

# **Risikoreporting zuhanden des Bundesrats**

**Bericht vom 28. Mai 2010 der Geschäftsprüfungskommissionen  
des National- und Ständerats**

**Stellungnahme des Bundesrates**

vom 18. August 2010

---

Sehr geehrte Frau Kommissionspräsidentin  
Sehr geehrter Herr Kommissionspräsident  
Sehr geehrte Damen und Herren

Der Bundesrat hat den Bericht vom 28. Mai 2010 der Geschäftsprüfungskommissionen (GPK) zur Kenntnis genommen. Er nimmt im Folgenden, wie von den GPK gewünscht, zu den dargelegten Problemen bzw. Mängeln im Risikomanagement des Bundes im Allgemeinen (vgl. Ziff. 2) und zu den einzelnen Empfehlungen im Besonderen (vgl. Ziff. 3) Stellung.

Wir versichern Sie, sehr geehrte Frau Kommissionspräsidentin, sehr geehrter Herr Kommissionspräsident, sehr geehrte Damen und Herren, unserer vorzüglichen Hochachtung.

18. August 2010

Im Namen des Schweizerischen Bundesrates

Die Bundespräsidentin: Doris Leuthard

Die Bundeskanzlerin: Corina Casanova

# Stellungnahme

## 1 Einführung

Mit der Verabschiedung der «Risikopolitik» im Dezember 2004 hat der Bundesrat die Grundlagen für das Risikomanagement des Bundes gelegt. Es wurde damit nicht etwas grundsätzlich Neues geschaffen. Vielmehr hat der Bundesrat damals, gestützt auf jahrelange, einschlägige Erfahrungen zahlreicher Verwaltungseinheiten, den Gegenstand, die Ziele und die Prozessabläufe eines modernen Risikomanagements für den Bund erstmals in einem Regelwerk verbindlich zusammengefasst.

Die Aufgaben der Bundesverwaltung decken ein weites Spektrum ab. Die Risiken, denen der Bund aufgrund dieser Tätigkeiten ausgesetzt ist, sind deshalb sehr unterschiedlich, sowohl aufgrund ihrer Art, als auch aufgrund ihrer möglichen Folgen. Entsprechend sind die Ausgangslage und die Erwartungen an das Risikomanagement in den Verwaltungseinheiten und Departementen sehr uneinheitlich. Der Bundesrat hat sich deshalb für ein dezentrales Umsetzungskonzept entschieden. Es ist ihm auch wichtig, dass in der Ausgestaltung des Risikomanagements des Bundes eine gewisse Flexibilität erhalten bleibt. Zudem legt der Bundesrat bei der Ausgestaltung seiner Planungs- und Kontrollinstrumente Wert auf ein vorteilhaftes Kosten-Nutzen-Verhältnis.

Das Risikomanagement wird seit seiner Einführung in der Bundesverwaltung ständig weiterentwickelt. Die Geschäftsprüfungskommissionen (GPK) anerkennen zu Recht, dass bereits beachtliche Fortschritte erzielt worden sind. Es ist aber auch unbestritten, dass es weitere Verbesserungsmöglichkeiten gibt. Der Bundesrat geht mit den GPK darin einig, dass insbesondere bei der Risikokonsolidierung auf Stufe Bund und bei der einheitlichen Umsetzung des Risikomanagements in den Departementen und Verwaltungseinheiten Schwerpunkte zu setzen sind. Erste Schritte in diese Richtung hat der Bundesrat bereits in die Wege geleitet.

## 2 Probleme und Mängel im Risikomanagement des Bundes sowie eingeleitete Verbesserungen

### 2.1 Risikokonsolidierung auf Stufe Bund

Als Hauptproblem bezeichnen die GPK die «fehlende Steuerung auf Bundesebene». Das vom Bundesrat beschlossene dezentrale Umsetzungskonzept erlaube es ihm nicht, eine Gesamtsicht der Kernrisiken, denen der Bund ausgesetzt ist, zu gewinnen. Auch stelle das Risikomanagement für den Bundesrat noch kein Steuerungsinstrument dar.

