Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Departement für Verteidigung, Bevölkerungsschutz und Sport VBS

**Bundesamt für Sport BASPO**
Ressourcen

Häusler Roland, 31.05.2023

# Information-Sicherheit-Management-System (ISMS) BASPO

## Handbuch Informationssicherheit BASPO

| Dokumentenkontrolle | |
|---|---|
| Gültig von / bis | 01.06.2023 |
| Version | 6.0 |
| Status | In Bearbeitung |
| Dokumenten-Art | Handbuch |
| Verteiler | |
| Dok.-Eigner | Wägli Hanspeter |
| Geltungsbereich | BASPO |
| Ablageort | GRC Toolbox (GRCS) |

## Prüfung

| Name | Rolle | Datum / Version |
|---|---|---|
| Roland Häusler | Leiter IT BASPO | 18.10.2018 |
| Roland Häusler | Leiter IT BASPO | 14.11.2019 |
| Roland Häusler | Leiter IT BASPO | 31.07.2020 |
| Roland Häusler | Leiter IT BASPO | 16.09.2021 |
| Amsler Fritz | ISBO | 18.04.2023 |
| Judith Schneider-Köppel | Betreiberin ISMS | 11.05.2023 |

Freigabe

| Name | Rolle | Datum / Version |
|---|---|---|
| Sandra Felix | InfoSiVe | 22.10.2018 / V02.00 |
| Sandra Felix | InfoSiVe | 03.12.2019 / V03.00 |
| Sandra Felix | InfoSiVe | 20.10.2020 / V04.00 |
| Sandra Felix | InfoSiVe | 18.10.2021 / V05.00 |
| Wägli Hanspeter | InfoSive | 01.06.2023 / V06.00 |

# Inhaltsverzeichnis

# Abbildungsverzeichnis



# Tabellenverzeichnis

# 1 Einleitung/Ausgangslage

## 1.1 Einführung

Die Informationssicherheit hat die **Verfügbarkeit**, die **Integrität**, die **Vertraulichkeit** und die **Nachvollziehbarkeit** aller Arten von Informationen (elektronische, papierbezogene, mündliche) gemäss den Anforderungen der Inhaber des Schutzobjekts Information angemessen sicherzustellen.

Die Informationssicherheit setzt sich (gemäss Weisungen über die Informationssicherheit im VBS (WIns VBS) Ziffer 1 Abs.2) aus den folgenden 3 Bereichen zusammen:

- Informationsschutz (siehe Kap. 1.5.1),
- IKT Sicherheit (siehe Kap. 1.5.2) und
- Datenschutz (siehe Kap. 1.5.3).

Informationen, welche einen Wert für das BASPO darstellen, müssen adäquat (risikobasiert) geschützt werden. Der Schutzbedarf und die Risiken bilden den zentralen Ausgangspunkt für alle Sicherheitsmassnahmen.

Die Informationssicherheit wird unter Einhaltung der Rechtsgrundlagen des Bundes und unter Beachtung interner und externer Anforderungen in einem Informationssicherheits-Managementsystem (ISMS) nach SN ISO/IEC 27001:2022 (WIns Ziffer 1 Abs.1) aufgebaut, betrieben und kontinuierlich verbessert. Die Vorgaben (siehe Kap. 1.7 / 6.1) für die Informationssicherheit im BASPO beinhalten die Prinzipien der Informationssicherheit (PIns) VBS und die relevanten Weisungen zur Informationssicherheit im VBS. Als Grundlage für die Informationssicherheit übernimmt das BASPO die PIns, insbesondere die darin aufgeführten Ziele und Prinzipien. Zusätzlich definiert das BASPO mit dem vorliegenden Handbuch und den Anhängen eigene spezifische Grundsätze und Vorgehensweisen.

Die Informationssicherheit ist ein Teilaspekt der Integralen Sicherheit, zu welcher ein von der Geschäftsleitung BASPO (GL BASPO) genehmigtes Sicherheitskonzept für die Integrale Sicherheit besteht.

Alle Anhänge gemäss Kap. 1.8 sind integraler Bestandteil des vorliegenden Handbuches.

## 1.2 Ziel und Zweck

Das Handbuch Informationssicherheit BASPO regelt die Ablauf- und Aufbauorganisation (inkl. deren Verantwortlichkeiten) im Bereich der Informationssicherheit im BASPO, soweit dies nicht schon im Sicherheitskonzept BASPO für die Integrale Sicherheit aufgeführt oder durch Vorgaben der zentralen Sicherheitsorganisation VBS (ISMS VBS) vorgegeben wird.

Der Betrieb des ISMS wird mit der Anwendung „**G**overnance-**R**isiko-**C**ompliance-**S**icherheit“ (GRCS BASPO) unterstützt. Vorgaben und Nachweise werden darin abgelegt und gepflegt.

