


Caspar Flück

---



## **Compliance im öffentlichen Sektor**

---

Untersuchung über den allfälligen Nutzen  
eines Compliance-Management-Systems in  
der öffentlichen Verwaltung am Beispiel des  
Bundesamtes für Gesundheit

---

---

Cahier de l'IDHEAP 256/2010

---



**Institut de hautes études en administration publique**  
Swiss Graduate School of Public Administration

**L'Université pour le service public**

## Zusammenfassung

Unter Compliance wird die Gesamtheit aller organisatorischen Massnahmen eines Unternehmens verstanden, die das gesetzestreuere Verhalten eines Unternehmens und seiner Mitarbeiter gewährleisten sollen. Dieser Begriff ist in der Privatwirtschaft – insbesondere im Banken- und Versicherungssektor – fest etabliert, und der Posten des sogenannten Compliance Officers erscheint jeweils prominent im Organigramm eines Unternehmens. Auch in der Bundesverwaltung taucht dieser Begriff im Zusammenhang mit dem Risikomanagement und dem Internen Kontrollsystem (IKS) hin und wieder auf, an einer effektiven Einführung von Compliance fehlt es aber (bisher). Der Amerikaner pflegt zu sagen «if you think compliance is expensive, try non compliance». Doch lässt sich diese für die Privatwirtschaft offensichtlich gültige Aussage tel quel auf den öffentlichen Sektor übertragen? Hätte die Einführung eines Compliance-Management-Systems tatsächlich einen Mehrwert im Vergleich zu den bisher vorhandenen Systemen zur Verhinderung von Rechts- und Reputationsrisiken? Diesen Fragen geht die vorliegende Arbeit nach, indem anhand von Dokumenten sowie Interviews analysiert wird, welche Compliance-Elemente auf Stufe Bund und innerhalb des Bundesamtes für Gesundheit (BAG) vorhanden sind und ob damit die Zielsetzung von Compliance erreicht wird. In verschiedenen Bereichen konnten konkrete Schwächen und dementsprechend grosses Verbesserungspotential festgestellt werden. Ein wesentlicher Mangel liegt in der fehlenden Compliance-Organisation, welche einen Überblick über die auf Stufe Bund und im BAG vorhandenen Rechts- und Reputationsrisiken erschwert und ein einheitliches Management von Compliance-Risiken verunmöglicht. Dementsprechend dürfte es unter den gegebenen Umständen schwierig sein, Rechts- und Reputationsrisiken mit den vorhandenen Systemen entsprechend der Zielsetzung von Compliance nachhaltig zu verhindern. Andererseits sind mit dem Risikomanagement Bund und der bundesweiten Einführung eines Internen Kontrollsystems (IKS) bereits erste Schritte in Richtung integriertes Riskmanagementsystem eingeleitet worden. Compliance wäre hier die ideale Ergänzung und könnte – sofern es von der Amtsführung getragen und vorgelebt wird – einen massgeblichen Beitrag zur Reduktion der Rechts- und Reputationsrisiken sowohl auf Stufe Bund als auch im BAG leisten. Demgemäss will die vorliegende Arbeit nicht die vorhandenen Systeme kritisieren, sondern vielmehr Verbesserungspotenzial aufzeigen, das es zu nutzen gilt.

## Résumé

Par Compliance, on entend l'ensemble des mesures organisationnelles d'une entreprise qui visent à assurer le respect des règles par l'entreprise et ses collaborateurs. Dans le secteur privé – surtout dans les banques et les assurances – la Compliance est un concept bien établi et le poste du Compliance Officer apparaît clairement dans l'organigramme des entreprises. Ce terme apparaît aussi de temps à autre au sein de l'administration fédérale, en relation avec la politique de gestion des risques et le système de contrôle interne (SCI); mais une introduction effective de la Compliance n'y a pas encore eu lieu (jusqu'ici). Les Américains ont l'habitude de dire «if you think compliance is expensive, try non compliance». Cette déclaration, apparemment valable pour le secteur privé, peut-elle cependant être transposée telle quelle au secteur public? L'introduction d'un système de management tel que la Compliance apporterait-elle effectivement une plus-value par rapport aux systèmes existants afin d'éviter les risques engendrant des conséquences juridiques ou causant une mauvaise réputation suite au non-respect de règles par des collaborateurs? La présente étude se penche sur ces questions et analyse, sur la base de documents et d'interviews, quels éléments de la Compliance existent au niveau de la Confédération et au sein de l'Office fédéral de la santé publique (OFSP) et s'ils sont propres à atteindre les objectifs visés par la Compliance.

Dans plusieurs domaines, on a pu constater des défauts et, par conséquent, un gros potentiel d'amélioration. Le problème principal est l'absence d'organisation au niveau de la Compliance. Cela complique la vue d'ensemble des risques juridiques et de ceux pouvant causer une mauvaise réputation qui existent au niveau de la Confédération et à l'OFSP et rend impossible un management homogène de ces risques. En conséquence et dans l'état actuel des choses, il pourrait s'avérer difficile d'éviter de manière durable la réalisation des risques susmentionnés au moyen des systèmes existants. D'un autre côté, la politique de gestion des risques au sein de la Confédération et l'introduction d'un système de contrôle interne (SCI) ont représenté les premiers pas en direction d'un système de gestion des risques intégré. La Compliance serait un complément idéal et pourrait – dans la mesure où la direction de l'Office la soutient et donne le bon exemple – contribuer à la réduction des risques décrits ci-dessus non seulement au niveau de la Confédération mais encore au sein de l'OFSP. La présente étude ne vise pas pour autant à critiquer les systèmes établis, mais bien plus à montrer le potentiel d'amélioration dont on pourrait tirer profit.

Caspar Flück

## Compliance im öffentlichen Sektor

Untersuchung über den allfälligen Nutzen eines  
Compliance-Management-Systems in der öffentlichen  
Verwaltung am Beispiel des Bundesamtes für Gesundheit

Cahier de l'IDHEAP 256/2010

Travail de mémoire

Rapporteur: Prof. Luzius Mader

© 2010 IDHEAP, Chavannes-Lausanne

ISBN 978-2-940390-33-5



**Institut de hautes études en administration publique**  
**Swiss Graduate School of Public Administration**  
Quartier UNIL Mouline – CH-1015 – Lausanne  
T : +41(0)21 557 40 00 – F : +41(0)21 557 40 09  
idheap@idheap.unil.ch – www.idheap.ch

**"If you think compliance is expensive, try non-compliance."**

Amerikanische Redensart

## INHALTSVERZEICHNIS

Abkürzungsverzeichnis .....	IV	
Zusammenfassung .....	VII	
Résumé.....	IX	
1	Problematik..... 1	
2	Ziel und Methodik der vorliegenden Arbeit..... 4	
2.1	Ziel der Arbeit .....	4
2.2	Forschungsfrage .....	4
2.3	Vorgehen und eingesetzte Untersuchungsmethodik .....	4
3	Compliance: Definition und Hintergrund..... 7	
3.1	Begriffsdefinition .....	7
3.2	Historische Entwicklung..... 9	
3.2.1	In der Privatwirtschaft .....	9
3.2.2	Im Bund .....	11
3.2.3	Im BAG .....	12
3.3	Sinn und Zweck von Compliance .....	13
3.3.1	Compliance-Risiken .....	13
3.3.2	Rechtliche und ökonomische Betrachtungsweise .....	14
3.3.3	Die Rolle des Staates .....	15
3.3.4	Risiken, die durch Compliance entstehen .....	16
3.3.5	Empirischer Nachweis über die Wirkung von Compliance .....	17
3.3.6	Zusammenfassung.....	17
3.4	Abgrenzung zu anderen Begriffen.....	18
3.4.1	Compliance und Corporate Governance.....	18

3.4.2	Compliance, IKS und Riskmanagement .....	19
3.5	IKS, Riskmanagement und Compliance in der Bundesverwaltung	23
3.5.1	Gesetzliche Anforderungen.....	23
3.5.2	Zuständigkeiten .....	26
3.6	Elemente eines Compliance-Management-Systems .....	26
3.6.1	Übersicht .....	26
3.6.2	Risikoanalyse .....	27
3.6.3	Regeln und Richtlinien.....	29
3.6.4	Information, Aufklärung und Ausbildung von Mitarbeitenden.....	31
3.6.5	Organisatorische Massnahmen .....	32
3.6.6	Beratung.....	37
3.6.7	Überwachung der Einhaltung der unternehmensinternen Vorgaben .....	37
3.6.8	Sanktionieren von Regelverstössen .....	40
4	Compliance im BAG und auf Stufe Bund .....	41
4.1	Risikoanalyse .....	41
4.1.1	Risikoanalyse im Bund .....	41
4.1.2	Die Compliance-Risiken des BAG.....	41
4.1.3	Zusammenfassung und Schlussfolgerung .....	45
4.2	Relevante Regeln und Richtlinien .....	46
4.2.1	Regeln und Richtlinien auf Stufe Bund .....	46
4.2.2	Regeln und Richtlinien des BAG.....	47
4.2.3	Zusammenfassung und Schlussfolgerung .....	49
4.3	Vermittlung des Compliance-Wissens .....	50
4.3.1	Compliance-Ausbildung auf Stufe Bund .....	50

4.3.2	Compliance-Ausbildung im BAG.....	51
4.3.3	Zusammenfassung und Schlussfolgerung .....	53
4.4	Compliance-Organisation.....	54
4.4.1	Compliance-Organisation im Bund.....	54
4.4.2	Compliance-Organisation im BAG .....	54
4.4.3	Zusammenfassung und Schlussfolgerung .....	56
4.5	Beratung .....	57
4.5.1	Beratung im Bund .....	57
4.5.2	Wahrnehmung der Beratungsfunktion im BAG .....	57
4.5.3	Zusammenfassung und Schlussfolgerung .....	58
4.6	Überwachung .....	59
4.6.1	Kontrolle und Überwachung im Bund .....	59
4.6.2	Compliance-Überwachung im BAG.....	60
4.6.3	Zusammenfassung und Schlussfolgerung .....	61
4.7	Sanktionssystem.....	62
4.7.1	Sanktionssystem des Bundes.....	62
4.7.2	Sanktionssystem des BAG.....	63
4.7.3	Zusammenfassung und Schlussfolgerung .....	63
4.8	Synthese.....	64
5	Schlussfolgerungen und Empfehlungen.....	66
Anhang	.....	71
Bibliographie.....		72

## ABKÜRZUNGSVERZEICHNIS

Abs.:	Absatz
AG:	Aktiengesellschaft
AJP:	Aktuelle Juristische Praxis
Art.:	Artikel
Aufl.:	Auflage
BAG:	Bundesamt für Gesundheit
BBl:	Bundesblatt
BBL:	Bundesamt für Bauten und Logistik
BGÖ:	Bundesgesetz über das Öffentlichkeitsprinzip der Verwaltung
BinfV:	Verordnung über die Informatik und Telekommunikation in der Bundesverwaltung
BIT:	Bundesamt für Informatik und Telekommunikation
BJ:	Bundesamt für Justiz
BoeB:	Bundesgesetz über das öffentliche Beschaffungswesen
BPG:	Bundspersonalgesetz
BPV:	Bundesamt für Privatversicherungen
BPV:	Bundspersonalverordnung
BRB:	Bundesratsbeschluss
bzw.:	beziehungsweise
CD-ROM:	Compact Disc Read-Only Memory
COSO:	The Committee of Sponsoring Organizations of the Treadway Commission
DB:	Direktionsbereich
Diss.:	Dissertation
DSG:	Datenschutzgesetz
EDI:	Eidgenössisches Departement des Innern
EDV:	Elektronische Datenverarbeitung
EFD:	Eidgenössisches Finanzdepartement
EFK:	Eidgenössische Finanzkontrolle
EFV:	Eidgenössische Finanzverwaltung
EJPD:	Eidgenössisches Justiz- und Polizeidepartement



E-Mail:	electronic mail
EPA:	Eidgenössisches Personalamt
etc.:	und so weiter
f.:	folgende
ff.:	fortfolgende
FHG:	Finanzhaushaltsgesetz
FHV:	Finanzhaushaltsverordnung
FINMA:	Eidgenössische Finanzmarktaufsicht
FKG:	Finanzkontrollgesetz
GP:	Gesundheitspolitik
GRECO:	Groupe d'Etats contre la Corruption
GS:	Generalsekretariat
Hrsg.:	Herausgeber
IAZ:	Interdepartementales Ausbildungszentrum
IKS:	Internes Kontrollsystem
IKT-Mittel:	Informatik- und Kommunikationsmittel
Inc.:	Incorporated
IRB:	Informatikrat des Bundes
IT:	Information und Telekommunikation
KUV:	Kranken- und Unfallversicherung
m.E.:	meines Erachtens
Mrd.:	Milliarde
NZZ:	Neue Zürcher Zeitung
OECD:	Organisation for Economic Co-operation and Development
OR:	Schweizerisches Obligationenrecht
OV-EJPD:	Organisationsverordnung für das Eidgenössische Justiz- und Polizeidepartement
P+O:	Sektion Personal und Organisation des BAG
PR:	Public Relations
REMM:	Resourceful, Evaluating, Maximizing Man
RVOG:	Regierungs- und Verwaltungsorganisationsgesetz
Rz.:	Randziffer
S.:	Seite

SARS:	Severe Acute Respiratory Syndrome
SBV:	Schweizerischer Bankverein
SCBP:	Swiss Code of Best Practice for Corporate Governance
SECO:	Staatssekretariat für Wirtschaft
SNB:	Schweizerische Nationalbank
sog.:	sogenannt
SOX:	Sarbanes-Oxley Act
SR:	Systematische Sammlung des Bundesrechts
StBOG:	Bundesgesetz über die Organisation der Strafbehörden des Bundes (Entwurf)
StGB:	Schweizerisches Strafgesetzbuch
UBS:	Union de Banques Suisses
UV:	Unfallversicherung
VBS:	Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport
VDSG:	Verordnung zum Bundesgesetz über den Datenschutz
VoeB:	Verordnung über das öffentliche Beschaffungswesen
VS:	Verbraucherschutz
WBT:	Web-based-Trainings
z.B.:	zum Beispiel
Ziff.:	Ziffer
zit.:	zitiert

## ZUSAMMENFASSUNG

Unter Compliance wird die Gesamtheit aller organisatorischen Massnahmen eines Unternehmens verstanden, die das gesetzestreue Verhalten eines Unternehmens und seiner Mitarbeiter gewährleisten sollen. Dieser Begriff ist in der Privatwirtschaft - insbesondere im Banken- und Versicherungssektor - fest etabliert, und der Posten des sogenannten Compliance Officers erscheint jeweils prominent im Organigramm eines Unternehmens. Auch in der Bundesverwaltung taucht dieser Begriff im Zusammenhang mit dem Riskmanagement und dem Internen Kontrollsystem (IKS) hin und wieder auf, an einer effektiven Einführung von Compliance fehlt es aber (bisher). Der Amerikaner pflegt zu sagen "if you think compliance is expensive, try non compliance". Doch lässt sich diese für die Privatwirtschaft offensichtlich gültige Aussage teils auf den öffentlichen Sektor übertragen? Hätte die Einführung eines Compliance-Management-Systems tatsächlich einen Mehrwert im Vergleich zu den bisher vorhandenen Systemen zur Verhinderung von Rechts- und Reputationsrisiken? Diesen Fragen geht die vorliegende Arbeit nach, indem anhand von Dokumenten sowie Interviews analysiert wird, welche Compliance-Elemente auf Stufe Bund und innerhalb des Bundesamtes für Gesundheit (BAG) vorhanden sind und ob damit die Zielsetzung von Compliance erreicht wird.

In verschiedenen Bereichen konnten konkrete Schwächen und dementsprechend grosses Verbesserungspotential festgestellt werden. Ein wesentlicher Mangel liegt in der fehlenden Compliance-Organisation, welche einen Überblick über die auf Stufe Bund und im BAG vorhandenen Rechts- und Reputationsrisiken erschwert und ein einheitliches Management von Compliance-Risiken verunmöglicht. Dementsprechend dürfte es unter den gegebenen Umständen schwierig sein, Rechts- und Reputationsrisiken mit den vorhandenen Systemen entsprechend der Zielsetzung von Compliance nachhaltig zu verhindern. Andererseits sind mit dem Risikomanagement Bund und der bundesweiten Einführung eines Internen Kontrollsystems (IKS) bereits erste Schritte in Richtung integriertes Riskmanagementsystem eingeleitet worden. Compliance

wäre hier die ideale Ergänzung und könnte - sofern es von der Amtsführung getragen und vorgelebt wird - einen massgeblichen Beitrag zur Reduktion der Rechts- und Reputationsrisiken sowohl auf Stufe Bund als auch im BAG leisten. Demgemäss will die vorliegende Arbeit nicht die vorhandenen Systeme kritisieren, sondern vielmehr Verbesserungspotenzial aufzeigen, das es zu nutzen gilt.

## RÉSUMÉ

Par Compliance on entend l'ensemble des mesures organisationnelles d'une entreprise qui visent à assurer le respect des règles par l'entreprise et ses collaborateurs. Dans le secteur privé - surtout dans les banques et les assurances - la Compliance est un concept bien établi et le poste du Compliance Officer apparaît clairement dans l'organigramme des entreprises. Ce terme apparaît aussi de temps à autre au sein de l'administration fédérale, en relation avec la politique de gestion des risques et le système de contrôle interne (SCI); mais une introduction effective de la Compliance n'y a pas encore eu lieu (jusqu'ici). Les américains ont l'habitude de dire "if you think compliance is expensive, try non compliance". Cette déclaration, apparemment valable pour le secteur privé, peut-elle cependant être transposée telle quelle au secteur public? L'introduction d'un système de management tel que la Compliance apporterait-elle effectivement une plus-value par rapport aux systèmes existants afin d'éviter les risques engendrant des conséquences juridiques ou causant une mauvaise réputation suite au non-respect de règles par des collaborateurs? La présente étude se penche sur ces questions et analyse, sur la base de documents et d'interviews, quels éléments de la Compliance existent au niveau de la Confédération et au sein de l' Office fédéral de la santé publique (OFSP) et s'ils sont propres à atteindre les objectifs visés par la Compliance.

Dans plusieurs domaines, on a pu constater des défauts et, par conséquent, un gros potentiel d'amélioration. Le problème principal est l'absence d'organisation au niveau de la Compliance. Cela complique la vue d'ensemble des risques juridiques et de ceux pouvant causer une mauvaise réputation qui existent au niveau de la Confédération et à l'OFSP et rend impossible un management homogène de ces risques. En conséquence et dans l'état actuel des choses, il pourrait s'avérer difficile d'éviter de manière durable la réalisation des risques susmentionnés au moyen des systèmes existants. D'un autre côté, la politique de gestion des risques au sein de la Confédération et l'introduction d'un système de contrôle interne (SCI) ont représenté les premiers pas en direction d'un

système de gestion des risques intégré. La Compliance serait un complément idéal et pourrait - dans la mesure où la direction de l'office la soutient et donne le bon exemple - contribuer à la réduction des risques décrits ci-dessus non seulement au niveau de la Confédération mais encore au sein de l'OFSP. La présente étude ne vise pas pour autant à critiquer les systèmes établis, mais bien plus à montrer le potentiel d'amélioration dont on pourrait tirer profit.

# 1 PROBLEMATIK

Gemäss Art. 5 Abs. 1 der Bundesverfassung (BV; SR 101) ist das Recht Grundlage und Schranke staatlichen Handelns. Sämtliche Verwaltungstätigkeit hat somit in Einklang mit den geltenden Gesetzen und Verordnungen zu erfolgen. Dieser als Legalitätsprinzip<sup>1</sup> bekannte Grundsatz ist Basis unserer demokratischen Ordnung und als solcher sicherlich nicht bestritten. Nur, in Anbetracht der stetigen Zunahme von Gesetzen, Verordnungen und internationalen Abkommen sehen sich Mitarbeiter der Bundesverwaltung schon allein aufgrund der schieren Masse an Rechtsvorschriften mit der stetigen Gefahr konfrontiert, durch Fehlritte vom Pfad der Rechtskonformität abzuweichen. Neben einer Zunahme der Regulierungsdichte haben auch neue Modelle der Verwaltungsführung (z.B. Outsourcing, Public Private Partnership) sowie die Globalisierung (z.B. internationale Pandemiebekämpfung) dazu geführt, dass es für das Management (Amtsleitung) enorm schwierig geworden ist, rechtskonformes Verhalten intern und extern sicherzustellen<sup>2</sup>. Rechtsverletzungen durch Verwaltungstätigkeiten können jedoch schwerwiegende Konsequenzen für die Finanzen und den Ruf des Bundes haben, wie nachfolgende Beispiele zeigen:

- Am 13. Juni 2006 stiess eine Sachbearbeiterin des Bundesamtes für Gesundheit (BAG) bei ihrer Arbeit auf brisante interne Dokumente. Diese wiesen darauf hin, dass das Amt ein privates PR-Büro beauftragt hat, eine Kampagne gegen die Volksinitiative "Ja zur Komplementärmedizin" zu führen. Sie übergab diese Dokumente den Medien, worauf eine breite mediale Berichterstattung über diesen "skandalösen" Plan des BAG stattfand, und die Geschäftsprüfungskommission des Ständerates nach einer Untersuchung das Amt sowie Bundesrat Pascal Couchepin rügte<sup>3</sup>.

---

<sup>1</sup> Vgl. zum Legalitätsprinzip: HÄFELIN/MÜLLER/UHLMANN, Rz. 368 ff.

<sup>2</sup> Vgl. auch BUFF, S. 167; EFK-LEITFADEN, S. 6.

<sup>3</sup> Vgl. Beobachter Online, Ausgabe 9/09, Zu wenig Schutz für Mutige, [http://www.beobachter.ch/justiz-behoerde/artikel/misstaende-aufdecken\\_zu-wenig-schutz-fuer-mutige/](http://www.beobachter.ch/justiz-behoerde/artikel/misstaende-aufdecken_zu-wenig-schutz-fuer-mutige/) (zuletzt eingesehen am 20. September 2010).

- In einer Mitteilung im Schweizerischen Handelsamtsblatt vom 1. Mai 2009 wurde bekanntgegeben, dass das Bundesamt für Bauten und Logistik (BBL) an Microsoft einen Auftrag für die Verlängerung von Lizenzen in der Höhe von 42 Millionen Franken über drei Jahre vergeben hat. Dieser Auftrag wurde zuvor jedoch nicht ausgeschrieben, sondern im freihändigen Verfahren abgewickelt. Gegen diesen Vergabeentscheid erhoben 18 Anbieter von Open-Source-Lösungen Beschwerde beim Bundesverwaltungsgericht. Dabei droht die Nichtigkeit des Vertrags mit Microsoft und das BBL müsste mit hohen Schadenersatzforderungen rechnen. Zur Zeit ist das Verfahren sistiert, da die Streitparteien auf eine aussergerichtliche Lösung setzen<sup>4</sup>.
- Am 1. April 2003 erliess das BAG zur Bekämpfung der Lungenkrankheit SARS ein Arbeitsverbot für Aussteller und Angestellte der Uhren- und Schmuckmesse Baselworld. Dagegen erhoben die Messe Schweiz AG und die Messe Basel AG Beschwerde beim Eidgenössischen Departement des Innern (EDI), und nach dessen abweisendem Entscheid Verwaltungsgerichtsbeschwerde beim Bundesgericht<sup>5</sup>. Daneben reichte die Messe Schweiz AG auch eine Schadenersatzforderung in zweistelliger Millionenhöhe beim Bund ein.
- Der Geheimdienst-Buchhalter Dino Belasi bezog während 5 Jahren (1994-1999) rund 9 Millionen CHF bei der SNB, dies mit Hilfe seines Rechnungsführerausweises und Vorschussmandaten für fiktive Kurse, die von seinen Vorgesetzten mitunterzeichnet waren. Später auch gestützt auf Vorschussmandate mit gefälschten Unterschriften. Der Fall flog schliesslich nur auf, weil Bellasi nach seinem Austritt aus dem VBS weiter

---

<sup>4</sup> *Jurius, Vergabe an Microsoft: Verfahren gegen Bund erneut sistiert*, in: Jusletter 26. Oktober 2009, [http://jusletter.weblaw.ch/\\_542?lang=de](http://jusletter.weblaw.ch/_542?lang=de) (zuletzt eingesehen am 20. September 2010).

<sup>5</sup> *Jurius, Entscheid des EDI teilweise beanstandet - Sars-Beschwerde nach Uhrenmesse*, in: Jusletter 24. Oktober 2005, [http://jusletter.weblaw.ch/\\_348?lang=de](http://jusletter.weblaw.ch/_348?lang=de) (zuletzt eingesehen am 20. September 2010).



Geld bezog; ein Revisionsbericht verwies auf eine Buchhaltung, die Bellasi nach seinem Abgang erstellt hatte<sup>6</sup>.

Oft fehlt es dem einzelnen Mitarbeiter am Bewusstsein für potentielle Gefahren, oder aber das Risiko wird schlicht unterschätzt<sup>7</sup>. Um rechtskonformes Verhalten innerhalb der Verwaltung zu gewährleisten, braucht es deshalb ein Instrument, das eine Verwaltungseinheit in ihrer Gesamtheit erfasst und kontrolliert, vom Amtsleiter über die mittleren Kaders bis hin zum einzelnen Angestellten. In der Privatwirtschaft hat sich zur Verhinderung von Rechts- und Reputationsrisiken seit den 90er Jahren das Konzept der Compliance etabliert. Nachfolgend soll nun am Beispiel des Bundesamtes für Gesundheit geprüft werden, welchen Mehrwert die Einführung eines Compliance-Management-Systems für die Bundesverwaltung haben könnte.

