



Anforderungen der Finanzaufsicht praktikabel umsetzen - ist das möglich?

it-sa 2019 **Nürnberg** **Halle 10.0 – Stand 421**

Frank Hensel **Leiter ISM-Services** **Beratung** **09.10.2019**

Dr. Jörg Kandels **Leiter ISM-Services** **Produkte** **10.10.2019**



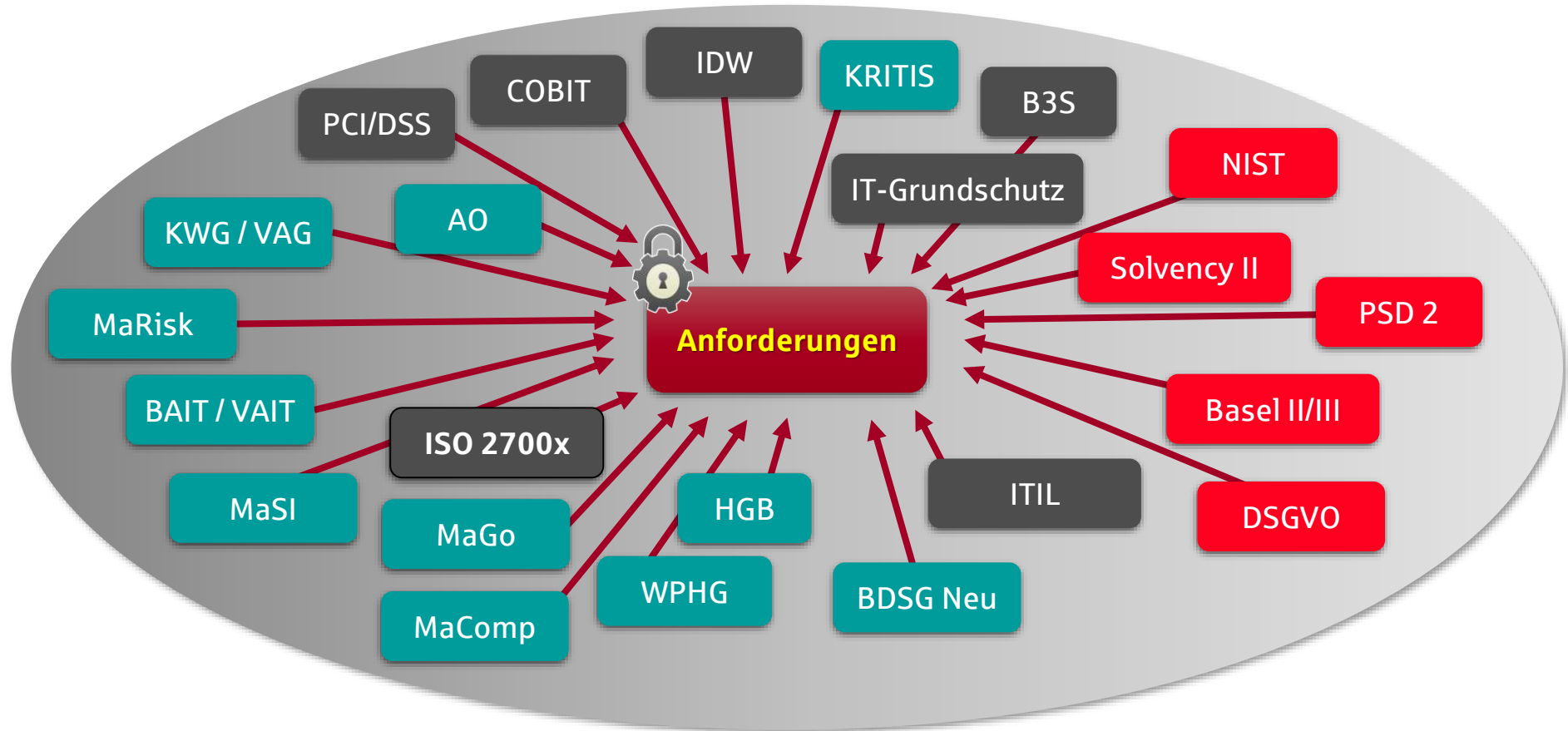
Unser breites Produktportfolio zur Informationssicherheit und Notfallplanung (> 20 Mitarbeiter)



Anforderungen der Finanzaufsicht praktikabel umsetzen

Alles klar – oder nicht

Was ist relevant ... wie passt das zusammen ... wer sammelt und kanalisiert die Flut ?