Mit dieser Kritik ist die auch nach Meinung des Bundesrates heute noch mangelhafte Konsolidierung der von den Departementen und der Bundeskanzlei gemeldeten Risiken angesprochen. Die Problematik wurde schon vor längerer Zeit erkannt und im Januar 2010 wurde beschlossen, den bestehenden Bottom-up-Ansatz mit einem Top-down-Ansatz zu ergänzen. Die Aufgaben der Generalsekretärenkonferenz (GSK) im Zusammenhang mit der Risikoberichterstattung zuhanden des Bundesrates wurden wie folgt präzisiert:

1. Es gibt Risiken bzw. Risikobereiche, die in mehreren oder gar in allen Departementen gleich oder in ähnlicher Form auftreten. Hier stellt sich die Frage, ob es möglich und auch sinnvoll ist, diese sogenannten Querschnittsrisiken auf Stufe Bundesrat umfassend zu analysieren und darzustellen. Eine Aggregation auf Stufe Bundesrat macht dann Sinn, wenn sich daraus ein Mehrwert ergibt. Wenn ein in mehreren Departementen auftretendes, dort als mehr oder weniger bedeutend eingestuftes Risiko aus der Sicht des Gesamtbundes ein Grossrisiko darstellt, muss der Bundesrat aus Transparenzgründen über das aggregierte Risiko informiert werden. Ein klarer Mehrwert kann auch darin bestehen, dass ein Risiko durch eine von allen Departementen gemeinsam beschlossene und umgesetzte Massnahme effizienter oder kostengünstiger reduziert werden kann. In einem ersten Schritt werden nun die Möglichkeiten einer Aggregation und damit einer departementsübergreifenden Risikobewirtschaftung in den Bereichen «IKT Datenabfluss», «IKT Systemausfall», «Informationsschutz» und «Bedrohung von Mitarbeitenden» näher geprüft. Der Bundesrat wird im Rahmen der Risikoberichterstattung 2010 über die Ergebnisse der Abklärungen orientiert.
2. Die Departemente und die Bundeskanzlei melden dem Bundesrat jährlich die (aus ihrer Sicht) wichtigsten Risiken. Darunter befinden sich solche, die auch aus Sicht des Gesamtbundes nicht ausser Acht gelassen werden dürfen. Im Rahmen der Risikoberichterstattung 2010 wird es Aufgabe der GSK sein, diese Risiken zu identifizieren und dem Bundesrat zu melden.
3. Es besteht keine Gewähr dafür, dass auf dem Weg der departementalen Risikoberichterstattungen *alle* aus der Sicht des Gesamtbundes wichtigen Risiken erfasst werden. Eine Vollständigkeitsprüfung durch die GSK ist deshalb unerlässlich.

## 2.2 **Einheitliche Umsetzung des Risikomanagements in den Departementen und Verwaltungseinheiten**

Jede Konsolidierung auf Stufe Gesamtbund setzt voraus, dass die Risiken in den Departementen und in den Verwaltungseinheiten nach den gleichen Grundsätzen bewirtschaftet werden. Erst eine einheitliche und möglichst homogene Umsetzung des Risikomanagements in den Departementen und der Bundeskanzlei ermöglicht es, einzelne Risiken miteinander zu vergleichen. Um diesem Ziel näher zu kommen, werden zurzeit folgende Massnahmen umgesetzt:

1. Die aktuelle «Risikopolitik» des Bundesrates legt die departementsinternen Prozesse nicht im Detail fest. Auch die Pflichtenhefte der Risikomanagerinnen und Risikomanager (Stufe Departement), der Risikocoaches (Stufe Verwaltungseinheit) und der weiteren Prozessbeteiligten (Risikoeigner, Massnahmenverantwortliche usw.) sind nicht vorgegeben. Dies führt dazu, dass die Risikopolitik auch innerhalb der Departemente nicht immer einheitlich umgesetzt wird. Die Begleitung bzw. Betreuung der Verwaltungseinheiten durch das Departement könnte oftmals besser sein. Die Risikomanagerin oder der Risikomanager des Departements muss einheitlich und verbindlich festlegen, wie Risiken zu erfassen sind (Verantwortlichkeiten, Massnahmenpläne, Ursachen, Bewertungen usw.). Unzulänglichkeiten müssen erkannt und korrigiert werden. Ausserdem muss in jedem Departement zentral

bestimmt werden, ab welcher Einstufung ein Risiko dem Departement gemeldet werden muss. Zudem braucht es klare Grundsätze für eine Risikostrategie. Fehlen solche strategisch-politische Vorgaben, so entsteht innerhalb des Departements keine gemeinsame Risikosprache und es ist bereits auf Stufe Departement schwierig, gleich gelagerte Risiken zu erkennen und gegebenenfalls zu aggregieren. Aus diesen Gründen hat die GSK im Mai 2009 diversen Verbesserungsmöglichkeiten in den departementsinternen Abläufen, insbesondere einem standardisierten Prozessablauf, zugestimmt.