---

<sup>6</sup> *EFV-AUSBILDUNGSUNTERLAGEN*, S. 2.

<sup>7</sup> *So auch EFK-LEITFADEN*, S. 6.

## 2 ZIEL UND METHODIK DER VORLIEGENDEN ARBEIT

### 2.1 ZIEL DER ARBEIT

Diese Arbeit soll am Beispiel des BAG untersuchen, ob und inwieweit Compliance in der Zentralverwaltung Eingang gefunden hat und umgesetzt wurde. Dabei werden die auf Stufe Bund sowie im BAG vorhandenen Compliance-Elemente analysiert und mit den theoretischen und (falls vorhanden) rechtlichen Anforderungen an ein Compliance-Management-System verglichen. Anhand dieses Vergleichs können wichtige Erkenntnisse über den Umgang mit Rechts- und Reputationsrisiken im BAG gewonnen und Empfehlungen zur Verbesserung des vorhandenen Systems abgegeben werden. Damit soll aufgezeigt werden, welchen Nutzen Compliance für die öffentliche Verwaltung haben könnte, und eine Diskussionsgrundlage für eine generelle Einführung von Compliance auf Stufe Bund geschaffen werden.

### 2.2 FORSCHUNGSFRAGE

Aufgrund den vorangegangenen Ausführungen lässt sich folgende Forschungsfrage formulieren:

Welchen Mehrwert/Nutzen hätte die Einführung eines Compliance-Management-Systems für das Bundesamt für Gesundheit?

### 2.3 VORGEHEN UND EINGESETZTE UNTERSUCHUNGSMETHODIK

Einleitend wird in dieser Arbeit dargestellt, was der Begriff Compliance bedeutet, wie sich dieses Konzept historisch entwickelt hat und welchen Sinn und Zweck es verfolgt. Ebenso wird untersucht, welche (gesetzlichen) Vorgaben bezüglich Compliance in der Bundesverwaltung vorhanden sind, und wer für deren Umsetzung zuständig ist. Die einzelnen Elemente eines Compliance-Konzepts werden dargelegt und erläutert, und es wird ebenfalls versucht, den Begriff der Compliance von anderen Begriffen wie Riskmanagement und Internes Kontrollsystem (IKS) abzugrenzen.

Anschliessend wird ausgehend von der Risikobeurteilung BAG vom 8. Mai 2009 untersucht, welche Unterlagen und Massnahmen im Bereich der einzelnen Compliance-Elemente in Bund und BAG vorhanden sind bzw. ergriffen wurden. Diese werden unter dem Gesichtspunkt der theoretischen Compliance-Anforderungen auf ihre Tauglichkeit für ein Compliance-Konzept überprüft. Die Analyse erfolgte einerseits auf der Basis von Dokumenten (Amtliche Dokumente, Gesetzestexte, Richtlinien, Prüfungsberichte) andererseits aufgrund von Gesprächen mit involvierten Mitarbeitern des BAG sowie der für das IKS zuständigen Person der Eidgenössischen Finanzverwaltung (EFV).

Bei der Textanalyse ging es vorab darum, Compliance-relevante Aspekte zu identifizieren und einem der Elemente des Compliance-Konzepts zuzuordnen. So konnte in einem ersten Schritt festgestellt werden, ob in den verschiedenen Bereichen überhaupt Compliance-Massnahmen vorhanden sind, und in einem zweiten Schritt, ob das Vorhandene den theoretischen Vorgaben entspricht. Die Resultate wiederum lassen Rückschlüsse zu, ob in dem jeweiligen Bereich Handlungsbedarf besteht und ob das BAG insgesamt genügend unternimmt, um Rechts- und Reputationsrisiken zu vermeiden. Da das BAG mit einer Vielzahl von Compliance-Risiken konfrontiert ist, und die Berücksichtigung sämtlicher Risiken den Rahmen dieser Arbeit sprengen würde, wurde die Analyse im Sinne von Fallstudien auf vier Risiken - eines aus jedem der vier Compliance-relevanten Rechtsgebiete - eingeschränkt.

Die Interviews wurden mit Personen aus dem BAG durchgeführt, welche direkt oder indirekt bereits mit Compliance in Berührung gekommen sind, sowie mit einer Person der EFV. Insgesamt wurden fünf Interviews durchgeführt, und zwar mit dem Risiko-Coach BAG (01.09.2009), dem Zuständigen für das IKS des BAG (08.09.2009), dem Leiter Personal und Organisation BAG (06.10.2009), dem Leiter Recht BAG (24.09.2009), sowie einer Mitarbeiterin der Abteilung Finanz- und Rechnungswesen der EFV (10.11.2009). Die Gespräche wurden mit Hilfe eines Fragebogens mit offenen Fragen geführt, anschliessend erfolgte eine Abschrift der Interviews, die den Gesprächspartnern zur Verifikation unterbreitet wurde. Die Interviews dauerten zwischen 30

Minuten und einer Stunde und wurden jeweils mit einer Darlegung des Hintergrunds und den Absichten dieser Arbeit eröffnet.

Anhand der Resultate aus Textanalyse und Interviews konnte festgestellt werden, ob wesentliche Unterschiede zwischen theoretischen Anforderungen an ein Compliance-Management-System und der BAG-Praxis bestehen. Anschliessend wurde jeweils geprüft, ob die festgestellten Differenzen allenfalls negative Auswirkungen auf die Compliance haben, bzw. eine solche sogar verunmöglichen. Ist dies der Fall, könnte die Einführung eines Compliance-Management-Systems tatsächlich einen Mehrwert für das BAG generieren.

### 3 COMPLIANCE: DEFINITION UND HINTERGRUND

#### 3.1 BEGRIFFSDEFINITION

Der Begriff Compliance stammt aus der anglo-amerikanischen Bankenwelt und leitet sich vom Englischen Ausdruck "to comply with" ab, was soviel bedeutet wie "befolgen, einhalten, übereinstimmen". In der Medizin wird Compliance als Bereitschaft eines Patienten zur aktiven Mitwirkung an therapeutischen Massnahmen bezeichnet<sup>8</sup>. Im wirtschaftsrechtlichen Kontext wird der Begriff anders definiert, wobei die verschiedenen Umschreibungen teilweise höchst unterschiedlich ausfallen, wie nachfolgende beispielhafte Aufzählung von Begriffsdefinitionen verdeutlicht:

Eidgenössische Finanzmarktaufsicht (FINMA): "Als Compliance gilt das Einhalten von gesetzlichen, regulatorischen und internen Vorschriften sowie die Beachtung von marktüblichen Standards und Standesregeln."<sup>9</sup>

JÄGER/RÖDL/CAMPOS NAVE: "Der Begriff Compliance bezeichnet die Gesamtheit aller zumutbaren Massnahmen, die das regelkonforme Verhalten eines Unternehmens, seiner Leitungs- und Aufsichtsorgane sowie seiner Organisationsmitglieder im Hinblick auf alle gesetzlichen Ge- und Verbote begründen."<sup>10</sup>

BUFF: "Unter Compliance wird ein Organisationskonzept verstanden, welches durch eine bestimmte Unternehmensorganisation das gesetzestreue Verhalten eines Unternehmens und seiner Mitarbeiter gewährleisten soll."<sup>11</sup>

HAUSCHKA: "Der Begriff Compliance wurde ebenso wie Corporate Governance aus der angelsächsischen Rechtsterminologie in das deut-

---

<sup>8</sup> THELESKLAUF, S. 447.

<sup>9</sup> FINMA-RUNDSCHREIBEN 08/24, Rz. 97.

<sup>10</sup> JÄGER/RÖDL/CAMPOS NAVE, S. 57.

<sup>11</sup> BUFF, S. 10f.

sche Wirtschaftsrecht übernommen. Er bedeutet in etwa Einhaltung, Befolgung, Übereinstimmung, Einhaltung bestimmter Gebote."<sup>12</sup>

ROTH: "Unter dem Begriff Compliance werden im Allgemeinen Strategien verstanden für das ordnungsgemässe Verhalten im Einklang mit geltenden Spielregeln."<sup>13</sup>

MÜLLER: "Compliance umfasst somit die Aufgabe und die Funktion, in einer Unternehmung die Voraussetzungen und das Bewusstsein zu schaffen, dass alle Mitarbeitenden sämtliche, für die Unternehmung relevanten Bestimmungen selbständig einhalten und einhalten können. Zudem ist Compliance für die Kontrolle und die Einhaltung der relevanten Bestimmungen besorgt."<sup>14</sup>

VETTER: "Compliance beschränkt sich deshalb nicht allein auf das Postulat der Rechtstreue eines Unternehmens, sondern umschreibt die Summe der organisatorischen Massnahmen eines Unternehmens, mit denen gewährleistet werden soll, dass sich die Geschäftsleitung wie auch die Mitarbeiter des Unternehmens rechtmässig verhalten."<sup>15</sup>

Gemeinsamer Nenner sämtlicher Definitionen ist die Einhaltung von Regeln. Dagegen beschränken sich einige Begriffsbestimmungen auf das regelkonforme Verhalten an sich, wobei andere die für das Erreichen dieses Verhaltens notwendigen Massnahmen, Konzepte, Organisationsstrukturen und Systeme miteinbeziehen. Nach der hier vertretenen Ansicht scheint dieser zweite Ansatz überzeugend, da mit Compliance eben gerade die notwendigen Instrumente für die Umsetzung regelkonformen Verhaltens geschaffen werden sollen. Im Vordergrund steht nicht allein die rechtliche, sondern auch die Management-Komponente. Dass Regeln einzuhalten sind, ist eine Binsenwahrheit, die allein zu wenig über Compliance aussagt. Entscheidend ist vielmehr die Umsetzung dieser Vorgabe: Wie muss ich mich organisieren, wie bilde ich meine Mitarbeiter aus, wie kontrolliere ich die Prozessabläufe, damit keine Regelverstösse auftreten? Dies ist der Kern von Compliance. Den Begriff

---

<sup>12</sup> HAUSCHKA, S. 2.

<sup>13</sup> ROTH, *Compliance*, S. 1.

<sup>14</sup> MÜLLER, S. 26.

<sup>15</sup> VETTER, S. 33.

lediglich auf regelkonformes Verhalten zu reduzieren, verkennt die Tragweite von Compliance, der die systemische Komponente, der Management-Aspekt immanent sind. Entsprechend wird der Begriff Compliance (bzw. Compliance-Konzept oder Compliance-Management-System) in der vorliegenden Arbeit im Sinne der Definitionen von BUFF, VETTER und MÜLLER verwendet.

In Bezug auf die Art der einzuhaltenden Regeln ist festzuhalten, dass mit Compliance nicht allein die Beachtung gesetzlicher Vorschriften sichergestellt werden soll, sondern darüber hinaus auch von "... regulations, rules, related self-regulatory organisation standards and codes of conduct... (together, *compliance laws, rules and standards*)"<sup>16</sup>. Neben Gesetzen und Verordnungen werden also auch unternehmensinterne Weisungen, Geschäftsordnungen, Merk- und Informationsblätter, Unterschriftenregelungen, Ethik-Richtlinien etc. miterfasst.

## 3.2 HISTORISCHE ENTWICKLUNG

### 3.2.1 IN DER PRIVATWIRTSCHAFT

Compliance hat ihren Ursprung in den USA und entstand im Wesentlichen als Folge strafrechtlicher Regelungen, welche die Kapitalgesellschaften für die kriminellen Handlungen ihrer Angestellten in die Verantwortung nahmen. Zuerst erfolgte Compliance auf freiwilliger Basis, später aufgrund gesetzlicher Verpflichtung. Neben der erwünschten präventiven Wirkung (Verhinderung von Rechtsverletzungen) konnte die Existenz von internen Compliance-Leitlinien auch erhebliche strafmildernde Wirkung für eine betroffene Gesellschaft zeitigen, da die Strafzumessung unter anderem von einer möglichen Mitschuld der Gesellschaft für das Handeln ihrer Angestellten abhängig war<sup>17</sup>.

Nach und nach wurde dieses Modell auch in Europa übernommen und gesetzliche Regelungen nach dem amerikanischen Vorbild erlassen. In der Schweiz wurde Anfang der 90er Jahre die gesetzliche Pflicht für Aktiengesellschaften verankert, dass die Obergrenze über die mit der

<sup>16</sup> BASEL COMMITTEE ON BANKING SUPERVISION, S. 7.

<sup>17</sup> Vgl. zum Ganzen: HOFSTETTER, S. 178.

Geschäftsführung betrauten Personen, namentlich im Hinblick auf die Befolgung der Gesetze, Statuten, Reglemente und Weisungen zu den unübertragbaren und unentziehbaren Aufgaben des Verwaltungsrates gehört (Art. 716a Abs. 1 Ziff. 5 OR, in Kraft seit 1. Juli 1992). Obwohl nicht explizit erwähnt, wird damit nichts anderes gesagt, als dass die Einhaltung von Compliance dem Verwaltungsrat eines Unternehmens obliegt. Als weitere Aufgabe kommt gemäss Art. 716a Abs. 1 Ziff. 2 OR die Festlegung der Organisation hinzu. Somit hat der Verwaltungsrat nicht nur über die Einhaltung der Compliance zu wachen, sondern er soll proaktiv die organisatorischen Grundlagen schaffen, die ein "compliantes" Verhalten seiner Mitarbeiter ermöglichen<sup>18</sup>. Als erste Schweizer Bank setzte der damalige Schweizerische Bankverein (SBV) 1992 einen konzernweiten Compliance-Officer ein, primär aus strategischen Überlegungen. Man war sich bewusst, dass ein weltweit in verschiedensten Bereichen der Finanzmärkte tätiges Institut einem stark wachsenden und weiter vergrössernden Risiko von Regelverstössen ausgesetzt war<sup>19</sup>. Nach und nach setzte sich dann die Erkenntnis durch, dass Compliance als Instrument der Führungskontrolle nicht nur für bankgeschäftliche Aktivitäten ein Thema sein kann. Vielmehr ist jedes Unternehmen daran interessiert, dass Fehlverhalten von Mitarbeitern mittels eines Compliance-Konzepts verhindert wird, und man sich als integrierter Geschäftspartner und attraktives Investitionsobjekt präsentieren kann<sup>20</sup>.

Weiteren Auftrieb erhielt Compliance in Folge der grossen Firmenzusammenbrüche in den USA zu Beginn dieses Jahrhunderts. Als Beispiel kann etwa der Fall des Energiekonzerns Enron aufgeführt werden, wo mit illegalen Geschäftspraktiken Riesenumsätze suggeriert und Verluste vertuscht wurden, um den Aktienkurs aufzublähen<sup>21</sup>. Man stellte sich die Frage, wie so etwas passieren konnte, und was falsch gelaufen war. Als politische Reaktion auf diese Exzesse und die offensichtlichen Missbräuche wurde in den USA im Jahr 2002 der sog. Sarbanes-Oxley Act (SOX) erlassen, der ausdrücklich vorschreibt, dass im Unternehmen

---

<sup>18</sup> Vgl. BACHMANN, S. 93.

<sup>19</sup> Vgl. ROTH, *Compliance*, S. 10 f.

<sup>20</sup> BÜFF, S. 24 f.

<sup>21</sup> Vgl. THIELEMANN, *Der Fall Enron*, S. 37.



geeignete Massnahmen zur Verhinderung und Aufdeckung von kriminellen Handlungen ergriffen werden müssen<sup>22</sup>. Ein weiterer Passus verpflichtet Unternehmen, genaue interne Kontrollen durchzuführen, und dass sie sich in der Gestaltung von internen Kontrollsystemen an einem internationalen Framework (z.B. COSO) orientieren müssen<sup>23</sup>. Diesem Act mussten sich auch ausländische Firmen unterwerfen, die in den USA börsenkotiert waren, weshalb die Schweizer Wirtschaftsverbände Druck machten, ähnliche Vorschriften in der Schweiz einzuführen. Dies hing damit zusammen, dass die amerikanischen Aufsichtsbehörden mit SOX mehr Kontrollmacht erhielten, und man diesen Kontrollen mit dem Hinweis auf ähnliche Regelungen im Heimatland vorbeugen wollte<sup>24</sup>. Mit dem Swiss Code of Best Practice for Corporate Governance stellte der Verband Enonomiesuisse 2002 erstmals Grundsätze für Corporate Governance für Schweizer Unternehmen aus allen Branchen auf, womit Riskmanagement und IKS auch hierzulande breit diskutiert wurden. Mit dem 2007 in Kraft getretenen revidierten Aktienrecht werden diese beiden Funktionen nun auch im OR ausdrücklich benannt. Gemäss Art. 663b Ziff. 12 OR muss der Anhang zur Jahresrechnung Angaben über die Durchführung einer Risikobeurteilung enthalten und nach Art. 728a Abs. 1 Ziff. 3 OR ist das Vorhandensein eines IKS Gegenstand der Prüfung durch die Revisionsstelle.

### 3.2.2 IM BUND

Soweit ersichtlich erscheint der Begriff Compliance auf Bundesebene erstmals in der vom Eidgenössischen Finanzdepartement (EFD) im Dezember 2004 erlassenen Risikopolitik. Dort werden "Rechtliche Risiken, Compliance" als eigenständige Risikokategorie aufgeführt<sup>25</sup>. Auch der Leitfaden der Eidgenössischen Finanzkontrolle (EFK) zum Aufbau eines Internen Kontrollsystems vom Oktober 2007 nimmt die Compliance-Thematik auf, wenn auch nur implizit<sup>26</sup>. Dies verdeutlicht, dass die Diskussion um Compliance in der Bundesverwaltung relativ neu ist und

---

<sup>22</sup> PANT, S. 292.

<sup>23</sup> ROTH, *Good Corporate Governance*, S. 34.

<sup>24</sup> Interview vom 10. November 2009.

<sup>25</sup> EFD RISIKOPOLITIK, S. 5.

<sup>26</sup> EFK-LEITFADEN, S. 5.

entsprechende Systeme bisher kaum vorhanden oder nur fragmentarisch entwickelt sind. Die Bestimmungen zum Riskmanagement und zum IKS wurden im Rahmen der Totalrevision des Finanzhaushaltsgesetzes im Jahre 2004 in Art. 39 Finanzhaushaltsgesetz (FHG; SR 611.0) aufgenommen<sup>27</sup>. Dies war einerseits sicherlich Folge der entsprechenden Entwicklungen in der Privatwirtschaft im Zusammenhang mit SOX, andererseits dürfte wohl auch der in Kapitel 1 erwähnte Fall Belasi Anlass zum Überdenken des bestehenden Kontrollsystems gegeben haben.

### 3.2.3 IM BAG

Innerhalb des BAG kam die Compliance-Thematik im Zusammenhang mit Nebenbeschäftigungen und der Geschenkkannahme auf. In der Geschäftsleitung, bei der Sektion Personal und Organisation (P+O) sowie bei den Führungskräften gab es diesbezüglich immer wieder Fragen, und es kam verschiedentlich zu Situationen, wo Unklarheit über die Anwendung der massgeblichen Vorschriften bestand. Zudem fehlte es an entsprechenden Richtlinien oder Weisungen im EDI oder im BAG. Vor etwa zwei Jahren kam in der Geschäftsleitung der Wunsch auf, diese Thematik genauer auszuleuchten, und in der Folge erging ein Auftrag an die Abteilung Recht zur Erarbeitung von Compliance-Leitlinien betreffend den Umgang mit Interessenkonflikten, die Annahme von Geschenken und anderen Vorteilen, die Ausübung von Nebenbeschäftigungen, die Annahme von Honorar und anderen Entschädigungen sowie die Korruptionsprävention<sup>28</sup>. Im Unterschied zu der Entwicklung auf Stufe Gesamtbund standen innerhalb des BAG gerade nicht die wirtschaftlichen und finanziellen Aspekte im Vordergrund, sondern vielmehr solche personalrechtlicher Natur im Zusammenhang mit Interessenkonflikten.

---

<sup>27</sup> Zu IKS, Riskmanagement und Compliance in der Bundesverwaltung vgl. Kapitel 3.5.

<sup>28</sup> Vgl. Interview vom 24. September 2009.

### 3.3 SINN UND ZWECK VON COMPLIANCE

#### 3.3.1 COMPLIANCE-RISIKEN

Compliance befasst sich mit der Verhinderung von sogenannten Compliance-Risiken. Darunter versteht man Verstösse gegen Gesetze, Vorschriften, Standards und Standesregeln, die rechtliche und regulatorische Sanktionen, finanzielle Verluste oder Reputationsschäden zur Folge haben können<sup>29</sup>. Diese Compliance-Risiken lassen sich in zwei Kategorien einteilen: Rechtsrisiken und Reputationsrisiken. Zu den Rechtsrisiken zählen solche, die eine Haftung des Unternehmens begründen können, z.B. durch zivilrechtliche Grundlagen, Strafrecht, Aufsichtsrecht oder haftungs- und sanktionsbegründende Bestimmungen im Rahmen der Selbstregulierung<sup>30</sup>. Ein Reputationsrisiko liegt dann vor, wenn die Kundschaft aufgrund von bestimmten Vorkommnissen das Vertrauen in die Unternehmung verliert. Dies kann dazu führen, dass bestehende Verträge vorzeitig aufgelöst werden, oder potentielle Kunden einen anderen Anbieter berücksichtigen<sup>31</sup>. Beim Reputationsrisiko handelt es sich um ein Derivatsrisiko<sup>32</sup>, das entsteht, wenn andere Risiken verwirklicht werden<sup>33</sup>. So kann bereits die Einleitung einer Strafuntersuchung gegen eine Privatperson oder ein Unternehmen dessen Ruf nachhaltig schädigen, selbst wenn es anschliessend zu keiner Verurteilung kommt<sup>34</sup>. Compliance will den Eintritt dieser Risiken verhindern, hat also primär eine präventive Funktion und gelangt proaktiv zur Anwendung (dies im Gegensatz zu *Liability*, wo primär die Abwendung von bereits eingetretenen Risiken auf dem Prozessweg im Vordergrund steht<sup>35</sup>).

---

<sup>29</sup> BASEL COMMITTEE ON BANKING SUPERVISION, S. 7; FINMARUNDSCHREIBEN 08/24, Rz. 98.

<sup>30</sup> ROTH, *Good Corporate Governance*, S. 122 f.

<sup>31</sup> MÜLLER, S. 43.

<sup>32</sup> Das ist ein abgeleitetes Risiko.

<sup>33</sup> ROTH, *Good Corporate Governance*, S. 124.

<sup>34</sup> Vgl. etwa den Swissair-Prozess gegen Eric Honegger: *Tages-Anzeiger Online* vom 8. Juni 2007, *Der Prozess war die Strafe*, <http://www.tagesanzeiger.ch/service/archiv/> (zuletzt eingesehen am 20. September 2010).

<sup>35</sup> ROTH, *Good Corporate Governance*, S. 128.

Gemäss ROTH gelten Compliance-Risiken als sogenannte "soft risks", da sie nicht mit mathematischen Modellen und szenarienbezogen durchgerechnet werden können und in diesem Sinne nicht messbar sind<sup>36</sup>. Jede Unternehmung muss deshalb die für sie relevanten Rechts- und Reputationsrisiken vor dem Hintergrund ihrer konkreten Aktivitäten bestimmen. Eine Bank ist mit anderen Risiken konfrontiert als eine Pharmakonzern, und dieser wiederum mit anderen Risiken als die öffentliche Verwaltung. Dementsprechend gibt es auch nicht *eine* allgemeingültige Compliance-Lösung, welche gleichermassen für alle privaten Unternehmen und öffentlichen Verwaltungseinheiten anwendbar ist. Vielmehr müssen die notwendigen Compliance-Massnahmen für jedes Unternehmen individuell festgelegt werden (tailored to the particular firm), entsprechend seinen spezifischen Aktivitäten und Bedürfnissen<sup>37</sup>.

Compliance will also die finanziellen und rechtlichen Konsequenzen von Regelverletzungen sowie Imageschäden verhindern. Damit ist auch gesagt, dass Verstösse gegen gesetzliche oder unternehmensinterne Vorschriften, die keine finanziellen oder sonstigen negative Folgen haben, nicht Thema von Compliance sind. Wenn ein Regelverstoss keine Konsequenzen hat, besteht nämlich gar kein Risiko für das Unternehmen.

### 3.3.2 RECHTLICHE UND ÖKONOMISCHE BETRACHTUNGSWEISE

Es ist in mehr oder weniger sämtlichen Rechtsstaaten ein selbstverständliches Prinzip, dass sich Unternehmen an das geltende Recht halten müssen<sup>38</sup>. Aus ökonomischer Sichtweise kann man aber gleichsam wie der REMM (Resourceful, Evaluating, Maximizing Man) schlicht die anfallenden Kosten dem möglichen Nutzen gegenüberstellen, und sich für die Inkaufnahme des Risikos entscheiden. Auf der einen Seite steht der Aufwand für die Compliance-Beratung, demgegenüber Bussgelder (z.B. Kartellstrafen), Schadenersatzforderungen, Anwaltskosten, Strafverfahren, Beschlagnahme von Vermögenswerten, Gefängnisstrafen

---

<sup>36</sup> ROTH, *Good Corporate Governance*, S. 88.

<sup>37</sup> BUFF, S. 20.

<sup>38</sup> HAUSCHKA, S. 2.

etc.<sup>39</sup>. Die Kosten für Non-Compliance können exorbitante Beträge erreichen. So musste etwa der Pharmakonzern Pfizer Inc. wegen illegaler und unethischer Vermarktung von Medikamenten eine Rekordbusse von 2,3 Mrd. \$ bezahlen<sup>40</sup>. Bei diesen Dimensionen von Strafzahlungen scheint sich die Redensart "if you think Compliance is expensive, try Non-Compliance" zu bewahrheiten. Vor diesem Hintergrund dürfte ein Unternehmen rasch zur Einsicht gelangen, dass es sich auch aus ökonomischer Sicht lohnt, in Compliance zu investieren.

