EFK mag dieses Vorgehen für VE mit geringen Risiken genügen, andere sollten sich aber vertiefter mit den Risiken und deren Steuerung auseinandersetzen. Die Haltung der EFK zur Notwendigkeit von Risikostrategien der VE wird in Kapitel 4.3, Empfehlung 2 dargelegt.

5.3 Eine Identifikation und Erfassung der Risiken Bottom-Up ist etabliert, erfolgt aber zu isoliert

EFV, Sektion Risikomanagement und Versicherungspolitik

Das Vorgehen zur Identifikation und Erfassung der Risiken wird einerseits im «Handbuch zum Risikomanagement Bund» und andererseits in den «Best-Practice-Dokumenten» der EFV beschrieben. Bei den Top-Risiken der Departemente prüft die EFV zudem, ob die Risikoerfassung methodologisch korrekt ist. Gegebenenfalls werden ungenügend beschriebene Risiken zur Nachbearbeitung an das Departement zurückgewiesen.

Die Validierung der Bundesratsrisiken durch die EFV bezüglich deren Vollständigkeit wurde in Kapitel 3 beschrieben.

Umsetzung in den geprüften Verwaltungseinheiten, besondere Feststellungen

Ausser bei MeteoSchweiz konnte die EFK bei keiner der geprüften VE eine durch Einbezug der Stakeholder entstandene, auf den gesetzlichen Aufgaben und Zielen basierende Risikoanalyse feststellen (fehlender Top-Down-Ansatz). Teilweise erfolgt die jährliche Aktualisierung der Risiken lediglich auf Basis bestehender Risikoübersichten aus der Anwendung «R2C». Eine vertiefte Auseinandersetzung mit Aufgaben, Zielen und dem Umfeld der VE bleibt aus.

Beurteilung

Die Vorgaben zur Identifikation und Erfassung von Risiken sowie die von der EFV zur Verfügung gestellten Hilfsmittel sind nach Ansicht der EFK gut.

Wie bereits ausgeführt, ist ein ausreichender Top-Down Ansatz nicht vorhanden. Dass die VE ihre Risikoidentifikation mehrheitlich auf der Basis einer Konsolidierung der operativen Risiken durchführen, ist nach Ansicht der EFK unter anderem eine Folge der ungenügenden Integration des RM in die Führungsprozesse (siehe Kapitel 2). Die dadurch ausbleibende «Top-Down-Sicht» birgt unter anderem folgende Gefahren:

- Ziele, Aufgaben und die damit verbundenen Risiken der VE werden weniger hinterfragt
- Das (strategische) Umfeld der VE wird weniger berücksichtigt
- Auf der Risikolandkarte der VE finden sich zahllose (operative) Kleinstrisiken, welche aufgrund der grossen Menge kaum noch zu steuern sind (Verzettelung).

Diese Mängel werden dann in die Analyse und Bewertung der Risiken mitgezogen und führen teilweise zu nicht adäquaten, weil auf operativer Ebene verbleibenden Massnahmen.

In den meisten der geprüften VE wurden diese Mängel bereits erkannt und Massnahmen eingeleitet. Die Leitungen der entsprechenden VE wurden zudem in den Schlussbesprechungen durch die EFK auf diese Schwäche ihres RM aufmerksam gemacht.

Die Empfehlungen 1 und 2 zielen in die Richtung der vermehrten strategischen Sicht auf das RM und den Top-Down-Ansatz. Eine weitere Empfehlung zu diesem Thema drängt sich daher nicht auf.

5.4 Auch bei der Analyse und Bewertung der Risiken steht die isolierte Betrachtung im Vordergrund

EFV, Sektion Risikomanagement und Versicherungspolitik

Das Vorgehen zur Analyse und Bewertung der Risiken wird wiederum im «Handbuch zum Risikomanagement Bund» und in den «Best-Practice-Dokumenten» der EFV beschrieben. Zudem erfolgt mit der Eingabe der Risiken in die Anwendung «R2C» eine gewisse Standardisierung. Bei Top-Risiken prüft die EFV, ob die Risikobewertung methodologisch korrekt ist. Die inhaltliche Korrektheit wird nur von der Linie überprüft; es findet keine neutrale Validierung statt.

Als Output der Risikoanalyse und -bewertung erwartet die EFV «eine verständliche Beschreibung jedes Risikos und eine Bewertung der Eintretenswahrscheinlichkeit und der Auswirkungen». Dazu gehören u. a. das Beschreiben des «credible worst case» und eine Prüfung, ob Wechselwirkungen zu anderen Risiken bestehen.

Umsetzung in den geprüften Verwaltungseinheiten, besondere Feststellungen

In der Praxis erfolgen die Risikoidentifikation und -analyse bzw. -bewertung oft in einem Zug. VE, welche ihre Risiken methodisch korrekt identifizieren, halten auch bei der Analyse und Bewertung die Vorgaben ein. Eine generelle Schwachstelle bei fast allen geprüften VE stellte die EFK bei der Analyse der Risiken auf Wechselwirkungen zu anderen Risiken fest.