## 1.3 Geltungsbereich

Dieses Dokument gilt für alle Mitarbeitenden des BASPO.

## 1.4 Begriffe und Definitionen

Die grundlegendsten Begriffe zur Informationssicherheit, wie
- Informationssicherheit-Managementsystem (ISMS),
- Schutzobjekt Information und
- Inhaberin oder Inhaber des Schutzobjektes Information

sind in der WIns (Ziffer 2) definiert.

## 1.5 Sicherheitsbereiche der Informationssicherheit

Die Informationssicherheit deckt die nachfolgend aufgeführten Themenbereiche ab.

### 1.5.1 Informationsschutz

Der Informationsschutz regelt alle Fragen betreffend dem Schutz von Informationen vor unberechtigter Offenbarung. Informationsschutz hat die **Vertraulichkeit** der Informationen zu gewährleisten.
Die Verordnung über den Schutz von Informationen des Bundes (Informationsschutzverordnung, ISchV) regelt im speziellen den Schutz von Informationen des Bundes und der Armee, soweit er im Interesse des Landes geboten ist. Sie legt insbesondere deren Klassifizierung und Bearbeitung fest.

### 1.5.2 IKT Sicherheit (Informatiksicherheit)

Die IKT Sicherheit hat sicherzustellen, dass elektronische Informationen geschützt und sicher bearbeitet werden. Für die IKT Sicherheit gelten die Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (Cyberrisikenverordnung, CyRV) und die Weisungen über die Informationssicherheit im VBS (WIns VBS).

Die CyRV regelt die Organisation der Bundesverwaltung zum Schutz vor Cyberrisiken, das Sicherheitsverfahren (Schutzbedarfsanalyse, Informationssicherheits- und Datenschutzkonzept) und die Netzwerksicherheit. Sie bestimmt die technischen, baulichen, organisatorischen und personellen Anforderungen und definieren die minimalen Sicherheitsanforderungen zum Schutz der Vertraulichkeit, Verfügbarkeit, Integrität und Nachvollziehbarkeit von Informationen und Daten (IKT-Grundschutz in der Bundesverwaltung).

### 1.5.3 Datenschutz

Der Datenschutz bezweckt den Schutz der Persönlichkeit vor widerrechtlicher oder unverhältnismässiger Bearbeitung von Personendaten.

Das Bundesgesetz über den Datenschutz (DSG) und die Verordnung zum Bundesgesetz über den Datenschutz (VDSG) geben die Grundsätze vor, die es bei der Bearbeitung von Personendaten einzuhalten gilt.

- Insbesondere dürfen Personendaten nur rechtmässig beschafft werden.
- Ihre Bearbeitung hat nach Treu und Glauben zu erfolgen und muss verhältnismässig sein.
- Personendaten dürfen nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde und der gesetzlich vorgesehen oder aus den Umständen ersichtlich ist.
- Wer Personendaten bearbeitet, hat sich über deren Richtigkeit zu vergewissern.

- Das DSG regelt die Bekanntgabe der Daten ins Ausland sowie das Auskunftsrecht.

Die Artikel 16 bis 25 DSG regeln die Bearbeitung von Personendaten durch Bundesorgane.

- Bundesorgane dürfen Personendaten nur bearbeiten, wenn eine gesetzliche Grundlage besteht.
- Für die Bearbeitung besonders schützenswerter Personendaten oder von Persönlichkeitsprofilen wird grundsätzlich eine formell gesetzliche Grundlage verlangt.
- Die Bekanntgabe von Personendaten an Dritte ist ebenfalls an das Vorliegen einer Rechtsgrundlage geknüpft, dies unter Vorbehalt der in Artikel 19 Abs.1 DSG vorgesehenen Ausnahmen.
- Personendaten dürfen nur durch ein Abrufverfahren zugänglich gemacht werden, wenn dies ausdrücklich vorgesehen ist.

## 1.6 Schnittstellen

Die Schnittstellen und Abhängigkeiten der Informationssicherheit zu anderen Sicherheitsbereichen werden im ISMS berücksichtigt. Dasselbe gilt auch für Abhängigkeiten zu internen und externen Lieferanten (z.B. BIT, FUB) sowie den Anspruchsgruppen (Stakeholder).

**Business Continuity Management (BCM)**
Mit dem Business Continuity Management (BCM) soll nach eingetretenem (Sicherheits-) Vorfall möglichst rasch der Normalbetrieb wieder sichergestellt werden. Die Geschäftsfortführung und Geschäftsaufrechterhaltung basiert auf den Richtlinien der C VBS zum Business Continuity Management (BCM).