### 3.3.3 DIE ROLLE DES STAATES

Während sich ein privates Unternehmen unter Inkaufnahme der rechtlichen (und finanziellen) Konsequenzen bewusst für die Nichteinhaltung von gesetzlichen Vorschriften entscheiden kann, ist ein analoges Verhalten für den Staat keine Option. Grundlage und Schranke des staatlichen Handelns ist das Recht (Art. 5 Abs. 1 BV). In dem Sinne muss der Staat und seine Verwaltung immer "compliant" sein. Sämtliche gesetzlichen Vorschriften sind einzuhalten, auch diejenigen, deren Verletzung keine unmittelbaren rechtlichen, finanziellen oder Image-Konsequenzen für die Verwaltungseinheit haben. Muss sich Compliance in der Bundesverwaltung demnach ausnahmslos auf alle Verwaltungsaktivitäten erstrecken? Dies wäre kaum realisierbar und würde auch wenig Sinn machen. Da Compliance als Teil des Riskmanagements verstanden wird<sup>41</sup>, fokussieren dessen Aktivitäten nur auf diejenigen Verwaltungstätigkeiten, wo Handlungsbedarf zur Risikoeindämmung identifiziert wurde. Über den Umfang von Compliance-Massnahmen wird somit

---

<sup>39</sup>Vgl. zum Ganzen: HAUSCHKA, *Kosten der Non-Compliance*, <http://www.compliancemagazin.de/printable/compliancefachbeitraege/kosten/luther060807.html> (zuletzt eingesehen am 20. September 2010).

<sup>40</sup>Vgl. NZZ Online vom 3. September 2009, *Rekordbusse für den Pharmakonzern Pfizer*, [http://www.nzz.ch/nachrichten/wirtschaft/aktuell/rekordbusse\\_fuer\\_de\\_n\\_pharmakonzern\\_pfizer\\_1.3477907.html](http://www.nzz.ch/nachrichten/wirtschaft/aktuell/rekordbusse_fuer_de_n_pharmakonzern_pfizer_1.3477907.html) (zuletzt eingesehen am 20. September 2010).

<sup>41</sup>Zur Abgrenzung Compliance-Riskmanagement vgl. unten, Kapitel 3.4.2.

abgestuft nach der Risikoexposition eines Unternehmens entschieden, nicht zuletzt um einer unnötigen Überregulierung vorzubeugen<sup>42</sup>.

Compliance beinhaltet also einen Riskmanagement-Aspekt und setzt erst dort ein, wo durch Regelverletzungen hoher Schaden entstehen kann und/oder eine hohe Eintretenswahrscheinlichkeit des Risikos besteht. In dem Sinne ist Compliance nicht (nur) ein Prinzip, das die Einhaltung von rechtlichen Vorgaben fordert, sondern befasst sich vielmehr mit dem Management von Rechts- und Reputationsrisiken, d.h. mit der Frage wie mit Rechts- und Reputationsrisiken umzugehen ist und wie diese eliminiert werden können<sup>43</sup>.

### 3.3.4 RISIKEN, DIE DURCH COMPLIANCE ENTSTEHEN

Schäden können auch dann entstehen, wenn eine Vorschrift zwar korrekt befolgt wird, aber inhaltlich falsch ist. Es geht also um die Frage, ob Compliance auch Risiken verhindern kann, die durch Compliance erst hervorgerufen werden. Wenn man sich in Erinnerung ruft, dass Compliance Rechts- und Reputationsrisiken verhindern will, und nicht primär die Befolgung von Regeln im Kadavergehorsam bezweckt, beinhaltet diese Zielsetzung auch eine kritische Reflexion der anzuwendenden Vorschriften. Der Basler Ausschuss für Bankenaufsicht hält entsprechend fest, dass "*standards of honesty and integrity*" für eine effektive Compliance notwendig sind<sup>44</sup>. Integrität verlangt aber nicht, dass Regeln in jedem Fall befolgt werden müssen, sondern fordert manchmal auch einen Bruch derselben in einem Akt zivilen Ungehorsams<sup>45</sup> (z.B. das Publikmachen ungebührlicher Unternehmenspraktiken, wenn interne Beschwerdewege nicht die erhoffte Besserung bringen). So beschränkt sich denn das Pflichtenheft eines Compliance-Officers nicht auf den Erlass von Richtlinien und Weisungen sowie die Kontrolle deren korrekten Umsetzung, sondern beinhaltet auch die Anpassung bestehender Regeln, sollten sich diese als falsch oder nicht mehr zeitgemäss erwei-

---

<sup>42</sup> LAMPERT, S. 145.

<sup>43</sup> Vgl. *Begriffsdefinition, Kapitel 3.1.*

<sup>44</sup> BASEL COMMITTEE ON BANKING SUPERVISION, S. 7.

<sup>45</sup> ROTH, *Compliance, Integrität und Regulierung*, S. 51.

sen<sup>46</sup>. In diesem Sinne sollte man Compliance nicht einseitig als eine Art "Unternehmenspolizei" verstehen, welche lediglich die Einhaltung von Regeln kontrollieren und allenfalls Mitarbeiter bestrafen will, sondern es geht auch um das Erkennen von Chancen und ein proaktives "Fitmachen" der Unternehmung für künftige regulatorische und gesellschaftliche Entwicklungen. Dies ist jedoch nur zu realisieren, wenn auch bestehende Weisungen, Richtlinien und Empfehlungen regelmässig auf ihre Praxistauglichkeit und ihre Wirkung hin überprüft und allenfalls angepasst werden.

### 3.3.5 EMPIRISCHER NACHWEIS ÜBER DIE WIRKUNG VON COMPLIANCE

Über die Wirkung von Compliance findet man zur Zeit nur spärliche empirische Daten. Gemäss KIMMICH sind bis ins Jahr 2006 gerade mal drei Studien der Frage nachgegangen, wie sich die Implementierung von Compliance-Konzepten auf das (illegale) Verhalten von Mitarbeitern auswirkt<sup>47</sup>. MATHEWS sowie MC KENDALL/WAGNER konnten beide keinen signifikanten Effekt von Codes of Conduct oder anderen Compliance-Programmen auf das widerrechtliche Verhalten eines Unternehmens feststellen<sup>48</sup>. Dagegen gelangen MC KENDALL/DE MARR/JONES-RIKKERS in einer späteren Studie zu der Ansicht, dass das ethische Klima einer Organisation durchaus einen Einfluss auf das Verhalten ihrer Mitarbeiter hat<sup>49</sup>. Somit verbleibt lediglich eine Studie, die Compliance eine risikoreduzierende Wirkung bezüglich Regelverletzungen attestiert. Dies ist gewiss zu wenig, um eine abschliessende Aussage über die Effekte von Compliance zu machen. Insofern muss die Frage vorerst offen gelassen werden, bis weitere wissenschaftliche Ergebnisse vorliegen.

### 3.3.6 ZUSAMMENFASSUNG

In Anlehnung an KLOTZ/DORN lassen sich Sinn und Zweck von Compliance etwa wie folgt zusammenfassen: *Compliance allgemein adressiert*

---

<sup>46</sup> BUFF, S. 60 f.

<sup>47</sup> KIMMICH, S. 63.

<sup>48</sup> MATHEWS, S. 107 ff.; MC KENDALL/WAGNER, S. 624 ff.

<sup>49</sup> MC KENDALL/DE MARR/JONES-RIKKERS., S. 373.

*also nicht die an sich triviale Selbstverständlichkeit, dass geltendes Recht zu befolgen ist. Vielmehr steht Compliance für die Forderung, potentielle Regelverstösse als Risiken zu betrachten, die im Rahmen des Risikomanagements eines Unternehmens mittels geeigneter organisatorischer, technischer und personeller Massnahmen zu behandeln sind. Die Höhe der Risiken bemisst sich nach den potenziellen Schäden als negative Folge fehlender oder mangelhafter (IT-)Compliance<sup>50</sup>:*

- *Freiheitsstrafen*
- *Bussgelder*
- *Zwangsgelder*
- *Schadenersatz*
- *Vertragsstrafen*
- *Umsatzausfälle*
- *Imageschäden*
- *Wettbewerbsnachteile*

Compliance fokussiert also auf diejenigen Tätigkeiten eines Unternehmens, wo gemäss Risikoanalyse ein erhöhtes Risiko für Rechtsverletzungen und dadurch für Rechts- oder Reputationsschäden besteht.

### 3.4 ABGRENZUNG ZU ANDEREN BEGRIFFEN

#### 3.4.1 COMPLIANCE UND CORPORATE GOVERNANCE

Gemeinhin wird Compliance als Element der Corporate Governance betrachtet<sup>51</sup>. So wird die Einhaltung der anwendbaren Normen etwa im Swiss Code of Best Practice for Corporate Governance (SCBP) als Aufgabe des Verwaltungsrates aufgeführt<sup>52</sup>. Ebendort wird Corporate Governance als "die Gesamtheit der auf das Aktionärsinteresse ausgerichteten Grundsätze, die unter Wahrung von Entscheidungsfähigkeit und Effizienz auf der obersten Unternehmensebene Transparenz und ein ausgewogenes Verhältnis von Führung und Kontrolle anstreben" bezeichnet<sup>53</sup>. Etwas allgemeiner umschrieben wird unter diesem Begriff ein System

<sup>50</sup> KLOTZ/DORN, S. 7.

<sup>51</sup> Z.B. BUFF, S. 66.

<sup>52</sup> SWISS CODE OF BEST PRACTICE FOR CORPORATE GOVERNANCE, S. 15.

<sup>53</sup> SWISS CODE OF BEST PRACTICE FOR CORPORATE GOVERNANCE, S. 8.



zur verantwortungsbewussten und effizienten Unternehmungsführung verstanden.<sup>54</sup>

### 3.4.2 COMPLIANCE, IKS UND RISKMANAGEMENT

Risikomanagementsysteme dienen zur effektiven und effizienten Identifikation, Bewertung und Steuerung von Risiken in einem Unternehmen<sup>55</sup>. Mit dem Riskmanagement wird die gesamte Palette an strategischen und operationellen Risiken abgedeckt, denen ein Unternehmen ausgesetzt ist. Es handelt sich also um eine Art Makroansicht sämtlicher Unternehmensrisiken. Unter operationellen Risiken versteht man die Gefahr von unmittelbaren oder mittelbaren Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder von externen Ereignissen eintreten<sup>56</sup>. Diese kann man entweder vermeiden, versichern oder minimieren und kontrollieren.

Das Interne Kontrollsystem umfasst gemäss der Richtlinie 15/2006 des Bundesamtes für Privatversicherungen (BPV) vom 1. Januar 2007 zur Corporate Governance, zum Risikomanagement und zum Internen Kontrollsystem "die unternehmensintern angeordneten Vorgänge, Methoden und Massnahmen, die dazu dienen, eine angemessene Sicherheit bezüglich der Risiken der Geschäftsführung zu gewährleisten, insbesondere in Bezug auf die Wirksamkeit von Geschäftsprozessen, die Zuverlässigkeit der finanziellen Berichterstattung und die Befolgung von Gesetzen und Vorschriften"<sup>57</sup>. Das IKS fokussiert demnach auf die operationellen Risiken, mit der Zielsetzung, diese zu minimieren und zu kontrollieren. In der praktischen Umsetzung werden dabei Prozesse definiert und anschliessend deren Einhaltung kontrolliert.

---

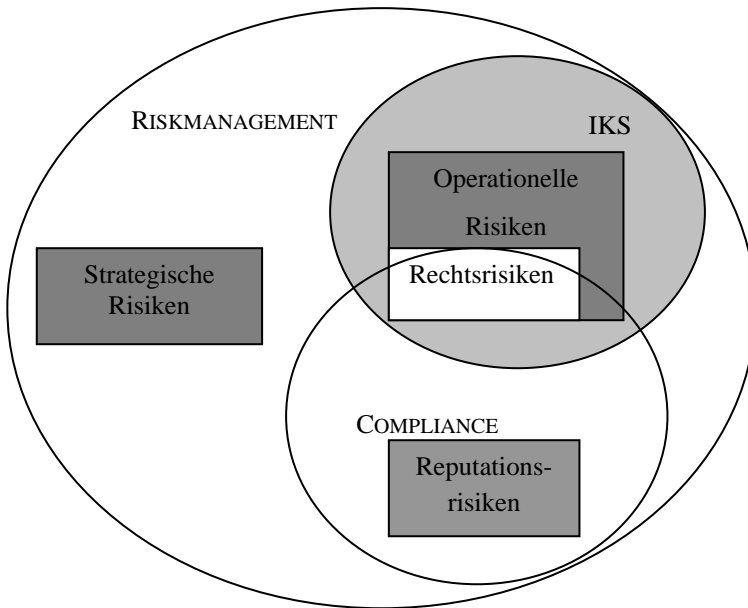
<sup>54</sup> Vgl. BUFF, S. 66; KLOTZ/DORN, S. 6; HAUSCHKA, S. 2; BPV-RICHTLINIE, S. 2.

<sup>55</sup> KLOTZ/DORN, S. 6.

<sup>56</sup> Basler Ausschuss für Bankenaufsicht, *Management operationeller Risiken - Praxisempfehlungen für Banken und Bankenaufsicht*, Februar 2003, S. 2, <http://www.bis.org/publ/bcbs96de.pdf> (zuletzt eingesehen am 20. September 2010).

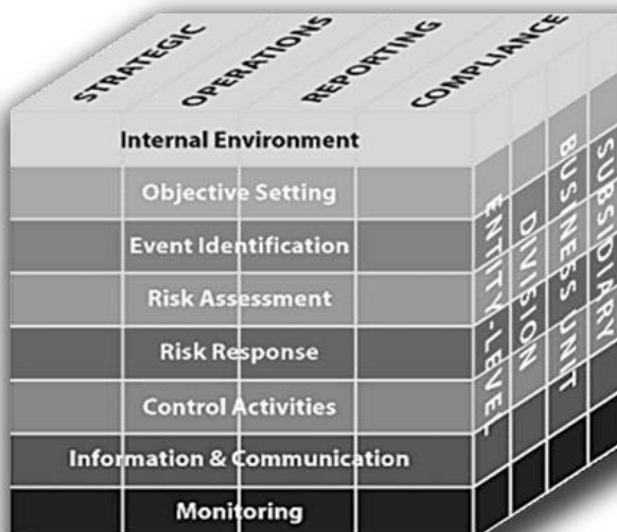
<sup>57</sup> BPV-RICHTLINIE, S. 3.

Compliance setzt sich die Vermeidung von Rechts- und Reputationsrisiken zum Ziel. Was die rechtlichen Risiken anbelangt, bilden diesen einen Teil der operationellen Risiken, wohingegen Reputationsrisiken davon nicht erfasst werden<sup>58</sup>. Daraus wird ersichtlich, dass eine enge Verknüpfung zwischen Compliance, Riskmanagement und IKS besteht. Zum einen ist Compliance in das Riskmanagement eingebunden, nämlich soweit sie sich mit der Vermeidung von Rechts- und Reputationsrisiken befasst. Ebenso besteht eine Schnittstelle zum IKS, und zwar was die Kontrolle der rechtlichen Risiken anbelangt. Allerdings geht Compliance viel weiter als das IKS, indem sie auch die Ausbildung der Mitarbeiter, die Beratung, das Reporting, das Sanktionieren von Regelverstößen sowie die Implementierung von Codes of Conduct umfasst. Zusätzlich zum IKS will Compliance auch den Eintritt von Reputationsrisiken vermeiden. In nachfolgender Grafik wird versucht, die Schnittstellen von IKS, Riskmanagement und Compliance zu visualisieren:



<sup>58</sup> Zur Abgrenzung von Compliance-Risiken und operationellen Risiken vgl. ROTH, *Good Corporate Governance*, S. 88 f.

So verstanden ist Compliance also auch Bestandteil des IKS, und das IKS bildet wiederum einen integralen Bestandteil des Risikomanagements<sup>59</sup>. Entsprechend hält der SCBP fest, die Compliance könne dem Internen Kontrollsystem zugewiesen werden, und das Interne Kontrollsystem decke, je nach den Besonderheiten der Gesellschaft, auch das Risikomanagement ab<sup>60</sup>. In der Literatur wird in diesem Zusammenhang häufig der sogenannte "COSO<sup>61</sup>-Würfel" referenziert:



Quelle: COSO

Das COSO Enterprise Risk Management (ERM) Modell ist ein umfassendes und allgemein anerkanntes Konzept zur Kontrolle und Steuerung in Wirtschafts- und Verwaltungsunternehmen<sup>62</sup>. Gemäss COSO umfasst

<sup>59</sup> ROTH, *Good Corporate Governance*, S. 84, 119.

<sup>60</sup> SWISS CODE OF BEST PRACTICE FOR CORPORATE GOVERNANCE, S. 15.

<sup>61</sup> The Committee of Sponsoring Organizations of the Treadway Commission ([www.coso.org](http://www.coso.org)).

<sup>62</sup> Vgl. TARANTINO, S. 178 ff.; BACHMANN, S. 94 f.

die interne Kontrolle vier Hauptkategorien bzw. Ziele (vertikale Kolonnen):

- Sicherstellung der strategischen Entscheidprozesse (strategic)
- Effektivität und Effizienz von Geschäftsprozessen (operations)
- Zuverlässigkeit der Informationen (reporting)
- Einhaltung der anwendbaren Gesetze und Vorschriften (compliance)

Die Erreichung dieser Ziele ist abhängig und beeinflusst von folgenden acht, in Wechselbeziehung stehenden Komponenten (horizontale Kolonnen):

- Internes Kontrollumfeld (internal environment)
- Zielsetzung (objective setting)
- Ereignisidentifikation (event identification)
- Risikobeurteilung (risk assessment)
- Risikoreaktion (risk response)
- Kontrollaktivitäten (control activities)
- Information und Kommunikation (information & communication)
- Überwachung (monitoring)

Auf der dritten Dimension wird schliesslich die organisatorische Einbindung anhand der verschiedenen Unternehmenseinheiten dargestellt. Sehr treffend bezeichnet TARANTINO das ERM-Modell als "Rubik's Cube" und erläutert, "*enterprise risk management is not strictly a serial process, where one component affects only the next. It is a multidirectional, iterative process in which almost any component can and does influence another*"<sup>63</sup>. Demnach sind IKS, Compliance und Riskmanagement also einzelne Elemente eines integralen Riskmanagement Systems, die ineinander übergehen und einander gegenseitig beeinflussen.

---

<sup>63</sup> TARANTINO, S. 178.

### 3.5 IKS, RISKMANAGEMENT UND COMPLIANCE IN DER BUNDES- VERWALTUNG

#### 3.5.1 GESETZLICHE ANFORDERUNGEN

Ausdrückliche gesetzliche Vorschriften zur Compliance sind im öffentlichen Recht nicht vorhanden. Dagegen finden sich im Finanzhaushaltsgesetz (FHG; SR 611.0), der Finanzhaushaltsverordnung (FHV; SR 611.01) sowie dem Finanzkontrollgesetz (FKG; SR 614.0) Bestimmungen zum Riskmanagement und zum Internen Kontrollsystem:

#### **Art. 39 FHG** Interne Kontrolle

<sup>1</sup> Der Bundesrat trifft die notwendigen Massnahmen, um:

- a. das Vermögen des Bundes zu schützen;
- b. die zweckmässige Verwendung der Mittel nach den Grundsätzen von Artikel 12 Absatz 4 sicherzustellen;
- c. Fehler und Unregelmässigkeiten bei der Rechnungsführung zu verhindern oder aufzudecken;
- d. die Ordnungsmässigkeit der Rechnungslegung und die verlässliche Berichterstattung zu gewährleisten.

<sup>2</sup> Er berücksichtigt dabei die Risikolage und das Kosten-Nutzen-Verhältnis.

#### **Art. 36 FHV** Internes Kontrollsystem

(Art. 39 FHG)

<sup>1</sup> Das interne Kontrollsystem umfasst regulatorische, organisatorische und technische Massnahmen.

<sup>2</sup> Die Finanzverwaltung erlässt im Einvernehmen mit der Finanzkontrolle und nach Rücksprache mit den Departementen die erforderlichen Weisungen.

<sup>3</sup> Die Direktoren und Direktorinnen der Verwaltungseinheiten sind verantwortlich für die Einführung, den Einsatz und die Überwachung des Kontrollsystems in ihrem Zuständigkeitsbereich.

**Art. 50 FHV Risikomanagement**

(Art. 39 FHG)

<sup>1</sup> Die Departemente und die Bundeskanzlei bewirtschaften die Risiken in ihrem Zuständigkeitsbereich nach den Weisungen des Bundesrates.

<sup>2</sup> Der Bund trägt das Risiko für Schäden an seinen Vermögenswerten und für die haftpflichtrechtlichen Folgen seiner Tätigkeit grundsätzlich selbst.

<sup>3</sup> Die Finanzverwaltung erlässt Weisungen über:

- a. den Abschluss von Versicherungsverträgen in besonderen Fällen;
- b. die vertragliche Übernahme der Haftung für Schäden Dritter;
- c. die freiwillige Ersatzleistung für Sachschäden, die Bundesbedienstete im Zusammenhang mit ihrer dienstlichen Tätigkeit erleiden;
- d. die finanzielle Erledigung von Sach- und Vermögensschäden.

<sup>4</sup> Sie koordiniert die Berichterstattung gegenüber dem Bundesrat.

Zudem bestimmt Art. 3 lit. b FHV, dass der Anhang der Jahresrechnung zusätzliche Angaben über Risikosituation und Risikomanagement enthalten muss. Die Überprüfung der internen Kontrollsysteme wird der EFK zugewiesen (Art. 6 lit. d FKG).

Bisher hat der Bundesrat noch keinen Gebrauch von seiner Kompetenz nach Art. 50 Abs. 1 FHV gemacht und Weisungen zum Riskmanagement erlassen. Grundlage für das Risikomanagement beim Bund bildet das vom Bundesrat am 3. Dezember 2004 verabschiedete Dokument "Risikopolitik" des EFD, wobei hier vor allem finanzielle Auswirkungen im Vordergrund stehen. Zielsetzung der Risikopolitik ist es, den homogenen, systematischen und konsequenten Umgang mit den vielfältigen Risiken in der Bundesverwaltung *verbindlich* festzulegen<sup>64</sup>. Trotz dieser Verbindlicherklärung hat das Dokument - auch nach Auffassung der EFK - keinen Weisungscharakter, und wird von den Verwaltungseinheiten gesamthaft betrachtet im Sinne von "best practice" angesehen<sup>65</sup>. Im

---

<sup>64</sup> EFD RISIKOPOLITIK, S. 2.

<sup>65</sup> EFK-QUERSCHNITTSPRÜFUNG, S. 13.

Kapitel "3.2 Die Risikoerfassung" wird "Rechtliche Risiken, Compliance" als ein Kriterium für die Gliederung von Risiken nach ihren Ursachen aufgeführt<sup>66</sup>. Die Verwaltungseinheiten haben die Resultate ihrer Risikoerfassung anschliessend in einem Risikokatalog in Tabellenform darzustellen<sup>67</sup>.

Bezüglich IKS ist auf den Leitfaden der EFK zum Aufbau eines Internen Kontrollsystems (IKS) vom Oktober 2007 zu verweisen. Dort wird unter Ziff. 1.1 ausgeführt, das IKS soll unter anderem für die Erreichung des Ziels "Einhaltung von Gesetzen, Verordnungen und Reglementen" eine angemessene Sicherheit bieten<sup>68</sup>. Damit ist eindeutig Compliance gemeint, auch wenn dieser Begriff im Leitfaden nicht benutzt wird. Deutlich kommt dies bei der exemplarischen Aufzählung der Risiken Aufsichtspflichtverletzung, Verbreitung sensibler Personeninformationen und Korruption unter Ziff. 1.2.3 zum Ausdruck. Diese Risiken könnten, so der Leitfaden, "*grossen Schaden anrichten, sowohl in Bezug auf den Ruf des Bundes als auch was Haftpflichtforderungen anbelangt*"<sup>69</sup>.

Zusammenfassend ist festzuhalten, dass für die Bundesverwaltung (und somit für die einzelnen Verwaltungseinheiten) eine rechtliche Pflicht zur Einführung von Riskmanagement und IKS besteht. Wenn man Compliance nun als Bestandteil dieser beiden Systeme betrachtet, wäre sie von der Umsetzungspflicht miterfasst. Nur, auf Gesetzes- und Verordnungsebene bestehen eben gerade keine Bestimmungen, welche ausdrücklich den Miteinbezug von Compliance bzw. die Einführung eines solchen Systems verlangen. Erst auf untergeordneter Ebene (Risikopolitik des Bundes, EFK-Leitfaden zum IKS) finden sich entsprechende Hinweise. Diese haben jedoch - wie oben ausgeführt - keinen verbindlichen Charakter, sondern sind eher als "best practice"-Ansätze zu verstehen. Folglich besteht keine ausdrückliche rechtliche Pflicht zur Umsetzung von Compliance, sondern nur die allgemeine Rechtspflicht, dass Gesetze und Verordnungen einzuhalten sind (was sich bereits aus dem Legalitätsprinzip ergibt). Die konkrete Ausgestaltung, das "wie wird die Einhal-

---

<sup>66</sup> EFD RISIKOPOLITIK, S. 5.

<sup>67</sup> EFD RISIKOPOLITIK, S. 6.

<sup>68</sup> EFK-LEITFADEN, S. 4.

<sup>69</sup> EFK-LEITFADEN, S. 6.

