SIZ

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**

Die SIZ GmbH – in aller Kürze
> 200 Mitarbeiter / Umsatz 2018: ca. 27 Mio. € / div. Spezialisierungen

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

Beratung und Unterstützung

Kompetenz zu
allen Sicherheitsfragen

Zertifizierung

ISMS und IT-Anwendungen

Audits und Penetrationstests

Schwachstellen
frühzeitig erkennen und abstellen

Sicherer IT-Betrieb

Aufbau und Betrieb von
ISO 27001-konformen
Informationssicherheits-
Managementsystemen (ISMS)

IDV-Suite

Lösung für alle Risikofelder im
Umgang mit IDV-Anwendungen

Risikobehandlung

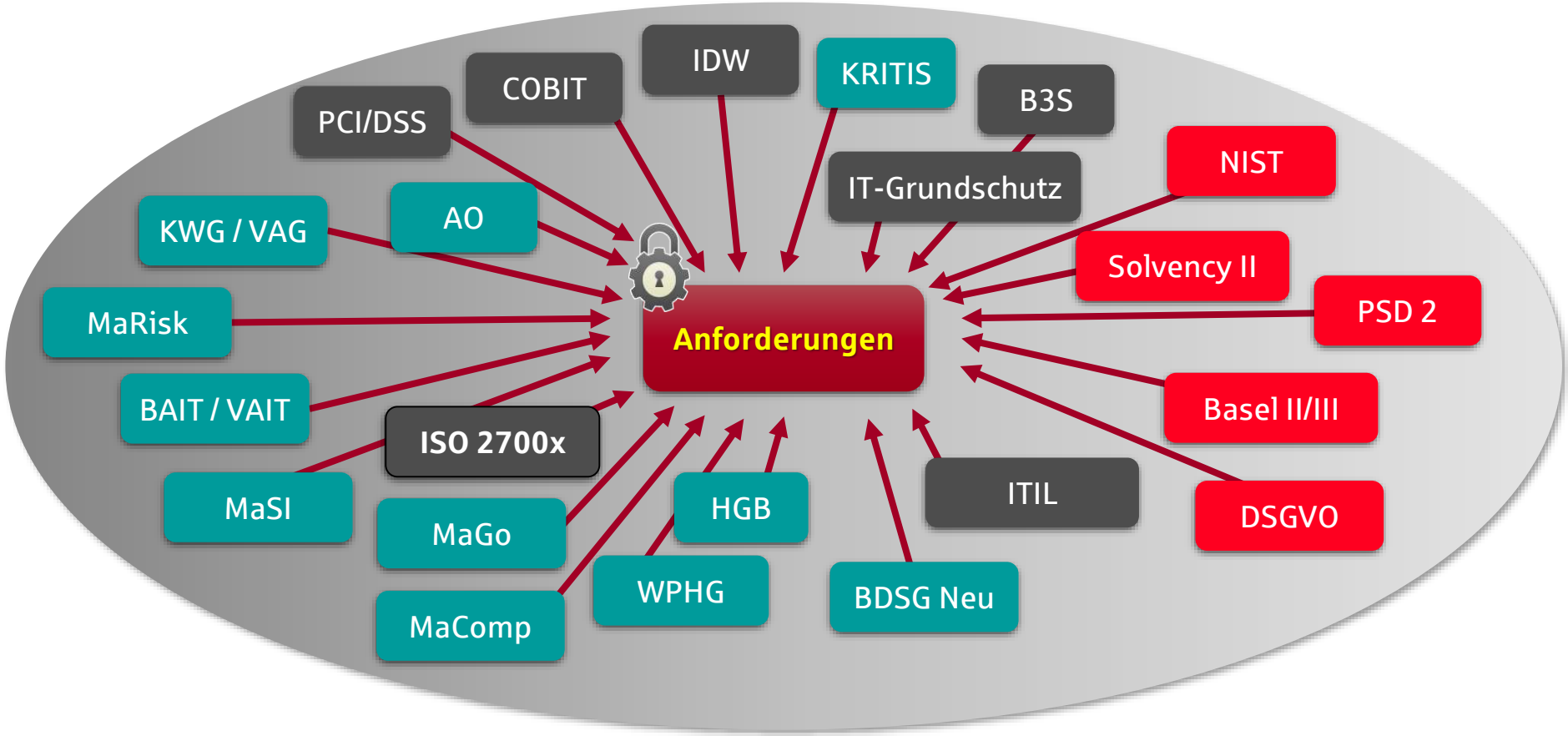
Informationssicherheits-Risiken
identifizieren, bewerten, behandeln