Beurteilung

Seitens der EFV besteht derzeit wenig Handlungsbedarf. Die Vorgaben sind verständlich und mit den bilateralen Gesprächen zwischen der EFV und der Generalsekretärin oder dem Generalsekretär des betreffenden Departements besteht eine geeignete Plattform, um Korrekturen anzubringen. Eine verstärkte methodische Unterstützung der VE bei der Analyse der Risiken hinsichtlich Wechselwirkungen dürfte nur erfolgreich sein, wenn gleichzeitig die VE die Risiken vermehrt aus dem strategischen Blickwinkel (Top-Down) identifizieren und analysieren.

Für die meisten VE gilt es, wie bei der Identifikation der Risiken, Fortschritte bei der Analyse und Bewertung der Risiken zu machen. Neben dem Einbringen der «Top-Down-Sicht» ist der Stakeholder-Perspektive (Empfänger einer möglicherweise gefährdeten Leistung, Lieferanten, Kantone etc.) auch bei der Risikoanalyse und -bewertung Rechnung zu tragen. Verstärkt werden sollte die Analyse der verschiedenen Risiken hinsichtlich ihrer Wechselwirkungen.

Die Bewertung der Risiken hat «netto», also unter Berücksichtigung bereits umgesetzter Massnahmen zu erfolgen. Die EFK sieht diesbezüglich ein erhebliches Potenzial zur Vereinfachung des RM. Mehrheitlich operative Risiken, welche durch Prozessoptimierungen (z. B. durch die Aufnahme zusätzlicher Kontrollen im Internen Kontrollsystem – IKS) nachhaltig vermindert wurden, könnten durchaus aus der Risikolandkarte der VE entfernt werden.

Es lässt sich keine VE- oder departementsübergreifende Abstimmung von Massnahmen feststellen, ferner werden keine Synergien systematisch erkannt bzw. genutzt. Ausgenommen sind Querschnittsrisiken (siehe Kapitel 6).

5.5 Bewältigung und Überwachung der Risiken als schwächstes Element im System

EFV, Sektion Risikomanagement und Versicherungspolitik

Das Vorgehen zur Bewältigung und Überwachung der Risiken wird im «Handbuch zum Risikomanagement Bund» und in einem «Best-Practice-Dokument» der EFV beschrieben. Die EFV gibt vor, dass die Kosten für im RM beschlossene Massnahmen in den Voranschlag einzufliessen haben. Jede beschlossene Massnahme muss einem Massnahmenverantwortlichen zugeordnet und mit einem Endtermin versehen sein. Eine grobe Kosten-Nutzenanalyse muss durchgeführt werden.

Die Überwachung der Risiken und der Massnahmen hat gemäss den Richtlinien über das RM durch den Risikoeigner zu erfolgen.

Umsetzung in den geprüften Verwaltungseinheiten, besondere Feststellungen

Die EFK stellte bei der Risikobewältigung und -überwachung an verschiedenen Stellen Verbesserungspotenzial fest. Auf Stufe VE werden Massnahmen teilweise ohne Umsetzungsverantwortlichen und ohne Endtermin in der Anwendung «R2C» geführt. Bei operativen Risiken wird als Umsetzungstermin vielfach «laufend» eingepflegt. Diese Option ist zulässig und in gewissen Fällen auch zweckmässig. Sie darf aber nicht als «bequemer» Ersatz für aktuelle, konkrete und griffige Massnahmen missbraucht werden.

Die Überwachung der Risiken und der entsprechenden Massnahmen kann auf Stufe VE in den meisten Fällen noch deutlich verbessert werden. Darüber hinaus konnte die EFK nur in wenigen Einzelfällen feststellen, dass zu den Risiken Indikatoren definiert wurden, anhand derer sich die Entwicklung ableiten lässt. Allerdings ist dies auch nicht für alle Risiken mit vernünftigem Aufwand möglich.

Die Umsetzung der Massnahmen wird in der Regel nur durch das periodische Aktualisieren des RM überwacht. Ein eigentliches Massnahmencontrolling haben nur wenige VE eingerichtet.

Beurteilung

Bezüglich Vorgaben und Überwachung durch die EFV besteht kein Handlungsbedarf.

Bei den VE ist teilweise deutlicher Verbesserungsbedarf bei der Formulierung, Terminierung und Zuteilung der Verantwortlichkeiten der Massnahmen vorhanden. So finden sich beispielsweise Massnahmen vom Typ «Interne Kontrollen», welche vorteilhafter im IKS oder im Prozessmanagement zu führen sind (siehe dazu die Bemerkung in Kapitel 5.4).

Bedingt durch das Fehlen von Risikostrategien der VE werden in der Regel auch keine Risikotoleranzen definiert. Risikominimierende Massnahmen werden ohne klares Ziel und ohne Kosten-Nutzen-Überlegungen umgesetzt.

Die Überwachung der Risiken und Massnahmen muss durch die Risikoeigner verstärkt werden. Je nach Grösse der VE und der Anzahl zu bewirtschaftender Risiken ist das Führen eines Massnahmencontrollings sinnvoll. Die VE wurden in den Schlussbesprechungen auf allfällige Schwächen hingewiesen. Der Ansatz einiger VE (ASTRA, MeteoSchweiz), die Massnahmenumsetzung in die Jahreszielvereinbarung des Massnahmenverantwortlichen aufzunehmen, ist für die EFK eine gute, wirkungsvolle Lösung.