**Krisenorganisation BASPO**
Mit der Krisenorganisation sollen ausserordentliche Lagen und Krisen behandelt werden. Die Krisenorganisation des BASPO und deren Arbeitsweise ist im Krisenhandbuch beschrieben.

## 1.7 Mitgeltende Dokumente

Die Rechtsgrundlagen werden durch das zentrale ISMS VBS bereitgestellt. BASPO-spezifische Vorgaben sind auf dem Intranet des BASPO publiziert und ISMS-spezifische im GRCS BASPO abgelegt.

## 1.8 Anhänge

Die nachfolgend aufgeführten Anhänge sind Bestandteil des vorliegenden Handbuches Informationssicherheit BASPO.

| Nr. | Titel |
|---|---|
| **A1** | Informationssicherheits-Risikomanagement (ISRM) |
| **A2** | Dokumenten-, Änderungs- und Ausnahmemanagement |
| **A3** | Bewertung der Leistungen und Sicherheitsvorfälle |
| **A4** | Kontinuierliche Verbesserung & IT Service Continuity Management |
| **A5** | Geltungsbereich ISMS |

Tabelle 1: Anhänge

# 2 Informationssicherheitsziele

Die Prinzipien der Informationssicherheit (PIns) VBS werden übernommen. Das BASPO definiert und leitet aus diesen eigene und messbare Informationssicherheitsziele ab, welche im Rahmen der Management-Bewertung jährlich überprüft und neu festgelegt werden.

# 3 Geltungsbereich des ISMS

Die Definition des Geltungsbereichs (Scope) richtet sich nach der Geschäftsordnung BASPO und orientiert sich an den Informationen aus den Geschäftsprozessen[1].

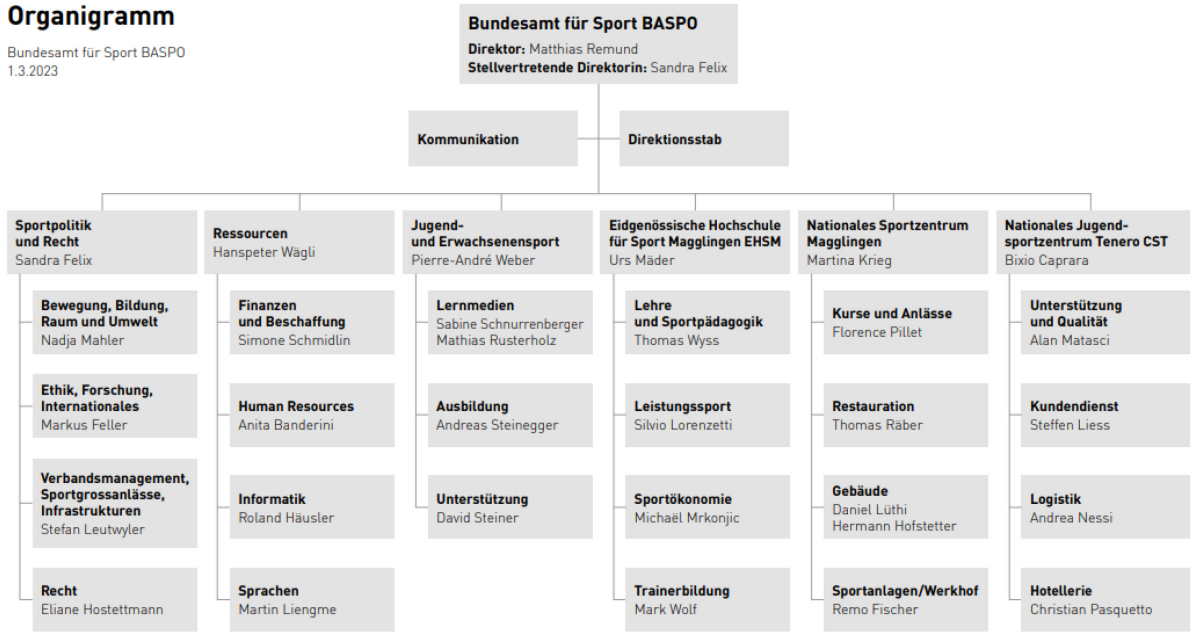



Abbildung 1: Organigramm BASPO

Der Geltungsbereich des ISMS umfasst das gesamte Bundesamt für Sport (BASPO) sowie deren Standorte und erstreckt sich über alle Informationen des BASPO und die zugeordneten Werte (Informationsträger) wie

- Personen/Geheimnisträger
- Informationsschutzobjekte
- IKT-Schutzobjekte
- physische Objekte

soweit sich diese im Verantwortungsbereich des BASPO befinden.

Der Geltungsbereich des ISMS ist im Anhang A5 zum Handbuch definiert.