„von Regeln sichergestellt“, bleibt jedoch weitgehend den einzelnen Verwaltungseinheiten überlassen.

### 3.5.2 ZUSTÄNDIGKEITEN

Die unmittelbare Zuständigkeit sowohl für die Durchführung des Riskmanagement als auch für die Einführung eines IKS liegt bei den Verwaltungseinheiten<sup>70</sup>. Verantwortlich für den Aufbau und den Einsatz eines IKS in einem Amt ist die Direktion (Art. 36 Abs. 3 FHV). Für die Risikopolitik übernehmen sowohl die Verwaltungseinheiten als auch die sogenannten Risikoeigner jeder Verwaltungseinheit die Verantwortung, wobei die Oberverantwortung für das Risikomanagement beim Bundesrat verbleibt<sup>71</sup>. Zuständigkeit und Verantwortung der Amtsdirektorinnen und Amtsdirektoren für die Erfüllung der ihnen übertragenen Aufgaben ergeben sich bereits aus Art. 45 des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG; SR 172.010). Demnach fällt auch die Umsetzung von Compliance als Bestandteil von IKS und Riskmanagement in die Zuständigkeit der einzelnen Bundesämter.

## 3.6 ELEMENTE EINES COMPLIANCE-MANAGEMENT-SYSTEMS

### 3.6.1 ÜBERSICHT

Ein Compliance-Konzept umfasst gemeinhin folgende Elemente<sup>72</sup>:

- Regeln und Richtlinien (Codes of Conduct)
- Information, Aufklärung und Ausbildung von Mitarbeitenden
- Organisatorische Massnahmen (Compliance Officer)
- Beratung
- Überwachung der Einhaltung der unternehmensinternen Vorgaben
- Sanktionieren von Regelverstössen

<sup>70</sup> EFD RISIKOPOLITIK, S. 11.

<sup>71</sup> EFD RISIKOPOLITIK, S. 10.

<sup>72</sup> BUFF, S. 9 f., 20, 290 f.; LAMPERT, S. 147 ff.



Ausgangspunkt für den Aufbau eines Compliance-Management-Systems ist aber in jedem Fall eine Bestandesaufnahme durch Identifikation der im Unternehmen vorhandenen Rechtsrisiken, sowie daraus abgeleitete Compliance-Massnahmen zur Risikovorbeugung<sup>73</sup>. Diese Risikoanalyse wird von verschiedenen Faktoren beeinflusst, wie etwa der Grösse und Struktur eines Unternehmens, den Geschäftstätigkeiten, möglicherweise bereits erfolgten Regelverstössen und der Eintretenswahrscheinlichkeit von Risiken.

### 3.6.2 RISIKOANALYSE

Wie zuvor erwähnt, fallen Rechtsrisiken und Reputationsrisiken in die Kategorie der Compliance-Risiken. Rechtliche Risiken resultieren aus Verstössen gegen Rechtsnormen, wobei vorab an öffentlich-rechtliche Grundlagen, das Strafrecht und zivilrechtliche Bestimmungen zu denken ist. Des weiteren fallen auch unternehmensinterne Regeln, Anordnungen und Weisungen darunter. Eine m.E. sinnvolle Strukturierung schlägt BUFF vor, indem er die relevanten (Risiko-)Bereiche nach betroffenen Rechtsgebieten einteilt<sup>74</sup>:

- Aufsichtsrechte (z.B. Börsenaufsicht)
- Strafrecht (z.B. Insiderstrafrecht, Korruption, Umweltrecht, sexuelle Belästigung am Arbeitsplatz, Steuerrecht)
- Vertraulichkeit und Interessenkonflikte (z.B. Datenschutz, Nebenbeschäftigungen)
- Kommunikation des Unternehmens (z.B. Internetproblematik)

Für die Einheiten der Zentralverwaltung dürften die Aufsichtsrechte wohl eine untergeordnete Rolle spielen, da sie selber nicht als Marktteilnehmer auftreten (anders dagegen die Organisationseinheiten des 3. und 4. Kreises) und in dem Sinne nicht einer den Markt kontrollierenden staatlichen Aufsichtsbehörde unterstehen. Dagegen unterliegen sie einer verstärkten internen Aufsicht durch Bundesrat und Parlament, die aufgrund ihrer hierarchischen Stellung Sanktionen verhängen können (z.B.

---

<sup>73</sup> LAMPERT, S. 144 f.; VETTER, S. 42.

<sup>74</sup> BUFF, S. 292 f.

disziplinarische Massnahmen wegen einer Aufsichtsbeschwerde). Öffentlich-rechtliche Institutionen sind jedoch sehr stark an verfahrensrechtliche Vorschriften gebunden (z.B. Vergaberecht), deren Missachtung schwerwiegende finanzielle Konsequenzen haben kann (z.B. Schadenersatzforderungen). Insofern wäre für den öffentlichen Sektor die Kategorie "Aufsichtsrechte" wohl durch das Rechtsgebiet "Verfahrensrechtliche Vorschriften" zu ersetzen. Allerdings ist dies nur eine grobe Einteilung, die lediglich eine Übersicht über die potenziellen Rechtsrisiken vermitteln soll. Die konkreten Risiken sind jedoch für jede Verwaltungseinheit gesondert zu ermitteln. Je nach Tätigkeitsfeld kann die Risikobeurteilung nämlich höchst unterschiedlich ausfallen, und dementsprechend sieht sich das eine Bundesamt vermehrt mit Risiken aus dem Bereich Strafrecht konfrontiert, ein anderes dagegen hat vor allem mit Vertraulichkeit und Interessenskonflikten zu kämpfen.

Wie unter Kapitel 3.3.1 dargelegt, handelt es sich bei Reputationsrisiken um abgeleitete Risiken, die in der Regel als Folge der Verwirklichung von anderen Risiken - z.B. Rechtsrisiken - entstehen. Allerdings gilt es zu bedenken, dass Reputationsschäden nicht immer Resultat von Rechtsverletzungen, sondern teilweise auch von korrektem rechtlichem Verhalten sind<sup>75</sup>. Insofern können sich bestimmte Reputationsrisiken durchaus direkt und unabhängig von anderen Risiken realisieren.

Unter Reputation wird das öffentliche Ansehen verstanden, das eine Person, Institution, Organisation oder allgemeiner ein (Kollektiv-)Subjekt mittel- oder langfristig genießt<sup>76</sup>. Die Folgen eines Reputationsschadens können dementsprechend vielfältig und einschneidend sein. So kann eine Bank etwa massive Abzüge an Kundengeldern erleiden<sup>77</sup>, oder Firmen müssen einen Rückgang beim Absatz ihrer Produkte hin-

<sup>75</sup> Vgl. etwa den Imageverlust des EJPD nach der Verhaftung von Roman Polanski: NZZ Online vom 4. Oktober 2009, *Korrekt gehandelt und doch vieles falsch gemacht*, [http://www.nzz.ch/nachrichten/startseite/korrekt\\_gehandelt\\_und\\_doch\\_vieles\\_falsch\\_gemacht\\_1.3779791.html](http://www.nzz.ch/nachrichten/startseite/korrekt_gehandelt_und_doch_vieles_falsch_gemacht_1.3779791.html) (zuletzt eingesehen am 20. September 2010).

<sup>76</sup> ROTH/ERNI, S. 19 f.

<sup>77</sup> Vgl. den Abzug von Kundengeldern bei der UBS in Folge des schwindenden Vertrauens: NZZ Online vom 10. Dezember 2007, *Zerstörtes Vertrauen*, [http://www.nzz.ch/nachrichten/wirtschaft/aktuell/zerstoertes\\_vertrauen\\_1.597027.html](http://www.nzz.ch/nachrichten/wirtschaft/aktuell/zerstoertes_vertrauen_1.597027.html) (zuletzt eingesehen am 20. September 2010).

nehmen. Solche Folgen hängen mit der charakteristischen Eigenschaft des Reputationsschadens zusammen, der sich dadurch auszeichnet, dass von vergangenem auf künftiges Verhalten geschlossen wird, und Vertrauen viel schneller zerstört als aufgebaut werden kann<sup>78</sup>. Für den Bund haben Reputationsschäden zwar keine unmittelbaren finanziellen Auswirkungen in Form von Verlust an Kundengeldern oder Umsatzeinbußen, aber dafür andere, ebenso schwerwiegende Konsequenzen. So könnte der Staat als Folge eines Vertrauensverlusts seine Glaubwürdigkeit verlieren, wodurch etwa vermehrt entgegen den Empfehlungen der Behörden abgestimmt wird, oder häufiger Referenden gegen eine Gesetzesvorlage ergriffen werden. Dies sind die Mittel des Volks, um den Staat für sein "ungebührliches" Verhalten abzustrafen. Da der Staat die Gesetzgebungskompetenz hat und mit Steuergeldern operiert, ist er m.E. einem höheren Reputationsdruck ausgesetzt als ein Unternehmen der Privatwirtschaft. Während man den Regelverstoss einer Firma unter Umständen als "Kavaliersdelikt" abtut, wird vom Staat erwartet, dass er sich in jedem Fall an die (von ihm erlassenen) Gesetze hält. Die öffentliche Verwaltung hat somit auch eine Art Vorbildfunktion. Ihr Verhalten muss dem eines Musterschülers entsprechen und darf nicht einmal den Anschein von Unkorrektheit erwecken.

### 3.6.3 REGELN UND RICHTLINIEN

Wurde die Risikoanalyse vorgenommen und die Compliance-Risiken eruiert, müssen gestützt darauf Regeln und Richtlinien erlassen werden, um bei den Mitarbeitern das Bewusstsein für die unternehmensspezifischen Gefahrenbereiche zu schaffen. Diese sog. Codes of Conduct<sup>79</sup> sollen die Vorgaben des geltenden Rechts in einfachen Worten erläutern und als Nachschlagewerk dienen. Über die rein gesetzlichen Vorgaben hinaus, können darin auch ethische Standards oder Unternehmensziele mit besonderer Bedeutung aufgenommen werden. Infolgedessen können

<sup>78</sup> ROTH, *Compliance, Integrität und Regulierung*, S. 21.

<sup>79</sup> *In der Praxis findet man unterschiedliche Bezeichnungen für Codes of Conduct, die aber allesamt synonym verwendet werden: Verhaltenskodex, Leitlinien, Leitfaden, Handbuch, Compliance-Manual, Mitarbeiter-Handbuch, Code of Compliance, Compliance Reglement, Compliance-Programm.*

Inhalt und Umfang eines Code of Conduct je nach Unternehmensgrösse und Tätigkeit stark variieren. Bei der Ausarbeitung dieses Verhaltenskodex handelt es sich um eine Aufgabe des Managements, d.h. der Geschäftsleitung und/oder des Verwaltungsrates, wobei sinnvollerweise vor Erlass der Endversion ein Feedback der Mitarbeiter berücksichtigt wird<sup>80</sup>. Gemäss LAMPERT sollten Codes of Conduct modular aufgebaut sein<sup>81</sup> und folgenden Inhalt haben<sup>82</sup>:

- a) "Mission Statement": Einleitend sollte die Geschäftsleitung Ziel und Zweck des Codes of Conduct darlegen, sowie auf die für das Unternehmen negativen Folgen bei Nichtbeachtung hinweisen. Um die Bedeutung des Dokuments zu unterstreichen, sollte diese Einleitung vom Geschäftsführer (Direktor) unterzeichnet werden.
- b) Darstellung der gesetzlichen Anforderungen: Es folgt eine kurze Darlegung des rechtlichen Rahmens für die Tätigkeitsschwerpunkte des Unternehmens. Dabei ist auf eine klare Sprache zu achten, möglichst verbunden mit praxisnahen Beispielen.
- c) Erwartetes Mitarbeiterverhalten: Aus dem Code of Conduct muss klar hervorgehen, welches Verhalten vom Mitarbeiter erwartet wird, und wie er in einer entsprechenden Situation vorzugehen hat. Dazu gehört auch die Bezeichnung von Ansprechpersonen (z.B. Rechtsabteilung, Compliance-Officer) und Meldestellen (z.B. Whistleblowing-Hotline), an die man sich bei Fragen und Unklarheiten oder bei Feststellung von Regelverstössen wenden kann.
- d) Weitere mögliche Inhalte: Je nach Unternehmen können weitere Verhaltensanweisungen aufgenommen werden (z.B. Anweisungen zum E-mail Verkehr oder zur Aufbewahrung von Dokumenten, Verhalten bei Behörden- oder Medienanfragen).

<sup>80</sup> Vgl. zum Ganzen: LAMPERT, S. 148 ff.; MÜLLER, S. 85; BUFF, S. 34 f. und S. 92 f.

<sup>81</sup> Evtl. ist nicht für alle Mitarbeiter der gesamte Verhaltenskodex relevant, weshalb es möglich sein muss, nur die für die jeweilige Tätigkeit massgeblichen Module zu konsultieren.

<sup>82</sup> LAMPERT, S. 148 f.

Der Code of Conduct ist jedem Mitarbeiter als Hard-copy auszuhändigen und/oder in das Intranet einzustellen, damit vollständiger Zugang zu den Compliance-relevanten Informationen gewährleistet ist. Ebenso sollte der Verhaltenskodex regelmässig überprüft und allenfalls an geänderte Rechtslagen angepasst oder aufgrund von Erfahrungswerten ergänzt werden.

Neben der Erweiterung der Wissensbasis in Bezug auf Compliance-relevantes Fehlverhalten, dient der Code of Conduct darüber hinaus auch der Identifikation der Mitarbeiter mit ihrem Unternehmen und hat somit eine indirekte positive Wirkung, da die Hürden für ein Fehlverhalten auf diese Weise angehoben werden<sup>83</sup>. Als weitere Wirkungen des Codes of Conduct können etwa die Funktion einer Orientierungshilfe bei moralischen Dilemma-Situationen oder die Einengung von Spielräumen für Opportunismus angeführt werden<sup>84</sup>.

#### 3.6.4 INFORMATION, AUFKLÄRUNG UND AUSBILDUNG VON MITARBEITENDEN

Ziel von Compliance ist es, die Mitarbeitenden hinsichtlich der unternehmensspezifischen Gefahren zu sensibilisieren. Ausbildung und Schulung der Mitarbeitenden ist hierbei eines der zentralen Elemente und Voraussetzung für die Wirksamkeit eines Compliance-Konzepts. Einerseits erhöht regelmässiges Training die Kenntnisse über die relevanten Gesetze und Regeln, andererseits signalisiert die Unternehmensleitung mit obligatorischen Aus- und Weiterbildungen, dass sie die von ihr erlassenen Weisungen auch umsetzen will und der Compliance somit einen hohen Stellenwert in der Unternehmung einräumt. Für die konkrete Umsetzung gibt es verschiedene Instrumente, wie Orientierungsveranstaltungen, Seminare, Workshops, Präsentationen, Newsletters, Videos oder auch interaktive Medien wie Web-based-Trainings (WBT) oder CD-ROM. Welches die geeigneten Instrumente für die Ausbildung sind, hängt von den Bedürfnissen und Möglichkeiten der Unternehmung so-

---

<sup>83</sup> JÄGER/RÖDL/CAMPOS NAVE, S. 84.

<sup>84</sup> Für eine ausführliche Aufzählung der Wirkungen eines Codes of Conduct vgl. ROTH, *Compliance, Integrität und Regulierung*, S. 64.

wie ihren spezifischen Geschäftstätigkeiten ab<sup>85</sup>. Zu beachten ist jedoch, dass die Information nicht allein passiv, d.h. zum Selbststudium der Mitarbeitenden, erfolgt. Die persönliche Schulung ist immer noch das geeignetste Mittel um Compliance-Standards zu vermitteln, weshalb neue Mitarbeitende ein spezielles Compliance-Schulungs-Modul besuchen sollten<sup>86</sup>. Um sicherzustellen, dass die relevanten Kenntnisse noch vorhanden sind, sollte diese Schulung in regelmässigen Abständen - etwa alle ein bis zwei Jahre - wiederholt werden<sup>87</sup>. Ebenso wäre es denkbar, die regelmässigen Schulungen mit einem Test zu verbinden, dessen Resultat anlässlich der jährlichen Personalentwicklungsgespräche berücksichtigt wird, und allenfalls Einfluss auf die Beurteilung und somit indirekt auf die Lohnentwicklung hat.

### 3.6.5 ORGANISATORISCHE MASSNAHMEN

Kern der organisatorischen Massnahmen zur Umsetzung eines Compliance-Konzepts ist der Compliance Officer bzw. die mit dieser Aufgabe betraute Stelle in einem Unternehmen. Dieser Compliance Funktion obliegt die Sicherstellung der Einhaltung von Gesetzesvorschriften und ethischen Standards sowie die Bewahrung der Reputation eines Unternehmens. Das Pflichtenheft eines Compliance Officers umfasst unter anderem Beratung, Management von Interessenkonflikten, Erlass von Weisungen, Richtlinien und Empfehlungen, Information, Aufklärung und Schulung von Mitarbeitenden, Überwachung, Kontrolle und Sanktionen, Kontakt mit Aufsichtsbehörden und Berichterstattung. Dabei soll der Compliance Officer nicht den Chef ersetzen, sondern sich mit dem Unternehmensumfeld befassen und allfälligen Handlungsbedarf für die Anpassung des internen Regelwerks aufzeigen, daneben aber auch ethische Grundwerte vermitteln und den Mitarbeitenden als partnerschaftlicher Berater zur Seite stehen<sup>88</sup>.

Die Compliance Funktion ist entsprechend der Grösse und Organisationskomplexität des Unternehmens sowie des Compliance-Risikos mit

---

<sup>85</sup> Vgl. zum Ganzen: BUFF, S. 527 f.

<sup>86</sup> MÜLLER, S. 86.

<sup>87</sup> LAMPERT, S. 151.

<sup>88</sup> Vgl. zum Ganzen: BUFF, S. 50, 59 ff., 529.

angemessenen Ressourcen und Kompetenzen auszustatten<sup>89</sup>. Für Finanzdienstleistungsbetriebe wird in der Literatur empfohlen, dass pro ca. 800-1000 Mitarbeitende eine Vollzeit-Compliance-Stelle zur Verfügung stehen sollte, damit ein durchschnittliches Compliance-Niveau erreicht werden kann<sup>90</sup>. Da an die im Compliance-Bereich tätigen Mitarbeitenden hohe Anforderungen gestellt werden, müssen sie entsprechend über die für eine effektive Aufgabenerfüllung notwendigen Fähigkeiten verfügen. So stellt der Basler Ausschuss für Bankenaufsicht etwa folgendes Anforderungsprofil auf:

*"In particular, compliance function staff should have the necessary qualifications, experience and professional and personal qualities to enable them to carry out their specific duties. Compliance function staff should have a sound understanding of compliance laws, rules and standards and their practical impact on the bank's operations. The professional skills of compliance function staff, especially with respect to keeping up-to-date with developments in compliance laws, rules and standards, should be maintained through regular and systematic education and training."*<sup>91</sup>

Zudem sollte der Compliance Officer eine Persönlichkeit mit Durchsetzungsvermögen und hoher innerbetrieblicher Akzeptanz sein<sup>92</sup>.

Damit die Compliance-Funktion ihre Aufgaben wahrnehmen kann, muss sie uneingeschränktes Auskunfts-, Zugangs- und Einsichtsrecht haben und von ertragsorientierten Geschäftsaktivitäten unabhängig in die Gesamtorganisation eingegliedert werden<sup>93</sup>. Dies bedeutet, dass die für Compliance verantwortliche Person im Unternehmen dem Vorstandsvorsitzenden direkt unterstellt und berichtspflichtig sein sollte<sup>94</sup>. Auch der Basler Ausschuss für Bankenaufsicht nennt die Unabhängigkeit als eines der grundlegenden Prinzipien für die Compliance-Funktion:

---

<sup>89</sup> FINMA-RUNDSCHREIBEN 08/24, Rz. 101.

<sup>90</sup> MÜLLER, S. 88.

<sup>91</sup> BASEL COMMITTEE ON BANKING SUPERVISION, S. 13.

<sup>92</sup> BUFF, S. 52 f.

<sup>93</sup> FINMA-RUNDSCHREIBEN 08/24, Rz. 100.

<sup>94</sup> WECKER/GALLA, S. 67.

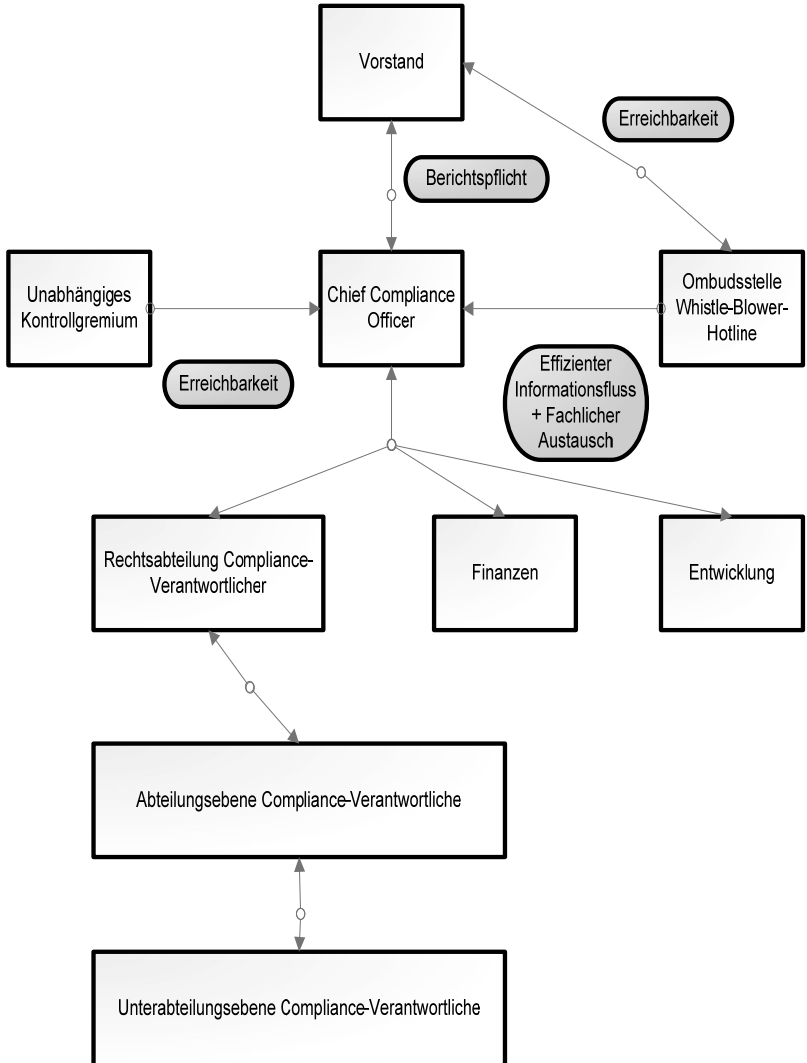
*"The concept of independence involves four related elements, each of which is considered in more detail below. First, the compliance function should have a formal status within the bank. Second, there should be a group compliance officer or head of compliance with overall responsibility for co-ordinating the management of the bank's compliance risk. Third, compliance function staff, and in particular, the head of compliance, should not be placed in a position where there is a possible conflict of interest between their compliance responsibilities and any other responsibilities they may have. Fourth, compliance function staff should have access to the information and personnel necessary to carry out their responsibilities."*<sup>95</sup>

Graphisch dargestellt, könnte die Struktur einer Compliance Organisation beispielsweise wie folgt aussehen:

---

<sup>95</sup> BASEL COMMITTEE ON BANKING SUPERVISION, S. 10.





Aus diesem Schema geht auch die Notwendigkeit der Zusammenarbeit der Compliance-Funktion mit anderen Stellen im Unternehmen hervor. Eine solche ist primär mit denjenigen Einheiten sinnvoll, die ebenfalls Kontroll- oder Überwachungsaufgaben wahrnehmen, wie etwa die interne Revision, das Controlling und der Rechtsdienst, soweit die Compliance-Funktion organisatorisch von diesem getrennt ist<sup>96</sup>.

Grundsätzlich ist nicht zwingend erforderlich, dass die Compliance Funktion von einem speziell (so) bezeichneten Compliance Officer umgesetzt wird. Gerade bei kleineren Unternehmen, welche die kritische Mitarbeiterzahl zur Schaffung einer 100%-Compliance Stelle nicht erreichen, kann ein Mitarbeiter die Compliance Aufgaben im Rahmen bestimmter, ihm dafür zugewiesener Stellenprozente übernehmen (z.B. 40%). Aufgrund langjähriger Erfahrung wird jedoch empfohlen, die Stelle des Compliance-Verantwortlichen mit Juristen zu besetzen und organisatorisch der Rechtsabteilung zuzuordnen. Daneben können aber durchaus auch Mitarbeiter der Abteilung Revision/Interne Kontrolle oder der Personalabteilung mit der Tätigkeit des Compliance-Verantwortlichen betraut sein<sup>97</sup>. Bei grösseren Unternehmen empfiehlt sich die Einrichtung einer eigenen Compliance-Abteilung, die unmittelbar dem verantwortlichen Vorstands- oder Geschäftsführungsmitglied untergeordnet ist und an dieses berichtet<sup>98</sup>. Dagegen kann die Compliance Funktion bei geringer Geschäfts- und Organisationskomplexität sowie geringem Compliance-Risiko auch in Teilzeitarbeit oder in Personalunion mit einer anderen internen Funktion, mit welcher keine Interessenkonflikte bestehen, oder in einem Outsourcing-Verhältnis mit einem externen Dienstleistungserbringer (z.B. Anwaltsbüro) betrieben werden<sup>99</sup>. Bei Bankunternehmen wird Compliance jedoch als eine "*core risk management activity*" angesehen, und entsprechend können zwar spezifische Aufgaben ausgelagert werden, aber sie müssen einer angemessenen Überwachung durch den "*head of compliance*" unterliegen<sup>100</sup>.