BCM und IT-Notfallplanung

Proaktive Vorbereitung
auf den Notfall

Anforderungen der Finanzaufsicht praktikabel umsetzen
Alles klar – oder nicht

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



Anforderungen der Finanzaufsicht praktikabel umsetzen
ISMS + IS-Risikomanagement: Was bedeutet das genau?

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-Grundschutzkataloge 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.

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.

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**.

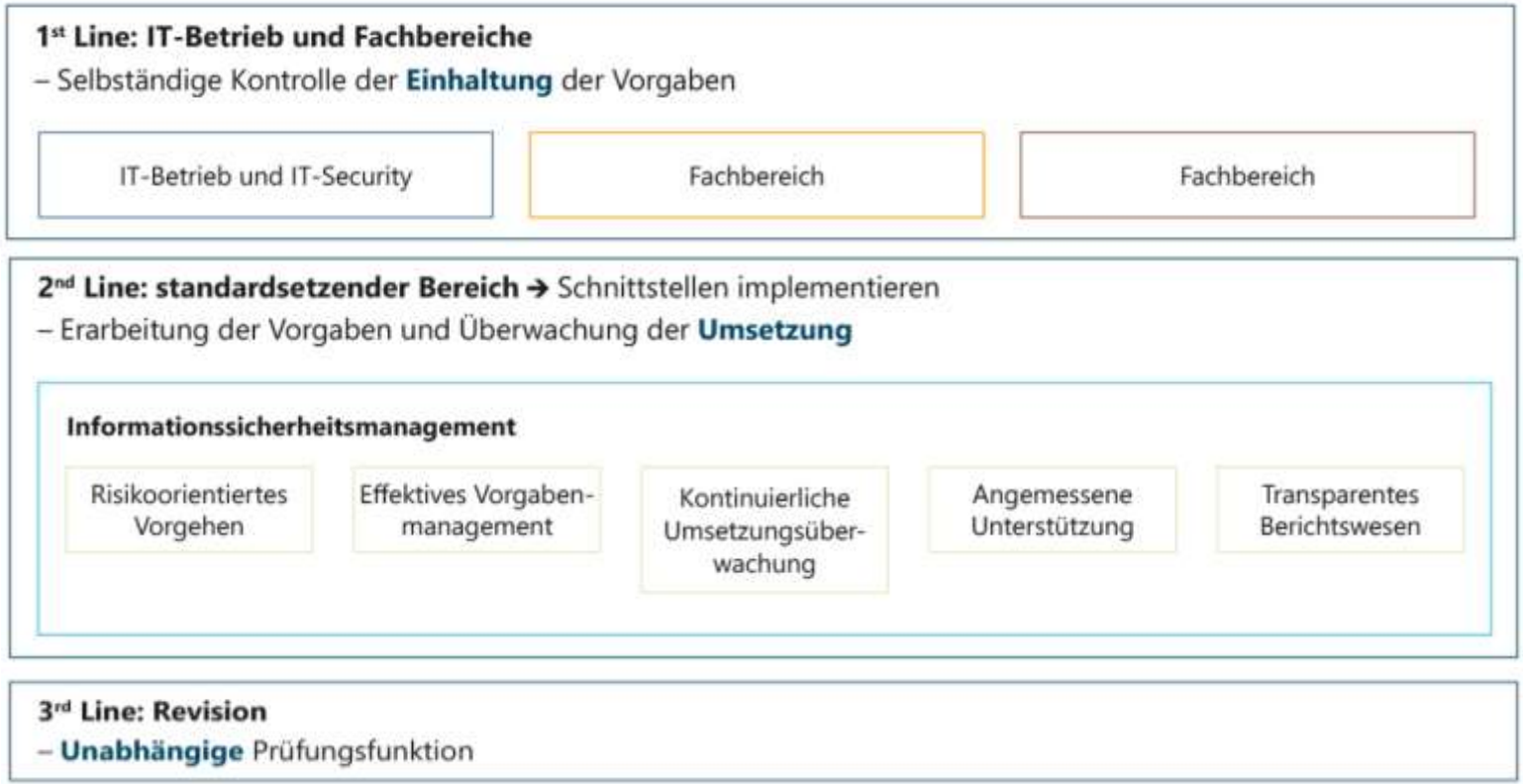
Die **Ergebnisse der Risikoanalyse sind** zu genehmigen und **in den Prozess** des **Managements** der **operationellen Risiken zu überführen**.