[1] vgl. GO BASPO, Kapitel 3.1 Prozessmodell

# 4 Einflussfaktoren (interne/externe Themen)

Die Einflussfaktoren (gem. ISO 27001 interne und externe Themen) auf die Informationssicherheit und das ISMS im BASPO, werden im Dokument „Einflussfaktoren ISMS BASPO“ geführt und gepflegt.

Die Einflussfaktoren werden im Rahmen der Managementbewertung jährlich überprüft und angepasst. Kurzfristige Änderungen werden durch den Informationssicherheitsverantwortlichen (InfoSiVe) beurteilt und durch den Betreiber ISMS berücksichtigt

# 5 Interessengruppen und deren Anforderungen

Besondere Interessengruppen (auch Stakeholder genannt) stellen Anforderungen an die Informationssicherheit und damit auch an das ISMS im BASPO. Diese internen und externen Parteien und ihre Anforderungen werden in der Stakeholderliste geführt und gepflegt.

Die Stakeholderliste wird im Rahmen der Managementbewertung jährlich überprüft und angepasst. Kurzfristige Änderungen werden durch den InfoSiVe beurteilt und durch den Betreiber ISMS berücksichtigt.

# 6 Vorgaben

## 6.1 Übergeordnete Vorgaben

Ein Verzeichnis zu den Rechtsgrundlagen zur Informationssicherheit ist im zentralen ISMS VBS vorhanden und wird durch den Bereich DCS (Digitalisierung und Cybersicherheit VBS) gepflegt. Darin sind alle relevanten Gesetze, Verordnungen und Vorgaben VBS (z.B. Weisungen, Reglemente) aufgeführt, die auch für das BASPO gelten. Alle übergeordneten Vorgaben sind auch für Dritte/externe Dienstleister, welche im Auftrag des BASPO arbeiten, verbindlich. Alle Verträge sind im Vertragsmanagement BASPO hinterlegt.

Des Weiteren ist eine kurze Übersicht über die aktuell gültigen Erlasse, Dokumente und Merkblätter der Informationssicherheit im Intranet unter Informationssicherheit VBS abrufbar.

## 6.2 BASPO-spezifische Vorgaben

Wo die Bundesvorgaben und die Vorgaben des ISMS VBS nicht ausreichen oder konkretisiert werden müssen, erstellt das BASPO eigene Vorgaben oder Anforderungen, welche den vorgegebenen Minimalstandard nicht unterschreiten. Für deren Umsetzung werden Sicherheitsmassnahmen definiert.

### 6.2.1 Erfüllung ISO 27001 Anforderungen

Die Erfüllung der Anforderungen von ISO 27001 wird im GRCS BASPO dokumentiert und nachgewiesen.

### 6.2.2 Anwendbarkeitserklärung (SoA)

Die Anwendbarkeitserklärung zu den 93 Controls gemäss ISO 27001 (Anhang A) wird im GRCS BASPO geführt und gepflegt. Für die Kontrollen werden Massnahmen definiert. Ihre Umsetzung wird mittels 3-Jahresplanung konkretisiert.

### 6.2.3 Schutzobjektinventar

Alle Schutzobjekte (Informationen und die zugeordneten Werte) werden zusammen mit den notwendigen Angaben (Schutzstufe, Schutzobjekt Verantwortlicher, Abhängigkeiten, etc.) im Schutzobjektinventar erfasst und durch die jeweiligen Inhaber der Schutzobjekte geführt und gepflegt.

### 6.2.4 Ausbildung und Sensibilisierung

Die Ausbildung und Sensibilisierung von Themen zur Informationssicherheit werden anhand des Sicherheitskonzeptes BASPO umgesetzt.
Aufklärung und Schulung sowie regelmässige Aktualisierungen zu den relevanten Richtlinien zielen darauf ab, dass sich Beschäftigte und ggf. Auftragnehmende ihrer Verantwortung für Informationssicherheit bewusst werden und auf welche Weise diesen Verantwortungen entsprochen wird.

### 6.2.5 Information und Kommunikation

Um Themen der Informationssicherheit angemessen zu kommunizieren, orientiert sich das ISMS am Kommunikationskonzept BASPO.

### 6.2.6 Dokumentenmanagement

Alle relevanten Dokumente zur Informationssicherheit und zum ISMS BASPO werden im GRCS gemäss Anhang A2 erstellt, gepflegt und gelenkt.

### 6.2.7 Berichtswesen und Reporting (Berichterstattung)

Die Berichterstattung über den Stand der Sicherheit wird jährlich oder bei besonderen Vorkommnissen dem Bereich DCS kommuniziert (Ziffer 12 WeFOS[2] und Ziffer 24 WIns VBS[3]).
Der Betreiber ISMS rapportiert an den Leiter ISMS. Im Vorfeld der Managementbewertung rapportiert der Betreiber ISMS zusätzlich an die zuständigen Personen der BASPO Sicherheitsorganisation.