2. In ihrer Funktion als Koordinationsstelle für das Risikomanagement des Bundes führt die Eidgenössische Finanzverwaltung (EFV) mit den Risikomanagerinnen und Risikomanagern der Departemente und der Bundeskanzlei periodisch Workshops durch. Behandelt werden breit gefächerte Themen im Zusammenhang mit der Weiterentwicklung des Risikomanagements des Bundes. Ziel dieser Besprechungen ist es, ein einheitliches Risikoverständnis zu entwickeln und zu einer homogenen Umsetzung der Risikopolitik in den Departementen und den Verwaltungseinheiten beizutragen.
3. Ab Sommer 2010 organisiert das Eidgenössische Personalamt in Zusammenarbeit mit der EFV, der Bundeskanzlei (Krisenmanagementausbildung des Bundes) und unter der Leitung eines externen Experten (Dr. Bruno Brühwiler, Euro Risk Limited, Zürich) den Kurs «Risiken verstehen und bewältigen; Umsetzen des Risikomanagements in der Bundesverwaltung». Die Zielgruppe bilden die Risikomanagerinnen und Risikomanager der Departemente und der Bundeskanzlei sowie die Risikocoaches der Verwaltungseinheiten. Der Bundesrat ist zuversichtlich, dass mit dieser auf den Bund zugeschnittenen Ausbildung für Risikospezialistinnen und -spezialisten ein weiterer Beitrag zu einer professionellen und einheitlichen Umsetzung des Risikomanagements geleistet wird.
4. Die «Risikopolitik» des Bundesrates von 2004 wird zurzeit einer Totalrevision unterzogen. Sie soll den inzwischen gewonnenen Erfahrungen einerseits und den internationalen Entwicklungen im Risikomanagement andererseits angepasst werden. Die neuen «Weisungen über die Risikopolitik des Bundes» werden die Grundsätze und Entscheide umfassen, die das Verhalten der Bundesverwaltung und ihrer Führungskräfte im Umgang mit ihren Risiken nach aussen und nach innen langfristig bestimmen. Es ist vorgesehen, die Weisungen im Verlaufe des Jahres 2010 in Kraft zu setzen. Gestützt darauf wird die EFV Richtlinien über das Risikomanagement erlassen. Diese sollen die Einzelheiten der Umsetzung des Risikomanagements in den Departementen und der Bundeskanzlei in Anlehnung insbesondere an die ISO-Norm 31000 regeln und die Grundlage schaffen für eine «unité de doctrine» und damit für die Vergleichbarkeit der Risiken.

## 2.3

### Fazit

Der Bundesrat ist mit der Problemanalyse und mit den von den GPK unterbreiteten Verbesserungsvorschlägen weitgehend einverstanden. Die zur Unterstützung und Ergänzung des dezentralen Umsetzungskonzepts empfohlene Einführung eines Top-down-Ansatzes bei der Risikokonsolidierung auf Stufe Bund hat er bereits in Angriff genommen. Der Bundesrat kann sich mit der damit einhergehenden Verstärkung der

Koordinationsfunktion der EFV einverstanden erklären, wenn das Parlament die dafür benötigten Ressourcen gutheisst. In diesem Sinne ist der Bundesrat bereit, dem Parlament eine moderate Aufstockung der Mittel zu beantragen. Hingegen lehnt er die Schaffung eines eigentlichen Kompetenzzentrums für das Risikomanagement weiterhin ab. Die Departemente und ihre Verwaltungseinheiten sollen wie bis anhin in ihrem Bereich die Hauptverantwortung tragen.

### 3 Stellungnahme zu den einzelnen Empfehlungen

*Empfehlung 1:* Der bestehende Bottom-up-Ansatz wird durch einen Top-down-Ansatz ergänzt.

Der Bundesrat wird insbesondere dazu aufgefordert, den Top-down-Ansatz zu stärken, indem er die Möglichkeit prüft, ein Koordinations- und Kompetenzzentrum zu schaffen.

Es wird auf die Ausführungen in den Ziffern 2.1 und 2.3 verwiesen. Ein ergänzender Top-down-Ansatz ist im Risikomanagement des Bundes – auf allen Ebenen – unabdingbar und befindet sich im Aufbau. Für dessen Umsetzung auf Stufe Bundesrat ist es jedoch nicht notwendig, ein eigentliches Kompetenzzentrum zu schaffen, das in die Zuständigkeiten der Departemente und der Bundeskanzlei eingreifen könnte. Nach Meinung des Bundesrates genügt derzeit eine moderate Aufstockung der Ressourcen der Koordinationsstelle in der EFV.