Die Früherkennung von Veränderungen an der Risikosituation über Indikatoren kann pragmatisch ohne aufwändige Messsysteme implementiert werden. Aus Sicht der EFK werden bereits bestehende Werte, wie zum Beispiel öffentlich zugängliche Indizes, Leistungs- und Controlling-Kennzahlen zu wenig für die Beurteilung der Risikoexposition genutzt. Damit fehlt ein wichtiges Steuerungs- und Entscheidungsinstrument.

5.6 Die Risikoberichterstattung und Kommunikation entsprechen der jeweiligen Amtskultur

EFV, Sektion Risikomanagement und Versicherungspolitik

Die Berichterstattung ergibt sich weitgehend aus dem Risikomanagementprozess und den Berichtsvorlagen der Anwendung «R2C». Diese Vorlagen sind auf die Rapportierung der Top- bzw. Bundesratsrisiken zugeschnitten und tragen durchgehend die Klassifizierung VERTRAULICH.

Das Handbuch weist auf die Wichtigkeit der internen Kommunikation der Risiken hin.

Umsetzung in den geprüften Verwaltungseinheiten, besondere Feststellungen

In den meisten geprüften Einheiten sind die Grundlagendokumente, teilweise auch die Risikoberichte, für die Mitarbeitenden verfügbar. Das RM ist bei allen geprüften VE periodisch, in der Regel jährlich, ein Thema in Veranstaltungen (Amtsrapporte etc.).

Der Zugang zum Risikocoach ist für die Mitarbeitenden bei allen geprüften VE gewährleistet. Der Risikocoach hat seinerseits in allen geprüften Fällen Zugang zur Direktion.

Dass die aus der Anwendung «R2C» heraus erzeugten Berichte als VERTRAULICH klassifiziert sind, zeigt auf Stufe VE negative Auswirkungen. Insbesondere im EDA musste die EFK feststellen, dass diese Klassifizierung einen Informationsaustausch über die Direktionen hinweg zusätzlich erschwert. Das RM erfolgt auch aus diesem Grund in «Silos».

Beurteilung

Die Vorgaben und Anleitungen der EFV zur Risikoberichterstattung und Kommunikation sind ausreichend. Das oder die Berichtstemplates sollten jedoch angepasst werden. Auf Stufe VE sollte die Klassifizierung VERTRAULICH nur angewendet werden, wenn der Informationsgehalt des Dokuments auch diesem Schutzbedarf entspricht.

Die VE kommunizieren Grundlagen und erkannte Risiken in der Regel gut. Die im Kapitel RM-Organisation beschriebenen Risikoboards stellen nach Ansicht der EFK eine sehr gute Möglichkeit zur Diskussion und Vertiefung von Risiken dar, bei welcher auch die Vertraulichkeit angemessen gewahrt wird.

Empfehlung 3 (Priorität 2)

Die EFK empfiehlt der EFV zu prüfen, ob die interne Risikokommunikation durch eine dem tatsächlichen Schutzbedarf entsprechende Klassifizierung der Berichte verbessert werden kann. Das Verhältnis zwischen Informationsschutz und Kommunikationsbedürfnis sollte ausgewogener sein.

Stellungnahme der EFV

Die EFV teilt die Einschätzung der EFK, ist aber der Auffassung, dass die geltenden Regeln dem Kommunikationsbedürfnis bereits heute Rechnung tragen: Die Verwendung von RM-Dokumenten ist im Handbuch RM Bund (Kap. 5.3.1, S. 40) mit Verweis auf die ISchV geregelt: Demnach dürfen klassifizierte Informationen nur jenen Personen zugänglich gemacht werden, die davon Kenntnis haben müssen. Dies verpflichtet einerseits die Geheimnisträger zu einem sorgsamen Umgang mit klassifizierter Information, andererseits erlaubt es den Departementen und VE, eigenen Kommunikationsbedürfnissen angemessen nachzukommen. Eine situative bzw. weiter differenzierte Klassifizierung würde der Wirksamkeit der geltenden Regeln hingegen schaden und wäre auch aus verwaltungsökonomischen Überlegungen nicht zielführend.

5.7 Das Risikomanagement Bund ist ein schlankes System

Das System RM basiert auf den von Bundesrat und EFV erstellten Dokumenten. Die VE geniessen bei der Umsetzung der darin enthaltenen Vorgaben grosse Freiheiten. Die EFK stellt fest, dass die VE praktisch einen eher einfachen, pragmatischen Ansatz in der Ausgestaltung ihres RM verfolgen.

Eine systembedingte Doppelspurigkeit besteht im Bereich der Risiken der IT-Projekte. Alle IT-Projekte werden mit ihren Risiken im «IKT-Cockpit» des ISB erfasst (projektinhärente Risiken). Sind die Risiken eines (Gross-)Projektes so hoch, dass sich ein Erfassen in der Anwendung «R2C» für die VE aufdrängt, müssen die Informationen ein zweites Mal erfasst werden. Bei korrekter Nutzung des RM müssten in diesen Fällen die strategischen Risiken in «R2C» erfasst werden, welche durch das Projekt für die VE entstehen.

Beurteilung

Die in einigen Fällen vorhandene Doppelspurigkeit beim Erfassen von IT-Projektrisiken ist nach Ansicht der EFK tragbar. Im Übrigen konnte sie kein wesentliches Potenzial für Effizienzsteigerungen und Vereinfachungen im RM-System Bund erkennen.

