

Die Risikopolitik des Bundes unterstützt die Departemente in der Erfüllung ihrer Aufgaben und ermöglicht eine umfassende und systematische Risikobetrachtung für die gesamte Bundesverwaltung. Sie dient zudem als Grundlage für ein effizientes und wirksames Versicherungsmanagement. Das Seco hat mit seinem breiten und vernetzten Aufgabengebiet ein ausgesprochen heterogenes Risikoprofil mit einer hohen potentiellen Risikoexponierung.

JÜRIG SCHEIDEGGER
MARTIN LUGINBÜHL

RISIKOMANAGEMENT BEIM BUND

Umsetzung des Risikomanagementprozesses im Seco

1. AUSGANGSLAGE

Nach geltender Regelung in der Finanzhaushaltverordnung und den Weisungen des *Eidgenössischen Finanzdepartements (EFD)* über die Risikoübernahme und Schadenerledigung für die Risiken des Bundes dürfen Verwaltungsstellen Versicherungspolicen nur mit ausdrücklicher Bewilligung der *Eidgenössischen Finanzverwaltung (EFV)* abschliessen. Im Rahmen einer Bestandaufnahme über die Versicherungssituation des Bundes stellten sich verschiedene Schwachpunkte heraus. Der Bundesrat hat daher im Juni 2003 das EFD beauftragt, eine Risiko- und Versicherungspolitik des Bundes zu formulieren.

Im Januar 2005 hat der Bundesrat die Departemente und die Bundeskanzlei angewiesen, die Risikopolitik umzusetzen und die Grundlagen für ein Risikomanagement zu legen. Ausserdem hat das EFD den Auftrag erhalten, → eine für das Risikomanagement zu verwendende IT-Applikation zu beschaffen, zu unterhalten und den Departementen zur Verfügung zu stellen sowie → die Berichterstattung zusammen mit den verantwortlichen Departementen zu organisieren und zu koordinieren.

2. RISIKOPOLITIK DES BUNDES

Die Risikopolitik des Bundes enthält Handlungsanweisungen an die Departemente und Verwaltungseinheiten, regelt die Verantwortlichkeiten und legt den konsequenten und systematischen Umgang mit den vielfältigen Risiken in der Bundesverwaltung fest. Der Geltungsbereich umfasst gemäss dem 4-Kreise-Modell die Verwaltungseinheiten des 1. und 2. Kreises, d. h. die Zentralverwaltung und die FLAG-Ämter [1]. Auf die Organisationen und Unternehmen des 3. und 4. Kreises [2] findet die Risikopolitik hingegen keine

direkte Anwendung. Die Departemente haben die Risiken aus den ihnen zugeordneten Organisationen im Sinne von Art. 19 des Verantwortlichkeitsgesetzes einzubeziehen. Die Umsetzung des Risikomanagements erfolgt beim Bund gestützt auf eine dezentrale Konzeption. Die Verantwortung für das Risikomanagement liegt daher bei den Departementen und ihren Verwaltungseinheiten.

Die Risikopolitik orientiert sich am klassischen Ansatz und umfasst die Phasen Identifizieren und Bewerten der Risiken (Risikoanalyse), Erstellen von Massnahmenplänen [3] sowie das Risikocontrolling. Mit Hilfe eines standardisierten IT-Tools (R2C), das von allen Departementen und der Bundeskanzlei angewendet wird, ist ein einheitliches Reporting gewährleistet.

Der Bund trägt die bestehenden und durch die Verwaltungseinheiten akzeptierten Restrisiken grundsätzlich selbst. Ausnahmsweise können – zum Beispiel wenn ein hohes finanzielles Risiko oder ein besonderes Haftungsrisiko besteht – Versicherungsverträge abgeschlossen werden. Der Abschluss und die aktive Bewirtschaftung von Versicherungspolicen erfolgt zentral durch die EFV.

