it-sicherheit stumm

Rochusstraße 16 | 50129 Bergheim

Mobil +49 177 8072315
Fon +49 2238 3033-18 | Fax -19

heike.stumm@stumm-it-sicherheit.de
stumm-it-sicherheit.de

Projektfahrplan

Einführung eines Informationssicherheits-Management-System (ISMS) nach IT-Grundschutz

Legende

Link zu einer anderen Datei *(auf Symbol klicken!)*

Verweis auf eine andere Seite

Inhalt

Legende 1

Einleitung 6

Schritt 1:
Benennung der Informations-
Sicherheits-Beauftragten (ISBs) 7

Schritt 2:
Übernahme der Regelungen aus dem
IT-Grundschutz 8

Schritt 3:
Gestaltung des ISMS 15

Schritt 4:
Schutzbedarfs-Festlegung 18

Schritt 5:
IT-Struktur-Analyse 20

Weitere Schritte:
Konzeption der Teilaufgaben nach
IT-Grundschutz 22

Schritt COMP-01:
Einführen des Compliance Management 27

Schritt ORG-01:
Richtlinie Organisatorische Regelungen 29

Schritt ORG-02:
Richtlinie Umgang mit Hard- und Software . . 30

Schritt ORG-03:
Richtlinie Betriebsmittelverwaltung 31

Schritt ORG-04:
Richtlinie Wartungs- und Reparaturarbeiten . . 32

Schritt ORG-05:
Richtlinie für Umzüge 33

Schritt ORG-06:
Berechtigungs-Management 34

Schritt ORG-07:
Umgang mit Informationen 36

Schritt ORG-08:
Vorgehensweise Löschen und Vernichten 37

Schritt ORG-09:
Regelungen zu Arbeitsplätzen 38

Schritt ORG-10:
Regelungen Telearbeit 39

Schritt PERS-01:
Schulung und Sensibilisierung 40

Schritt PERS-02:
Umsetzen der personellen Regelungen 41

Schritt OPS-01:
Regelungen Administration 42

Schritt OPS-02:
Fernwartung 43

Schritt OPS-04:
Archivierung 46

Schritt OPS-05:
Datensicherung 47

Schritt OPS-06:
Patch- und Änderungs-Management 48

Schritt OPS-07:
Software-Lebenszyklus 49

Schritt OPS-09:
Kryptokozept 52

Schritt SRV-01:
Server-Administration 53

Schritt SRV-02:
Administration von Windows-Servern 54

Schritt SRV-03:
Administration von Unix-Servern 55

Schritt SRV-04:
Virtualisierung 56

Schritt SRV-05:
Speicherlösungen 57

Schritt SRV-06:
IBM z-Systeme 58

Schritt APP-01:
Office-Anwendungen 59

Schritt APP-02:
Fileserver 60

Schritt APP-03:
Groupware 61

Schritt APP-05:
Verzeichnisdienste 64

Schritt APP-07:
Web-Anwendungen 68

Schritt CLNT-01:
Client-Administration 71

Schritt CLNT-02:
Windows-Clients 72

Schritt CLNT-04:
Mac-Clients 75

Schritt PERI-01:
Druck-Geräte 76

Schritt PERI-02:
IoT-Geräte 77

Schritt PERI-03:
Eingebettete Systeme 78

Schritt MOB-01:
Laptops 79

Schritt MOB-02:
Smartphones und Tablets 80

Schritt NET-01:
Netzarchitektur 84

Schritt NET-02:
Netzmanagement 85

Schritt NET-03:
VPN 86

Schritt NET-04:
WLAN 87

Schritt NET-05:
Router und Switches 88

Schritt DER-01:
Detektion von sicherheitsrelevanten
Ereignissen 89

Schritt DER-02:
Protokollierung 90

Schritt DER-04:
Firewall 93

Schritt TK-02:
Voice over IP 95

Schritt TK-03:
Fax 96

Schritt INF-01:
Bauliche Infrastruktur 97

Schritt IND-01:
Betriebs- und Steuerungstechnik 98

Schritt ÌND-02:
Industrielle Komponenten 99

Schritt BCM-01:
Notfall-Management 100

Schritt BCM-02:
Behandlung von Sicherheitsvorfällen 102

Schritt USR-01:
Nutzerrichtlinie 103

Einleitung

Das folgende Dokument soll Sie durch den Prozess führen, der zur Einführung eines Informations-Sicherheits-Management-Systems (ISMS) nach BSI Standard 200 (IT-Grundschutz) erforderlich ist. Dieses ISMS erfüllt damit **automatisch** auch den ISO Standard ISO 27001/27002, da der IT-Grundschutz lediglich eine Konkretisierung dieses Standards ist. Ebenso werden damit die für den Schutz personenbezogener Daten geforderten Technisch-Organisatorischen Maßnahmen (TOMs) eingeführt.