6 Die Steuerung von Querschnittsrisiken ist systembedingt lückenhaft

Das von der EFK geprüfte ISB wurde durch die GSK als Risikoeigner eines Querschnittsrisikos (Cyberrisiko) bezeichnet. Ein Querschnittsrisiko besteht aus aggregierten Quellrisiken, also Risiken, welche über verschiedene VE gleich oder ähnlich aufkommen.

Querschnittsrisiken sind typischerweise in den Bereichen Informatikeinsatz, Finanzen, Personal, Bauten und Logistik zu finden. Am Beispiel des geprüften ISB konnte festgestellt werden, dass eine Risikostrategie für die vom Fachamt zu steuernden Querschnittsrisiken fehlt.

Die EFV organisiert zu den verschiedenen Querschnittsrisiken des Bundes jeweils Sitzungen, an welchen der Risikoeigner und Vertreter der VE mit Quellrisiken teilnehmen. Eine erste Herausforderung besteht in der Beschreibung und Bewertung des Querschnittsrisikos. So muss für die Bewertung (Eintretenswahrscheinlichkeit und Auswirkungen) ein Konsens gefunden werden. Da das für das Querschnittsrisiko verantwortliche Fachamt in der Regel nicht über eine Weisungskompetenz gegenüber den anderen VE (Eigner der Quellrisiken) verfügen, muss auch die Massnahmenumsetzung einvernehmlich erfolgen. Diese erfolgt dann wiederum in Verantwortung der VE, ein übergeordnetes Umsetzungscontrolling fehlt.

Bei der Kommunikation der Querschnittsrisiken stellte die EFK eine weitere Schwachstelle fest. Die nach dem Beschluss des Bundesrates fehlende systematische Rückmeldung kann eine VE, welche ein Amtsrisiko zur Thematik des Querschnittsrisikos führt, von der Kommunikation der Massnahmen zur Reduktion des Querschnittsrisikos ausschliessen. In der Prüfung war dies bei MeteoSchweiz der Fall. Diese VE war nicht über das oben erwähnte Querschnittsrisiko «Cyberrisiko» informiert (weder über dessen Existenz noch über die Massnahmen), führt aber ein gleiches Risiko auf Stufe Amt.

Bedingt durch das Selektions- und Meldeverfahren können auch potenzielle Quellrisiken übersehen werden, die bei vielen VE vorhanden sind, jedoch auf Stufe VE nicht so gravierend sind, dass sie weitergemeldet werden. In ihrer Summe über die gesamte BVerw könnte sich das Führen eines Querschnittsrisikos anbieten.

Beurteilung

Die Querschnittsrisiken sind, richtig angewandt, ein gutes Instrument zu einer effizienten, wirkungsvollen Risikobewirtschaftung. Für VE, welche als Eigner eines Querschnittsrisikos bezeichnet werden, entstehen am Beispiel des geprüften ISB folgende Herausforderungen:

- Die Risikostrategie muss sowohl die VE-spezifischen Anforderungen als auch die sich aus dem oder den Querschnittsrisiken ergebenden Erfordernisse abdecken. Der im Handbuch vorhandene Ansatz zu einer Risikostrategie für einzelne Querschnittsrisiken (Anhang 10 «Factsheets Querschnittsrisiken Bund») ist noch nicht ausreichend.
- Die Querschnittsrisikoeigner sind gegenüber den betroffenen übrigen VE in der Regel nicht weisungsberechtigt. Dadurch und aufgrund der dezentralen Massnahmenverantwortlichkeit und des fehlenden Umsetzungscontrollings kann der Führungskreislauf nicht geschlossen werden.

- Eine unvollständige oder fehlende Kommunikation von und zu den Eignern der Quellrisiken der geführten Querschnittsrisiken wiederum birgt einerseits die Gefahr von Doppelspurigkeiten (gleiche Massnahmen werden durch den Eigner des Querschnittsrisikos, aber auch durch den nicht informierten Eigner des Quellrisikos eingeleitet). Noch ungünstiger wären aber sich widersprechende Massnahmen bei Querschnitts- und Quellrisikoeigner.

Die EFV weist zurecht darauf hin, dass sie keine Kompetenzen habe, die grundlegenden systemischen Mängel zu beheben. Um beispielsweise die VE zur Umsetzung einmal beschlossener Massnahmen zur Risikoadressierung zu verpflichten, bräuchte es einen Bundesratsbeschluss oder die Initiative der Generalsekretärenkonferenz. Die EFK erachtet es gleichwohl als Aufgabe der EFV, im Rahmen ihres Auftrages zur kontinuierlichen Weiterentwicklung des RM solche Anpassungen zu lancieren und zu treiben.

Empfehlung 4 (Priorität 1)

Die EFK empfiehlt der EFV konkrete Massnahmen zu ergreifen, um risikomindernde Massnahmen bei Querschnittsrisiken für alle VE als verbindlich erklären und deren Umsetzung überwachen zu lassen.

Sollte dies nicht möglich sein, empfiehlt die EFK der EFV, ein neues Risiko aufzunehmen, das der fehlenden Verbindlichkeit und Überwachung der Massnahmen bei Querschnittsrisiken Rechnung trägt.