3. UMSETZUNG IM SECO

Die *Geschäftsleitung (GL)* Seco hat im Juni 2005 beschlossen, die *Interne Revision (IR)* der Direktion für Arbeit auf das gesamte Seco auszudehnen und damit zusätzlich zur Arbeitslosenversicherung u. a. die Querschnittsfunktionen sowie die Leistungsbereiche Arbeitsbedingungen, Standortförderung, Wirtschaftliche Entwicklungszusammenarbeit, Bilaterale Wirtschaftsbeziehungen, Welthandel sowie Wirtschaftspolitik in die Finanzaufsicht einzubeziehen. Die GL Seco hat zu



JÜRIG SCHEIDEGGER,
LIC. RER. POL., MITGLIED GL,
SECO, BERN



MARTIN LUGINBÜHL,
DIPL. KAUFMANN HKG,
LEITER INTERNE REVISION,
SECO, BERN

Abbildung 1: **RISIKOKATEGORIEN**

Risikokategorie	Risiken
Finanzielle und wirtschaftliche Risiken	Risiken im Zusammenhang mit dem Finanzmanagement sowie ungenügender Sparsamkeit und Wirtschaftlichkeit. Abhängigkeiten des Seco von Dritten und/oder Risiken im Zusammenhang mit subsidiären Leistungen des Seco.
Rechtliche Risiken/Compliance	Risiken im Zusammenhang mit dem Vollzug der Verwaltungsaufgaben und der Einhaltung von rechtlichen Bestimmungen und Verträgen.
Prozess-/Organisationsrisiken	Risiken aus der IT (Infrastruktur, Applikationen, Projekte), den Verfahren, der Kompetenzverteilung, der Dokumentation, des Know-how sowie Fehleinschätzungen bzw. Nichterkennen von Entwicklungen. Risiken aus dem Bereich Human Resources.
Risiken aus ungenügender Wirkung	Risiko, dass die Massnahmen nicht die gewünschte Wirkung erzielen.
Risiken aus Betrug, Fahrlässigkeit, Irrtum	Verhaltensrisiken, persönliche Bereicherung, Missbrauch, Korruption.
Reputationsrisiken	Imagerisiko gegenüber Vollzugsstellen und der Öffentlichkeit.
Gesellschaftliche/ Politische Risiken	Risiken aus dem gesellschaftlichen Umfeld und/oder aus dem politischen System wie Nichterkennen von gesellschaftlichen Entwicklungen sowie politischer Entscheide (Verfassungs-/Gesetzesänderungen).
Sachrisiken/technische Risiken/ Elementarrisiken	Risiko der Zerstörung bzw. Beschädigung von bundeseigenen Gebäuden, Einrichtungen, technischen Anlagen, Daten oder Kulturgütern (inklusive Betriebsunterbruch).
Technologische/ Naturwissenschaftliche Risiken	Risiken, die sich aus der Entwicklung, Lancierung und Zulassung von technologischen/ naturwissenschaftlichen Neuanwendungen ergeben (inkl. Spätfolgen).

diesem Zweck eine Risikoanalyse in Auftrag gegeben mit dem Ziel, eine Grundlage für die risikoorientierte Mehrjahresprüfplanung der IR zu schaffen. Gleichzeitig soll mit der Risikoanalyse die Basis zur Umsetzung der Risikopolitik des Bundes erarbeitet werden.

3.1 Risikoidentifikation. Die Risikoidentifikation erfolgte durch die Leistungsbereiche auf der Basis einheitlicher Kriterien (Abbildung 1), welche sich an die Vorgaben der Risikopolitik anlehnen. Diese umfassen alle potentiellen Gefahren, welche die Ordnungsmässigkeit, Rechtmässigkeit, Wirtschaftlichkeit und Sicherheit der eingesetzten Mittel beeinträchtigen. Dabei sind nicht nur finanzielle und vergangenheitsorientierte, sondern auch zukünftige und operationelle Sachverhalte massgebend. Die daraus abgeleiteten und aufgrund der Prozesse und Aufgaben definierten Risikofelder wurden in einem nach Gesamtführung, Querschnittsfunktionen sowie Leistungsbereichen gegliederten Risikokatalog (Abbildung 2) erfasst. Daraus resultierten insgesamt 195 Risikofelder.