Ausrichtung am Risiko als übergeordnetes Prinzip - Bewertung und Steuerung erforderlich

MaRisk AT 7.2

IT-Systeme ... und die zugehörigen IT-Prozesse müssen die Integrität, ... Verfügbarkeit, ... Authentizität ... Vertraulichkeit der Daten sicherstellen.

Für diese Zwecke ist bei **der Ausgestaltung der IT-Systeme und der zugehörigen IT-Prozesse** grundsätzlich auf **gängige Standards** abzustellen, ...

Die Eignung der IT-Systeme und der zugehörigen Prozesse **ist regelmäßig** von den fachlich und technisch zuständigen Mitarbeitern **zu überprüfen**.

BAIT / VAIT

Ausgestaltung der IT-Systeme und ... IT-Prozesse grundsätzlich auf **gängige Standards** abzustellen.

Zu diesen zählen ... die IT-Grundsatzkataloge des Bundesamts für Sicherheit in der Informationstechnik und der **internationale Sicherheitsstandard ISO/IEC 2700X** der International Organization for Standardization.

BAIT / VAIT

konkretisierende, den **Stand der Technik** berücksichtigende **Informationssicherheitsrichtlinien** und **Informationssicherheitsprozesse**

BAIT

Wegen der **grundlegenden Bedeutung der IT** für das Institut ist auch **für jeden sonstigen Fremdbezug von IT-Dienstleistungen vorab** eine **Risikobewertung** durchzuführen.

BAIT / VAIT

Das Institut hat ... das **Informationsrisikomanagement**, das **Informationssicherheitsmanagement**, den **IT-Betrieb** und die **Anwendungsentwicklung** quantitativ und qualitativ **angemessen mit Personal** auszustatten.

BAIT / VAIT

Die **Anforderungen des Instituts zur Umsetzung der Schutzziele** in den Schutzbedarfskategorien **sind festzulegen** und in geeigneter Form zu dokumentieren (**Sollmaßnahmenkatalog**).

BAIT / VAIT

Die **Risikoanalyse** auf Basis der **festgelegten Risikokriterien** hat auf Grundlage eines **Vergleichs der Sollmaßnahmen mit den jeweils wirksam umgesetzten Maßnahmen** zu erfolgen.

Sonstige **risikoreduzierende Maßnahmen** aufgrund unvollständig umgesetzter Sollmaßnahmen **sind wirksam zu koordinieren, zu dokumentieren, zu überwachen und zu steuern**.

Die **Ergebnisse der Risikoanalyse** sind zu genehmigen und **in den Prozess des Managements der operationellen Risiken zu überführen**.

BAIT / VAIT

u.v.m.