Die Vorgehensweise ist dabei standardisiert einfach gehalten:

Es ist vorgesehen, dass Sie die Anforderungen des IT-Grundschutz zunächst unverändert für Ihren IT-Verbund übernehmen. Dazu sind entsprechende „Regelungen“ vorformuliert, in denen lediglich das Wording auf Ihren IT-Verbund angepasst werden soll. Änderungen am Inhalt sind an dieser Stelle noch nicht vorgesehen.

Für Konkretisierungen und Änderungen wird eine zweite Ebene von Dokumenten bereitgestellt.

Schritt 1: Benennung der Informations-Sicherheits-Beauftragten (ISBs)

Der Prozess beginnt damit, dass das Management den Informations-Sicherheits-Beauftragten bzw. die Informations-Sicherheits-Beauftragte (ISB) und den bzw. die Stellvertreter/in (stv. ISB) benennt und damit die Einführung des ISMS beauftragt. In den Dokumenten sind die beiden Rollen in der Regel in der Mehrzahl (ISBs) verwendet, um gendergerechte Formulierungen zu erleichtern.

Veranlassen Sie die Beauftragung des ISMS durch das Management mit dem *Musterauftrag ISB-ISMS-01*.

Zur Terminüberwachung der einzelnen Schritte wird ein *Ablaufplan* zur Verfügung gestellt. Es bietet sich an, erledigte Aufgaben in diesem Plan farblich besonders zu markieren.

Schritt 2:
Übernahme der Regelungen aus dem IT-Grundschutz

Das ISMS basiert auf dem IT-Grundschutz (BSI Standard 200). Dieser gibt Anforderungen vor, die bei Planung, Betrieb oder Nutzung von IT bezogen auf unterschiedliche Systeme, Anwendungen oder die Infrastruktur dafür zu beachten sind.

Wir gehen davon aus, dass diese Anforderungen komplett beachtet werden – wenn auch nicht unbedingt umgesetzt. Deswegen werden die Anforderungen im vollen Umfang als Regelung für den IT-Verbund übernommen, im weiteren Verlauf der Einführung aber entschieden, ob und in welchem Umfang sie umgesetzt werden sollen. Die Dokumentation dieser Entscheidung erfolgt im weiteren Verlauf der Bearbeitung.

Zunächst soll nur die Übernahme der Regelungen erfolgen. Dazu müssen die Musterregelungen im Wording auf den IT-Verbund angepasst werden. Dies ist Aufgabe der ISBs.

Weisen Sie den *Auftrag ISB-ISMS-02* zur Erstellung der Regelungs-Dokumente zu Dokumentationszwecken den ISBs zu.

Die nachfolgenden Betrachtungen gehen von einem „Standard-IT-Verbund“ aus. Wird nur ein anwendungsbezogener IT-Verbund definiert, kann auf einige dieser Regelungen verzichtet werden, wenn keine entsprechenden Systeme im Verbund verwendet werden. Die folgenden Musterdokumente sind üblicherweise zu überarbeiten:

Themenkomplex ISMS:

- *01 – Dokument ISMS 01 Regelungen ISMS*
- *02 – Dokument DER 3-01 Regelungen Audit*
- *03 – Dokument DER 3-02 Regelungen IS-Revisionen für Bundesbehörden* (nur bei Bundesbehörden)

Themenkomplex Compliance (COMP):

- *01 – Dokument ORP.5 Regelungen Compliance Management*
- *02 – Dokument CON.07 Regelungen Auslandsreisen*
- *03 – Dokument CON.02 Regelungen Datenschutz*
- *04 – Dokument OPS 2-01 Regelungen Outsourcing als Kunde*
- *05 – Dokument OPS 3-01 Regelungen Outsourcing als Dienstleistung*
  (nur wenn der IT-Verbund Outsourcing für andere anbietet)