3.2 Risikobewertung. Die Bewertung der Risikofelder erfolgte durch den Führungsstab, die Ressorts- und Leistungsbereichsleiter sowie deren Teams aufgrund des in der Risikopolitik des Bundes vorgegebenen Bewertungsrasters (Abbildung 3). Es wurden die Brutto- und Restrisiken nach den Kriterien der möglichen Eintretenswahrscheinlichkeit sowie der Auswirkung eines Ereignisses mit Bewertungsmöglichkeit zwischen 1 und 6 bewertet (Brutto- und Nettobewertung) [4]. Die Höhe des Risikos wurde dabei durch die Multiplikation der Eintretenswahrscheinlichkeit mit der Auswirkung berechnet (Risikofaktor). Extremwerte wurden mit den betroffenen Bereichen besprochen und bereinigt. Durch die einheitliche Anwendung des gleichen Rasters ergeben sich Seco-weit vergleichbare Risikofaktoren.

3.3 Risikoanalyse. Der Risikokatalog und die Bewertungen wurden in einer Risikoanalyse zusammengefasst und zuhanden der GL Seco ausgewertet. Dabei lag das Schwergewicht im wesentlichen auf folgenden Top-Risiken:

Abbildung 2: **AUFBAU DES RISIKOKATALOGES**

Gesamtführung	Querschnittsfunktionen	Leistungsbereiche
Strategie Unternehmenskultur Organisation Controlling Kommunikation/Medienbetreuung Katastrophenvorsorge usw.	Human Resources Finanzrechnung Informatik	Führungsprozesse Geschäftsprozesse Informatik Vollzugsstellen

serer nicht-finanzieller Schaden auftreten kann. Diese Gebiete erhalten bei der Risikosteuerung ebenfalls ein hohes Gewicht.

Zusätzlich zu den Top-Risiken wurden themenspezifische Risikoprofile wie → Beschaffungswesen; → Kommunikation; → IT; → Vollzug; → Betrug und Korruption sowie → Führung (Strategie, Unternehmenskultur, Human Resources, Wissensmanagement, Controlling) erstellt, um eine Übersicht über die Risikoausprägung der verschiedenen Leistungsbereiche zu erhalten (Abbildung 4).

Die GL Seco hat die Auswertungen an einer Sitzung besprochen mit dem Ziel, die Kohärenz zwischen den einzelnen Bereichen sicherzustellen. Gleichzeitig hat sie den Risikomanagementprozess initialisiert.

3.4 Risikomanagementprozess. Um ein leistungsfähiges und funktionierendes Risikomanagement zu gewährleisten, hat die GL Seco die Verantwortung für den Risikomanage-

mentprozess (Abbildung 5) übernommen. Sie ist in diesem Zusammenhang u. a. zuständig für das Risikoportefeuille der Kernrisiken sowie die Genehmigung der Massnahmenpläne.

Damit das Risikomanagement auf einer gesicherten Grundlage basiert, wurden die Bereiche beauftragt, in einem ersten Schritt die vorliegenden Risikoeinschätzungen zu verifizieren sowie die Kernrisiken auf einen allfälligen zusätzlichen Handlungsbedarf zu überprüfen und gegebenenfalls Massnahmenpläne zu erstellen. Diese beinhalten je Risikofeld u. a. eine Kurzbeschreibung der zusätzlich notwendigen Kontrollen und Massnahmen zur weiteren Minimierung der Restrisiken sowie die Termine für die entsprechende Umsetzung. Die Massnahmenpläne werden durch eine zentrale Stelle im IT-Tool R2C für das Reporting an das Departement und die EFV erfasst. In einem zweiten Schritt ist die laufende Steuerung der bestehenden Risiken, die Früherkennung von potentiell kritischen Situationen sowie das Erfassen und Melden von Veränderungen in den Kernrisiken vorgesehen.