*Empfehlung 2:* Der Bundesrat legt Richtlinien für einheitliche Kriterien der Risikobeurteilung fest und sorgt dafür, dass sie angewendet werden.

In den bereits erwähnten «Weisungen über die Risikopolitik des Bundes» wird der Bundesrat die Grundsätze und Eckwerte der Risikopolitik festlegen. Die Einzelheiten der Umsetzung des Risikomanagements werden hingegen in Richtlinien der EFV geregelt. Es liegt auf der Hand, dass alle Risiken nach den gleichen Kriterien beurteilt werden müssen. Sonst sind sie nicht vergleichbar. Die Beurteilungskriterien müssen deshalb einheitlich und verbindlich vorgegeben werden.

*Empfehlung 3:* Der Bundesrat sorgt dafür, dass in der Bewertung der Bundesrisiken die a priori nicht-finanziellen Hauptrisiken systematisch und homogen berücksichtigt werden.

Nichtfinanzielle Auswirkungen von Risiken (Funktionsstörung der Regierungs- und Verwaltungstätigkeit, Beeinträchtigung der Reputation) werden im Risikomanagement des Bundes schon heute als zusätzliche subsidiäre Bewertungskriterien berücksichtigt. Die Risikomanagerinnen und Risikomanager der Departemente und der Bundeskanzlei haben zu diesem Zweck eine Schadensausmass-Matrix erarbeitet. Die Handhabung dieser Bewertungskriterien ist in der Praxis allerdings nicht ganz

einfach. Im Rahmen der Richtlinien der EFV über das Risikomanagement sollen alle Bewertungskriterien möglichst praxistauglich und einheitlich festgelegt werden.

*Empfehlung 4:* Der Bundesrat sorgt dafür, dass alle Verwaltungseinheiten das gleiche Instrument nutzen, um erkannte Risiken zu verwalten. Zu diesem Zweck trifft er die nötigen Massnahmen, um einen genügenden Informationsschutz zu gewährleisten.

Schon heute werden alle für die Departemente und die Bundeskanzlei relevanten Risiken mit einer einzigen, gemeinsamen Informatikanwendung beschrieben, bewirtschaftet, gesteuert, überwacht und dokumentiert. Nur so ist eine aussagekräftige und mit vertretbarem Aufwand realisierbare Risikoberichterstattung zuhanden des Bundesrates möglich. Dies soll als Vorgabe auch in den «Weisungen über die Risikopolitik des Bundes» festgeschrieben werden. Weiter ist darauf hinzuweisen, dass die im Sommer 2008 von der Eidgenössischen Finanzkontrolle angeregte Überprüfung des Informatiksicherheits- und Datenschutzkonzepts inzwischen durchgeführt und abgeschlossen wurde. Die notwendigen Verbesserungen wurden bereits umgesetzt.

*Empfehlung 5:* Der Bundesrat sorgt dafür, dass Rückmeldungen gegenüber den Departementen und bis hin zu den Verwaltungseinheiten im Rahmen der Neudefinition des Risikomanagement-Konzepts als Steuerungsinstrument in dieses Konzept integriert wird.

Der Bundesrat geht mit den GPK einig, dass im Bereich der Informationsflüsse zwischen den verschiedenen Ebenen im Risikomanagement (Bundesrat, Departement, Verwaltungseinheit) noch Verbesserungspotenzial besteht. Im Rahmen der Richtlinien der EFV über das Risikomanagement soll dem Problem die nötige Beachtung geschenkt werden.

*Empfehlung 6:* Der Bundesrat ergreift geeignete Massnahmen, damit die Querschnittsrisiken angemessen erkannt und im Reporting 2010 schon ausgewiesen werden, beispielsweise in einem Anhang, welcher Aufschluss gibt über die konsolidierten Querschnittsrisiken.

Wie in Ziffer 2.1 bereits dargelegt, will der Bundesrat die Problematik der Querschnittsrisiken schrittweise angehen. Es geht hier nicht um ein mechanisches Zusammenzählen von Departementsrisiken. Vielmehr (und vor allem) sind auch die Wechselwirkungen zwischen den Einzelrisiken bzw. den einzelnen Aspekten zu berücksichtigen. Erste Arbeitssitzungen von IKT-Spezialisten haben bereits stattgefunden. Der Bundesrat soll im Rahmen der Risikoberichterstattung 2010 über erste Erkenntnisse orientiert werden.