[2] Weisungen über die Führung und Organisation der Sicherheit im VBS (WeFOS)

[3] Weisungen über die Informationssicherheit im VBS (WIns VBS)

# 7 Aufbauorganisation

## 7.1 Departement VBS

Oberste Rollenträgerin im Departement ist die Sicherheitsverantwortliche VBS (SIVE VBS, Departementsvorsteherin). Diese hat die Aufgaben an den Generalsekretär VBS delegiert.

## 7.2 Sicherheitsorganisation BASPO

Jede Verwaltungseinheit verfügt über einen Sicherheitsverantwortlichen (SIVE VE), welcher normalerweise dem Leiter der VE entspricht. Im BASPO wurde dies an den Chef Ressourcen delegiert.

Die Sicherheitsorganisation des BASPO ist dem SiVe BASPO unterstellt und die operative Führung wird durch den Chef Integrale Sicherheit (C Int Sich BASPO) wahrgenommen.
Die Sicherheitsorganisation BASPO wird auf Grund der Vielfältigkeit und den geografischen Gegebenheiten als Matrixorganisation geführt und umfasst folgende Rollen:

| Abkürzung | Rolle | Stammorganisation |
|---|---|---|
| | | |
| **B ISMS** | Betreiberin ISMS BASPO | Informatik |
| **C Int. Sich BASPO** | Chef Integrale Sicherheit | Stab Ressourcen |
| **C Obj Sich CST** | Chef Objektsicherheit CST | CST Logistik |
| **C Int Sich CST** | Chef Integrale Sicherheit CST | CST Logistik |
| **C Obj Sich NSM** | Chef Objektsicherheit NSM | Bereich NSM |
| **DSB** | Datenschutzberaterin | Rechtsdienst |
| **C Ges** | Gesundheitsschutz | Stab NSM |
| **GPV** | Geschäftsprozessverantwortlicher | Bereiche BASPO |
| **ISBO** | Informationssicherheitsbeauftragter BASPO | Stab Ressourcen |
| **L ISMS** | Leiter Informationssicherheitsmanagement System ISMS 27001 | Informatik |
| **Risk B** | Risikoberater | Bereich Ressourcen |
| **SiVe** | Sicherheitsverantwortlicher BASPO | Ressourcen |
| | | |

Tabelle 2: Rollen Sicherheitsorganisation BASPO

Die Aufbauorganisation, wie auch die Funktionen/Rollen und deren Verantwortlichkeiten in der Informationssicherheit im BASPO sind im Kapitel 7.4 beschrieben.

## 7.3 Sicherheitsgremien VBS / BASPO

Das VBS und das BASPO setzen für die strategische und operative Behandlung der Sicherheit entsprechende Gremien ein. Die Departementalen Gremien werden hier aufgeführt, da diese gegenüber dem BASPO teilweise über Weisungsbefugnisse verfügen.

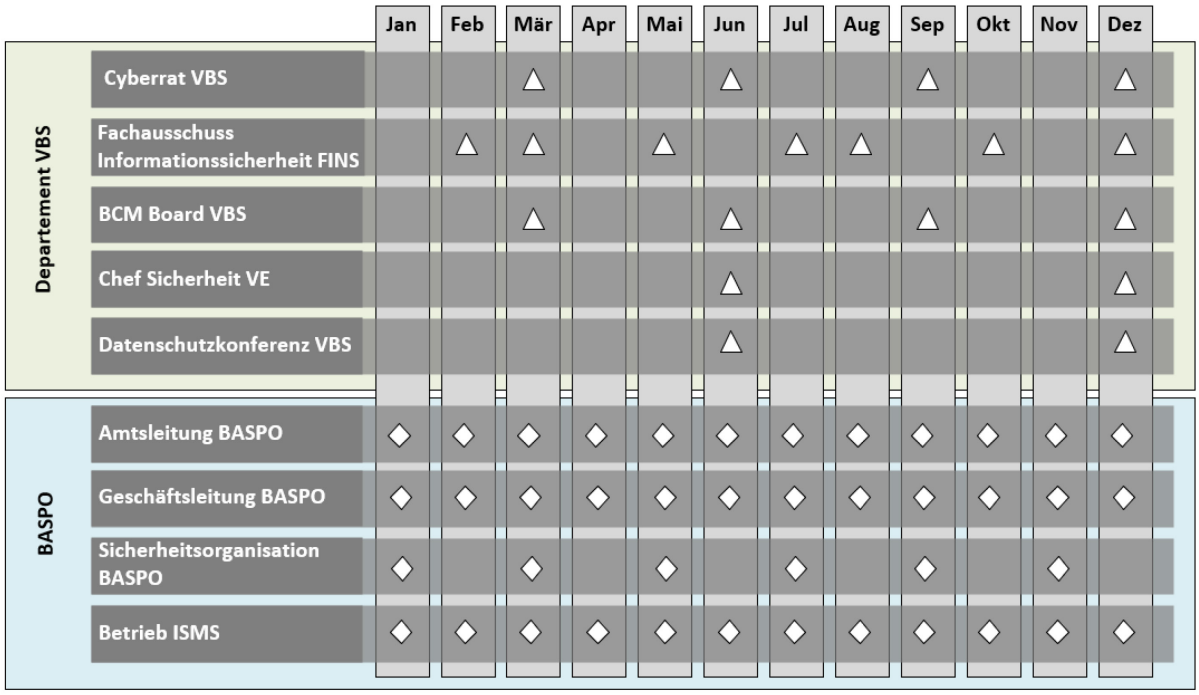
**Cyberrat VBS**
Der Cyberrat VBS ist ein Informations- und Konsultativorgan des Generalsekretärs VBS. Behandelt werden auf strategischer Ebene Themen zur Gesamtsicherheit sowie departmentsübergreifende Themen.