Stellungnahme der EFV

Die EFV teilt die Einschätzungen der EFK nur bedingt und kommt zu anderen Schlüssen: Aus unserer Sicht sind die geltenden Regeln zur Bewertung und Bewirtschaftung von Querschnittsrisiken (QSR) zweckmässig und effektiv. Wichtig ist:

1. Das RM folgt der Verwaltungsorganisation. Für die Bewirtschaftung der QS- und Quellrisiken sind die Risiko- und Massnahmeneigner verantwortlich.
2. Ein ergänzendes Monitoring kann vom QSR-Eigner durchgeführt werden.
3. Die fachgerechte Bewirtschaftung wird an den Koordinationssitzungen sichergestellt.
4. Eskalationsstufen bei Differenzen sind die GSK und letztlich der Bundesrat. Allfällig festgestellte Probleme gründen aus Sicht der EFV nicht in Mängeln des Regelwerks, sondern dessen konsequenter Anwendung.

Die EFV wird das Handbuch entsprechend ergänzen.

Empfehlung 5 (Priorität 1)

Die EFK empfiehlt der EFV, die Risikoeigner zu verpflichten, die geführten Querschnittsrisiken, die entsprechende Risikostrategie und die Massnahmen allen Risikocoaches und Direktoren zugänglich zu machen. Die Information muss es den Verantwortlichen der VE ermöglichen, zu beurteilen ob ein entsprechendes Quellrisiko vorhanden ist und ob mit dem Eigner des Querschnittsrisikos Kontakt aufgenommen werden muss.

Stellungnahme der EFV

Die EFV teilt die Einschätzungen der EFK nur bedingt. Die Aggregierung von Querschnittsrisiken ist bewusst als Topdown-Prozess angelegt. Die geltenden Regeln garantieren effiziente Abläufe und stellen sicher, dass die relevanten Risiken erfasst werden, auch wenn sie sensible Informationen enthalten. Die EFV wird sich dafür einsetzen, dass die Regeln von allen zuständigen Stellen in der Praxis angewendet werden und der Informationsfluss optimal gestaltet wird. Dies hätte indes am Fall MeteoSchweiz nichts geändert, da sich das aggregierte Risiko aus fachlichen Gründen auf die Quellrisiken der zentralen IKT-Leistungserbringer beschränkt.

Anhang 1: Rechtsgrundlagen

Rechtstexte
Finanzhaushaltgesetz FHG vom 7. Oktober 2005 (SR 611.0)
Finanzhaushaltverordnung FHV vom 5. April 2006 (SR 611.01)
Informationsschutzverordnung ISchV vom 4. Juli 2007 (SR 510.411)
Weisungen des Bundesrates über die Risikopolitik des Bundes vom 24. September 2010 (BBl 2010-2062 6549)
Richtlinien über das Risikomanagement Bund, EFV, 31. März 2016

Anhang 2: Abkürzungen

ASTRA	Bundesamt für Strassen
BCM	Business Continuity Management
BK	Bundeskanzlei
BVerw	Bundesverwaltung
DV	Departementsvorsteherin oder Departementsvorsteher
EDA	Eidgenössisches Departement für auswärtige Angelegenheiten
EFK	Eidgenössische Finanzkontrolle
EFV	Eidgenössische Finanzverwaltung
EZV	Eidgenössische Zollverwaltung
GSK	Generalsekretärenkonferenz
GPK	Geschäftsprüfungskommission
IKS	Internes Kontrollsystem
IKT	Informations- und Kommunikationstechnologie
ISB	Informatiksteuerungsorgan des Bundes
KD	Konsularische Direktion
RM	Risikomanagement
VE	Verwaltungseinheit