BAIT / VAIT
u.v.m.

Three Lines of Defence

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

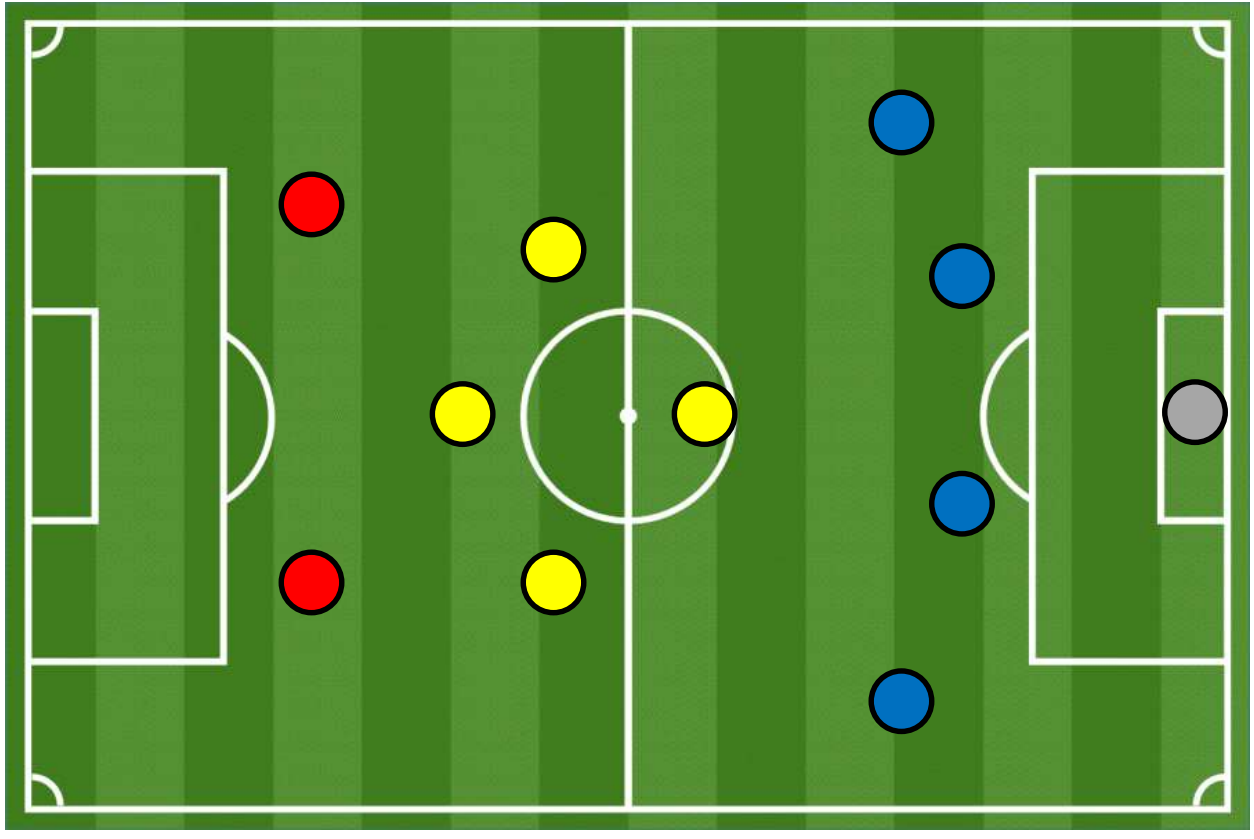
Fragen wir die Aufsicht!