Anforderungen

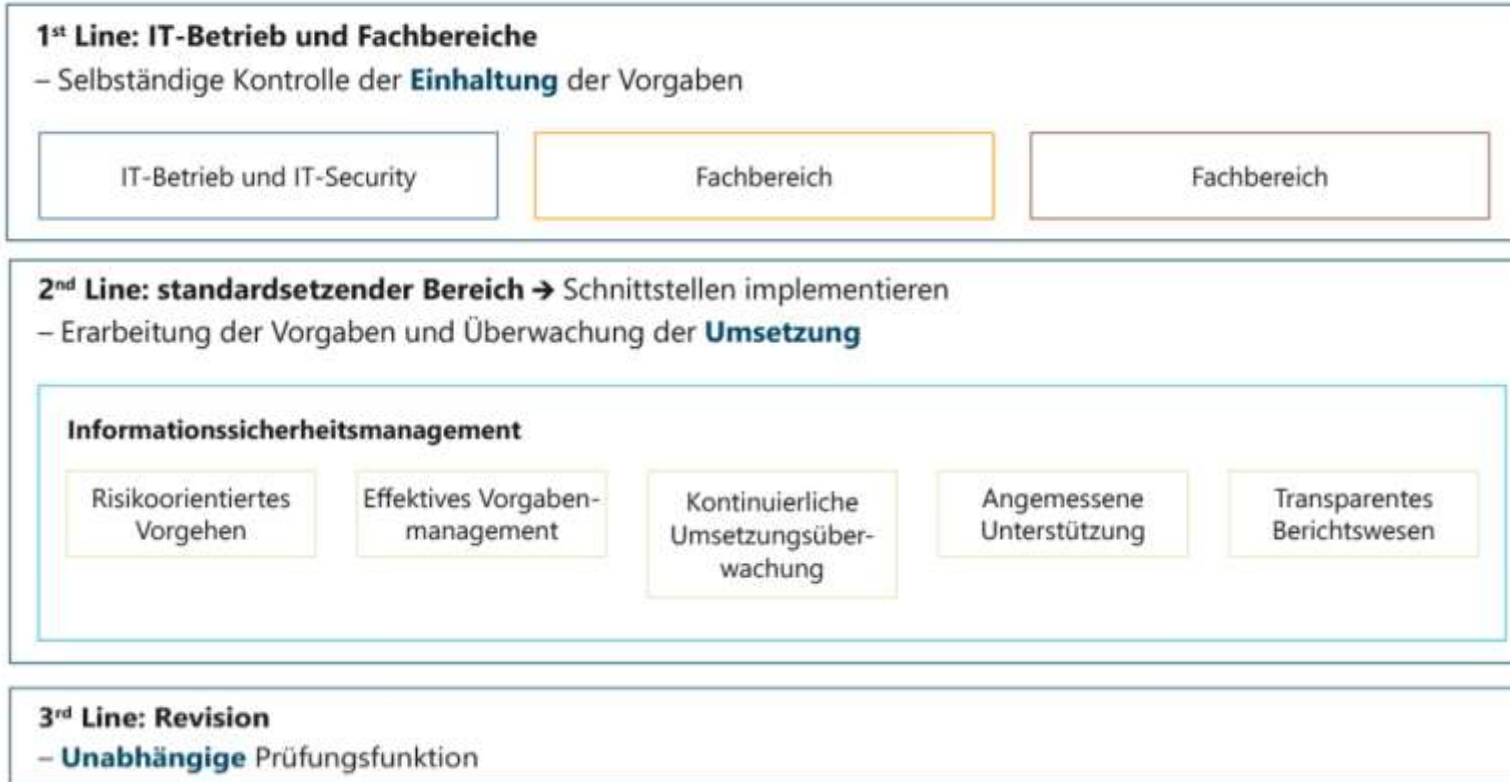
IT-Systeme & zugehörige IT-Prozesse
Integrität – Verfügbarkeit – Vertraulichkeit

konkretisierende Richtlinien & Leitlinien
Maßnahmen nach Stand der Technik
Sollmaßnahmen / -katalog
Wirksame Umsetzung
Risikobewertung / -analyse
Kontrolle / Audit
u.v.m.

Three Lines of Defence

Aber: Wer macht eigentlich was? Oder : Toll, ein Anderer macht's?




Fragen wir die Aufsicht!