Themenkomplex Organisation (ORG):

- *01 – Dokument ORP-01 Organisatorische Regelungen*
- *02 – Dokument ORP-04 Regelungen zum Identitäts- und Berechtigungsmanagement*
- *03 – Dokument OPS-01-02-03 Regelungen zum Informations- und Datenträgeraustausch*
- *04 – Dokument CON-06 Regelungen Löschen und Vernichten*
- *05 – Dokument INF-07 Regelungen Büroarbeitsplatz*
- *06 – Dokument INF-08 Regelungen Häuslicher Arbeitsplatz*
- *07 – Dokument INF-09 Regelungen Mobiler Arbeitsplatz*
- *08 – Dokument INF-10 Regelungen Besprechungs- Veranstaltungs- Schulungsräume*
- *09 – Dokument OPS 1-02-04 Regelungen zur Telearbeit*
  (nur wenn mit Beschäftigten dauerhaft Telearbeit vereinbart ist)

Themenkomplex Personelles (PERS):

- *01 – Dokument ORP-02 Personalbezogene Regelungen*
- *02 – Dokument ORP-03 Regelungen Sensibilisierung und Schulung*

Themenkomplex IT-Betrieb (OPS):

- *01 – Dokument OPS 1-01-02 Regelungen Ordnungsgemäße IT-Administration*
- *02 – Dokument OPS 1-02-02 Regelungen zur Archivierung*
- *03 – Dokument CON.03 Regelungen Datensicherung*
- *04 – Dokument OPS 1-01-03 Regelungen zum Patch- und Änderungsmanagement*
- *05 – Dokument CON.04 Regelungen Standardsoftware*
- *06 – Dokument OPS 1-01-06 Regelungen Software-Tests- und –Freigaben*
- *07 – Dokument CON.05 Regelungen Fachanwendungen*
- *08 – Dokument OPS 2-04 Regelungen Fernwartung*
- *09 – Dokument CON.01 Regelungen Umgang mit Verschlüsselung*
- *10 – Dokument Regelungen OPS-2-2 Cloud-Nutzung*
  (nur wenn Cloud-Dienste genutzt werden)

Themenkomplex Serversicherheit (SRV):

- *01 – Dokument SYS 1-01 Regelungen Server*
- *02 – Dokument SYS 1-02-02 Regelungen Windows Server 2012*
  (nur wenn entsprechende Server verwendet werden oder für die analoge Anwendung für andere Windows-Server)
- *03 – Dokument SYS 1-03 Regelungen Unix-Server*
  (nur wenn entsprechende Server verwendet werden)
- *04 – Dokument SYS 1-05 Regelungen Virtualisierung*
  (nur wenn Virtualisierung eingesetzt wird, gilt auch für Terminalserver)
- *05 – Dokument SYS 1-08 Regelungen Speicherlösungen*
- *06 – Dokument SYS 1-07 Regelungen IBM z-Systeme*
  (nur wenn z-Systeme eingesetzt werden)

Themenkomplex Anwendungssicherheit (APP):

- *01 – Dokument APP 1-01 Regelungen Office-Produkte*
- *02 – Dokument APP 1-02 Regelungen Web-Browser*
- *03 – Dokument APP 3-03 Regelungen Fileserver*
- *04 – Dokument APP 5-01 Regelungen Groupware*
- *05 – Dokument APP 5-02 Regelungen Exchange und Outlook*
  (nur wenn Exchange/Outlook verwendet werden)
- *06 – Dokument APP 4-03 Regelungen Relationale Datenbanken*
- *07 – Dokument APP 2-01 Regelungen Verzeichnisdienste*
- *08- Dokument APP 2-02 Regelungen Active Directory*
  (nur wenn AD verwendet wird)
- *09 – Dokument APP 3-04 Regelungen Samba*
  (nur wenn Samba-Server verwendet werden)
- *10 – Dokument APP 3-06 Regelungen DNS-Server*
  (nur wenn DNS verwendet wird)
- *11 – Dokument APP 3-02 Regelungen Webserver*
  (nur wenn Webserver eingesetzt werden)
- *12 – Dokument APP 3-01 Regelungen Webanwendungen*
  (nur wenn Webanwendungen entwickelt werden)
- *13 – Dokument APP 1-04 Regelungen Mobile Anwendungen (Apps)*
  (nur wenn Apps dienstlich verwendet werden)
- *14 – Dokument APP 2-03 Regelungen OpenLDAP*
  (nur wenn OpenLDAP eingesetzt wird)
- *15 – Dokument APP 4-02 Regelungen SAP-ERP-System*
  (nur wenn SAP verwendet wird)
- *16 – Dokument APP 4-06 Regelungen SAP ABAP Programmierung*
  (nur wenn ABAP Programmierung erfolgt)