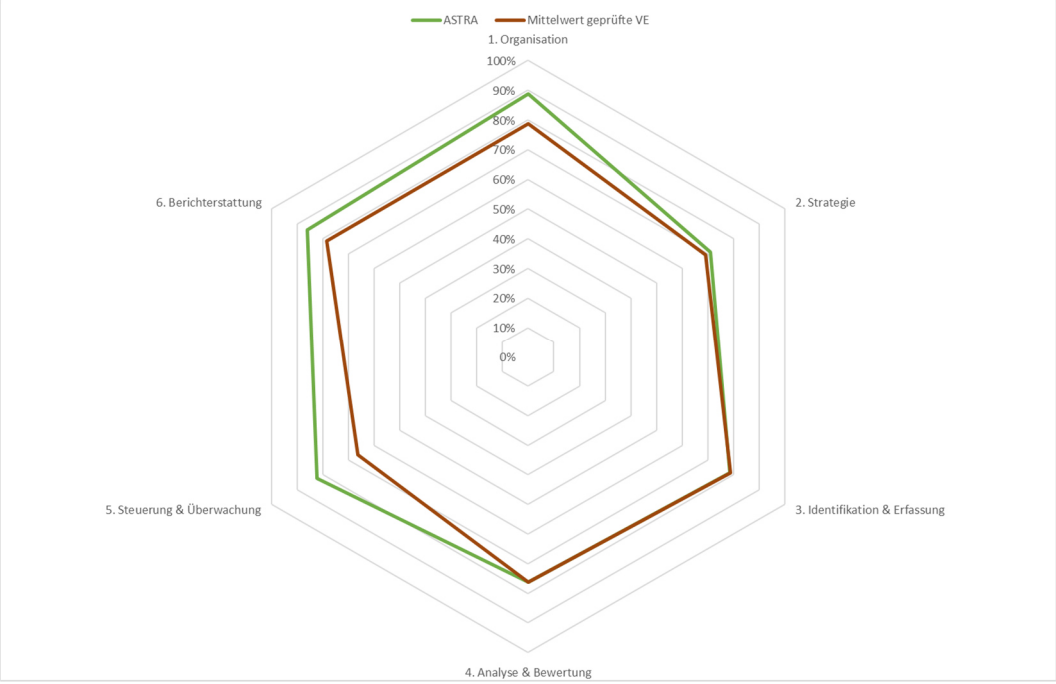
Priorisierung der Empfehlungen

Die Eidg. Finanzkontrolle priorisiert die Empfehlungen nach den zugrunde liegenden Risiken (1 = hoch, 2 = mittel, 3 = klein). Als Risiken gelten beispielsweise unwirtschaftliche Vorhaben, Verstösse gegen die Recht- oder Ordnungsmässigkeit, Haftungsfälle oder Reputationsschäden. Dabei werden die Auswirkungen und die Eintrittswahrscheinlichkeit beurteilt. Diese Bewertung bezieht sich auf den konkreten Prüfgegenstand (relativ) und nicht auf die Relevanz für die Bundesverwaltung insgesamt (absolut).

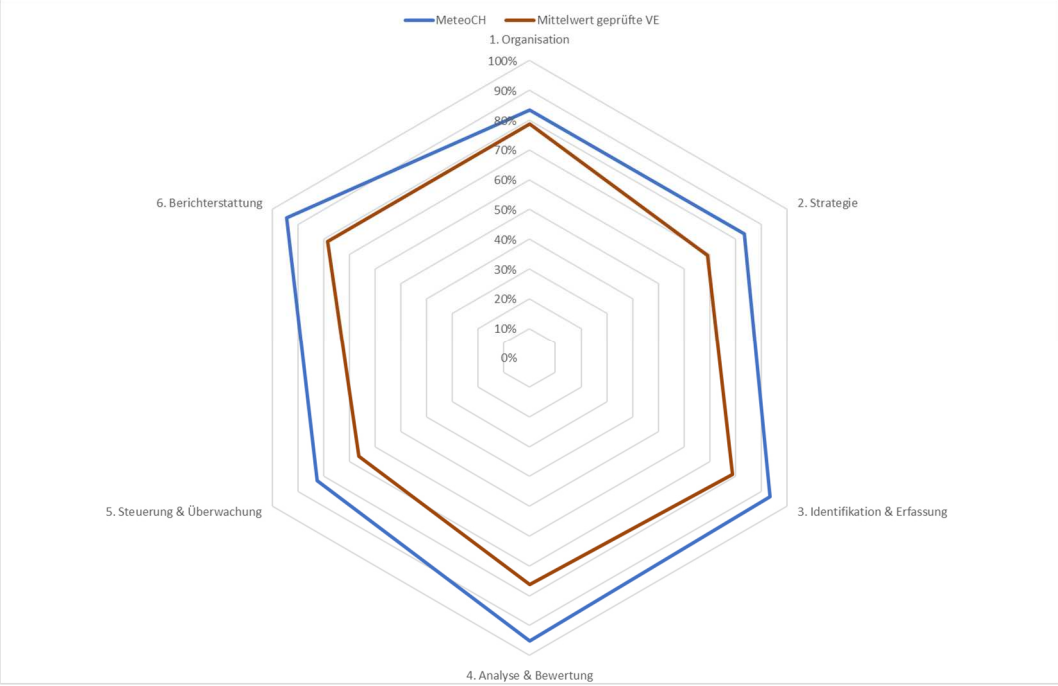
Anhang 3: Illustration der Prüfungsergebnisse

Die nachfolgenden Grafiken zeigen die Reifegrade des RM bei den geprüften VE auf.