© 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



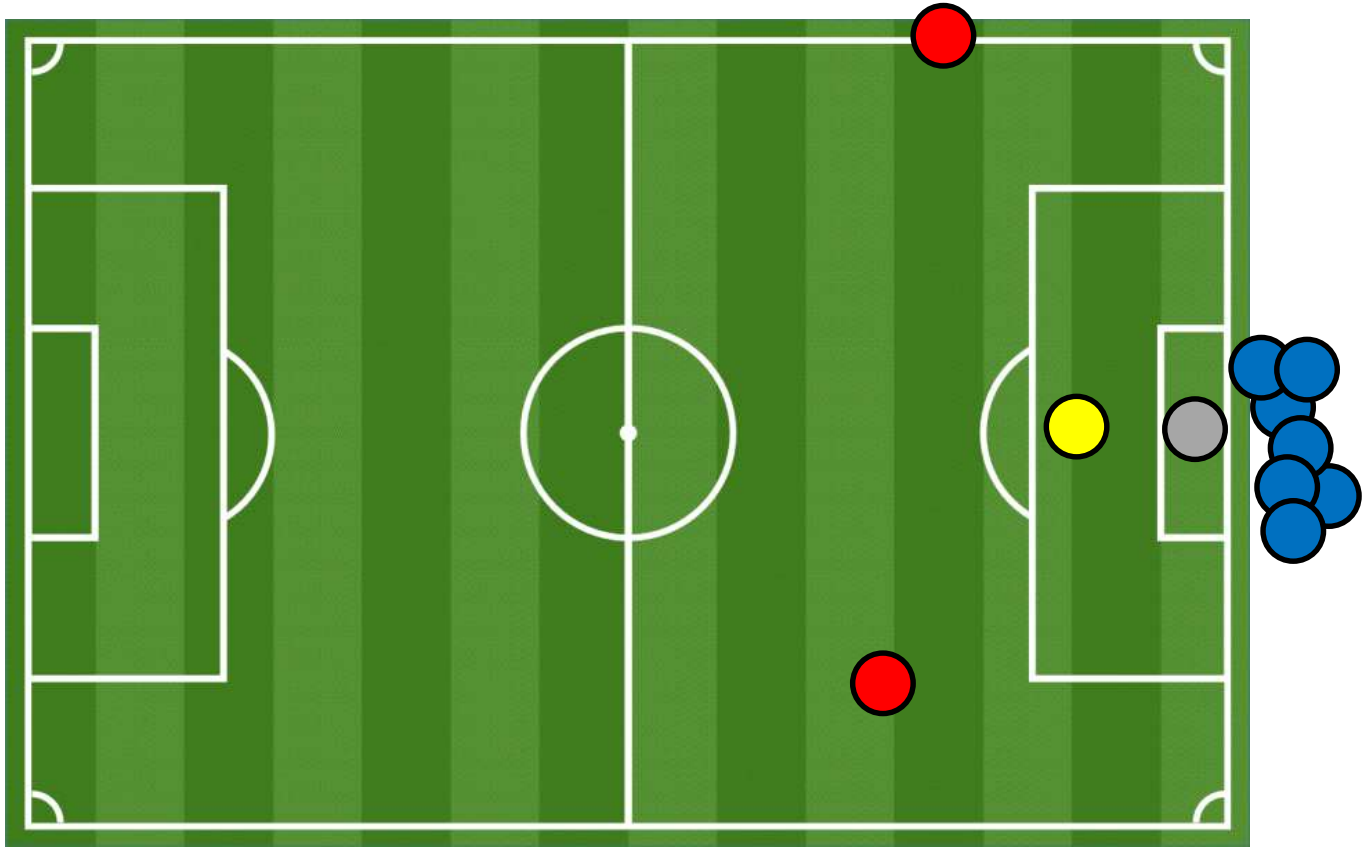
Sturm

Mittelfeld

Verteidigung