Themenkomplex Clientsicherheit (CLNT):

- *01 – Dokument SYS 2-01 Regelungen Clients*
- *02 – Dokument SYS 2-02-02 Regelungen Windows 8-1*
  (nur wenn Windows 8.1 verwendet wird oder in analoger Anwendung für ältere Versionen)
- *03 – Dokument SYS 2-02-03 Regelungen Windows 10*
  (nur wenn Win 10 verwendet wird oder in analoger Anwendung für spätere Versionen)
- *04 – Dokument SYS 2-03 Regelungen Unix-Client*
  (nur wenn Unix-Clients eingesetzt werden)
- *05 – Dokument SYS 2-04 Regelungen Client unter MacOS*
  (nur wenn Mac-Clients eingesetzt werden)

Themenkomplex Peripheriegeräte (PERI):

- *01 – Dokument SYS 4-01 Regelungen Drucker – Kopierer – Multifunktionsgeräte*
- *02 – Dokument SYS 4-04 Regelungen IoT-Geräte*
  (nur wenn Internet of Things Komponenten eingesetzt werden)
- *03 – Dokument SYS 4-03 Regelungen Eingebettete Systeme*
  (nur wenn eingebettete Systeme eingesetzt werden)

Themenkomplex Mobilgeräte (MOB):

- *01 – Dokument SYS 3-01 Regelungen Laptops*
- *02 – Dokument SYS 3-02-01 Regelungen Smartphones und Tablets*
- *03 – Dokument SYS 3-02-02 Regelungen Mobile Device Management*
  (nur wenn Mobile Device Management erforderlich ist)
- *04 – Dokument SYS 3-02-03 Regelungen iOS*
  (nur wenn iOS-Geräte eingesetzt werden)
- *05 – Dokument SYS 3-02-04 Regelungen Android*
  (nur wenn Android-Systeme eingesetzt werden)

- *06 – Dokument SYS 3-04 Regelungen Mobile Datenträger*
- *07 – Dokument SYS 3-03 Regelungen Mobiltelefon*

Themenkomplex Netzsicherheit (NET):

- *01 – Dokument NET 1-01 Regelungen Netzarchitektur und –design*
- *02 – Dokument NET 1-02 Regelungen Netzmanagement*
- *03 – Dokument NET 3-01 Regelungen Router und Switches*
- *04 – Dokument NET 2-01 Regelungen WLAN-Betrieb*
  (nur wenn WLAN eingesetzt wird)
- *05 – Dokument NET 2-02 Regelungen WLAN-Nutzung*
  (nur wenn WLAN für dienstliche Zwecke genutzt wird)
- *06 – Dokument NET 3-03 Regelungen VPN*

Themenkomplex Detektion und Reaktion (DER):

- *01 – Dokument DER.1 Regelungen Detektion von sicherheitsrelevanten Ereignissen*
- *02 – Dokument OPS 1-01-05 Regelungen zur Protokollierung*
- *03 – Dokument OPS 1-01-04 Regelungen zum Schutz vor Schadsoftware*
- *04 – Dokument NET 3-02 Regelungen Firewall*

Themenkomplex Telekommunikation (TK):

- *01 – Dokument NET 4-01 Regelungen TK-Anlage*
- *02 – Dokument NET 4-02 Regelungen VoIP*
  (nur wenn Voice over IP eingesetzt wird)
- *03 – Dokument NET 4-03 Regelungen Fax*
  (für Faxgeräte und Faxserver)

Themenkomplex Bauliche Infrastruktur (INF):

- *01 – Dokument INF-01 Regelungen Gebäude*
- *02 – Dokument INF-02 Regelungen RZ und Serverraum*
- *03 – Dokument INF-03 Regelungen Elektrotechnische Verkabelung*
- *04 – Dokument INF-04 Regelungen IT-Verkabelung*
- *05 – Dokument INF-06 Regelungen Datenträgerarchiv*