Abbildung 5: **RISIKOMANAGEMENTPROZESS**

Input	Aktivitäten	Wer	Output	bis
Risikoanalyse Seco (alle Risikofelder)	Verifizieren Bewertungen ↓	→ Prozesse und Ressourcen (PR) → Leistungsbereiche	→ Aktualisierte Risikoanalyse je Bereich → Meldung Änderungen Kernrisiken an PRFI	30.6.2006 (einmalig)
Risikoanalyse Seco (Kernrisiken)	Überprüfen Handlungsbedarf Kernrisiken ↓	→ PR → Leistungsbereiche	Massnahmenpläne Kernrisiken an PRFI	30.6.2006 (einmalig)
→ Risikoanalyse Seco (alle Risikofelder) → Risikoveränderungen → Früherkennung potentiell kritischer Situationen → Massnahmenpläne → Revisionsberichte	Risikosteuerung ↓	→ PR → Leistungsbereiche	→ Aktualisierte Risikoanalyse je Bereich → Meldung Änderungen Kernrisiken und Massnahmenpläne an PRFI	laufend jährlich bis 30.09.
→ Änderungen Kernrisiken → Massnahmenpläne Kernrisiken	Erfassen Kernrisiken und Massnahmen ↓	Finanzen (PRFI)	→ Aktualisiertes Risikoportefeuille Kernrisiken (IT-Tool R2C)	jährlich bis 30.10.
→ Risikoportefeuille Kernrisiken → Schadenereignisse	Reporting an GS EVD	PRFI	Durch die GL Seco genehmigter Bericht an das GS EVD. Inhalt: → Kernrisiken und Massnahmenpläne → Schadenstatistik	jährlich bis 30.11.
→ Vorfall mit besonderer Tragweite → Schadenereignis	Krisenmanagement	→ Leitung PR → Leitung Leistungsbereiche	Meldung an GL Seco	fallweise
→ Aktualisierte Risikoanalyse der Bereiche → Risikomanagementprozess	Audit	Interne Revision	→ Aktualisierte Risikoanalyse Seco → Revisions- und Statusberichte	periodisch

4. ROLLE DER INTERNEN REVISION

Gemäss praktischem Ratschlag 2100-3 des IIA [5] ist die Rolle der IR im Risikomanagementprozess aufgrund der Organisationsstruktur, den Fähigkeiten der Mitarbeitenden sowie den spezifischen Gegebenheiten auszugestalten. Die GL Seco hat unter Berücksichtigung dieser Vorgaben beschlossen, der IR im Risikomanagementprozess eine aktive Rolle im Sinne einer Steuerungs- und Koordinationsfunktion zu übertragen. Die Aufgaben umfassen → die fachtechnische Unterstützung der Bereiche, → die periodische Aktualisierung der Risikoanalyse als Input für das Risikoportefeuille, → das Erstellen periodischer Statusberichte sowie → die periodische Prüfung der Wirksamkeit des Risikomanagementprozesses.

Damit können das Know-how und die bestehende Organisation optimal genutzt werden.

Die IR wurde weiter beauftragt, im Rahmen ihrer laufenden Prüfungstätigkeit die Vollständigkeit und Richtigkeit der identifizierten Risiken sowie die Risikoeinschätzungen zu verifizieren.