---

<sup>96</sup> Vgl. BUFF, S. 530 ff.

<sup>97</sup> Vgl. zum Ganzen: BUFF, S. 54 f.

<sup>98</sup> LAMPERT, S. 147.

<sup>99</sup> FINMA-RUNDSCHREIBEN 08/24, Rz. 105.

<sup>100</sup> BASEL COMMITTEE ON BANKING SUPERVISION, S. 15.

### 3.6.6 BERATUNG

Der Code of Conduct bietet den Mitarbeitenden als Nachschlagewerk eine wichtige Hilfestellung um Compliance-relevante Probleme im Alltag selbständig und rechtskonform zu bewältigen. Allerdings treten immer wieder Situationen auf, welche in den Leitlinien oder anderen Regelwerken nicht behandelt werden. Daher ist es wichtig, dass sich Mitarbeitende im Zweifelsfall jederzeit an eine dafür eingerichtete Beratungsstelle wenden können, die sie kompetent über das korrekte Vorgehen im Einzelfall berät. Hierfür steht grundsätzlich der Compliance-Officer bzw. die mit dieser Funktion betraute Person oder Organisationseinheit zur Verfügung (z.B. die Rechtsabteilung)<sup>101</sup>. Damit die angebotene Beratung auch in Anspruch genommen wird, ist Vertrauen der Mitarbeitenden in die Fachkompetenz des Compliance-Verantwortlichen vorausgesetzt, weshalb der Aufbau eines partnerschaftlichen Verhältnisses zwischen der Compliance-Stelle und den einzelnen Geschäftsbereichen unerlässlich ist. Die Schwierigkeit liegt in der Praxis darin, die Balance zwischen Beratung und interner Kontrolle zu halten<sup>102</sup>.

### 3.6.7 ÜBERWACHUNG DER EINHALTUNG DER UNTERNEHMENSINTERNEN VORGABEN

Der Kontrolle und der Überwachung der Einhaltung von Compliance-Anforderungen kommt eine zentrale Bedeutung zu. Je höher nämlich die Chance ist, dass das Fehlverhalten eines Mitarbeitenden entdeckt und sanktioniert wird, desto geringer ist der Anreiz, gegen Unternehmensvorschriften zu verstossen<sup>103</sup>. Um eine effiziente Kontrolle zu gewährleisten, stehen etwa folgende Instrumente zur Verfügung<sup>104</sup>:

- Vier-Augen-Prinzip: Für geschäftsrelevante und risikobehaftete Handlungen empfiehlt sich die Anwendung des sog. Vier-Augen-Prinzips. Dies bedeutet, dass alle relevanten Akten von zwei Personen kontrolliert werden. Dieses Instrument ist jedoch nur dann wirksam, wenn die zweite Person auch tatsäch-

---

<sup>101</sup> Vgl. zum Ganzen: LAMPERT, S. 151.

<sup>102</sup> BÜFF, S. 534.

<sup>103</sup> MÜLLER, S. 101.

<sup>104</sup> Vgl. zum Ganzen: MÜLLER, S. 101 ff.; LAMPERT, S. 153 ff.

lich eine materielle Kontrolle durchführt und nicht einfach ihr Visum auf das Dokument setzt, ohne eine Überprüfung vorzunehmen.

- Checklisten: Checklisten sind einerseits ein Hilfsmittel für die Mitarbeitenden zur Verrichtung ihrer Aufgaben, andererseits sind sie auch ein Kontrollinstrument der Vorgesetzten zur Überprüfung der Handlungen ihrer Untergebenen. Massgebend ist die Verständlichkeit der Checklisten und ihre einfache Auffindbarkeit.
- Prüfung und Befragung von Mitarbeitenden: Ein weiteres sinnvolles Kontrollinstrument ist die Durchführung regelmässiger Mitarbeiterbefragungen oder die Überprüfung von Geschäftsvorgängen (Audits). Diese können auch stichprobeartig und unangekündigt erfolgen. Die Organisation und Durchführung von Prüfungen und Mitarbeiterbefragungen kommt in der Regel dem Compliance-Officer bzw. der mit dieser Aufgabe betrauten Stelle zu.
- EDV-Tools: In Arbeitsabläufe können mit Hilfe von EDV-Tools in dem Sinne Kontrollinstrumente eingebaut werden, dass beispielsweise ein Vorgang nur abgeschlossen werden kann, wenn das Vorliegen bestimmter Dokumente oder Sachverhalte quittiert wird. Zudem sollten die Geschäftsabläufe registriert werden, damit im Nachhinein auch rekonstruiert werden kann, wer wann welche Handlungen vorgenommen hat.

Eine massgebliche Voraussetzung für eine wirksame Kontrolle im Compliance-Bereich ist die regelmässige Informationsbeschaffung. Fehlt es an den entsprechenden Informationen, kann kaum effizient überwacht und kontrolliert werden. Es ist Aufgabe der Compliance-Stelle, die relevanten Informationen zu beschaffen und sie an die Geschäftsleitung und den Verwaltungsrat weiterzuleiten<sup>105</sup>. Im Wesentlichen stehen hier zwei Informationsbeschaffungsinstrumente im Vordergrund, das Reporting und das sog. "Whistleblowing".

---

<sup>105</sup> BUFF, S. 535.

### Reporting:

Unter Reporting wird die regelmässige Berichterstattung über Compliance-relevante Sachverhalte an die Compliance-Stelle verstanden. Diese wiederum leitet die Informationen an die obersten Führungsorgane weiter<sup>106</sup>. Ebenso sind die Ergebnisse der Compliance-Anstrengungen eines Unternehmens regelmässig der Unternehmensleitung vorzulegen und mit dieser zu besprechen<sup>107</sup>. Dies ist die gängige Art der Informationsbeschaffung.

### Whistleblowing:

To blow the whistle bedeutet auf Deutsch in etwa "jemanden verpfeifen". Damit wird der Vorgang bezeichnet, wo ein Mitglied oder ein Angestellter eines privaten Unternehmens oder der öffentlichen Verwaltung illegale, unmoralische oder unrechtmässige Praktiken enthüllt<sup>108</sup>. Gelangen diese Informationen erst einmal an die Öffentlichkeit, kann dies für ein Unternehmen erhebliche Kosten verursachen (z.B. Busse) und mit einem Prestigeverlust einhergehen. Deshalb sollte jedes Unternehmen ein Interesse daran haben, interne Beschwerdewege einzurichten, die jeder Mitarbeiter gehen kann, der Kritik an unternehmensethisch relevanten Sachverhalten anbringen möchte. So besteht die Möglichkeit, unrechtmässiges Verhalten ohne den Einbezug externer Partner zu korrigieren und negative Folgen zu vermeiden<sup>109</sup>. Als Instrument zur Aufdeckung von Missständen werden deshalb in Unternehmen häufig sog. "Whistleblowing-Hotlines" eingerichtet, die telefonisch oder online - teils durch spezialisierte Call-Center - betrieben werden<sup>110</sup>. Dieses interne Whistleblowing bewegt sich im Spannungsfeld zwischen Zivilcourage und Denunziantentum, weshalb der Umgang mit solchen Meldungen viel Fingerspitzengefühl verlangt. Die Hinweise von Mitarbeitenden müssen streng vertraulich behandelt werden, ausser der Hinweisgeber erteilt eine ausdrückliche Ermächtigung zur Offenlegung. Zudem sollte

---

<sup>106</sup> BUFF, S. 537.

<sup>107</sup> LAMPERT, S. 153.

<sup>108</sup> CARRANZA/MICOTTI, S. 982.

<sup>109</sup> Vgl. zum Ganzen: BUFF, S. 553.

<sup>110</sup> BAUER, S. 191.

die meldende Person auch über den weiteren Verlauf und das Ergebnis der Angelegenheit informiert werden, sofern nicht datenschutzrechtliche Aspekte dagegen sprechen. Um den Whistleblower zu schützen, sollten auch anonyme Meldungen akzeptiert werden. Wird unternehmensintern kommuniziert, dass auch anonymen Hinweisen nachgegangen wird, entfaltet dies im Übrigen präventiv eine erhöhte Abschreckungswirkung<sup>111</sup>.

### 3.6.8 SANKTIONIEREN VON REGELVERSTÖSSEN

Sanktionen bei Verstößen bilden den Gegenpart zu Belohnungen bei Erfolgen. Idealerweise sollten die bei Unternehmen weitverbreiteten Incentive-Systeme mit einem Sanktionssystem verknüpft werden: bei Bonuszahlungen oder Beförderungen sind nicht nur Erfolge, sondern auch Regelverletzungen zu berücksichtigen<sup>112</sup>. Um dem Anliegen des rechtskonformen Verhaltens der Mitarbeitenden Nachdruck zu verschaffen, muss ein Unternehmen im Falle von Verstößen disziplinarische Konsequenzen androhen. Disziplinarische Massnahmen wirken abschreckend, womit ihnen auch eine präventive Funktion zukommt. Falls es zu einem Verstoß kommt, muss konsequent gehandelt werden. Wenn nämlich der Androhung von Sanktionen keine Taten folgen, entsteht der Eindruck, Verstöße würden sanktionslos hingenommen oder gar toleriert. Betreffend den Inhalt der Sanktionen bestehen unterschiedlich weitreichende Massnahmen, wie Abmahnung, finanzielle Sanktionen (z.B. Gehaltskürzung, Streichung eines Bonus), interne Versetzung oder die Kündigung als schärfstes Mittel<sup>113</sup>. Wichtig ist in jedem Fall, dass die ausgesprochene Massnahme der konkreten Situation gerecht wird, d.h. verhältnismässig ist<sup>114</sup>.

---

<sup>111</sup> Vgl. zum Ganzen: LAMPERT, S. 153 f.

<sup>112</sup> ROTH, *Good Corporate Governance*, S. 99.

<sup>113</sup> Vgl. zum Ganzen: LAMPERT, S. 152.

<sup>114</sup> BUFF, S. 558.

## 4 COMPLIANCE IM BAG UND AUF STUFE BUND

### 4.1 RISIKOANALYSE

#### 4.1.1 RISIKOANALYSE IM BUND

Die Risikoanalyse in sämtlichen Verwaltungseinheiten des Bundes hat gemäss dem vom Bundesrat am 3. Dezember 2004 verabschiedeten Dokument "Risikopolitik" des EFD zu erfolgen. Zuerst werden im Sinne einer Bestandesaufnahme sämtliche Risiken in einem Risikokatalog erfasst. Anschliessend werden die erfassten Risiken aufgrund ihrer finanziellen Auswirkungen (potentielle Schadenhöhe) sowie ihrer Eintretenswahrscheinlichkeit bewertet, und eine Risikoliste sowie ein Risikoprofil erstellt. Aus der Liste ist die Rangordnung der Risiken ersichtlich. Die ersten zehn Risiken auf der Liste sowie alle Risiken mit einem Schadenpotenzial von über 5 Millionen Franken bilden die Kategorie der sogenannten Kernrisiken, welchen die Verwaltungseinheit besondere Aufmerksamkeit zu schenken hat. Für die derart identifizierten Risiken mit Handlungsbedarf werden anschliessend im Rahmen der Risikobewältigung Massnahmen zur Eindämmung formuliert und umgesetzt<sup>115</sup>.

#### 4.1.2 DIE COMPLIANCE-RISIKEN DES BAG

Die Risikoerfassung im BAG erfolgt bottom-up durch die verschiedenen Facheinheiten. Erachtet die Einheitsleitung eine Risikomeldung an die Amtsleitung als notwendig, füllt der Risikoeigner bzw. die verantwortliche Person des betreffenden Aufgabenbereichs ein Meldeformular aus und stellt dieses der Sektion Planung, Controlling und Organisationsinstrumente zu, welche die gemeldeten Risiken plausibilisiert und zu einem Risiko-Portfolio Amt konsolidiert. Dieses wird der Geschäftsleitung anlässlich der zweimal jährlich stattfindenden operativen Steuerungsrunde zur Diskussion und Verabschiedung unterbreitet. Zur Erfassung der potenziellen Risiken steht ein Formular für Risikomeldun-

---

<sup>115</sup> Vgl. zum Ganzen: EFD RISIKOPOLITIK, S. 5 ff.

gen<sup>116</sup> zur Verfügung, das sich primär an die Sektionsleitenden richtet und von diesen ausgefüllt und dem Risiko-Coach zugestellt wird. In einem Hilfsdokument<sup>117</sup> finden sich Anweisungen, wie das Formular auszufüllen ist, sowie Erläuterungen zu den verschiedenen Risikokategorien. Rechtliche Risiken/Compliance figurieren in der Kategorie 2 und werden wie folgt beschrieben: *Risiken im Zusammenhang mit dem Vollzug der Verwaltungsaufgaben und der Einschaltung von rechtlichen Bestimmungen und Verträgen. Beispiele für Risiken der Kategorie 2: Aufsichts- oder Informationspflichtverletzung, Vertragsverletzung.*

Die letzte Risikobeurteilung der Geschäftsleitung datiert vom 8. Mai 2009<sup>118</sup> und enthält im Risikoportfolio insgesamt fünf Risiken der Kategorie 2 (rechtlich, Compliance):

- GP 9: Fehlen der gemäss BRB bewilligten Mittel fürs Gesundheitsberuferegister
- KUV 7: Externe Dienstleister für Aufsichtstätigkeit und Leistungen
- KUV 3a: Aufsichtstätigkeiten (Juristische und finanzielle Aufsicht KV)
- KUV 3b: Aufsichtstätigkeit (Juristische Aufsicht UV)
- VS 11: Informatik-Applikationen im DB VS

Betrachtet man die Beschreibung der Risiken im Risikokatalog (S. 3 ff.), ist einerseits auffallend, dass nur die Risiken GP 9 und VS 11 als ausschliessliche Compliance-Risiken eingestuft sind, die drei anderen Risiken hingegen noch weiteren Kategorien zugeordnet werden. Andererseits ist eine Mehrzahl von Risiken mit der Kategorie 2 gekennzeichnet, obwohl sie im Risikoportfolio BAG auf Seite 2 nicht in dieser Spalte aufgeführt sind (KUV 2: Leistungskatalog und Tarife; KUV 6: Führung,

<sup>116</sup> BAG-Intranet, *Formular zur Erfassung von Risiken*, <http://wwwi.bag.admin.ch/rm/pcoi/pc/documents/Formular%20Erfassung%20Risiken.xls> (zuletzt eingesehen am 20. September 2010).

<sup>117</sup> BAG-Intranet, *Erläuterungen zum Formular Risikomeldungen*, 13. Dezember 2006, <http://wwwi.bag.admin.ch/rm/pcoi/pc/documents/Erläuterungen%20Formular%20Risikomanagement.pdf> (zuletzt eingesehen am 20. September 2010).

<sup>118</sup> Risikobeurteilung BAG, S. 2.



Personal, Finanzen; KUV 8: Insolvenzfonds und Finanzkrise; KUV 9: Einführung der Versichertenkarte; KUV 10: Strategie Kosten-/Prämienentwicklung; KUV 11: Strategie Qualitätssicherung; KUV 12: Qualitätsindikatoren und ihre Kommunikation; VS 5: Rekurs/Haftpflicht nach Fehlentscheid). Risikoportfolio und Risikokatalog liefern also erste Anhaltspunkte, mit welchen Compliance-Risiken das BAG konfrontiert ist oder konfrontiert sein könnte. Wenn man sich jedoch die Definitionen von Compliance sowie der Compliance-Risiken in Erinnerung ruft, und die Risikobeurteilung vor diesem Hintergrund kritisch hinterfragt, bestehen m.E. Zweifel, ob tatsächlich alle unter der Kategorie 2 aufgeführten Risiken als Compliance-Risiken zu qualifizieren sind. So sind beispielsweise gerade die Risiken GP 9 und VS 11 gemäss ihrer Beschreibung nicht Resultat einer "Nichteinhaltung von Gesetzen und Regeln durch Mitarbeitende" sondern offensichtlich Folge von mangelnden finanziellen Ressourcen. Hierbei handelt es sich zwar um operationelle Risiken, jedoch geht es nicht um Verstösse gegen Gesetze, Vorschriften oder Standards.

Als Konsequenz muss folglich auch die Frage gestellt werden, ob allenfalls Compliance-Risiken für das BAG bestehen, welche nicht in die Risikobeurteilung aufgenommen wurden. Um dies zu beurteilen, ist zu prüfen, in welchen Bereichen der Bund oder das BAG Massnahmen ergriffen oder Aktivitäten entwickelt haben, die implizit auf das Vorhandensein eines Compliance-Risikos schliessen lassen. Anhand dieser Überprüfung wurden folgende Dokumente identifiziert:

- Auf Bundesebene wurde erst kürzlich (Juni 2009) vom Eidgenössischen Personalamt (EPA) ein Faltblatt zur Korruptionsprävention an sämtliche Mitarbeitende der Bundesverwaltung verteilt<sup>119</sup>. Bei der Korruption handelt es sich um ein "klassisches" Compliance-Thema, das ins Rechtsgebiet des Strafrechts fällt und in vielen Werken zur Compliance abgehandelt wird<sup>120</sup>.

<sup>119</sup> Vgl. EPA KORRUPTIONSPRÄVENTION.

<sup>120</sup> Z.B. BUFF, S. 351 ff.; ROTH, Compliance, S. 34 ff.

- Ebenso vom EPA stammen die Richtlinien zu Nebenbeschäftigungen und öffentlichen Ämtern vom 27. März 2006<sup>121</sup>.
- Per 1. Januar 2005 trat die Weisung des EDI über die Nutzung der Informatik- und Kommunikationsmittel (IKT-Mittel) in Kraft, wo unter anderem auch die private Nutzung von Internet und der private E-Mail-Verkehr geregelt wird<sup>122</sup>.
- Am 6. Mai 2009 erfolgte eine Mitteilung vom Generalsekretariat des Eidgenössischen Departement des Innern (GS-EDI) an alle Mitarbeiter des EDI betreffend die private Nutzung des Internetzugangs<sup>123</sup>. Darin wird festgehalten, dass der Zugriff auf Facebook die Netzwerkinfrastruktur belastet und damit die geschäftliche Nutzung des Internets beeinträchtigt. Die Bundesangestellten wurden dazu aufgefordert, in Eigenverantwortung die Nutzung von Facebook für private Zwecke zu unterlassen.
- Am 1. Juni 2006 erliess das EDI Weisungen zur Behandlung von Gesuchen gestützt auf das Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung (BGÖ)<sup>124</sup>.
- Infolge des Inkrafttretens des neuen Bundespersonalgesetzes erliess die Amtsleitung des BAG am 30. Juli 2002 neue Arbeitszeitbestimmungen<sup>125</sup>. Dabei geht es im Wesentlichen um die Sicherstellung der Erreichbarkeit der Mitarbeitenden, da es für das Image der Verwaltung schlecht ist, wenn die zuständigen Fachpersonen nicht erreichbar sind.

<sup>121</sup> Vgl. EPA-RICHTLINIEN ZU NEBENBESCHÄFTIGUNGEN.

<sup>122</sup> BAG-Intranet, Weisung des EDI über die Nutzung der Informatik- und Kommunikationsmittel, 1. Januar 2005, <http://wwwi.bag.admin.ch/edv/allg/sicherheit/> (zuletzt eingesehen am 20. September 2010).

<sup>123</sup> Vgl. Anhang "Masshalten beim Zugriff auf Facebook".

<sup>124</sup> BAG-Intranet, Weisungen für die Behandlung von Gesuchen gestützt auf das Bundesgesetz vom 17. Dezember 2004 über das Öffentlichkeitsprinzip der Verwaltung (BGÖ), 1. Juni 2006, <http://wwwi.bag.admin.ch/recht/Oeffentlichkeitsprinzip/EDI-Weisung%20BGÖ-D.doc> (zuletzt eingesehen am 20. September 2010).

<sup>125</sup> BAG-Intranet, Änderungen arbeitszeitlicher Bestimmungen als Folge des neuen Personalrechts ab 2. August 2002, 30. Juli 2002, [http://wwwi.bag.admin.ch/stab\\_alg/DG/documents/bag/BAG.%20Ansprechzeiten.%20Weisung%20Amtsleitung.pdf](http://wwwi.bag.admin.ch/stab_alg/DG/documents/bag/BAG.%20Ansprechzeiten.%20Weisung%20Amtsleitung.pdf) (zuletzt eingesehen am 20. September 2010).

- An der Sitzung der Geschäftsleitung BAG vom 1. Oktober 2008 wurde die Rechtsabteilung beauftragt, Leitlinien zum Umgang mit Interessenkonflikten, der Annahme von Geschenken, der Ausübung von Nebenbeschäftigungen, der Annahme von Honorar sowie zur Korruptionsprävention zu erarbeiten. In der Folge wurde der Geschäftsleitung im August 2009 eine erste Version der sog. Compliance-Leitlinien des BAG vorgelegt, die in überarbeiteter Form am 3. Februar 2010 genehmigt wurden<sup>126</sup>.
- Wegen dringendem Handlungsbedarf in den Facheinheiten wurde im BAG ein System zum Vertragsmanagement erarbeitet, welches heute auf dem Intranet unter der Bezeichnung "Schulungsordner CONTRAT" abgerufen werden kann. Für den Bereich des öffentlichen Beschaffungswesens findet sich zudem ein Link auf das Anwendungshandbuch BoeB/VoeB der Beschaffungskommission des Bundes<sup>127</sup>.

Bei all diesen Massnahmen geht es um die Vermeidung von rechtlichen Sanktionen, finanziellen Verlusten oder Reputationsschäden, die als Folge von Verstössen gegen Gesetze oder Weisungen entstehen können. Es liegen also durchaus weitere Compliance-Risiken vor (Korruption, Interessenkonflikte, Internetproblematik, verfahrensrechtliche Vorschriften), die jedoch nicht in der Risikobeurteilung des BAG erscheinen bzw. allenfalls wieder aus dieser gelöscht wurden.

#### 4.1.3 ZUSAMMENFASSUNG UND SCHLUSSFOLGERUNG

Zusammenfassend ist festzuhalten, dass im BAG eine Übersicht über sämtliche Compliance-Risiken fehlt. Zwar besteht eine Risikobeurteilung gemäss den Vorgaben der Risikopolitik Bund. Allerdings sind

<sup>126</sup>BAG-Intranet, *Compliance-Leitlinien*, [http://wwwwi.bag.admin.ch/b\\_l/p\\_o/neues\\_intranet/Hauptseite/compliance\\_leitlinien/index.php](http://wwwwi.bag.admin.ch/b_l/p_o/neues_intranet/Hauptseite/compliance_leitlinien/index.php) (zuletzt eingesehen am 20. September 2010)

<sup>127</sup>BAG-Intranet, *Schulungsordner CONTRAT*, [http://wwwwi.bag.admin.ch/b\\_l/kpp/1\\_Vertragsmanagement/Schulungsordner%20CONTRAT.php](http://wwwwi.bag.admin.ch/b_l/kpp/1_Vertragsmanagement/Schulungsordner%20CONTRAT.php) (zuletzt eingesehen am 20. September 2010).

einerseits nicht sämtliche als Compliance-Risiken aufgeführten Risiken auch als solche zu beurteilen, andererseits fehlen massgebliche Compliance-Risiken (z.B. Korruption) auf dieser Liste. Des weiteren fehlt es auch an einer Übersicht der Risiken auf Stufe Bund. Der Bundesrat nimmt lediglich Kenntnis von den einzelnen Übersichten der Departemente, womit es ihm an einer Konzernsicht im bestehenden Risikomanagement mangelt<sup>128</sup>. Dies macht es äusserst schwierig, die Compliance-Risiken des BAG herauszufiltern, und es ist davon auszugehen, dass die oben aufgeführte Risikoaufzählung lückenhaft und unvollständig ist. Es ist jedoch auch nicht Ziel dieser Arbeit, alle Compliance-Risiken des BAG systematisch zu erfassen und zu beurteilen<sup>129</sup>. Ebenso würde es den Rahmen dieser Arbeit sprengen, wenn sämtliche oben identifizierten Risiken in die Überprüfung der weiteren Compliance-Elemente mit einbezogen würden. In der Folge wird die Analyse im Sinne einer Fallstudie auf folgende vier Compliance-Risiken eingeschränkt:

1. Aufsichtstätigkeiten KUV
2. Interessenkonflikte
3. Internet-Problematik
4. Korruption

Diese Auswahl erfolgte unter dem Gesichtspunkt der unter Kapitel 3.6.2 aufgeführten vier Rechtsgebiete, damit aus jeder Kategorie ein Risiko behandelt wird.

## 4.2 RELEVANTE REGELN UND RICHTLINIEN

### 4.2.1 REGELN UND RICHTLINIEN AUF STUFE BUND

Grundlage für das Verhalten von Bundesangestellten bildet der vom Bundesrat am 19. April 2000 gutgeheissene Verhaltenskodex der allgemeinen Bundesverwaltung. In sieben Leitsätzen wird darin die Berufsethik des Bundes verankert. Es ist offenkundig, dass dieser Ver-

<sup>128</sup> *EFK-QUERSCHNITTSPRÜFUNG*, S. 18.