Themenkomplex Industrielle Systeme (IND)
(nur wenn und soweit diese eingesetzt werden):

- *01 – Dokument IND-1 Regelungen Betriebs- und Steuerungstechnik*
- *02 – Dokument IND 2-01 Regelungen ICS-Komponenten*
- *03 – Dokument IND 2-02 Regelungen Speicherprogrammierbare Steuerung*
- *04 – Dokument IND 2-03 Regelungen Sensoren und Aktoren*
- *05 – Dokument IND 2-04 Regelungen Maschinen*
- *06 – Dokument IND 2-07 Safety Instrumented Systems*

Themenkomplex Notfallvorsorge (BCM):

- *01 – Dokument DER.4 Regelungen Notfallmanagement*
- *02 – Dokument DER 2-01 Regelungen Behandlung von Sicherheitsvorfällen*
- *03 – Dokument DER 2-02 Regelungen Forensik*
- *04 – Dokument DER 2-03 Regelungen Bereinigung*

Vermerken Sie Terminsetzungen aus den Aufträgen zur Überwachung im *Ablaufplan*.

Schritt 3:
Gestaltung des ISMS

Es sind die **grundlegenden Vorgaben zur Gestaltung des ISMS** zu erarbeiten. Dies ist weitgehend Aufgabe der ISBs. Zunächst sind dazu der zu verfolgende *Informations-Sicherheits-Prozess* und die Organisation der Informations-Sicherheit in der Informations-Sicherheits-Leitlinie zu beschreiben. (....)

Schritt 4:
Schutzbedarfs-Festlegung

An dieser Stelle weichen wir von der Standardvorgehensweise ab und ziehen die Schutzbedarfsbetrachtung vor. Die IT-Grundschutz-Methodik (BSI-Standard 200-2) wird dennoch eingehalten, es handelt sich nur um eine Abweichung in der Reihenfolge. (...)

Schritt 5:
IT-Struktur-Analyse

Mit der **IT-Struktur-Analyse** werden die Bestandteile des IT-Verbundes (Geschäftsprozesse, Anwendungen, IT-Systeme, Gebäude und Räume) erfasst, damit die erforderlichen Bausteine des IT-Grundschutz auf sie angewandt werden können. Die Analyse wird von den ISBs durchgeführt, dies wird durch *Auftrag ISB-GSA-01* dokumentiert. Machen Sie sich zunächst mit der Vorgehensweise für die IT-Struktur-Analyse anhand des *BSI Standard 200-2* vertraut. (...)

Weitere Schritte: Konzeption der Teilaufgaben nach IT-Grundschutz

Für die Bearbeitung der weiteren Themenfelder ist keine feste Reihenfolge einzuhalten, auch die Bearbeitung der einzelnen Themen innerhalb der Themenfelder ist in der Regel zeitlich frei wählbar (auf Ausnahmen wird im Folgenden hingewiesen). Die folgenden Aufgaben sind innerhalb der Themenkomplexe zu konzipieren:

Themenkomplex Compliance (COMP):

- COMP-01: Compliance Management

Themenkomplex Organisation (ORG):

- ORG-01: Richtlinie Organisatorische Regelungen
  – ist für den Themenkomplex als erstes zu erarbeiten
- ORG-02: Umgang mit Hard- und Software
- ORG-03: Betriebsmittelverwaltung
- ORG-04: Vorgaben für Wartungs- und Reparaturarbeiten
- ORG-05: Vorgaben für Umzüge
- ORG-06: Berechtigungsmanagement
- ORG-07: Umgang mit Informationen
- ORG-08: Vorgaben zum Löschen und Vernichten von Informationsträgern
- ORG-09: Regelungen für Arbeitsplätze
- ORG-10: Telearbeit
  (nur wenn mit Beschäftigten dauerhaft Telearbeit vereinbart ist)

Themenkomplex Personelles (PERS):

- PERS-01: Schulungskonzept
- PERS-02: Personalbezogene Regelungen

Themenkomplex IT-Betrieb (OPS):