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

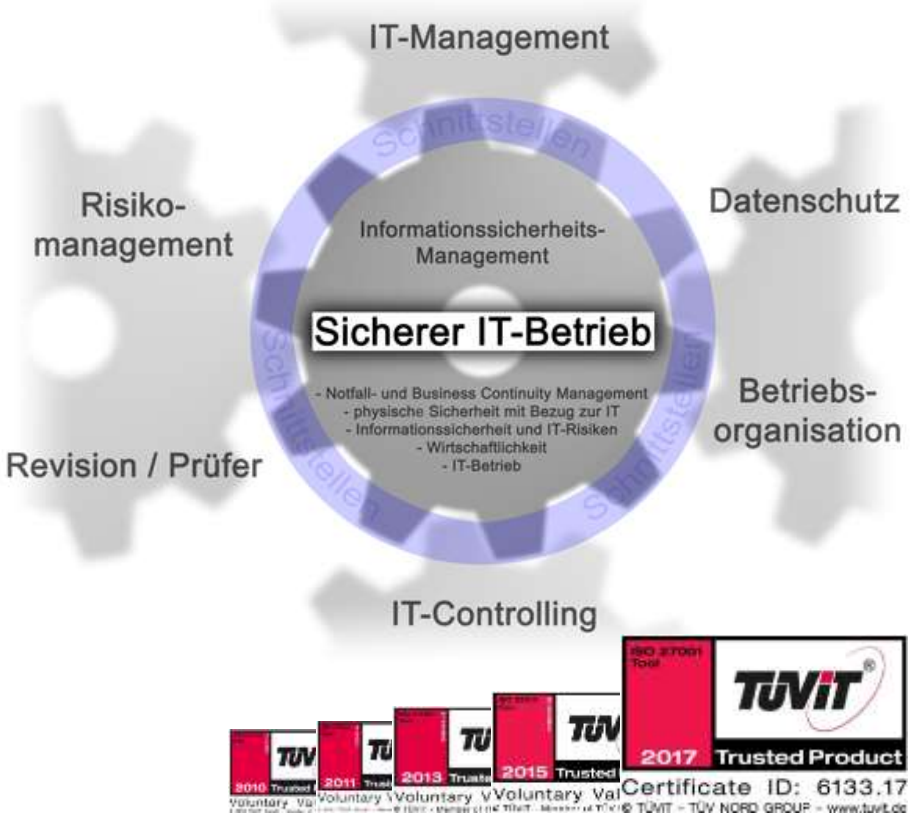
So stehen die Verteidigungslinien bei vielen Banken/Versicherungen