Anmerkungen: 1) FLAG-Amt: Führung mit Leistungsauftrag und Globalbudget. 2) Organisationen/Unternehmen ausserhalb der Bundesverwaltung, die jedoch mit öffentlich-rechtlichen Aufgaben des Bundes betraut sind. 3) Ein Massnahmenplan stellt ein Arbeitsinstrument für die

Risikobewältigung dar. Er zeigt insbesondere auf, wie die Eintretenswahrscheinlichkeit und/oder die Schadenhöhe eines Risikos reduziert werden können. 4) Bei der Bruttobewertung werden die Risiken ohne Berücksichtigung der vorhandenen Sicherungs- und Kontrollmassnahmen

bewertet (Bruttorisiken). Bei der Nettobewertung werden die Kontrollen und Massnahmen berücksichtigt (Restrisiken). 5) Institute of Internal Auditors.

5. FAZIT

Mit der Realisierung des Risikomanagements hat das Seco dem Auftrag des Bundesrats zur Umsetzung der Risikopolitik des Bundes Rechnung getragen. Die systematische Erfassung und Bewertung der Risikopotenziale ermöglicht den Bereichen ein gesteigertes Risikobewusstsein und unterstützt die Risikobewältigung. Zudem werden durch die fundierten Risikoinformationen und grössere Risikotransparenz die Entscheidungsgrundlagen im Seco verbessert. Damit dem Risikomanagement der notwendige Stellenwert beigegeben wird, hat die GL die Verantwortung für den Risikomanagementprozess übernommen. Dieser beinhaltet die Steuerung der bestehenden Risiken sowie das Führen eines Risikoportefeuilles über die Kernrisiken. Diese werden im Rahmen eines einheitlichen Meldesystems jährlich an das Departement und die EFV zwecks Umsetzung der Versicherungspolitik weitergeleitet. Der Risikomanagementprozess Seco wird periodisch durch die IR geprüft. Dadurch sollen die Wirksamkeit und die kontinuierliche Verbesserung sichergestellt werden. ■

RESUME

Gestion des risques et Confédération

Ayant constaté plusieurs points faibles dans la couverture d'assurances de la Confédération, le Conseil fédéral a décidé, en janvier 2005, de charger les départements et la Chancellerie fédérale de mettre en œuvre une politique de risque définie par l'Administration fédérale des finances. Cette politique comprend des instructions concernant la gestion du risque et définit une pratique cohérente et systématique face aux multiples risques encourus par l'administration fédérale. La direction du *Secrétariat d'Etat à l'économie (seco)* a attribué un mandat d'analyse des risques, à réaliser avec le soutien de l'organe interne de révision, pour établir la base d'une procédure de gestion des risques et un plan d'audit pluriannuel. Dans une première phase et suivant les critères définis par la politique de risque de la Con-

fédération, 195 domaines à risque ont été identifiés en collaboration avec les unités du seco. Dans une deuxième phase, l'état-major de direction ainsi que les chefs des centres de prestations et des secteurs ont d'abord évalué ces risques à l'aide d'une grille standardisée, puis les ont hiérarchisés et documentés dans le cadre d'une procédure d'analyse des risques. Le rapport de synthèse a mis l'accent sur les principaux risques bruts (TOP-Bruttorisiken) comme base du plan d'audit pluriannuel de l'organe de révision interne, ainsi que sur les principaux risques financiers résiduels (TOP-Restrisiken) qui présentent un dommage potentiel supérieur à 5 millions de CHF et/ou une probabilité d'occurrence supérieure à la moyenne et jouent par conséquent un rôle crucial dans la gestion des risques des unités. La

direction du seco, qui est responsable de la gestion des risques, s'est penchée sur les résultats et a chargé les unités de mettre en pratique la procédure de gestion des risques en se fondant sur l'analyse des risques. Cette analyse implique notamment l'examen des risques résiduels sous l'angle de l'acceptation du risque et des mesures à prendre le cas échéant, ainsi que la mise en application de la procédure de gestion des risques. Au seco, les risques résiduels sont saisis par un service central dans un outil informatique, pour rapport au Département fédéral de l'économie, dont dépend le seco. La décision de la direction du seco attribue à l'organe interne de révision un rôle actif dans la gestion des risques, conformément aux Modalités pratiques d'application 2100-3 de l'IIA. JS/ML