- OPS-01: Regelungen zur Administration
- OPS-02: Fernwartung
- OPS-03: Cloud-Nutzung
  (nur wenn Cloud-Dienste genutzt werden)
- OPS-04: Archivierung
- OPS-05: Datensicherung
- OPS-06: Patch- und Änderungs-Management
- OPS-07: Software-Lebenszyklus
- OPS-08: Entwicklung von Fachanwendungen
- OPS-09; Kryptokonzept

Themenkomplex Serversicherheit (SRV):

- SRV-01: Allgemeine Regelungen zur Serversicherheit
- SRV-02: Windows Server 2012
  (nur wenn entsprechende Server verwendet werden oder für die analoge Anwendung für andere Windows-Server)
- SRV-03: Unix-Server
  (nur wenn entsprechende Server verwendet werden)
- SRV-04: Virtualisierung
  (nur wenn Virtualisierung eingesetzt wird, gilt auch für Terminalserver)
- SRV-05: Speicherlösungen
- SRV-06: IBM z-Systeme
  (nur wenn z-Systeme eingesetzt werden)

Themenkomplex Anwendungssicherheit (APP):

- APP-01: Office-Produkte
- APP-02: Fileserver
- APP-03: Groupware
- APP-04: Relationale Datenbanken
- APP-05: Verzeichnisdienste
- APP-06: DNS-Server (nur wenn DNS verwendet wird)
- APP-07: Mobile und Web-Anwendungen
  (nur wenn diese dienstlich verwendet werden)
- APP-08: SAP (nur wenn SAP verwendet wird)

Themenkomplex Clientsicherheit (CLNT):

- CLNT-01: Allgemeine Regelungen zur Clientsicherheit
  – für den Themenkomplex als erstes zu erarbeiten
- CLNT-02: Windows-Clients
  (nur wenn Windows Clients eingesetzt werden)
- CLNT-03: Unix-Client
  (nur wenn Unix-Clients eingesetzt werden)
- CLNT-04: Client unter MacOS
  (nur wenn Mac-Clients eingesetzt werden)

Themenkomplex Peripheriegeräte (PERI):

- PERI-01: Drucker – Kopierer – Multifunktionsgeräte
- PERI-02: IoT-Geräte
  (nur wenn Internet of Things Komponenten eingesetzt werden)
- PERI-03: Eingebettete Systeme
  (nur wenn eingebettete Systeme eingesetzt werden)

Themenkomplex Mobilgeräte (MOB):

- MOB-01: Laptops
- MOB-02: Smartphones und Tablets
- MOB-03: Mobile Datenträger

Themenkomplex Netzsicherheit (NET):

- NET-01: Netzarchitektur und -design
- NET-02: Netzmanagement
- NET-03: VPN
- NET-04: WLAN
- NET-05: Router und Switches

Themenkomplex Detektion und Reaktion (DER):

- DER-01: Detektion von sicherheitsrelevanten Ereignissen
- DER-02: Protokollierung
- DER-03: Schutz vor Schadsoftware
- DER-04: Firewall

Themenkomplex Telekommunikation (TK):

- TK-01: TK-Anlage
- TK-02: VoIP
  (nur wenn Voice over IP eingesetzt wird)
- TK-03: Fax
  (für Faxgeräte und Faxserver)

Themenkomplex Bauliche Infrastruktur (INF):

- INF-01: Bauliche Sicherheit

Themenkomplex Industrielle Systeme (IND)
(nur wenn und soweit diese eingesetzt werden):

- IND-01: Betriebs- und Steuerungstechnik
- IND-02: Industrielle Komponenten

Themenkomplex Notfallvorsorge (BCM):

- BCM-01: Notfallmanagement
- BCM-02: Behandlung von Sicherheitsvorfällen

Themenkomplex Nutzer-Richtlinie (USR):

- USR-01: Nutzerrichtlinie

Schritt COMP-01: Einführen des Compliance Management

Beim Compliance Management handelt sich um den Abgleich rechtlicher Anforderungen an Informationen innerhalb der Organisation. Diese können bezogen auf die jeweilige Information in Konflikt zueinander stehen. So kann zum Beispiel für die gleiche Information eine datenschutzrechtliche Anforderung auf Löschung (z. B. nach 90 Tagen, da personenbezogene Daten enthalten sind) und eine steuerrechtliche Anforderung auf Speicherung (z. B für 10 Jahre als Teil eines Rechnungsbeleges) bestehen. Es ist Aufgabe der Organisation, diese Konflikte zu erkennen und einen standardisierten Weg zu ihrer Auflösung zu definieren. Für diese Aufgabe ist eine verantwortliche Person zu benennen, die im Folgenden als Compliance Manager bezeichnet wird. Legen Sie fest, wer diese Funktion im IT-Verbund übernehmen soll (ggf. auch mehrere Personen für unterschiedliche Teilbereiche des Verbundes).