**Fachausschuss Informationssicherheit FINS**
Das Gremium FINS ist ein operatives Informations- Koordinationsgremium, welches durch das GS-VBS geführt wird; dieses hat beratenden Charakter. Der Teilnehmerkreis des Fachorgans Informationssicherheit VBS ist durch die Weisungen über die Informationssicherheit (WIns) VBS (Ziffer 8) nicht vorgegeben. Der ISBO BASPO nimmt am Fachausschuss Informationssicherheit VBS teil.

**BCM Board VBS**
Zur Koordination und Information wird auf Stufe Departement das BCM Board unter der Leitung des GS VBS geführt. Es dient vorwiegend dazu, BCM Themen und Aufgaben zu koordinieren und Erfahrungen über die Verwaltungseinheiten hinweg auszutauschen. Teilnehmende sind alle BCM Verantwortlichen der VBS Verwaltungseinheiten.

**Chef Sicherheit VE**
Behandelt generelle Sicherheitsthemen der Verwaltungseinheiten. Teilnehmende sind die Chefs Integrale Sicherheit der Verwaltungseinheiten. Das Gremium wird durch das GS-VBS geführt.

**Datenschutzkonferenz VBS**
Fachgremium zum Thema Datenschutz. Die Teilnehmerin seitens BASPO an der Datenschutzkonferenz VBS ist der Datenschutzberaterin BASPO; dies ist durch die Datenschutzweisungen VBS (Ziffer 6) vorgegeben.




Die übergeordneten Sicherheitsgremien tagen quartalsweise oder nach Bedarf.

**Amtsleitung BASPO (AL BASPO)**
Die AL BASPO behandelt Sicherheitsthemen auf strategischer Ebene.

**Geschäftsleitung BASPO (GL BASPO)**
Die GL BASPO behandelt operative Sicherheitsthemen, welche das gesamte BASPO betreffen. Das Gremium dient unter anderem auch dazu, die Geschäftsprozessverantwortlichen direkt zum Thema Integrale Sicherheit zu informieren und einzubinden.

**Sicherheitsorganisation BASPO**
Die Sicherheitsorganisation BASPO führt unter der Leitung des C Int Sicherheit regelmässige treffen durch. Es behandelt Aufgaben und Themen der Integralen Sicherheit BASPO. Teilnehmende sind die verantwortlichen Rollenträger des jeweiligen Sicherheitbereiches.

**Betrieb ISMS**
Innerhalb der Informatik BASPO findet wöchentlich ein operativer Abgleich zum ISMS Betrieb statt. Teilnehmende sind die Betreiberin ISMS und der Leiter ISMS. Ziel ist, das Tagesgeschäft zu priorisieren, Anliegen und Aufgaben möglichst zeitnah zu behandeln. Es trägt zur kontinuierlichen Weiterentwicklung des ISMS BASPO bei.

## 7.4 Funktionen und Rollen

Für alle aufgeführten Funktionen und Rollen gibt es Stellvertretungen.

### 7.4.1 Informationssicherheitsverantwortliche (InfoSiVe)

Die **AKVs** sind in den Weisungen über die Informationssicherheit (WIns) VBS (Ziffer 6) definiert. **Inhaber der Rolle** ist der Chef Ressourcen, welcher als SiVe die Gesamtsicherheit verantwortet.

### 7.4.2 Datenschutzberaterin

Die **AKVs** sind in den Datenschutzweisungen VBS (Ziffer 5) definiert. Die Rolle der Datenschutzberaterin ist im Rechtsdienst BASPO angesiedelt.