<sup>129</sup> *Dies wäre allenfalls eine zu ergreifende Massnahme als Folge dieser Arbeit.*

haltenskodex den unter Kapitel 3.6.3 aufgeführten Anforderungen an einen Code of Conduct nicht zu genügen vermag. So dürfte es für einen Mitarbeitenden beispielsweise schwer zu beurteilen sein, ab wann die Annahme eines Geschenks seine Unabhängigkeit und Handlungsfähigkeit beeinträchtigen könnte<sup>130</sup>. Bezüglich der Risiken Korruption und Interessenkonflikte bestehen zudem spezifische Verhaltensanweisungen des EPA in Form des Faltblatts Korruptionsprävention<sup>131</sup> und den Richtlinien zu Nebenbeschäftigungen und öffentlichen Ämtern<sup>132</sup>, wobei es hier Überschneidungen gibt (z.B. finden sich auch in der Broschüre Korruptionsprävention Anweisungen zu Nebenbeschäftigungen). Relevant für die Internetproblematik sind die gestützt auf die Bundesinformatikverordnung (BinfV; SR 172.010.58) erlassenen Weisungen des Informatikrats des Bundes (IRB) über die Informatiksicherheit in der Bundesverwaltung<sup>133</sup>. In diesem Zusammenhang zu berücksichtigen sind des Weiteren das Bundesgesetz über den Datenschutz (DSG; SR 235.1) sowie die Verordnung zum Bundesgesetz über den Datenschutz (VDSG; SR 235.11). Dagegen fehlt es auf Bundesebene an Vorgaben zur Aufsichtstätigkeit KUV (was logisch ist, da dieses Risiko nur einen Direktionsbereich eines Amtes betrifft).

#### 4.2.2 REGELN UND RICHTLINIEN DES BAG

Auf Stufe Departement finden sich - soweit ersichtlich - nur zum Risiko Internet-Problematik Verhaltensanweisung an die Mitarbeitenden. Zum einen ist dies die Weisung über die Nutzung der Informatik- und Kommunikationsmittel (IKT-Mittel)<sup>134</sup>, zum anderen die Mitteilung des GS-EDI vom 6. Mai 2009 bezüglich "Masshalten beim Zugriff auf Facebook"<sup>135</sup>. Diese Mitteilung beschränkt sich allerdings auf Vorgaben

<sup>130</sup> Vgl. EPA VERHALTENSKODEX, Ziff. 4.

<sup>131</sup> Vgl. EPA KORRUPTIONSPRÄVENTION.

<sup>132</sup> Vgl. EPA-RICHTLINIEN ZU NEBENBESCHÄFTIGUNGEN.

<sup>133</sup> BAG-Intranet, Weisungen des IRB über die Informatiksicherheit in der Bundesverwaltung, 27. September 2004, <http://wwwwi.bag.admin.ch/edv/allg/sicherheit/> (zuletzt eingesehen am 20. September 2010).

<sup>134</sup> BAG-Intranet, Weisung des EDI über die Nutzung der Informatik- und Kommunikationsmittel, 1. Januar 2005, <http://wwwwi.bag.admin.ch/edv/allg/sicherheit/> (zuletzt eingesehen am 20. September 2010).

<sup>135</sup> Vgl. Anhang: Mitteilung "Masshalten beim Zugriff auf Facebook".

zur Nutzung der Internetplattform Facebook und gibt keine generellen Anweisungen zum Umgang mit dem Internet.

Im BAG wurde die Abteilung Recht anlässlich der Geschäftsleitungssitzung vom 1. Oktober 2008 beauftragt, verschiedene Merkblätter im Zusammenhang mit Interessenkonflikten zu erarbeiten. In der Folge wurde der Geschäftsleitung am 26. August 2009 der Entwurf eines Code of Conduct betreffend den Umgang mit Interessenkonflikten, die Annahme von Geschenken und anderen Vorteilen, die Ausübung von Nebenbeschäftigungen, die Annahme von Honoraren und anderen Entschädigungen sowie die Korruptionsprävention vorgelegt. Im Anschluss an diese Sitzung wurde das Dokument überarbeitet und am 3. Februar 2010 durch die Geschäftsleitung unter dem neu festgelegten Titel "Compliance-Leitlinien" definitiv genehmigt. Diese Leitlinien enthalten Erläuterungen zum relevanten gesetzlichen Rahmen und detaillierte Vorgaben zum korrekten Verhalten der Mitarbeitenden, versehen mit konkreten Beispielen aus der Praxis. Ebenso werden die bei Fragen oder Unklarheiten zuständigen Anlaufstellen bezeichnet (in der Regel die direkte Führungskraft), und weitere massgebliche Dokumente sind als Beilagen enthalten (z.B. Faltblatt Korruptionsprävention)<sup>136</sup>. Zwar werden in den Compliance-Leitlinien des BAG lediglich zwei Risiken abgehandelt (Interessenkonflikte und Korruption), aber inhaltlich entsprechen sie weitgehend den unter Kapitel 3.6.3 aufgeführten Vorgaben. Dies etwa im Gegensatz zum Leitbild des BAG, welches eben gerade nicht konkrete Handlungsanweisungen enthält, sondern die übergeordnete Philosophie, die grundsätzlichen Unternehmensprinzipien beschreibt, welche die Mitarbeitenden leiten sollen<sup>137</sup>.

Betreffend das Risiko Aufsichtstätigkeiten KUV ist eine schriftliche Regelung der Prozessabläufe als Massnahme vorgesehen<sup>138</sup>. Die entsprechenden Richtlinien und Verhaltensanweisungen werden zur Zeit

<sup>136</sup> BAG-Intranet, *Compliance-Leitlinien*, [http://wwwi.bag.admin.ch/b\\_lp\\_o/neues\\_intranet/Hauptseite/compliance\\_leitlinien/index.php](http://wwwi.bag.admin.ch/b_lp_o/neues_intranet/Hauptseite/compliance_leitlinien/index.php) (zuletzt eingesehen am 20. September 2010).

<sup>137</sup> BAG-Intranet, *Unser Leitbild, Bundesamt für Gesundheit*, S. 3, [http://wwwi.bag.admin.ch/b\\_lp\\_o/neues\\_intranet/Hauptseite/neu\\_personalpolitik/files/BAG\\_Leitbild\\_D.pdf](http://wwwi.bag.admin.ch/b_lp_o/neues_intranet/Hauptseite/neu_personalpolitik/files/BAG_Leitbild_D.pdf) (zuletzt eingesehen am 20. September 2010).

<sup>138</sup> RISIKOBEURTEILUNG BAG, S. 5.

erarbeitet und könnten allenfalls zu einem späteren Zeitpunkt direkt in die Compliance-Leitlinien des BAG aufgenommen oder via Verweis referenziert werden.

Am 9. September 2009 wurden im Intranet des BAG Regeln zum Umgang mit E-Mails aufgeschaltet. Diese enthalten detaillierte Anweisungen darüber, wie eine E-Mail abzufassen ist (Sprache, Signatur, Betreff, Anrede etc.) sowie Empfehlungen zur Bearbeitung und Anregungen zur Reduktion der E-Mail Flut<sup>139</sup>. Ebenso im Intranet befindet sich unter der Rubrik Informatik eine Zusammenfassung wichtiger Informationen zum Thema Sicherheit mit entsprechenden Links zu den relevanten Dokumenten<sup>140</sup>.

#### 4.2.3 ZUSAMMENFASSUNG UND SCHLUSSFOLGERUNG

In Bezug auf Compliance-relevante Regeln und Richtlinien zeigt sich in der Bundesverwaltung ein sehr heterogenes Bild. Aktivitäten zu bestimmten Gefahrenbereichen sind auf allen Hierarchiestufen zu erkennen, wobei teilweise Überschneidungen und/oder Wiederholungen vorliegen. Hierbei besteht eine grosse Gefahr, dass gleiche Sachverhalte in der Praxis unterschiedlich gehandhabt werden. Zudem ergibt sich durch die Vielzahl der Regelungen und der fehlenden Übersicht eine erhebliche Unsicherheit für den einzelnen Mitarbeitenden, wie er sich in einer bestimmten Situation zu verhalten hat. So finden sich etwa Ausführungen zu Interessenkonflikten in vier verschiedenen Dokumenten (Verhaltenskodex Bund, Faltblatt Korruption, Richtlinien zu Nebenbeschäftigungen und Compliance-Leitlinien des BAG). Für einen Mitarbeitenden ist wohl kaum verständlich, welche Regelung er nun primär beachten muss, bzw. ob er mit der Konsultation eines der Dokumente sämtliche notwendigen Informationen besitzt.

<sup>139</sup> BAG-Intranet, *Alles rund um E-Mails*, [http://wwwwi.bag.admin.ch/stab\\_alg/KOM/intkom/index%20richtlinien.php](http://wwwwi.bag.admin.ch/stab_alg/KOM/intkom/index%20richtlinien.php) (zuletzt eingesehen am 20. September 2010).

<sup>140</sup> BAG-Intranet, *Sicherheit - Secure*, <http://wwwwi.bag.admin.ch/edv/allg/sicherheit/> (zuletzt eingesehen am 20. September 2010).

Der Verhaltenskodex der allgemeinen Bundesverwaltung ist sehr kurz gehalten und kaum geeignet, regelkonformes Verhalten der Bundesangestellten sicherzustellen. Dagegen finden sich spezifische und ausführliche Regelungen in den Compliance-Leitlinien des BAG, die damit den Compliance-Anforderungen an die Erfassung und Regelung der rechtlichen Risiken am ehesten gerecht werden. Durch die kontinuierliche Ergänzung mit weiteren risikorelevanten Verhaltensweisen können sie zu einem umfassenden Regelwerk für sämtliche Compliance-Risiken des BAG ausgebaut werden. Diesbezüglich stellt sich die Frage, ob die für die gesamte Bundesverwaltung relevanten Risikobereiche (z.B. Korruption und Interessenkonflikte) nicht besser umfassend und abschließend im Verhaltenskodex der allgemeinen Bundesverwaltung zu regeln wären. Damit würde aber weiterhin das Problem bestehen, dass die Mitarbeitenden mit mehreren Codes of Conduct konfrontiert sind und sich im Einzelfall die für sie wichtigen Bestimmungen selber "zusammensuchen" müssten. Diesem Dilemma könnte m.E. mit folgender Lösung begegnet werden: Anstatt sowohl auf Stufe Bund wie auch auf Stufe Amt je einen Code of Conduct zu erarbeiten, wäre es sinnvoller, dass jede Verwaltungseinheit ihren eigenen Code of Conduct führt, derart gestaltet, dass in einem ersten Teil allgemeine, für die gesamte Bundesverwaltung geltende Verhaltensregeln nach den Vorgaben des EPA oder des Bundesrates kodifiziert sind (z.B. Nebenbeschäftigungen, Korruption, Datenschutz, Internet etc.) und in einem zweiten Teil jedes Departement und jedes Amt seine tätigkeitsspezifischen Risikobereiche seinen Bedürfnissen entsprechend selber regeln kann.

#### 4.3 VERMITTLUNG DES COMPLIANCE-WISSENS

##### 4.3.1 COMPLIANCE-AUSBILDUNG AUF STUFE BUND

Bundesintern bieten das EPA, das Bundesamt für Informatik und Telekommunikation (BIT) und das Interdepartementale Ausbildungszentrum (IAZ) eine breite Palette an Aus- und Weiterbildungen an, die von Leadership-Seminaren über Projektmanagement-Kurse bis hin zu Kursen



zur Brandbekämpfung und erste Hilfe reichen<sup>141</sup>. Darunter gibt es auch Ausbildungen, die durchaus Compliance-Relevanz haben, wie etwa einen Kurs zum Datenschutz. Zudem können für Bereiche, die durch das Ausbildungsangebot des Bundes nicht abgedeckt sind, auch externe Angebote berücksichtigt werden. Aus- und Weiterbildungen erfolgen auf freiwilliger Basis, obligatorische Weiterbildungen im Compliance-Bereich für sämtliche Mitarbeitenden des Bundes sind nicht vorgesehen.

#### 4.3.2 COMPLIANCE-AUSBILDUNG IM BAG

Vorab ist festzuhalten, dass es im BAG keine obligatorischen Weiterbildungen betreffend den Umgang mit Compliance-Risiken für die Mitarbeitenden gibt. Allerdings werden die Mitarbeitenden zu freiwilligen Aus- und Weiterbildungen ermutigt<sup>142</sup>, an welchen sich das Amt gemäss den Grundsätzen der internen Ausbildungsrichtlinien finanziell beteiligen kann. Neben EPA, BIT und IAZ bieten auch das GS-EDI<sup>143</sup> sowie das BAG<sup>144</sup> selbst Aus- und Weiterbildungskurse an.

Verantwortlich für die Erarbeitung der ihrer Aufgabe entsprechenden Fachkompetenzen sind die Mitarbeitenden selber, wobei die Führungskräfte eine Mitverantwortung tragen und den Ausbildungsbedarf ihrer Untergebenen regelmässig abklären sollten<sup>145</sup>. Grundsätzlich ist es also

---

<sup>141</sup> Vgl. EPA, *Ausbildungszentrum der Bundesverwaltung (AZB), Programm 2010*, <http://www.epa.admin.ch/dienstleistungen/bildung/index.html?lang=d> (zuletzt eingesehen am 20. September 2010).

<sup>142</sup> So lautet jedenfalls der Grundsatz der Ausbildungsrichtlinien BAG: "In diesem Sinne setzt sich das BAG zum Ziel, lebenslanges Lernen seiner Mitarbeitenden zu fördern und zu ermöglichen", BAG-Intranet, *Ausbildungsrichtlinien BAG*, Ziff. 3, [http://wwwi.bag.admin.ch/b\\_l/p\\_o/neues\\_intranet/Hauptseite/aus\\_weit\\_erbildung/files/Ausbildungsrichtlinien\\_d.pdf](http://wwwi.bag.admin.ch/b_l/p_o/neues_intranet/Hauptseite/aus_weit_erbildung/files/Ausbildungsrichtlinien_d.pdf) (zuletzt eingesehen am 20. September 2010).

<sup>143</sup> Vgl. Intranet GS-EDI, *Personal*, <http://intranet.gsedi.admin.ch/personaldienst/index.html?lang=de> (zuletzt eingesehen am 20. September 2010).

<sup>144</sup> BAG-Intranet, *Aus- und Weiterbildung*, [http://wwwi.bag.admin.ch/b\\_l/p\\_o/neues\\_intranet/Hauptseite/aus\\_weit\\_erbildung/index.php](http://wwwi.bag.admin.ch/b_l/p_o/neues_intranet/Hauptseite/aus_weit_erbildung/index.php) (zuletzt eingesehen am 20. September 2010).

<sup>145</sup> BAG-Intranet, *Ausbildungsrichtlinien BAG*, Ziff. 4.4 und 4.5, [http://wwwi.bag.admin.ch/b\\_l/p\\_o/neues\\_intranet/Hauptseite/aus\\_weit\\_erbildung/files/Ausbildungsrichtlinien\\_d.pdf](http://wwwi.bag.admin.ch/b_l/p_o/neues_intranet/Hauptseite/aus_weit_erbildung/files/Ausbildungsrichtlinien_d.pdf) (zuletzt eingesehen am 20. September 2010).

den Mitarbeitenden überlassen, ob und wie sie sich beruflich weiter entwickeln wollen.

Die Wissensvermittlung zu den vier Compliance-Risiken Korruption, Interessenkonflikte, Aufsichtstätigkeiten KUV und Internet-Problematik ist höchst unterschiedlich. So werden die Mitarbeitenden betreffend Korruption und Interessenkonflikte via Kaskadensitzungen und Intranet-Newsticker auf die im Intranet zur Verfügung gestellten Compliance-Leitlinien und weitere Dokumente (Faltblatt Korruptionsprävention) aufmerksam gemacht. Mit anderen Worten liegt es also an jedem einzelnen Mitarbeitenden, sich unter Inanspruchnahme der im Intranet vorhandenen Hilfsmittel die notwendigen Kenntnisse in diesen Bereichen im Selbststudium zu erarbeiten.

Zur Internet-Problematik gibt es innerhalb des BAG keine spezifischen Informations- oder Weiterbildungsveranstaltungen. Hingegen bietet das BIT einen eintägigen Internet-Grundkurs an, wo unter anderem auch der Sicherheitsaspekt thematisiert wird<sup>146</sup>. Betreffend den Umgang mit E-Mails wurden im Intranet des BAG Regeln und Anweisungen aufgeschaltet, die mit Links zu weiteren relevanten Dokumenten zu diesem Thema versehen sind<sup>147</sup>. Allerdings erfolgte hierzu keine aktive Information der Mitarbeitenden, sondern diesen ist es selber überlassen, sich über die neuen Vorgaben zu informieren (oder eben auch nicht). Ob die Einführung der neuen Regeln bezüglich E-Mails via Intranet tatsächlich erfolgreich ist, wird sich unmittelbar im täglichen E-Mail Verkehr widerspiegeln. Ebenfalls im Intranet finden sich unter der Rubrik Informatiksicherheit Links auf weitere relevante Dokumente bezüglich Nutzung der Informatik- und Kommunikationsmittel (z.B. die BinFV oder die Weisung des EDI über die Nutzung der IKT-Mittel<sup>148</sup>).

---

<sup>146</sup> BIT, *Internet Grundkurs*,  
<http://www.bit.admin.ch/edu/kurse/kursdetails/index.html?linkto=deta ils&kursno=220d> (zuletzt eingesehen am 20. September 2010).

<sup>147</sup> BAG-Intranet, *Alles rund um E-Mails*,  
[http://wwwi.bag.admin.ch/stab\\_alg/KOM/intkom/index%20richtlinien.php](http://wwwi.bag.admin.ch/stab_alg/KOM/intkom/index%20richtlinien.php) (zuletzt eingesehen am 20. September 2010).

<sup>148</sup> BAG-Intranet, *Weisung des EDI über die Nutzung der Informatik- und Kommunikationsmittel*, 1. Januar 2005,  
<http://wwwi.bag.admin.ch/edv/allg/sicherheit/> (zuletzt eingesehen am 20. September 2010).

Was die Aufsichtstätigkeiten KUV anbelangt, werden zur Zeit die Prozessabläufe schriftlich festgehalten, womit den Mitarbeitenden ein Hilfsmittel zur Verfügung steht, um sich die erforderliche Sachkompetenz für die Aufsichtstätigkeit selbständig anzueignen. Weitergehende Massnahmen, wie z.B. Workshops oder interne Weiterbildungsveranstaltungen, sind (momentan) nicht vorgesehen.

#### 4.3.3 ZUSAMMENFASSUNG UND SCHLUSSFOLGERUNG

Zwar ist festzuhalten, dass im BAG und auch auf Stufe Bund eine grosse Menge an Compliance-relevanten Informationen vorhanden sind. Allerdings liegt die Verantwortung, sich das notwendige Compliance-Wissen anzueignen, primär bei den Mitarbeitenden selber. Diese müssen sich die erforderlichen Kenntnisse entweder im Selbststudium erarbeiten, oder eine entsprechende Ausbildung beantragen, was wiederum bedingt, dass sie einerseits überhaupt von den Regelungen und Anforderungen in einem bestimmten Compliance-Bereich Kenntnis haben, und sich andererseits ihrer diesbezüglichen fachlichen Defizite bewusst sind. Nur dann wird ein Mitarbeiter von sich aus aktiv Weiterbildungsmaßnahmen ergreifen. Daneben ist natürlich auch die direkte Führungskraft dafür verantwortlich, dass sämtliche ihrer Mitarbeitenden über die notwendigen Kenntnisse verfügen, damit sie ihre Aufgaben korrekt erfüllen können. Bei diesbezüglichen Mängeln kann anlässlich des Personalentwicklungsgesprächs etwa der Besuch einer Weiterbildung als Massnahme angeordnet werden.

Gerade bei den vier untersuchten Compliance-Risiken hat sich gezeigt, dass die Wissensvermittlung vor allem im Selbststudium und auf freiwilliger Basis stattfindet. Es erfolgt auch keine nachträgliche Kontrolle oder Prüfung, ob die Mitarbeitenden die zur Verfügung gestellten Informationen tatsächlich auch genutzt und sich das erforderliche Wissen angeeignet haben. Des Weiteren fehlt es an regelmässigen Wiederholungs-Schulungen. Demnach ist davon auszugehen, dass der Wissensstand bezüglich Compliance-Risiken von Mitarbeiter zu Mitarbeiter höchst unterschiedlich ist. Der Selbststudium-Charakter sowie die Freiwilligkeit der Weiterbildungen dürfte bei den Mitarbeitenden zudem den

Eindruck vermitteln, das Wissen in diesen Bereichen sei weniger wichtig und die Geschäftsleitung ordne ihm auch keine grosse Priorität zu. Unter Umständen trifft dies tatsächlich zu, und es besteht weder das Bedürfnis noch der Wille, die internen Aktivitäten bei der Mitarbeiterschulung zu intensivieren. Will man aber tatsächlich erreichen, dass sämtliche Mitarbeitenden zumindest über die grundlegenden Compliance-Risiken informiert sind, sollte m.E. eine obligatorische Einführungsschulung für neue Mitarbeitende erfolgen, wo ihnen die Compliance-Leitlinien sowie allenfalls weitere wichtige Regelwerke erklärt und das Basiswissen aktiv vermittelt wird. So wird zum einen sichergestellt, dass bei jedem Mitarbeiter ein Minimum an Grundwissen vorhanden ist, und zum anderen können die wichtigsten Dokumente für ein späteres Selbststudium vorgestellt und die zuständigen Ansprechpersonen für Rückfragen oder Unklarheiten benannt werden. Dies wäre eine Art Minimallösung, die später beliebig ausgebaut werden könnte, sowohl inhaltlich als auch durch regelmässige Wiederholungs-Schulungen.

#### 4.4 COMPLIANCE-ORGANISATION

##### 4.4.1 COMPLIANCE-ORGANISATION IM BUND

Auf Stufe Bund fehlt es an Vorgaben bezüglich einer Compliance-Organisation und entsprechend findet sich auch keine den Ämtern übergeordnete Compliance-Stelle, welche die Aktivitäten in diesem Bereich bundesweit koordiniert und die Verwaltungseinheiten bei der Umsetzung berät. Dies steht im Gegensatz zum Riskmanagement und zum IKS, wo mit der Risikopolitik Bund und dem Leitfaden IKS zwei Dokumente vorhanden sind, die für die gesamte Bundesverwaltung gültige Grundsätze festlegen und mit dem EFD bzw. der EFV auch eine zuständige Stelle bezeichnet wird.

##### 4.4.2 COMPLIANCE-ORGANISATION IM BAG

Im BAG wurde bisher weder die Position eines Compliance Officers geschaffen, noch wurde die Compliance Funktion einer bestimmten Person oder einer bestimmten Organisationseinheit zugewiesen. Ent-

sprechend ist diese Position/Aufgabe auch nicht im BAG-Organigramm aufgeführt. Vielmehr sind es verschiedene Akteure innerhalb des BAG, die Compliance-Aufgaben wahrnehmen, teils aufgrund von zugewiesenen Einzelaufträgen, teils im Rahmen ihres amtsinternen Pflichtenhefts. So war es beispielsweise Aufgabe der Rechtsabteilung, die neuen Compliance-Leitlinien zu erarbeiten. Als Schnittstelle zu Compliance fungiert der Risiko-Coach des BAG, der die (Compliance-)Risikomeldungen der Facheinheiten plausibilisiert und zu einem Risikoportfolio konsolidiert. In diesem Zusammenhang sind auch die Risikoeigner der einzelnen Facheinheiten zu erwähnen, die durch Einreichung des Risiko-Meldeformulars an die Sektion Planung, Controlling und Organisationsinstrumente massgeblichen Einfluss darauf haben, dass überhaupt Compliance-Risiken in das Portfolio einfließen. Die Umsetzung der Massnahmen zur Vermeidung des Risikoeintritts obliegt wiederum den zuständigen Abteilungsleitern, die ebenfalls für den notwendigen Kenntnisstand und die dafür erforderliche Ausbildung ihrer Mitarbeitenden Verantwortung tragen.

Die weitaus meisten Compliance-Aufgaben werden jedoch von der Sektion P+O wahrgenommen. Einerseits ist es ihre Aufgabe, Richtlinien und Verhaltensanweisungen an die Mitarbeitenden zu erlassen, andererseits müssen sie die Einhaltung von internen und externen Richtlinien sicherstellen, sei es durch Sanktionen oder die Anordnung von Massnahmen. Wobei hier zu präzisieren ist, dass die Kompetenz zur Eröffnung von Disziplinaruntersuchungen und die Freistellung vom Dienst grundsätzlich dem EDI zukommt (Art. 98 und 103 i.V.m. Art. 2 der Bundespersonalverordnung [BPV, SR 172.220.111.3]).

Das IKS wird separat und unabhängig vom Riskmanagement geführt und liegt in der Prozessverantwortung der Sektion Finanz- und Rechnungswesen<sup>149</sup>. Die im BAG umgesetzte Minimallösung fokussiert primär auf finanzielle Aspekte, Compliance-spezifische Funktionen werden keine wahrgenommen<sup>150</sup>.

---

<sup>149</sup> Interview vom 1. September 2009.

<sup>150</sup> Interview vom 8. September 2009.