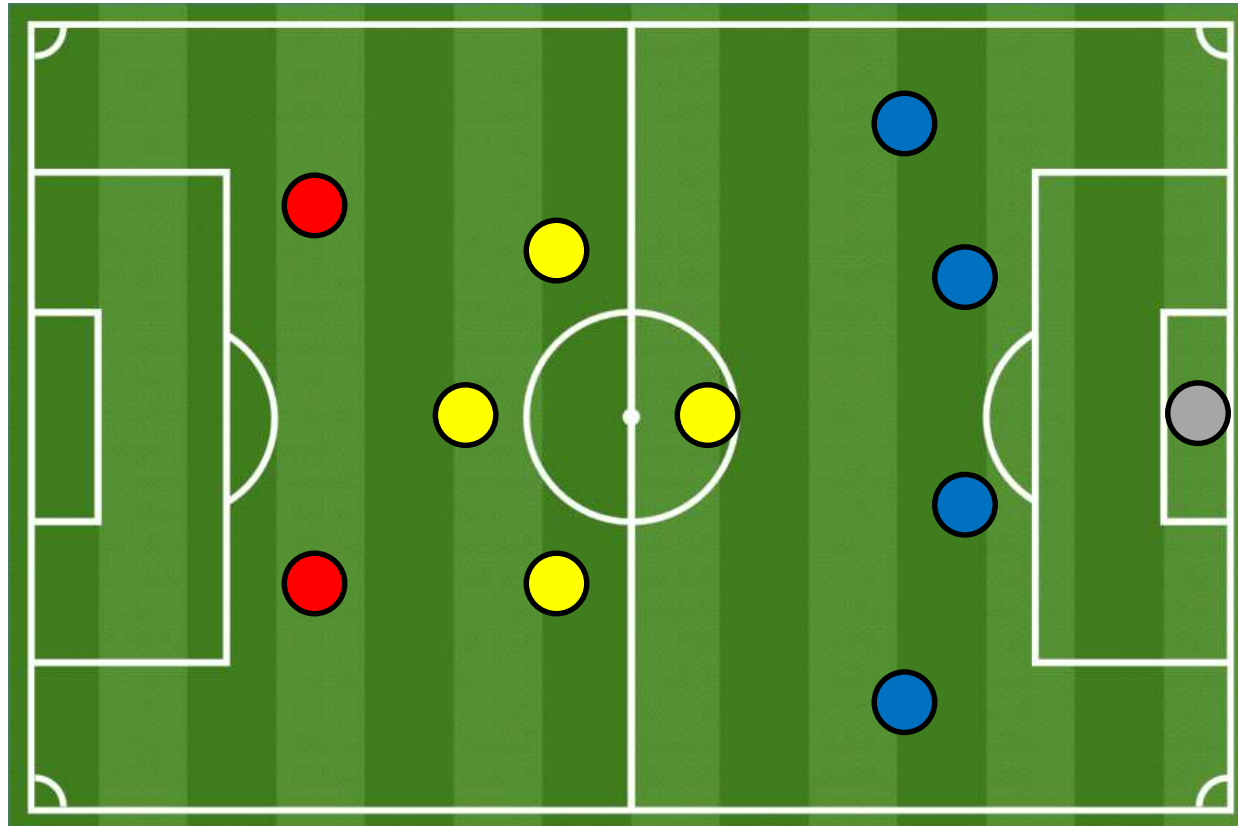


© Quelle: Eigene Darstellung – in Anlehnung an Three-Lines-of-Defence-Modell aus dem Occasional Paper Nr. 11 der BIS, 2015, Bank for International Settlements (BIS).

Die „3-Lines of defense“ – wo steht wer und wie viele machen was?