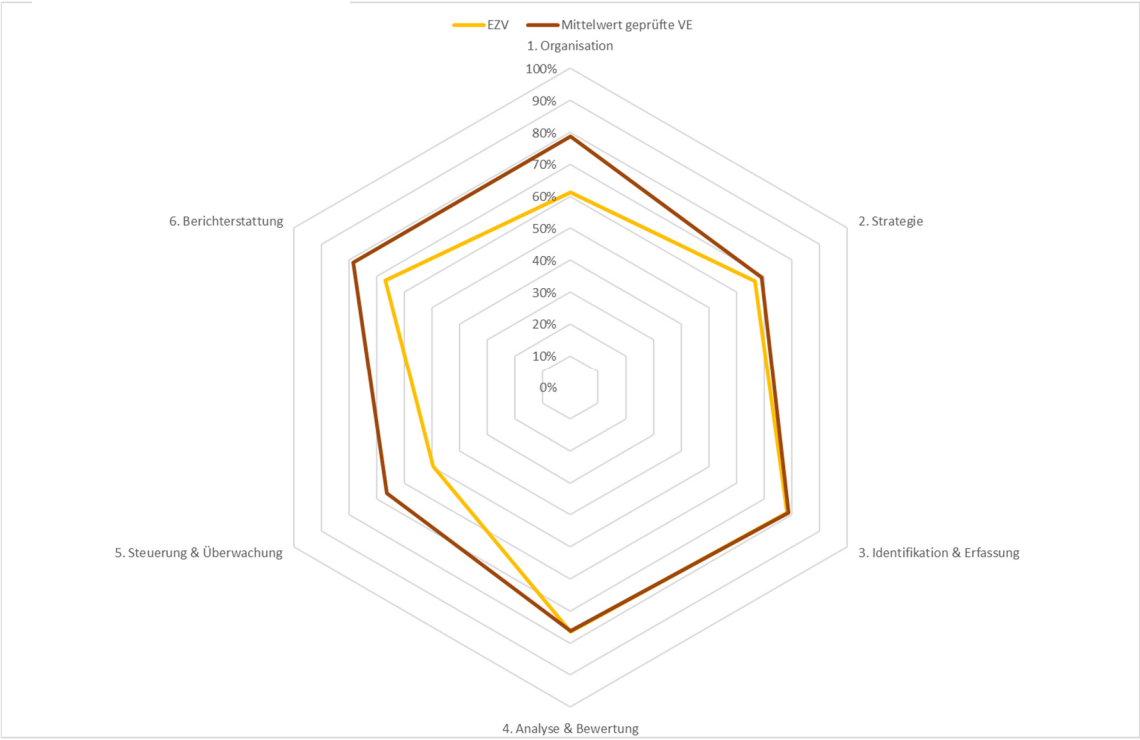
ASTRA



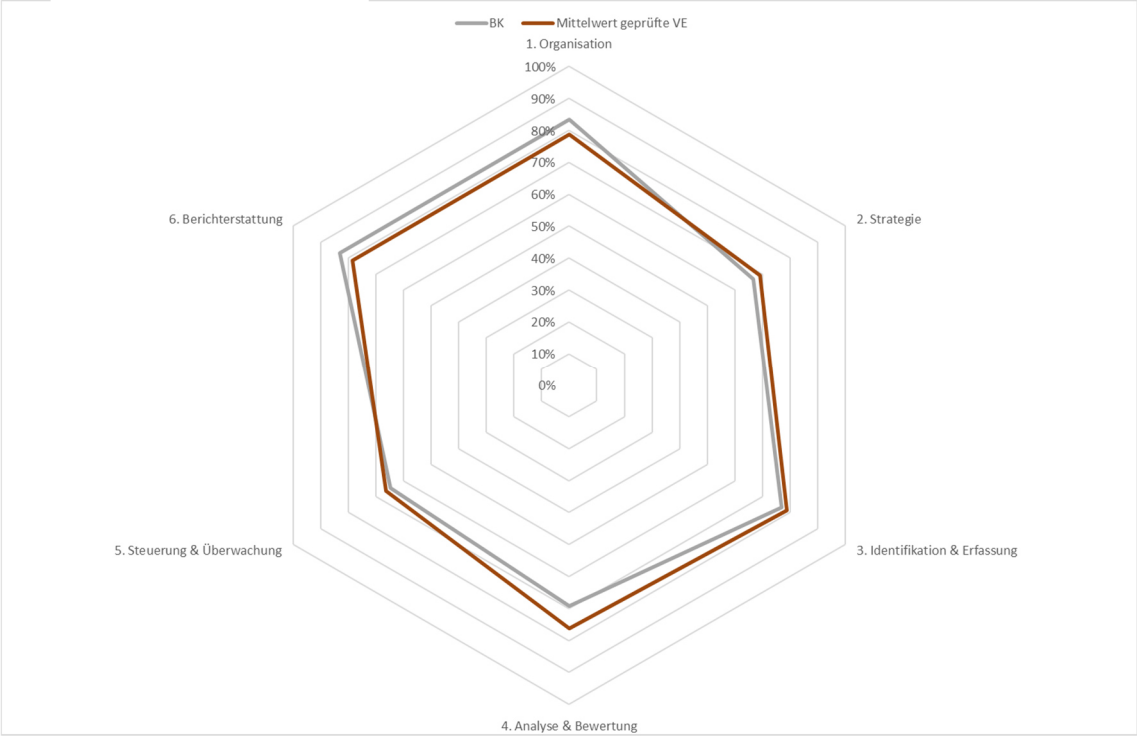
MeteoSchweiz



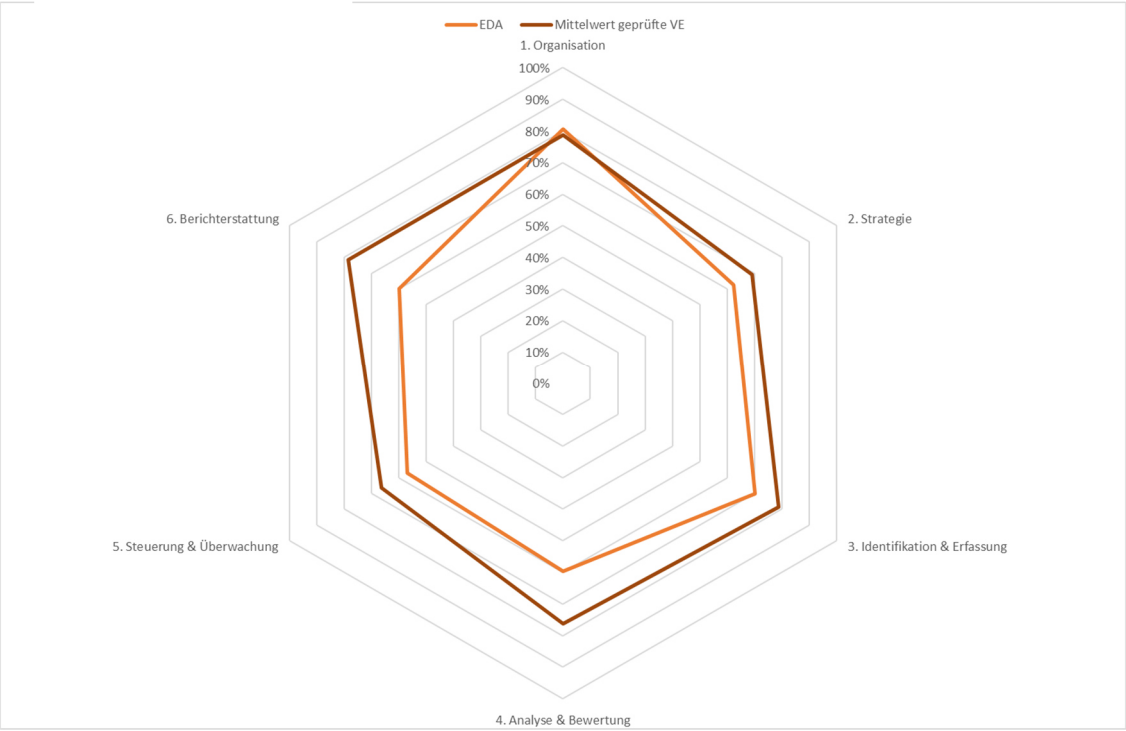
EZV


EZV
Mittelwert geprüfte VE
1. Organisation
2. Strategie
3. Identifikation & Erfassung
4. Analyse & Bewertung
5. Steuerung & Überwachung
6. Berichterstattung
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

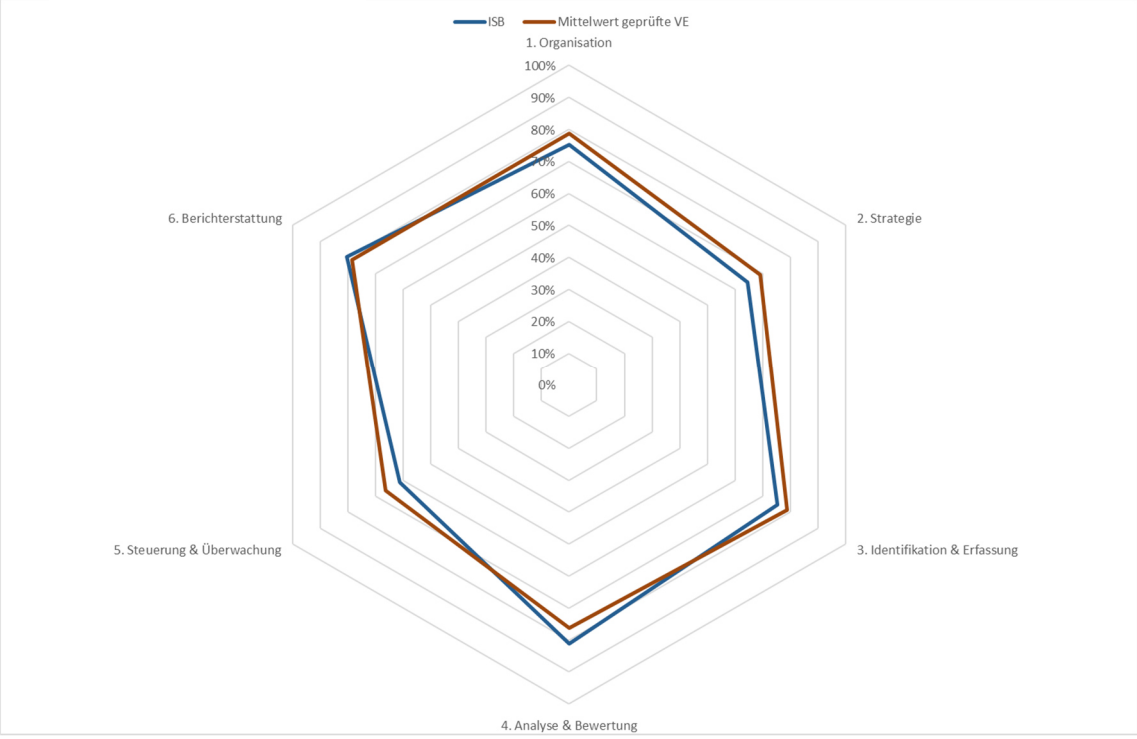
BK


BK
Mittelwert geprüfte VE
1. Organisation
2. Strategie
3. Identifikation & Erfassung
4. Analyse & Bewertung
5. Steuerung & Überwachung
6. Berichterstattung
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%

EDA


EDA
Mittelwert geprüfte VE
1. Organisation
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2. Strategie
3. Identifikation & Erfassung
4. Analyse & Bewertung
5. Steuerung & Überwachung
6. Berichterstattung

ISB


ISB
Mittelwert geprüfte VE
1. Organisation
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2. Strategie
3. Identifikation & Erfassung
4. Analyse & Bewertung
5. Steuerung & Überwachung
6. Berichterstattung