#### 4.4.3 ZUSAMMENFASSUNG UND SCHLUSSFOLGERUNG

Wie aufgezeigt, fehlt es dem BAG an einer eigentlichen Compliance-Organisation. Die Funktion des Compliance Officers wird weder von einer bestimmten Person noch einer dafür zuständigen Organisationseinheit wahrgenommen. Die einem Compliance Officer obliegenden Pflichten sind im BAG auf verschiedene Personen und Facheinheiten verteilt. So sind primär die Führungskräfte für das Management von Interessenkonflikten zuständig, allenfalls in Rücksprache mit der Sektion P+O<sup>151</sup>. Der Erlass von Weisungen, Richtlinien und Empfehlungen sowie Kontrolle und Sanktionierung von Regelverletzungen ist Aufgabe der Sektion P+O, dagegen liegt die Information, Aufklärung und Schulung der Mitarbeitenden hauptsächlich im Verantwortungsbereich der Führungskräfte bzw. der Mitarbeitenden selber. Auch die Beratung von Mitarbeitern ist auf verschiedene Stellen verteilt und wird von den direkten Führungskräften, der Sektion P+O und (in der Praxis) auch von der Abteilung Recht wahrgenommen. Die Nachteile einer fehlenden Compliance-Organisation ohne klare Zuweisung von Pflichten und Kompetenzen sind offenkundig. Die Verteilung von Compliance-Aufgaben und Compliance-Kompetenzen auf viele verschiedene Akteure birgt die Gefahr, dass Regeln und Richtlinien uneinheitlich, widersprüchlich oder gar nicht angewendet werden. Will man unter den gegebenen Umständen ein durchschnittliches Compliance-Niveau erreichen, bedingt dies einen erheblichen Koordinationsaufwand mit regelmässigem Informationsaustausch unter sämtlichen involvierten Akteuren. Eine derart formalisierte Informationspflicht besteht jedoch nicht. Des Weiteren erschwert die fehlende Organisation eine amtsinterne Übersicht über Compliance-relevante Aktivitäten und Probleme. Die Berichterstattung an die Amtsleitung dürfte wohl lediglich einzelfallbezogen und eingeschränkt auf bestimmte Compliance-Bereiche erfolgen.

Auch für den einzelnen Mitarbeitenden ist wohl schwer abschätzbar, welche Konsequenzen seine Handlungen haben bzw. bis zu welchem Punkt abweichendes Verhalten toleriert (und auch nicht sanktioniert)

---

<sup>151</sup>BAG-Intranet, *Compliance-Leitlinien*, S. 5, 7 und 10 (*An wen wende ich mich?*), [http://www.wi.bag.admin.ch/b\\_l/p\\_o/neues\\_intranet/Hauptseite/compliance\\_leitlinien/index.php](http://www.wi.bag.admin.ch/b_l/p_o/neues_intranet/Hauptseite/compliance_leitlinien/index.php) (zuletzt eingesehen am 20. September 2010).

wird. Problematisch wäre z.B. der Fall, wo die direkte Führungskraft die Annahme einer offerierten Übernachtung im 5-Sterne Hotel gutheisst und der Mitarbeiter im nachhinein von der Sektion P+O gerügt wird, weil er gegen das Verbot der Geschenk- und Vorteilsannahme verstossen hat. Hierbei gilt es zu bedenken, dass einige Vorgesetzte gegenüber langjährigen Mitarbeitern evtl. toleranter betreffend Regelverletzungen sind, als es etwa eine ausserhalb der Organisationseinheit stehende, unbefangene Person wäre. Die Schaffung einer Compliance-Stelle mit klar definierten Aufgaben und Kompetenzen könnte solchen Problemen vorbeugen und würde klarerweise einen Mehrwert generieren.

## 4.5 BERATUNG

### 4.5.1 BERATUNG IM BUND

Wie unter Kapitel 4.4.1 ausgeführt, gibt es keine zentrale Bundesstelle, welche mit Compliance-Aufgaben betraut ist. Dementsprechend ist auch die Beratung zu Compliance-Risiken nicht zentralisiert, sondern die Mitarbeitenden der Bundesverwaltung müssen sich je nach Risiko an verschiedene Stellen wenden. Bei Fragen im Zusammenhang mit Korruption hat zwar das EPA ein Faltblatt zur Korruptionsprävention herausgegeben, die Beratung der Mitarbeitenden obliegt aber den direkten Vorgesetzten bzw. den zuständigen Stellen der einzelnen Verwaltungseinheiten<sup>152</sup>. Gleiches gilt auch für die Beratung zu Interessenkonflikten. Für Supportfragen zur Informatik steht dagegen das Servicedesk des BIT zur Verfügung<sup>153</sup>.

### 4.5.2 WAHRNEHMUNG DER BERATUNGSFUNKTION IM BAG

Mangels Einrichtung einer Compliance-Stelle im BAG müssen sich die Mitarbeitenden je nach Compliance-Risiko an verschiedene Personen und Organisationseinheiten wenden. Bei Fragen im Zusammenhang mit Interessenkonflikten und Korruption ist primär die direkte Führungskraft

<sup>152</sup> EPA KORRUPTIONSPRÄVENTION, S. 4.

<sup>153</sup> BAG-Intranet, Organisation der Informatik, [http://www.wi.bag.admin.ch/edv/allg/org/org\\_edv.php](http://www.wi.bag.admin.ch/edv/allg/org/org_edv.php) (zuletzt eingesehen am 20. September 2010).

zu kontaktieren. Subsidiär bzw. alternativ steht auch die Sektion P+O für Anfragen zu Verfügung<sup>154</sup>. Was die Internet-Problematik anbelangt, wird zwar nicht explizit auf eine diesbezügliche Beratungsstelle verwiesen, aber da die Regeln zum Umgang mit E-Mails von der Abteilung Kommunikation erlassen wurden, wird diese Stelle auch für allfällige Rückfragen ansprechbar sein. Ebenso können sich die Mitarbeitenden bezüglich IT-Probleme an die Sektion IT- und Facility Management wenden, obschon hier eher Fragestellungen technischer Natur im Vordergrund stehen und weniger solche von Compliance-Relevanz.

Fragen zum Risikobereich der Aufsichtstätigkeiten KUV werden abteilungsintern durch die zuständigen Personen gelöst. Die verschiedenen Aufsichtsthemen sind auf einzelne Mitarbeiter verteilt, die von ihren Kollegen als Spezialisten beigezogen werden. Da hier besondere Fachkenntnisse erforderlich sind, wäre es ohnehin wenig sinnvoll, die Beratung in solchen Fragen einer Compliance-Stelle zu übertragen, die vielmehr generelle, das gesamte Amt betreffende Risikosituationen behandelt.

#### 4.5.3 ZUSAMMENFASSUNG UND SCHLUSSFOLGERUNG

Die fehlende Compliance-Organisation im BAG widerspiegelt sich unmittelbar in der Beratungsfunktion. Aufgrund der Zuordnung von Compliance-Aufgaben an verschiedene Organisationseinheiten und Personen dürfte für den einzelnen Mitarbeitenden nicht immer ersichtlich sein, an welche Stelle er sich bei Fragen bezüglich des korrekten Vorgehens wenden soll. Zudem besteht erhebliche Gefahr, dass die Beratung je nach zuständiger Person unterschiedlich ausfällt (z.B. erachtet ein Abteilungsleiter die Annahme eines bestimmten Geschenks als unproblematisch, wogegen ein anderer in einer ähnlichen Situation die Annahme nicht gutheisst). Des weiteren ist unklar, welchen Stellenwert die Beratung überhaupt hat. Entscheidet sich beispielsweise eine Fachinheit trotz gegenteiliger Stellungnahme der Rechtsabteilung einen

---

<sup>154</sup> BAG-Intranet, *Compliance-Leitlinien*, S. 5, 7 und 10 (An wen wende ich mich?), [http://www.wi.bag.admin.ch/b\\_1/p\\_o/neues\\_intranet/Hauptseite/compliance\\_leitlinien/index.php](http://www.wi.bag.admin.ch/b_1/p_o/neues_intranet/Hauptseite/compliance_leitlinien/index.php) (zuletzt eingesehen am 20. September 2010).



juristisch fehlerhaften Vertrag zu unterzeichnen, bestehen kaum Interventionsmöglichkeiten. Auch dies ist Folge der fehlenden Zuordnung von Kompetenzen an eine für solche Aufgaben bestimmte Compliance-Stelle. Im Sinne einer einheitlichen Anwendung der rechtlichen Vorschriften wäre folglich zu empfehlen, für generelle, das gesamte Amt betreffende Compliance-Risiken nur eine einzige Beratungsstelle - im Idealfall die noch zu schaffende Stelle eines Compliance Officers - zu bezeichnen.

## 4.6 ÜBERWACHUNG

### 4.6.1 KONTROLLE UND ÜBERWACHUNG IM BUND

Die Verwaltungseinheiten des Bundes sind insbesondere bezüglich der Finanzen einem rigorosen Controlling- und Reporting-System unterworfen (vgl. FHG, FHV, FKG). Die Einhaltung der rechtlichen Vorgaben wird durch die Eidgenössische Finanzkontrolle überprüft, teils durch Stichproben (Art. 6 FKG). Unter anderem wird auch geprüft, ob die EDV-Anwendungen im Bereich des Finanzgebarens die erforderliche Sicherheit und Funktionalität aufweisen und ob die vom Informatikrat (IRB) erlassenen Weisungen eingehalten werden (Art. 6 lit. h FKG). In Bezug auf Interessenkonflikte besteht (soweit ersichtlich) auf Stufe Gesamtbund keine institutionalisierte Reportingpflicht oder Kontrolle. Der Vollständigkeit halber sei an dieser Stelle noch auf die präventive Rechtskontrolle durch das Bundesamt für Justiz (BJ) hingewiesen, welches sämtliche Entwürfe für rechtsetzende Erlasse auf ihre Verfassungs- und Gesetzmässigkeit, auf ihre Übereinstimmung und Vereinbarkeit mit dem geltenden nationalen und internationalen Recht, auf ihre inhaltliche Richtigkeit sowie, in Zusammenarbeit mit der Bundeskanzlei, auf ihre gesetzestechnische und sprachlich-redaktionelle Angemessenheit überprüft (Art. 7 Abs. 3 Organisationsverordnung für das Eidgenössische Justiz- und Polizeidepartement [OV-EJPD; SR 172.213.1]). Die in vorliegender Arbeit thematisierten Risikobereiche beschlagen jedoch nicht Rechtsetzungsprozesse, sondern Problemsituationen, welche sich aus alltäglichen Verwaltungstätigkeiten ergeben, weshalb die spezifische Kontrollfunktion des BJ hierbei gerade nicht von Relevanz ist.

Zur Zeit besteht für die Bundesverwaltung keine gesetzliche Regelung, welche die Mitarbeitenden verpflichtet, festgestellte Unregelmässigkeiten zu melden<sup>155</sup>. Bei Korruptionsverdacht kann bei der EFK per E-Mail oder telefonisch Meldung erstattet werden, wobei die Anonymität des Whistleblowers gewahrt wird<sup>156</sup>. In der Praxis wird diese Plattform jedoch wenig genutzt, da sie bei den Mitarbeitenden der Bundesverwaltung kaum bekannt ist. Beim Staatssekretariat für Wirtschaft (SECO) gehen gemäss GRECO<sup>157</sup>-Evaluationsbericht pro Jahr durchschnittlich gerade mal zwischen fünf bis zehn Meldungen ein<sup>158</sup>. Der Entwurf zum Bundesgesetz über die Organisation der Strafbehörden des Bundes (StBOG) wurde jedoch zum Anlass genommen, einen neuen Artikel 22a mit dem Titel "Anzeigepflichten, Anzeigerechte und Schutz" in das Bundespersonalgesetz (BPG; SR 172.220.1) aufzunehmen. Absatz 1 dieses Artikels verpflichtet die Angestellten, alle von Amtes wegen zu verfolgende Verbrechen oder Vergehen, die sie bei ihrer amtlichen Tätigkeit festgestellt haben, den Strafverfolgungsbehörden, ihren Vorgesetzten oder der EFK zu melden. Des Weiteren sind sie gemäss Absatz 4 berechtigt, andere Unregelmässigkeiten der EFK zu melden, welche den Sachverhalt abklärt und die notwendigen Massnahmen trifft<sup>159</sup>. Gemäss Botschaft handelt es sich bei diesen Unregelmässigkeiten nicht nur um strafrechtliche Vorwürfe, sondern beispielsweise auch um verschwenderische oder unnötige Ausgaben<sup>160</sup>. Mit diesem neuen Gesetzesartikel werden die Empfehlungen der GRECO und der Arbeitsgruppe der OECD gegen Korruption im internationalen Handelsverkehr umgesetzt.

#### 4.6.2 COMPLIANCE-ÜBERWACHUNG IM BAG

Das BAG verfügt über diverse Kontrollinstrumente. So gelangt etwa das Vier-Augen-Prinzip zur Anwendung, und wichtige Dokumente werden ohnehin immer in die Linie gegeben und letzten Endes sogar von mehr als vier Augen kontrolliert. Einige Fachbereiche arbeiten auch mit

<sup>155</sup> CARRANZA/MICOTTI, S. 990; GRECO-EVALUATIONSBERICHT, Rz. 130.

<sup>156</sup> EPA KORRUPTIONSPRÄVENTION, S. 5.

<sup>157</sup> Groupe d'Etats contre la Corruption.

<sup>158</sup> GRECO-EVALUATIONSBERICHT, Rz. 155.

<sup>159</sup> BBl 2008 8189, 8209.

<sup>160</sup> BBl 2008 8125, 8182.

Checklisten (z.B. Rechtsetzung) und als EDV-Hilfsmittel wird im BAG das elektronische Geschäftserfassungssystem iGeko verwendet, wo sämtliche relevanten Dokumente eines Geschäfts abgelegt werden und nachvollziehbar ist, wer wann welche Handlung vorgenommen hat. Dagegen sind regelmässige Mitarbeiterbefragungen oder Prüfungen der Prozessabläufe für die in der vorliegenden Arbeit behandelten vier Risikobereiche nicht vorgesehen.

Betreffend die Risiken im Risikoportfolio des BAG wird von den Fach-einheiten anlässlich der periodischen Steuerungsrounds ein Statusbericht eingefordert<sup>161</sup>. Zum Risiko Aufsichtstätigkeiten KUV findet in dem Sinne ein institutionalisiertes Reporting statt. Dagegen fallen Compliance-Risiken, die nicht ins Risikoportfolio aufgenommen wurden, aus diesem "Reporting-Netz" heraus. So ist innerhalb des Amtes kein spezifisches Reporting für die Compliance-Risiken Korruption, Interessenkonflikte und Internet-Problematik vorgesehen. Da es an einer zentralen Compliance-Stelle fehlt, die Meldungen zum Fehlverhalten in diesen Bereichen sammelt und gebündelt an die Direktion weiterleitet, erfolgt die Information höchstens einzelfallbezogen durch die zuständige Führungskraft direkt an die Geschäftsleitung.

BAG-intern besteht keine Whistleblowing-Hotline bzw. eine Anlaufstelle für solche Meldungen. Stellt ein Mitarbeiter Unregelmässigkeiten fest, kann er dies entweder seinem Vorgesetzten oder der EFK melden, wobei er sich in aller Regel wohl für Letztere entscheiden dürfte, da dort seine Anonymität gewährleistet ist<sup>162</sup>.

#### 4.6.3 ZUSAMMENFASSUNG UND SCHLUSSFOLGERUNG

Grundsätzlich scheinen die Kontrollmechanismen innerhalb des BAG gut zu funktionieren. Durch die Kontrolle von Dokumenten innerhalb der Linie sowie allenfalls zusätzlich durch die Rechtsabteilung sollten Regelverstösse in der Regel erkannt werden. In Bezug auf das Reporting zu Compliance-Risiken fehlt es an klaren Regeln, an wen wann und in welcher Form Bericht zu erstatten ist. Da dies schlussendlich im Ermes-

<sup>161</sup> Vgl. *Interview vom 1. September 2009.*

<sup>162</sup> *EPA KORRUPTIONSPRÄVENTION*, S. 5.

sen der zuständigen Führungskräfte liegt, dürfte die Berichterstattung sehr heterogen sein, was wiederum einer Gesamtübersicht zu den festgestellten Compliance-Verletzungen abträglich ist. Dieses Problem ist natürlich ebenfalls direkte Konsequenz der fehlenden Compliance-Organisation (vgl. Kapitel 4.4).

Auch bezüglich Whistleblowing besteht im BAG und in der Bundesverwaltung Verbesserungsbedarf. Zu begrüßen ist sicherlich die Aufnahme von Artikel 22a in das Bundespersonalgesetz, womit das Whistleblowing in der Bundesverwaltung auf eine gesetzliche Basis gestellt wird. Wünschenswert wäre allerdings, dass mit Inkrafttreten des neuen Artikels auch die Anlaufstelle für Whistleblower der EFK innerhalb der Bundesverwaltung vermehrt als solche in Erscheinung tritt. Konsultiert man nämlich die Web-Site der EFK, wird nicht auf ihre spezifische Funktion im Zusammenhang mit Whistleblowing hingewiesen. Beinahe scheint es so, als wolle man diesen Aspekt ihrer Tätigkeit vor den Bundesangestellten verheimlichen. Whistleblowing kann jedoch nur dann als Instrument zur Aufdeckung von Missständen von Nutzen sein, wenn der potentielle Whistleblower weiss, an wen er sich wenden muss, und keine Repressalien zu befürchten hat. Insofern ist mit Inkrafttreten von Art. 22a BPG allein noch nichts gewonnen.

## 4.7 SANKTIONSSYSTEM

### 4.7.1 SANKTIONSSYSTEM DES BUNDES

Bei Verletzung von arbeitsrechtlichen Pflichten steht gemäss Artikel 99 BPV eine ganze Palette von Disziplinar massnahmen zur Verfügung: Verwarnung, Verweis, Änderung des Aufgabenkreises, Lohnkürzung von höchstens 10% während längstens eines Jahres, Busse bis zu Fr. 3'000, Änderung der Arbeitszeit und Änderung des Arbeitsortes. Je nach Schwere des Regelverstosses kann auch eine fristlose Kündigung in Betracht fallen (Art. 12 Abs. 7 BPG). Betreffend Korruption sind die strafrechtlichen Bestimmungen der Artikel 322<sup>quater</sup> StGB (sich bestechen lassen) sowie Artikel 322<sup>sexies</sup> StGB (Vorteilsannahme) relevant. Die Disziplinarrechtliche Zuständigkeit innerhalb der Bundesverwaltung

wird von den Departementen geregelt, sofern es sich nicht um hohe Bundesangestellte handelt, wofür der Bundesrat zuständig bleibt (Art. 2 BPV).

#### 4.7.2 SANKTIONSSYSTEM DES BAG

Auf Stufe Departement ist bezüglich der Internet-Problematik die Weisung des EDI über die Nutzung der Informatik- und Kommunikationsmittel massgebend. Art. 15 dieser Weisung sieht Massnahmen bei unzulässiger Nutzung von IKT-Mitteln vor<sup>163</sup>. So kann der Linienvorgesetzte oder die Amtsleitung anordnen, dass ein Benutzer bestimmte IKT-Mittel nur noch zu dienstlichen Zwecken oder gar nicht mehr verwenden darf. Für weitere Disziplinar-massnahmen wird auf die Personalgesetzgebung und für strafrechtlich relevante Verstösse auf die zuständige Strafjustizbehörde verwiesen.

Das BAG selber hat keine spezifischen Disziplinar-massnahmen zu den vier untersuchten Compliance-Risiken erlassen.

#### 4.7.3 ZUSAMMENFASSUNG UND SCHLUSSFOLGERUNG

Die Sanktionen bei Regelverstössen von Bundesangestellten sind im Wesentlichen in der Bundespersonalgesetzgebung zu finden (BPG und BPV). Weiterführende oder zusätzliche disziplinarische Massnahmen sind im BAG nicht vorhanden, abgesehen von Artikel 15 der Weisung des EDI über die Nutzung der IKT-Mittel. Da Artikel 99 BPV die potentiellen Sanktionen lediglich nach dem Kriterium Fahrlässigkeit und Vorsatz/Grobfahrlässigkeit unterscheidet, ansonsten aber keine weiteren Rahmenbedingungen betreffend der Anordnung von Massnahmen festlegt, verfügen die Departemente diesbezüglich über einen erheblichen Ermessensspielraum. Entsprechend uneinheitlich dürfte das Disziplinarrecht innerhalb der Bundesverwaltung wohl angewendet werden. Innerhalb des BAG fristet das Sanktionswesen eher ein stiefmütterliches

---

<sup>163</sup> BAG-Intranet, Weisung des EDI über die Nutzung der Informatik- und Kommunikationsmittel, 1. Januar 2005, <http://www.wi.bag.admin.ch/edv/allg/sicherheit/> (zuletzt eingesehen am 20. September 2010).

Dasein. Gemäss Auskunft des Leiters der Sektion P+O werden kaum je disziplinarische Massnahmen angeordnet oder fristlose Kündigungen ausgesprochen. Die Entlassung einer BAG-Mitarbeiterin wegen Verletzung der Treupflicht ist vor diesem Hintergrund eher als Ausnahme zu werten<sup>164</sup>. Wie in Kapitel 3.6.8 erwähnt, ist ein Sanktionssystem jedoch nur dann wirksam, wenn es auch konsequent angewendet wird. Insofern scheint das Bundesdisziplinarrecht im BAG nur wenig Wirksamkeit zu entfalten. Vielmehr besteht der Eindruck, die Mitarbeitenden würden sich auf die tolerante Haltung ihres Vorgesetzten verlassen, als dass sie disziplinarische Massnahmen fürchten.

#### 4.8 SYNTHESE

In nachfolgender Tabelle werden im Sinne einer Übersicht die wesentlichen gewonnenen Erkenntnisse in geraffter Form zusammengestellt.

Compliance-Elemente	Situation im BAG	Empfehlung	Nutzen
Risikoanalyse* (4.1)	Fehlende Übersicht über Compliance-Risiken, da diese nur teilweise vom Risikoportfolio erfasst werden	Risikoanalyse auf alle Compliance-Risiken ausdehnen	Risiken können frühzeitig erkannt und entsprechende Massnahmen zur Reduktion eingeleitet werden
Regeln und Richtlinien (4.2)	Compliance-Leitlinien vorhanden, aber diese beschränken sich auf zwei Compliance-Risiken	Weitere risikorelevante Verhaltensweisen in die Compliance-Leitlinien aufnehmen	Bei Mitarbeitenden wird ein Bewusstsein für Gefahrenbereiche geschaffen und damit Fehlverhalten reduziert
Vermittlung des Compliance-	Sehr heterogener Wissensstand über relevante Risiken bei	Obligatorische Einführungsschulung zum Thema Compli-	Den Mitarbeitenden wird ein minimales Grund-

<sup>164</sup> Vgl. Beobachter Online, Ausgabe 9/09, *Zu wenig Schutz für Mutige*, [http://www.beobachter.ch/justiz-behoerde/artikel/missstaende-aufdecken\\_zu\\_wenig-schutz-fuer-mutige/](http://www.beobachter.ch/justiz-behoerde/artikel/missstaende-aufdecken_zu_wenig-schutz-fuer-mutige/) (zuletzt eingesehen am 20. September 2010).

Wissens (4.3)	Mitarbeitenden	ance für Mitarbeitende	wissen über Compliance vermittelt, und somit korrektes Verhalten gefördert
Compliance-Organisation (4.4)	Keine eigentliche Compliance-Organisation vorhanden	Schaffung einer Compliance-Stelle mit klar definierten Aufgaben und Kompetenzen	Einheitliche Auslegung von Regeln und Richtlinien, klar Zuständigkeiten, Übersicht und vereinfachte Koordination von Compliance-Aktivitäten
Beratung (4.5)	Beratungsfunktion ist verteilt auf verschiedene Personen und Organisationseinheiten	Bezeichnung einer einzigen Beratungsstelle für Compliance-Angelegenheiten (Compliance-Stelle bzw. Compliance-Officer)	Nutzung von Synergien beim Beratungsaufwand, einheitliche Anwendung der rechtlichen Vorschriften
Überwachung (4.6)	Kontrollmechanismen funktionieren gut innerhalb des BAG; noch unbefriedigende Regelung des Whistleblowing im Bund	Bestehende Kontrollinstrumente beibehalten; Ausbau des Whistleblowing	Aufdeckung von Missständen
Sanktionssystem (4.7)	Kaum je Anordnung disziplinarischer Massnahmen	Sanktionssystem konsequent umsetzen	Prävention durch abschreckende Wirkung

\* Die Risikoanalyse ist zwar kein Compliance-Element im engeren Sinne, wird der Einfachheit halber jedoch in dieser Spalte aufgeführt, da sie unabdingbare Voraussetzung für den Aufbau eines Compliance-Management-Systems ist (vgl. Kapitel 3.6.1).

## 5 SCHLUSSFOLGERUNGEN UND EMPFEHLUNGEN

Die Analyse im 4. Kapitel hat aufgezeigt, dass sowohl auf Stufe Gesamtbund als auch im BAG bestimmte Compliance-Elemente vorhanden sind und auch umgesetzt werden. Ein Compliance-Management-System in eigentlichen Sinne besteht jedoch nicht, da es insbesondere am zentralen Element der Compliance-Organisation mangelt. Auf Stufe Bund sind die EFV (Riskmanagement, IKS, Controlling), das EPA (Nebenbeschäftigungen, Korruption, Ausbildung) sowie die EFK (Finanzkontrolle, Whistleblowing) diejenigen Bundestellen, welche bisher im Compliance-Bereich aktiv waren. Die bisherigen Aktivitäten erfolgten jedoch gerade nicht unter dem Titel "Compliance", sind deshalb kaum koordiniert und tendenziell auf einzelne Aspekte der Compliance-Problematik limitiert. Entsprechend fragmentarisch und unübersichtlich sind die auf Bundesebene vorhandenen Vorgaben und Unterlagen zu dieser Thematik. Auch im BAG sind verschiedene Stellen (Rechtsabteilung, Sektion P+O, Sektion Planung, Controlling und Organisationsinstrumente, Sektion Finanz- und Rechnungswesen) mit Compliance befasst, ohne dass die Compliance-Funktion jedoch einer bestimmten Organisationseinheit oder einer bestimmten Person zugewiesen wird. Es liegt also eine Diskrepanz zwischen Corporate-Compliance auf Stufe Bund und Group-Compliance auf Amtsebene vor. Einerseits gibt der Bund bestimmte für die gesamte Bundesverwaltung gültige Massstäbe vor (z.B. Korruption, Riskmanagement, IKS), die konkrete Implementierung und Umsetzung obliegt jedoch den einzelnen Ämtern. Somit haben wir es mit einer relativ schwach ausgestalteten Corporate-Compliance auf Gesamt-Bundesebene, die lediglich die Rahmenbedingungen festlegt, und einer sehr heterogenen Group-Compliance auf Ebene der Verwaltungseinheiten zu tun.