So gewinnt man im Fußball

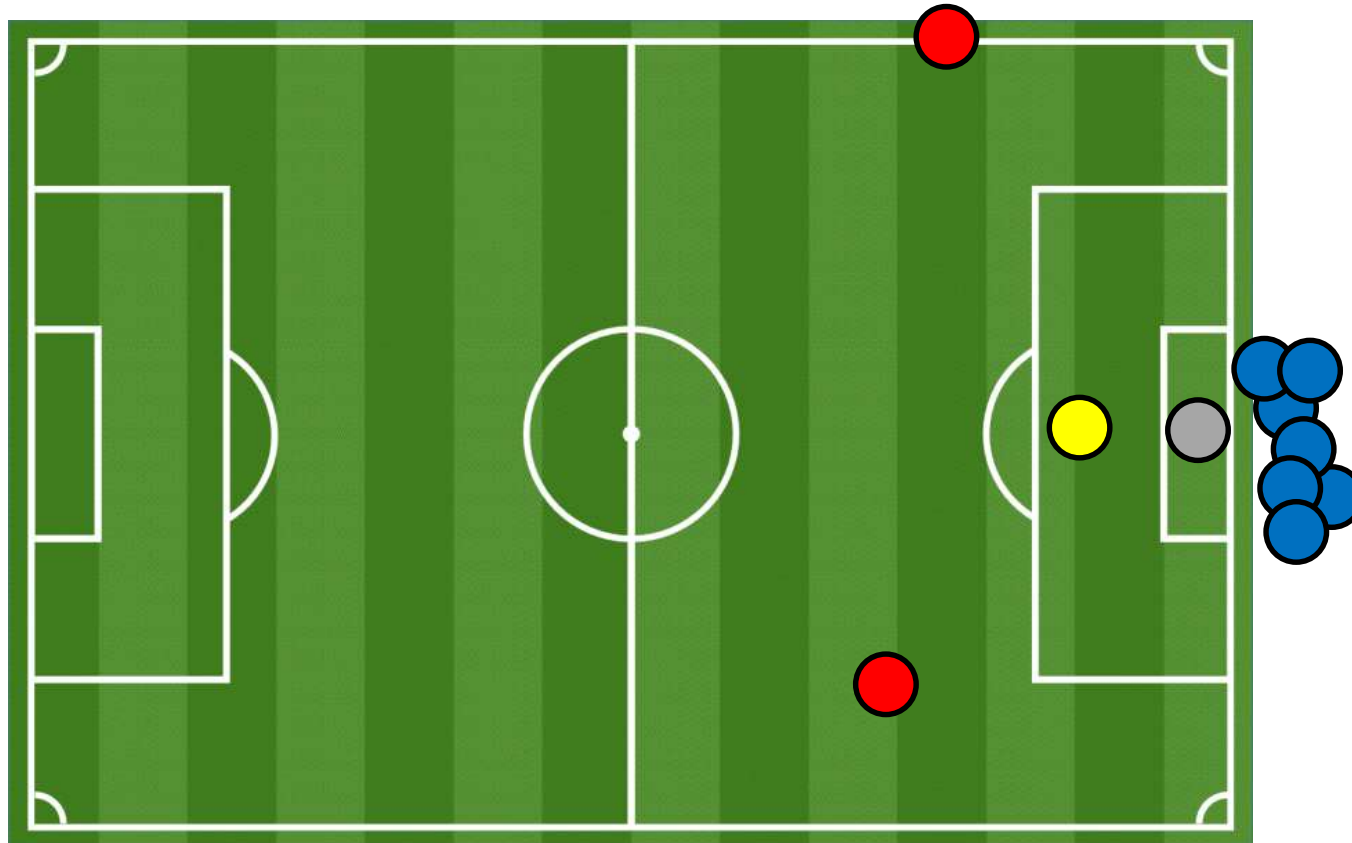
-  Sturm
-  Mittelfeld
-  Verteidigung

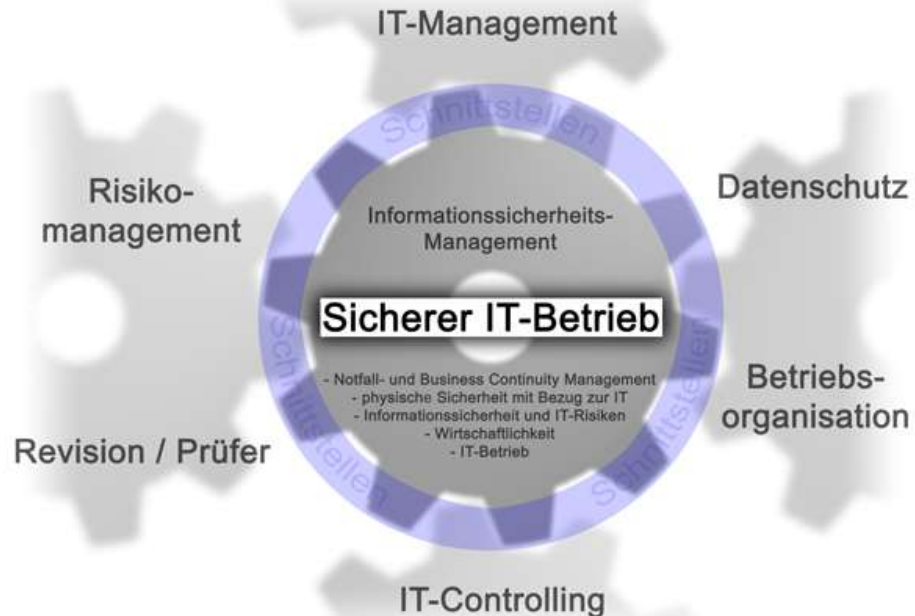


Die „3-Lines of defense“ – wo steht wer und wie viele machen was?

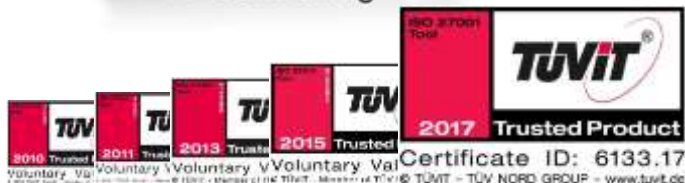
So stehen die Verteidigungslinien bei vielen Banken/Versicherungen

-  1. Line (Betrieb)
-  2. Line (ISM)
-  3. Line (Revision)





- **Prozessmodell** zum ISMS
- **aktuelle branchenspezifische Regulatorik** (MaRisk, BAIT / VAIT, ...)
- gängige **Standards** (ISO2700X, COBIT, BSI, IDW, ...)
- **"Best Practice"-Ansätze** zur Umsetzung
- **Muster und Leitfäden**
- **Nachschlagewerk und Dokumentationswerkzeug**
- **Audit-Methode und IS-Risikomanagement**
- **Regelmäßige Aktualisierung**



Eine ISMS-Lösung muss alle Verteidigungslinien adressieren

„Sicherer IT-Betrieb“ enthält Anforderungen für alle Verteidigungslinien (egal wer es macht)

Sicherer IT-Betrieb

Prozess und Aktivitäten

COBIT

Finanzaufsicht

IDW

ISO 27001

Konzern

ISO 2700x

IT-Grundschutz

ITIL

Umsetzungshilfen

ITM-Radar

KRITIS

OPDV

2. Line Anforderungen

0 Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Context of the organization

5 Leadership