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

Produkt Informationssicherheit - Sicherer IT-Betrieb

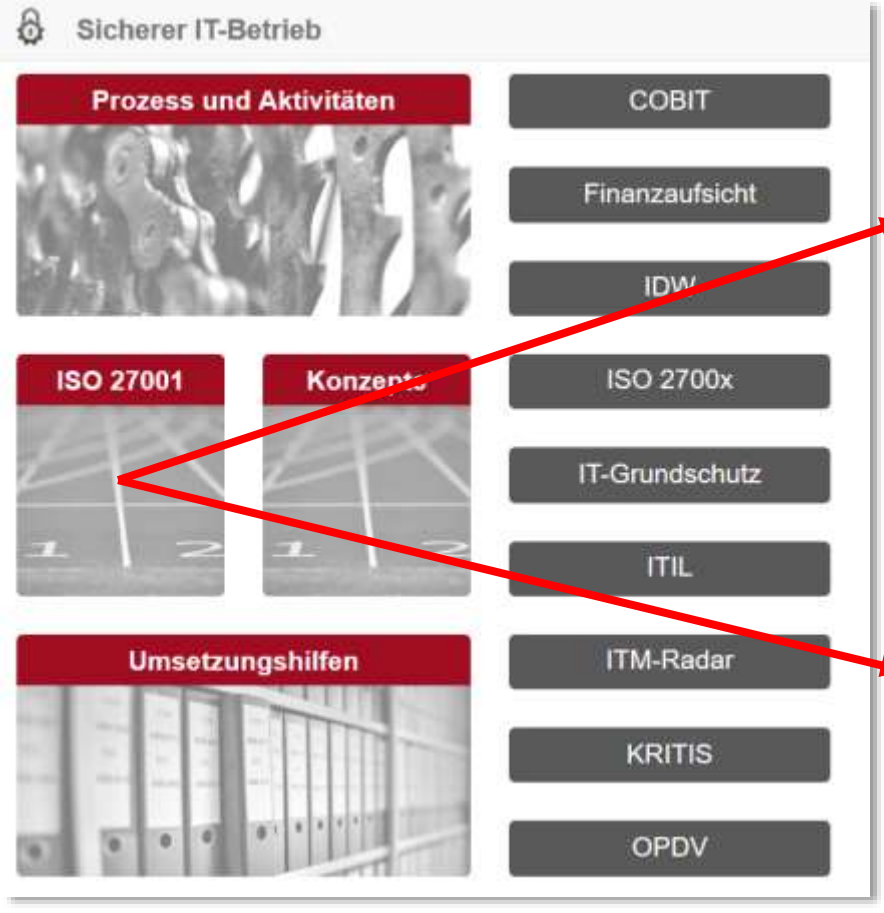
ISO27001-Informationssicherheits-Management mit „Sicherer IT-Betrieb“

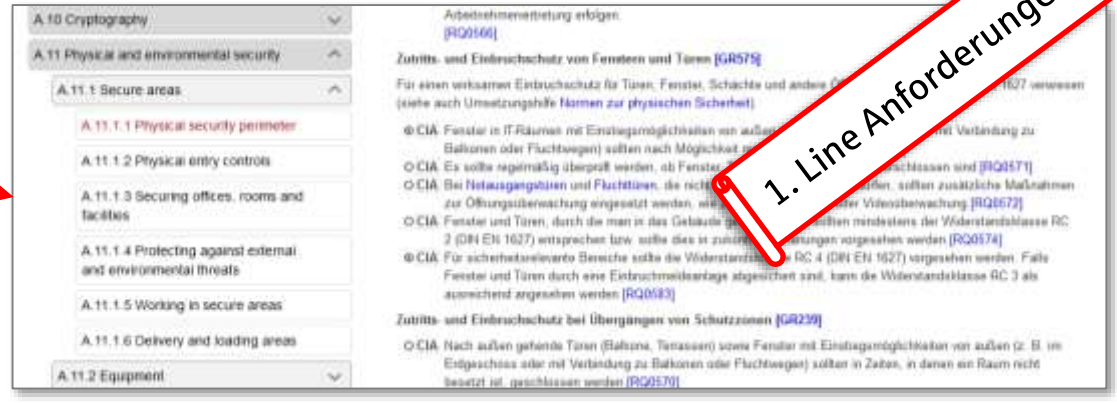


- **Prozessmodell** zum ISMS
- **aktuelle branchenspezifische Regulatorik** (MaRisk, BAIT / VAIT, …)
- gängige **Standards** (ISO2700X, COBIT, BSI, IDW, …)
- **"Best Practice"**-Ansätze zur Umsetzung
- **Muster und Leitfäden**
- **Nachschlagewerk** und **Dokumentationswerkzeug**
- **Audit-Methode und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