**Anforderungsprofil**

- Abgeschlossenes Studium der Rechtswissenschaften (Jurist)
- Kenntnisse der gesetzlichen Regelungen, bereichsspezifischen datenschutzrechtlichen Regelungen und der einschlägigen Spezialvorschriften
- Unabhängigkeit bei der Aufgabenerfüllung, hohe Fachkunde und Zuverlässigkeit

### 7.4.3 Informatiksicherheitsbeauftragter der Organisation (ISBO)

**Vorgaben** sind in der Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV) (Art. 14) definiert.
Die Rolle des ISBO ist organisatorisch dem Stab des Bereiches Ressourcen zugeordnet.

**Anforderungsprofil**

- Abgeschlossenes (Fach-)Hochschulstudium Fachrichtung Informatik oder Wirtschaftsinformatik (oder vergleichbare Ausbildung)
- Weiterbildung oder mehrjährige einschlägige Berufserfahrung im Informations- und/oder IT-Sicherheitsbereich

## 7.4.4 Leiter ISMS

Der Leiter ISMS ist verantwortlich für die BASPO-spezifische Umsetzung der Weisung der Informationssicherheitsverantwortlichen VBS über die Informationssicherheit (WSVIns VBS). Er verantwortet die kontinuierliche Weiterentwicklung des ISMS BASPO.

**Anforderungsprofil**

- Abgeschlossenes (Fach-)Hochschulstudium Fachrichtung Informatik oder Wirtschaftsinformatik (oder vergleichbare Ausbildung)
- Fachkenntnisse in den Bereichen ISO 27000ff, Informationssicherheitsmanagementsystem ISMS oder weiteren Managementsystemen
- Fachkompetenz in den Bereichen Risikomanagement, Notfall- und Krisenmanagement

## 7.4.5 Betreiber ISMS

Sie betreibt im Auftrag des Leiters ISMS das Managementsystem gemäss den VBS-Vorgaben sowie den Vorgaben des BASPO. Die **AKVs** sind in der Stellenbeschreibung beschrieben. Die Rolle der Betreiberin ISMS BASPO ist im Teilbereich Informatik angesiedelt.

**Anforderungsprofil**

- Abgeschlossenes (Fach-)Hochschulstudium Fachrichtung Informatik oder Wirtschaftsinformatik (oder vergleichbare Ausbildung)
- Fachkenntnisse in den Bereichen ISO 27001 und 27002
- Kenntnisse zum Projektmanagement, Risikomanagement, zu Aufbau und Betrieb des Schutzobjektinventars

## 7.4.6 Inhaberin oder der Inhaber des Schutzobjektes Information

Die **AKVs** sind in den Weisungen über die Informationssicherheit (WIns) VBS (Ziffer 11) definiert.

## 7.4.7 Risikoeigner

Die **AKVs** sind in den Weisungen über die Informationssicherheit (WIns) VBS (Ziffer 10) sowie den Risikorichtlinien Bund (Kap. 3 Funktionen und Verantwortlichkeiten) beschrieben.

## 7.4.8 Rollenträger BASPO

| Rolle | Name/Vorname | Bereich | Funktion Stammorganisation |
|---|---|---|---|
| InfoSiVe | Wägli Hanspeter | RES | Chef Ressourcen |
| Datenschutzberaterin | Panicali Sabrina | SP / RD | Juristin Rechtsdienst |
| ISBO | Amsler Fritz | RES / Stab | ISBO |
| Leiter ISMS (GPV) | Häusler Roland | RES / IT | Leiter Informatik |
| Betreiber ISMS | Schneider-Köppel Judith | RES / IT | ICT-Controllerin / Betrieb ISMS |
| C Sich BASPO | Amsler Fritz | RES / Stab | C Int Sicherheit |

Tabelle 3: Rollenträger BASPO

# 8 Ablauforganisation

Das Informationssicherheits-Managementsystem (ISMS) (gemäss WIns VBS) hat zum Zweck, durch Regelwerke, Prozesse, Vorgaben und Verbesserungsmechanismen die Steuerung, Messung und Kontrolle der Vertraulichkeit, Integrität, Verfügbarkeit und Nachvollziehbarkeit von Informationen unter Berücksichtigung der bestehenden Risiken zu gewährleisten. Mit dem ISMS BASPO wird sicherstellt, dass dessen Anforderungen in die Geschäftsprozesse der Organisation integriert werden.