5.1 Leadership and commitment

5.2 Policy

5.3 Organizational roles, responsibilities and authorities

- o CIA Es sollte ein **Informationssicherheits-Beauftragter (ISE)** benannt werden, der für die Durchführung des ISM verantwortlich ist. [RC0014]
- o CIA Der ISB sollte der Unternehmensführung direkt unterstellt sein. Ihm sollte muss gemäß Tz. 4.29 VWT ein direktes Berichtsrecht an die Unternehmensführung. [RC0015]
- o CIA Die Kompetenzen des ISB sollten ausreichend geregelt sein, um die ISM-Entscheidungs- und Weisungsbefugnisse notwendig. [RC0017]
- o CIA Es sollte gemäß Tz. 4.19 BAIT eine Vertretung (z.B. durch einen Stellvertreter) (auch bei Teilzeitbeschäftigung), da manche Aufgaben ständig anfallen. [RC0018]
- o CIA Es sollten gemäß Tz. 4.19 BAIT mit der Unternehmensführung ausreichende personelle Ressourcen für die operativen Aufgaben des ISB vorhanden sein. Diese sollten durch weitere Mitarbeiter unterstützt werden, sollten diese in dieser Funktion dem ISB unterstehen. [RC0019]
- o CIA Die Aufgabeberechnung des ISB sollte schriftlich festzulegen. [RC0020]
- o CIA Die Bestellung des ISB sollte gemäß Tz. 4.18 BAIT muss gemäß Tz. 4.20 VWT bekannt gegeben werden. [RC0021]