Das Fehlen eines Compliance-Management-Systems bringt folgende Probleme mit sich:

- Fehlende Übersicht über die Compliance-Risiken im Bund und im BAG
- Fehlende Übersicht über relevante Regeln und Richtlinien



- Gefahr von Doppelspurigkeiten und Wiederholungen von Vorschriften
- Fehlende obligatorische Vermittlung von Compliance-Wissen an die Mitarbeitenden
- Unklare Zuständigkeiten und Kompetenzen
- Gefahr der uneinheitlichen und widersprüchlichen Anwendung der Compliance-Regeln
- Keine klaren Vorgaben zum Reporting in Compliance-Angelegenheiten
- Ungenügende Umsetzung des Whistleblowing
- Keine konsequente Durchsetzung von Sanktionen

Ist für den einzelnen Mitarbeiter nicht klar, welche Regeln nun gelten und wer für einen bestimmten Bereich zuständig ist, und fehlt es an einer konsequenten Sanktionierung von Fehlverhalten, so besteht eine erhöhte Gefahr von Rechtsverletzungen. Diese können unabsichtlich geschehen (z.B. mangelndes Wissen aufgrund fehlender Ausbildung) oder in Ausnutzung von regulatorischen Lücken oder unkundigen Vorgesetzten absichtlich begangen werden. So hat sich etwa eine Sachbearbeiterin des BAG bei Entdeckung der geplanten Kampagne gegen die Volksinitiative "Ja zur Komplementärmedizin" direkt an die Medien gewandt, da sie einerseits nicht wusste, dass es im Bund überhaupt eine Anlaufstelle für Whistleblower bei der EFK gibt, und andererseits der EFK auch nicht zutraut, einen solchen Missstand beheben zu können. Vielmehr brauche es eine unabhängige Stelle, die auch rechtliche Hilfe biete<sup>165</sup>. Mit der Einrichtung einer vertrauenswürdigen und kompetenten Meldestelle und entsprechender Information der Mitarbeiter hätte der durch die Veröffentlichung der Informationen resultierende Reputationsschaden wohl vermieden werden können. Je besser die Mitarbeitenden bezüglich Compliance-Risiken ausgebildet sind und je klarer Zu-

---

<sup>165</sup> Vgl. *Beobachter Online*, Ausgabe 9/09, *Zu wenig Schutz für Mutige*, [http://www.beobachter.ch/justiz-behoerde/artikel/missstaende-aufdecken\\_zu-wenig-schutz-fuer-mutige/](http://www.beobachter.ch/justiz-behoerde/artikel/missstaende-aufdecken_zu-wenig-schutz-fuer-mutige/) (zuletzt eingesehen am 20. September 2010).

ständigkeiten und Kompetenzen geregelt sind, desto geringer ist die Fehlerquote und damit das Risiko von Rechtsverletzungen.

Als Resultat der Analyse ist somit festzuhalten, dass das Management von Rechts- und Reputationsrisiken auf Stufe Gesamtbund und im BAG zur Zeit verbesserungsfähig ist. Zwar sind verschiedene Bestrebungen auf Bundes- und Amtsstufe im Gange, um dieses Manko zu beheben, allerdings gehen diese viel zu wenig weit und entfalten deshalb kaum risikominimierende Wirkung. Die Einführung eines Compliance-Management-Systems könnte hier einen substantiellen Beitrag zur Verminderung der Compliance-Risiken des BAG leisten. Als erster Schritt ist die Schaffung einer zuständigen Compliance-Stelle auf Bundesstufe (z.B. beim EPA) und innerhalb des BAG (Compliance-Officer) zu empfehlen. Wenn sämtliche Compliance-Aktivitäten gebündelt von einer Stelle ausgehen, werden Doppelspurigkeiten und damit Unklarheiten vermieden, die Zuständigkeit bei Beratungsbedürfnissen ist klar geregelt und der Reporting- sowie Informationsfluss in Compliance-Angelegenheiten läuft in vorgegebenen Bahnen. Des weiteren kann ein Compliance-Officer der Geschäftsleitung eine Übersicht über die Compliance-Risiken des BAG liefern und spezifische Massnahmen zur Risikovermeidung vorschlagen (z.B. im Bereich der Mitarbeiterausbildung, des Controlling oder der Schaffung von Regeln und Richtlinien). Die Einführung eines Compliance-Management-Systems hat also in mehrfacher Hinsicht einen unmittelbaren Nutzen für das BAG. Demnach lässt sich die eingangs gestellte Forschungsfrage positiv beantworten, da die Schaffung eines solchen Systems tatsächlich einen Mehrwert für das Amt generiert. Auch eine Mehrheit der interviewten Personen beurteilt dies grundsätzlich ähnlich, wenn auch unterschiedliche Ansichten darüber bestehen, wie Compliance konkret umzusetzen wäre. Dies sollte jedoch kein Hindernis für eine grundsätzliche Einführung darstellen. Compliance ist, wie dargelegt, eben gerade kein vorgefertigtes, starres System, sondern kann äusserst flexibel für jedes privatwirtschaftliche und öffentlichrechtliche Unternehmen je nach seinen Bedürfnissen massgeschneidert werden.

Unter dem Eindruck der als "Finanzkrise" bekannten Verwerfungen im globalen Finanzsystem in den vergangenen zwei Jahren könnte man

durchaus zum Schluss gelangen, dass Compliance in der praktischen Umsetzung versagt hat und nicht geeignet ist, um Rechts- und Reputationsrisiken zu verhindern. Dieses Fazit wäre wohl etwas voreilig und unreflektiert. M.E. scheint es eher so, dass Compliance allein nicht ausreicht, um eine regelkonformes Verhalten der Mitarbeiter sicherzustellen. Vielmehr bedarf es auch an Integrität, ohne welche Compliance nicht denkbar ist<sup>166</sup>. Compliance allein besagt lediglich, was man tun oder unterlassen muss, weil man es soll. Dagegen bedeutet Integrität, dass man das will, was man aufgrund eigener Reflexion soll<sup>167</sup>. Damit Compliance erfolgreich ist, braucht es in einem Unternehmen also ein solides ethisches Umfeld, dem sich jeder Mitarbeiter stellen muss. Entsprechend ist die Antwort zur Forschungsfrage mit einem "aber" zu ergänzen. Die Einführung von Compliance kann nämlich nur dann einen Mehrwert generieren, wenn der Code of Conduct kein zahnloser Papiertiger bleibt, sondern das Management die kodifizierten Regelungen und ethischen Werte auch tatsächlich vorlebt und bereit ist, bei Fehlverhalten die entsprechenden Konsequenzen zu ziehen, und zwar bis hinauf in die höchsten Führungsebenen.

Im Gegensatz zu privatwirtschaftlichen Unternehmen, wo das Primat der Gewinnmaximierung gilt, arbeitet der Staat nicht gewinnorientiert, sondern ist dem öffentlichen Interesse verpflichtet. Sein Ziel ist also nicht einseitig auf die Erhöhung des Shareholder Values ausgerichtet. Entsprechend besteht für Mitarbeitende der öffentlichen Verwaltung wenig Anreiz, durch das Eingehen von hohen Risiken oder die absichtliche Missachtung von Normen einen möglichst hohen Gewinn zu erzielen und dadurch Vorteile in Form von Bonuszahlungen oder internen Aufstiegsmöglichkeiten zu erlangen. Die Hauptgefahr von Regelverletzungen bei Verwaltungstätigkeiten liegt somit weniger bei absichtlich begangenen Widerhandlungen, sondern eher im fahrlässigen Bereich, wo Fehler aufgrund mangelnden Wissens über relevante rechtliche Regelungen und Vorgaben geschehen.

Die Aufgaben des Staates sind in den letzten Jahren deutlich umfangreicher und komplexer geworden, gleichzeitig werden neue Führungsin-

---

<sup>166</sup> Vgl. THIELEMANN, *Compliance und Integrity*, S. 14.

<sup>167</sup> RÖTH, *Compliance, Integrität und Regulierung*, S. 48.

strumente für das Management nur zögerlich und sehr heterogen eingeführt (z.B. IKS). Entsprechend ist Compliance m.E. ein geeignetes Instrument, um dem Management eine solide und regelkonforme Amtsführung zu erleichtern. Gerade weil Compliance kein starres System ist, sondern in seinem Umfang und seiner materiellen Tiefe sehr flexibel und für jedes Unternehmen individuell ausgestaltet werden kann, kann es auch problemlos im öffentlichen Sektor eingeführt werden. Dies scheint umso mehr angezeigt, als dass Riskmanagement und IKS bereits umgesetzt sind und Compliance die ideale Ergänzung zu diesen beiden Elementen ist, um ein integriertes Riskmanagementsystem gemäss CO-SO zu schaffen.

## ANHANG

Mitteilung "Masshalten beim Zugriff auf Facebook", GS-EDI, 6. Mai 2009:



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra

Eidgenössisches Departement des Innern EDI  
Generalsekretariat GS-EDI

### Mitteilung

06.05.2009

---

#### **Masshalten beim Zugriff auf Facebook**

Geschätzte Mitarbeiterinnen und Mitarbeiter

In der Bundesverwaltung wird die private Nutzung der Büroinfrastruktur (Telefon, Natel, Kopiergerät, Mail, Internetzugang etc.) toleriert, sofern dies in einem vernünftigen Mass erfolgt.

Das neueste und vielleicht beliebteste Kommunikationsmittel im Web ist Facebook. In der Bundesverwaltung ist der Zugriff auf Facebook die zweithäufigste Art des Internetzugriffs ist. 25% der gesamten Datenmenge, die vom Internet heruntergeladen wird, wird durch Facebook verursacht.

Diese gewaltige Datenmenge belastet unsere Netzwerkinfrastruktur und beeinträchtigt damit die geschäftliche Nutzung des Internets.

Trotzdem wollen wir den Zugriff auf Facebook nicht einfach per sofort verbieten. Stattdessen vertrauen wir darauf, dass die Bundesangestellten in Eigenverantwortung die Nutzung von Facebook für private Zwecke unterlassen und die technische Sperrung von Facebook somit nicht notwendig sein wird.

Das Bundesamt für Informatik und Telekommunikation (BIT) wird die Situation beobachten und die Generalsekretärenkonferenz (GSK) wird zu einem späteren Zeitpunkt eine neue Lagebeurteilung vornehmen.

Mit freundlichen Grüßen

Der Generalsekretär

Pascal Strupler

## BIBLIOGRAPHIE

### LITERATUR

Die nachfolgenden Autoren werden, wo nicht anders angegeben, mit ihrem Namen sowie der Randziffer oder der Seitenzahl der Fundstelle zitiert.

BACHMANN DANIEL, Compliance - Rechtliche Grundlagen und Risiken, in: Der Schweizer Treuhänder, Ausgabe 1-2/2007, S. 93 ff.

BAUER SILVIA C., Datenschutzrechtliche Compliance im Unternehmen, in: Gregor Wecker/Hendrik van Laak (Hrsg.), Compliance in der Unternehmerpraxis, 2. Aufl., Wiesbaden 2009, S. 169 ff.

BUFF HERBERT, Compliance, Diss., Zürich 2000.

CARRANZA CARLOS JAICO/MICOTTI SÉBASTIEN, Whistle-Blowing: problèmes et perspectives, in: AJP 8/2007, S. 981 ff.

HAEFELIN ULRICH/MÜLLER GEORG/UHLMANN FELIX, Allgemeines Verwaltungsrecht, 5. Aufl., Zürich/St. Gallen 2006.

HAUSCHKA CHRISTOPH E., Allgemeine Unternehmensorganisation, in: Christoph E. Hauschka (Hrsg.), Corporate Compliance, Handbuch der Haftungsvermeidung im Unternehmen, München 2007, S. 1 ff.

HOFSTETTER BRIGITTE, Interessenkonflikte im Universalbankensystem, Diss., Bern 1999.

JÄGER AXEL/RÖDL CHRISTIAN/CAMPOS NAVE JOSÉ A., Praxishandbuch Corporate Compliance, 1. Aufl., Weinheim 2009.

KIMMICH PETER, Effective Corporate Compliance Programs: The Impact of the 2004 Amendments to the U.S. Federal Sentencing Guidelines for Organizations, Diss., St. Gallen 2006.

KLOTZ MICHAEL/DORN DIETRICH-W., IT-Compliance - Begriff, Umfang und relevante Regelwerke, in: Knut Hildebrand/Stefan Meinhardt (Hrsg.), Compliance & Risk Management, Praxis der Wirtschaftsinformatik, HMD Heft 263, Heidelberg 2008, S. 5 ff.

LAMPERT THOMAS, Compliance-Organisation, in: Christoph E. Hauschka (Hrsg.), Corporate Compliance, Handbuch der Haftungsvermeidung im Unternehmen, München 2007, S. 142 ff.

MATHEWS M., Codes of Ethics: Organizational Behavior and Misbehavior, in: W. Frederick (Hrsg.), Research in Corporate Social Performance, JAI Press, Connecticut 1987, S. 107 ff.

MC KENDALL M.A./WAGNER J.A., Motive, Opportunity, Choice, and Corporate Illegality, Organization Science, Vol. 8, Nr. 6, 1997, S. 624 ff.

MC KENDALL M.A./DE MARR B./JONES-RIKKERS C., Ethical Compliance Programs and Corporate Illegality: Testing the Assumptions of the Corporate Sentencing Guidelines, Journal of Business Ethics, Vol. 37, Nr. 4, S. 367 ff.

MÜLLER THOMAS, Compliance-Management, Dargestellt am Beispiel der Versicherungswirtschaft, Zürich/Basel/Genf 2007.

PANT MICHAEL, Versicherungslösungen, in: Christoph E. Hauschka (Hrsg.), Corporate Compliance, Handbuch der Haftungsvermeidung im Unternehmen, München 2007, S. 272 ff.

ROTH MONIKA, Compliance: Begriff Bedeutung Beispiele, Basel/Genf/München 2000 (*zit. Compliance*).

ROTH MONIKA, Compliance, Integrität und Regulierung, Ein wirtschaftlicher Ansatz in 10 Thesen, Zürich/Basel/Genf 2005 (*zit. Compliance, Integrität und Regulierung*).

ROTH MONIKA, Good Corporate Governance: Compliance als Bestandteil des internen Kontrollsystems, Ein Handbuch für die Praxis, Zürich/St. Gallen 2007 (*zit. Good Corporate Governance*).

ROTH MONIKA/ERNI MARIO, Regulation und Reputation, Der Finanzplatz Schweiz und die Compliance seiner Unternehmen, Zürich/St. Gallen 2008.

TARANTINO ANTHONY, Manager's guide to compliance, Best practice and case studies, New Jersey 2006.

THELESKLAF DANIEL, Outsourcing von Compliance-Dienstleistungen, Compliance als Teil des Risk Managements, in: Der Schweizer Treuhänder, Ausgabe 5/2001, S. 447 ff.

THIELEMANN ULRICH, Compliance und Integrity - Zwei Seiten ethisch integrierter Unternehmenssteuerung, Lektionen aus dem Compliance-Management eines Nahrungsmittelkonzerns und einer Grossbank, St. Gallen 2005 (*zit. Compliance und Integrity*).

THIELEMANN ULRICH, Der Fall Enron(s), Ein Anlass, über den wirtschaftlichen Status von Managementintegrität nachzudenken, in: Forum Wirtschaftsethik, 2/2005, S. 37 ff., Fundstelle: <http://www.alexandria.unisg.ch/EXPORT/DL/29219.pdf> (*zit. Der Fall Enron*).

VETTER EBERHARD, Compliance in der Unternehmerpraxis, in: Gregor Wecker/Hendrik van Laak (Hrsg.), Compliance in der Unternehmerpraxis, 2. Aufl., Wiesbaden 2009, S. 33 ff.

WECKER GREGOR/GALLA STEFAN, Pflichten der Geschäftsleitung & Aufbau einer Compliance Organisation, in: Gregor Wecker/Hendrik van Laak (Hrsg.), Compliance in der Unternehmerpraxis, 2. Aufl., Wiesbaden 2009, S. 49 ff.

## GRUNDLAGEN / MATERIALIEN:

### **Basler Ausschuss für Bankenaufsicht**

BASEL COMMITTEE ON BANKING SUPERVISION, Compliance and the compliance function in banks, April 2005.

### **Bundesamt für Gesundheit (BAG)**

RISIKOBEURTEILUNG BAG, Erste operative Steuerungsrunde 2009 - Risikobeurteilung, 8. Mai 2009.

### **Bundesamt für Privatversicherungen (BPV)**

BPV-RICHTLINIE 15/2006 zur Corporate Governance, zum Risikomanagement und zum Internen Kontrollsystem, 1. Januar 2007, Fundstelle:



<http://www.finma.ch/archiv/bpv/d/dokumentation/00548/00613/01081/index.html?lang=de> (zuletzt eingesehen am 20. September 2010).

### **Economiesuisse**

SWISS CODE OF BEST PRACTICE FOR CORPORATE GOVERNANCE, Juli 2002, Fundstelle:

[http://www.economiesuisse.ch/web/de/pdf%20download%20files/pospap\\_swiss-code\\_corp-govern\\_20080221\\_de.pdf](http://www.economiesuisse.ch/web/de/pdf%20download%20files/pospap_swiss-code_corp-govern_20080221_de.pdf) (zuletzt eingesehen am 20. September 2010).

### **Eidgenössisches Finanzdepartement (EFD)**

EFD RISIKOPOLITIK, Grundlagen für das Risikomanagement beim Bund, Dezember 2004, Fundstelle:

<http://www.efd.admin.ch/dokumentation/zahlen/00578/00996/index.html?lang=de> (zuletzt eingesehen am 20. September 2010).

### **Eidgenössische Finanzmarktaufsicht (FINMA)**

FINMA-RUNDSCHREIBEN 08/24, Überwachung und interne Kontrolle Banken, 20. November 2008, Fundstelle:

<http://www.finma.ch/d/regulierung/Documents/finma-rs-2008-24.pdf> (zuletzt eingesehen am 20. September 2010).

### **Eidgenössische Finanzkontrolle (EFK)**

EFK-QUERSCHNITTSPRÜFUNG, Risikoanalyse auf Stufe Amt und Bund, 7. Juli 2008, Fundstelle:

[http://www.efk.admin.ch/pdf/8208BE\\_def\\_Bericht.pdf](http://www.efk.admin.ch/pdf/8208BE_def_Bericht.pdf) (zuletzt eingesehen am 20. September 2010).

EFK-LEITFADEN, Aufbau eines Internen Kontrollsystems (IKS), 2. Aufl., Oktober 2007, Fundstelle:

[http://www.efk.admin.ch/pdf/Brosch%C3%BCre\\_IKS\\_d.pdf](http://www.efk.admin.ch/pdf/Brosch%C3%BCre_IKS_d.pdf) (zuletzt eingesehen am 20. September 2010).

### **Eidgenössische Finanzverwaltung (EFV)**

EFV-AUSBILDUNGSUNTERLAGEN, Internes Kontrollsystem für die finanzrelevanten Geschäftsprozesse in der Bundesverwaltung, Folien und Aufgabenstellungen zum Kurs, November 2007.

**Eidgenössisches Personalamt (EPA)**

EPA KORRUPTIONSPRÄVENTION, Leitlinien zu Personalfragen, Juni 2009, Fundstelle:

<http://www.epa.admin.ch/dokumentation/publikationen/00277/index.html?lang=de> (zuletzt eingesehen am 20. September 2010).

EPA-RICHTLINIEN ZU NEBENBESCHÄFTIGUNGEN und öffentlichen Ämtern, 27. März 2006, Fundstelle:

<http://www.epa.admin.ch/dokumentation/dokumentenubersicht/index.html?lang=de> (zuletzt eingesehen am 20. September 2010).

EPA VERHALTENSKODEX der allgemeinen Bundesverwaltung vom 19. April 2000, Fundstelle:

<http://www.epa.admin.ch/dokumentation/grundlagen/index.html?lang=de> (zuletzt eingesehen am 20. September 2010).

**Groupe d'Etats contre la Corruption (GRECO)**

GRECO-EVALUATIONSBERICHT über die Schweiz, Erste und Zweite Evaluationsrunde, Strassburg, 4. April 2008, Fundstelle:

[http://www.bj.admin.ch/content/dam/data/kriminalitaet/korruption\\_greco/ber-greco-i-ii-d.pdf](http://www.bj.admin.ch/content/dam/data/kriminalitaet/korruption_greco/ber-greco-i-ii-d.pdf) (zuletzt eingesehen am 20. September 2010).

## In der gleichen Reihe Dans la même collection

N°	Autoren, Titel und Datum – Auteurs, titres et date
243	LADNER Andreas, SCHWARZ Daniel, FIVAZ Jan Die Positionierung der Nationalratskandidierenden 2007 Eine explorative Analyse der Antworten auf die Fragen der Online-Wahlhilfe smartvote
244	PASQUIER Martial, LARPIN Blaise Analyse der politisch-administrativen Probleme und der Governance der öffentlichen Arbeitslosenkassen
245	EGLIN-CHAPPUIS Noëmi Governance von Universitätsbibliotheken Optimierungsmöglichkeiten aus institutioneller Sicht
246	NAHRATH Stéphane, KNOEPFEL Peter, CSIKOS Patrick, GERBER Jean-David Les stratégies politiques et foncières des grands propriétaires fonciers au niveau national Etude comparée
247	KNOEPFEL Peter, NAHRATH Stéphane, CSIKOS Patrick, GERBER Jean-David Les stratégies politiques et foncières des grands propriétaires fonciers en action Etude de cas
248	ABUN-NASR Sonia Strategie für eine Informationsgesellschaft in der Schweiz Eine zehnjährige Politik im Lichte empirischer Analyse
249	SOGUEL Nils, BIZZOZERO Giordano, ZIEHLI Sonja Vergleich 2008 der Kantons- und Gemeindefinanzen Comparatif 2008 des finances cantonales et communales
250	PASQUIER Martial, FIVAT Etienne Crise à l'Université de Genève. Une étude de cas.
251	FIECHTER Julien Politische Gemeinden und lokale Autonomie in der Schweiz
252	LADNER Andreas, FELDER Gabriela, GERBER Stefani, FIVAZ Jan Die politische Positionierung der europäischen Parteien im Vergleich
253	MEILLAND Philomène Le principe de transparence dans le canton de Vaud
254	BERCLAZ Michel Le rôle des employeurs dans la réinsertion professionnelle
255	SOGUEL Nils, ZIEHLI Sonja Vergleich 2009 der Kantons- und Gemeindefinanzen Comparatif 2009 des finances cantonales et communales



## L'IDHEAP en un coup d'œil

### **Champ**

L'IDHEAP, créé en 1981, se concentre sur l'étude de l'administration publique, un champ interdisciplinaire (en anglais Public Administration) visant à développer les connaissances scientifiques sur la conduite des affaires publiques et la direction des institutions qui en sont responsables. Ces connaissances s'appuient sur plusieurs disciplines des sciences humaines et sociales, comme le droit, l'économie, le management et la science politique, adaptées aux spécificités du secteur public et parapublic. L'IDHEAP est le seul institut universitaire suisse totalement dédié à cet important champ de la connaissance.

### **Vision**

A l'interface entre théorie et pratique de l'administration publique, l'IDHEAP est le pôle national d'excellence contribuant à l'analyse des mutations du secteur public et à une meilleure gouvernance de l'Etat de droit à tous ses niveaux, en pleine coopération avec ses partenaires universitaires suisses et étrangers.

### **Mission**

Au service de ses étudiants, du secteur public et de la société dans son ensemble, l'IDHEAP a une triple mission qui résulte de sa vision:

- Enseignement universitaire accrédité au niveau master et post-master, ainsi que formation continue de qualité des élus et cadres publics;
- Recherche fondamentale et appliquée en administration publique reconnue au niveau national et international, et valorisée dans le secteur public suisse;
- Expertise et conseil indépendants appréciés par les organismes publics mandataires et enrichissant l'enseignement et la recherche.

## Principales prestations

### 1. Enseignement: former les élus et cadres actuels et futurs du secteur public

- Doctorat en administration publique
- MPA (Master of Public Administration)
- Master PMP (Master of Arts in Public Management and Policy)
- DEAP (Diplôme exécutif en action publique)
- Certificat universitaire d'un cours trimestriel du MPA
- SSC (Séminaire pour spécialistes et cadres)

### 2. Recherche: ouvrir de nouveaux horizons pour l'administration publique

- Projets de recherche fondamentale ou appliquée
- Directions de thèses de doctorat
- Publications scientifiques (ouvrages et articles)
- Colloques et conférences scientifiques
- Cahiers et Working Papers de l'IDHEAP

### 3. Expertise et conseil: imaginer et mettre en œuvre des solutions innovatives

- Mandats d'expertise et de conseil auprès du secteur public et parapublic

### 4. Services à la cité: contribuer à la connaissance du service public

- Bibliothèque spécialisée en administration publique
- Sites Badac.ch, gov.ch, ivote.ch
- Renseignements aux collectivités publiques
- Interventions médiatiques
- Articles et conférences de vulgarisation