Eine ISMS-Lösung muss alle Verteidigungslinien adressieren

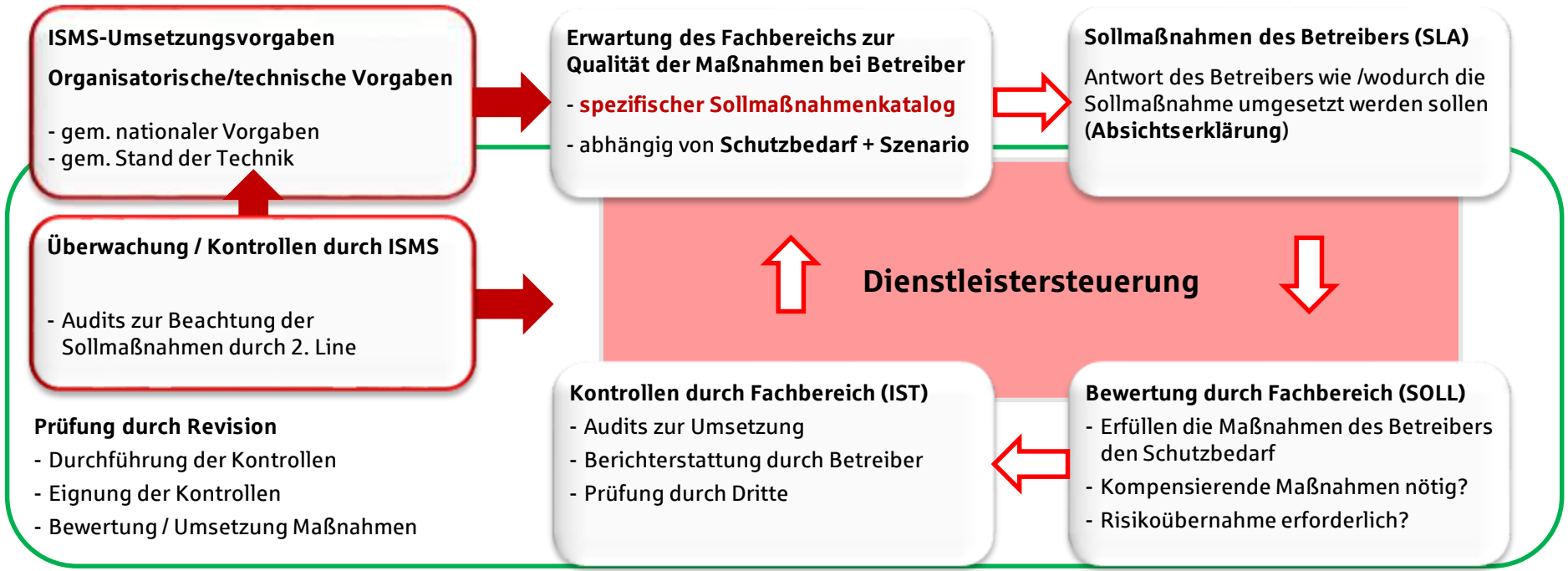
„Sicherer IT-Betrieb“ enthält Anforderungen für alle Verteidigungslinien (egal wer es macht)





Anforderungen der Finanzaufsicht praktikabel umsetzen
Sollmaßnahmen und Dienstleister

Finanzinstitute haben viele Dienstleister



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

SITB

Lösung für das Informationssicherheits-Management

Lösung für das IT-Management

Prozess-/IS-/DS-Risikomanagement

Strukturanalyse – Schutzbedarf – VVT

Sollmaßnahmen und Assets

Das neue Produkt ist mehr als die Summe der einzelnen Bestandteile

Ri.Ma.G

Risk, Management & Governance

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