1. Line Anforderungen

A.10 Cryptography

A.11 Physical and environmental security

A.11.1 Secure areas

A.11.1.1 Physical security perimeter

A.11.1.2 Physical entry controls

A.11.1.3 Securing offices, rooms and facilities

A.11.1.4 Protecting against external and environmental threats

A.11.1.5 Working in secure areas

A.11.1.6 Delivery and loading areas

A.11.2 Equipment

Arbeitsumgebung erfolgen. [RC0166]

Zutritts- und Einbruchschutz von Fenstern und Türen [GR575]

Für einen wirksamen Einbruchschutz für Türen, Fenster, Schächte und andere Öffnungen (siehe auch Umsetzungshilfe **Nämen zur physischen Sicherheit**)

- o CIA Fenster in IT-Räumen mit Einsteigsmöglichkeiten von außen (z.B. im Erdgeschoss) sollten durch eine Verriegelung zu Balkonen oder Fluchtwegen) sollten nach Möglichkeit gesichert werden. [RC0571]
- o CIA Es sollte regelmäßig überprüft werden, ob Fenster und Türen richtig geschlossen sind. [RC0571]
- o CIA Bei **Notausgängen** und **Fluchttüren**, die nicht gesichert werden können, sollten zusätzliche Maßnahmen zur Überwachungsüberwachung eingesetzt werden, wie z.B. Videoüberwachung. [RC0572]
- o CIA Fenster und Türen, durch die man in das Gebäude gelangen kann, sollten mindestens der Widerstandsklasse RC 2 (DIN EN 1627) entsprechen bzw. sollte dies in zusätzlichen Anforderungen vorgesehen werden. [RC0574]
- o CIA Für sicherheitsrelevante Bereiche sollte die Widerstandsklasse RC 4 (DIN EN 1627) vorgesehen werden. Falls Fenster und Türen durch eine Einbruchmeldeanlage abgesichert sind, kann die Widerstandsklasse RC 3 als ausreichend angesehen werden. [RC0583]

Zutritts- und Einbruchschutz bei Übergängen von Schutzzonen [GR239]

- o CIA Nach außen gefinde Türen (Balkone, Terrassen) sowie Fenster mit Einsteigsmöglichkeiten von außen (z. B. im Erdgeschoss oder mit Verbindung zu Balkonen oder Fluchtwegen) sollten in Zeiten, in denen ein Raum nicht besetzt ist, geschlossen werden. [RC0570]

Finanzinstitute haben viele Dienstleister



Die bisher eigenständig erfolgreichen „Inseln“ SITB und SIMON wachsen in 2020 zur modularen Komplettlösung zusammen!



Lösung für das
Informationssicherheits-
Management



Prozess-/IS-/DS-Risikomanagement
Strukturanalyse – Schutzbedarf – VVT
Sollmaßnahmen und Assets



Lösung für das
IT-Management



Risk

Prozessrisiken
Auslagerungsrisiken
Projektrisiken
IS-/IT-Risiken
Schutzbedarf
Notfall-Kritikalität

Management

Prozesse / IKS
Projekte / -Kapazitäten
IT-Kosten
Verträge / Dienstleister
IT-Architektur / -Infrastruktur
Informationssicherheits-
Management
Datenschutz-Management
Notfallmanagement

Governance

Internationale/nationale
Vorschriften
Internationale/nationale
Standards
Strategische Planung und
IT-Strategie

**Sie haben Fragen zu Beratungsthemen oder Produkt?
Wir sind am Stand 10.0 - 421 gerne für Sie da!**



Frank Hensel

Leiter ISM-Services

Telefon: +49 228 4495 7412

E-Mail: frank.hensel@siz.de



Dr. Jörg Kandels

Leiter ISM-Services

Telefon +49 228 4495 7397

E-Mail: joerg.kandels@siz.de