## 8.1 Übersicht ISMS BASPO

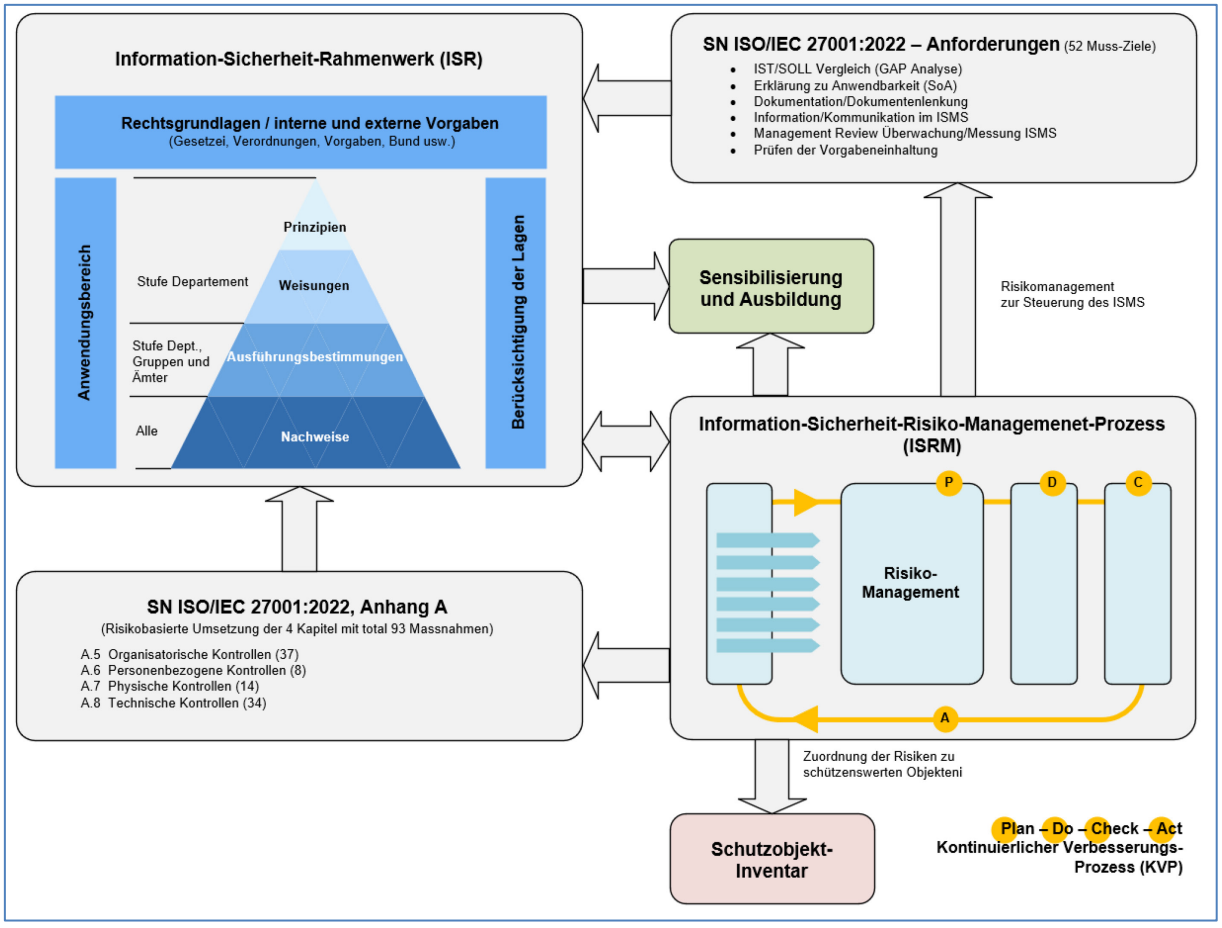



Abbildung 2: ISMS BASPO

Die Ablauforganisation des BASPO richtet sich nach dem Standard ISO 27001/2. Die Grundsätze, Prozesse und Definitionen zum Risikomanagement in der Informationssicherheit sind im Anhang A1: Informationssicherheits-Risikomanagement (ISRM) detailliert beschrieben.

## 8.2 Betrieb des ISMS

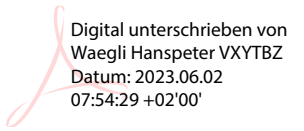
Das ISMS im BASPO wird durch die Rolle „Betreiber ISMS “ (gemäss Aufbauorganisation Kap. 7) betrieben und gepflegt. Diese ist dem Leiter ISMS unterstellt, der im Auftrag des SiVe für das ISMS verantwortlich ist.

# 9 Inkrafttreten

Das Inkrafttreten erfolgt mit der Unterschrift durch den Informationssicherheitsverantwortlichen (InfoSiVe) BASPO.

*Magglingen, .....*

Waegli Hanspeter VXYTBZ




.....

Hanspeter Wägli
Informationssicherheitsverantwortlicher (SiVe) BASPO