Die Hauptaufgabe bei der Einführung ist, die für das **Compliance Management** (Umgang mit rechtlichen Anforderungen) definierten Lösungen festzuhalten. Dazu sind die folgenden Dokumente zu erstellen:

- **Eine Beschreibung, wie der Compliance Management Prozess ablaufen soll**
  zu erstellen durch den ausgewählten Compliance Manager gemäß *Auftrag CM-COMP-01*
  anhand Musterdokument *Dokument COMP-01-01* Prozess Compliance Management
- **Ein Formular für die Erfassung der Rechtsanforderungen durch die Informationseigentümer**
  zu erstellen durch den ausgewählten Compliance Manager gemäß *Auftrag CM-COMP-02*
  anhand Musterdokument *Dokument COMP-01-02* Muster Erfassung Rechtsanforderungen (Excel-Liste)
- **Eine Richtlinie zum Umgang mit IT auf Auslandsreisen**
  zu erstellen durch den ausgewählten Compliance Manager gemäß *Auftrag CM-COMP-03*
  anhand Musterdokument *Dokument COMP-01-03* Richtlinie IT auf Auslandsreisen
- **Eine Richtlinie für den Umgang mit Outsourcing als Kunde**
  zu erstellen durch den ausgewählten Compliance Manager gemäß *Auftrag CM-COMP-04*
  anhand Musterdokument *Dokument COMP-01-04* Richtlinie Outsourcing als Kunde

- **Formulare zur Steuerung des Workflows zum Compliance Management, wie er in Dokument COMP-01-01 beschrieben wird**
  zu erstellen durch den ausgewählten Compliance Manager gem. *Auftrag CM-COMP-05* anhand des Musterdokumentes *Dokument COMP-02-01* Dokumentation Auflösung eines Anforderungskonfliktes (für Konflikte bei Informationen unterschiedlicher Eigentümer und gemäß *Auftrag CM-COMP-06* für Konflikte bei Informationen im Bereich eines Informationseignetümers anhand des Musterdokumentes *Dokument COMP-02-02* Muster Ausnahmeantrag

Es ist weiterhin eine Vorgehensweise für die **Klassifizierung von Informationen** durch den benannten Compliance Manager festzulegen (*Auftrag CM-COMP-07*). Hierfür wurde keine Vorgabe erarbeitet, die Dokumentation erfolgt in der Richtlinie zum Dokumentenmanagement, die in der Regel für die Organisation bereits beschrieben ist (aber ggf. anders heißt).

Außerdem ist gemäß den Vorgaben aus der Richtlinie COMP-01-03 eine **Übersichtsliste von Ländern** zu erstellen, in die mobile IT-Geräte mitgenommen werden dürfen. Dies wird auch dem benannten Compliance Manager übertragen (*Auftrag CM-COMP-08*).

Abschließend sind die laufenden **Aufgaben** für das Compliance Management noch den zuständigen Stellen zuzuordnen. Dies ist für den benannten Compliance Manager das Ermitteln von Anforderungskonflikten nach der Prozessbeschreibung zum Compliance Management (*Auftrag CM-COMP-09*). Die Informationseigentümer sollen Übersichten über die rechtlichen Anforderungen in ihrem Bereich führen (*Auftrag IE-COMP-01*), Anforderungskonflikte in ihrem Bereich mittels Ausnahmeantrag anzeigen (*Auftrag IE-COMP-02*) und bei Bedarf Mitnahmeanträge für IT auf Auslandsreisen nach der entsprechenden Richtlinie stellen (*Auftrag IE-COMP-03*).

Alle oben genannten Aufträge sind durch die ISBs zu erstellen und den zuständigen Personen/ Organisationseinheiten zuzuleiten.

Vermerken Sie Terminsetzungen aus den Aufträgen zur Überwachung im *Ablaufplan*.