Integration der Informationssicherheit

Erfahrungen bei der Umsetzung der Anforderung ISMS.1.A9

Riechen Consulting GmbH www.riechen.consulting +49 351 2684949

Die häufigsten ISB-Klagen

- Mit mir will hier niemand reden.
- Von der Technik hab ich keine Ahnung und dann soll ich die Sicherheitsvorgaben machen.
- Ich erfahre immer als letzter, wenn etwas eingeführt wird.
- Ich bin hier immer der Verhinderer.
- Als ISB bin ich am Ende meiner Karriere angekommen, ich werde nie wieder befördert.

ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse (B)

- Informationssicherheit MUSS in alle Geschäftsprozesse sowie Fachaufgaben integriert werden.
- Es MUSS dabei gewährleistet sein, dass nicht nur bei neuen Prozessen und Projekten, sondern auch bei laufenden Aktivitäten alle erforderlichen Sicherheitsaspekte berücksichtigt werden.
- Der oder die Informationssicherheitsbeauftragte (ISB) MUSS an sicherheitsrelevanten Entscheidungen ausreichend beteiligt werden.
- Informationssicherheit SOLLTE außerdem mit anderen Bereichen in der Institution, die sich mit Sicherheit und Risikomanagement beschäftigen, abgestimmt werden.

Agenda

Prozesse

Umsetzungsplanung

- Risikoanalyse abgeschlossen
- Handlungsoptionen bestimmt, Aufwandsschätzung durchgeführt
- Management-Entscheidung liegt vor: **Risikoreduktion**
- Termin: bis zum nächsten Audit
- Und nun?

Was macht eigentlich die IT-Abteilung?

- Tagesgeschäft in der „Linienorganisation“
  - Bereitstellen und Überwachung von Diensten
  - Abarbeiten von „Standard-Änderungen“
  - Bearbeiten von „Vorfällen“ (Incidents) am Helpdesk
  - Beseitigung von Störungen
- Änderungen
  - Aufwand gering (z.B. unter 5 PT)
  - Risiko überschaubar
- Projekte
  - Eigene Organisationsform erforderlich (Projektmanagement)

Anforderungsmanagement - Aufgaben

- Projektskizze / Business Case
  - mit Fachanwender und IT gemeinsam erstellen
- Stellungnahme von
  - Compliance Management (Rechtsabteilung)
  - DSB
  - ISB
  - Personalvertretung
- Weiterleitung an
  - Änderungsmanagement oder
  - Projektmanagement

Anforderungs-Manager

- Organisatorisch angebunden an
  - IT oder
  - Projektmanagement oder
  - Organisationsabteilung
- Initiiert die Umsetzung von Sicherheitsmaßnahmen als
  - Änderung oder
  - Projekt

Änderungs-Management

OPS.1.1.3 Patch- und Änderungsmanagement

- … beinhaltet kein vollständiges Änderungsmanagement, sondern lediglich die Kernaspekte zur Informationssicherheit. In größeren Institutionen ist es sinnvoll, darüber hinaus ein Änderungsmanagement systematisch zu strukturieren. Hierzu können Standardwerke, wie z. B. der Change-Management-Prozess der „IT Infrastructure Library“ (ITIL), herangezogen werden …

Änderungsantrag (Change Request)

- Zweck der Änderung (Grund, Ziel)
- Antragsteller, Ausführende, Tester
- Priorität, Kategorie
- Risiken
- Auswirkungen (Downtime, betroffene Dienste + Nutzer, Termine)
- Aufwand (einmalige und wiederkehrende Sach- und Personalaufwände)
- Rückfallplan, Abbruchkriterien
- Evaluierung

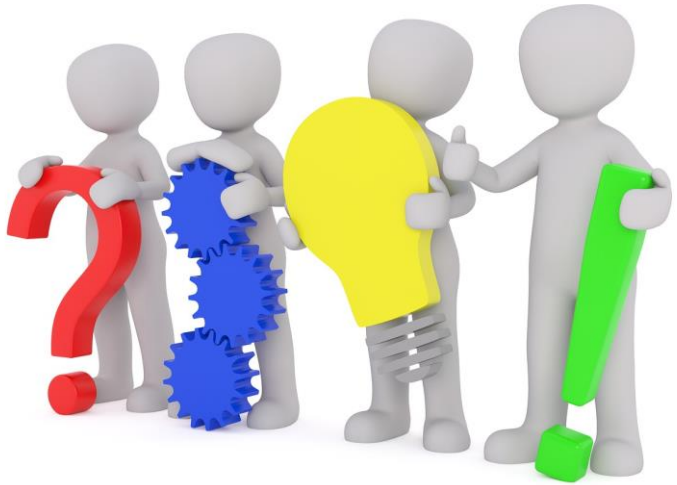
Change Advisory Board (CAB)

- Leitung: Change Manager
- Bewertet Change Requests
- Regelmäßig (z.B. wöchentlich)
- Teamleiter aus der IT-Abteilung, **ISB**
- Bei Bedarf: Experten
- Dringlichkeitssitzung: ECAB

Projekt-Management

Projekt

- Organisationsform, die ein oder mehrere Produkte in Übereinstimmung mit einem Business Case liefern soll
- Ein Projekt
  - ist zeitlich befristet
  - realisiert Veränderungen
  - ist einzigartig
  - ist bereichsübergreifend
  - hat Risiken / Unsicherheiten



Projektmanagement nach PRINCE2

- Zeit
- Kosten
- Qualität
- Umfang
- Risiken
- Nutzen

Business Case

- Business Case = Projektskizze = Projektantrag
- „Warum wird das Projekt durchgeführt?“
- Inhalt:
  - Gründe
  - Optionen
  - Nutzen
  - Negative Nebeneffekte
  - Zeit
  - Kosten
  - Hauptrisiken

Organisation

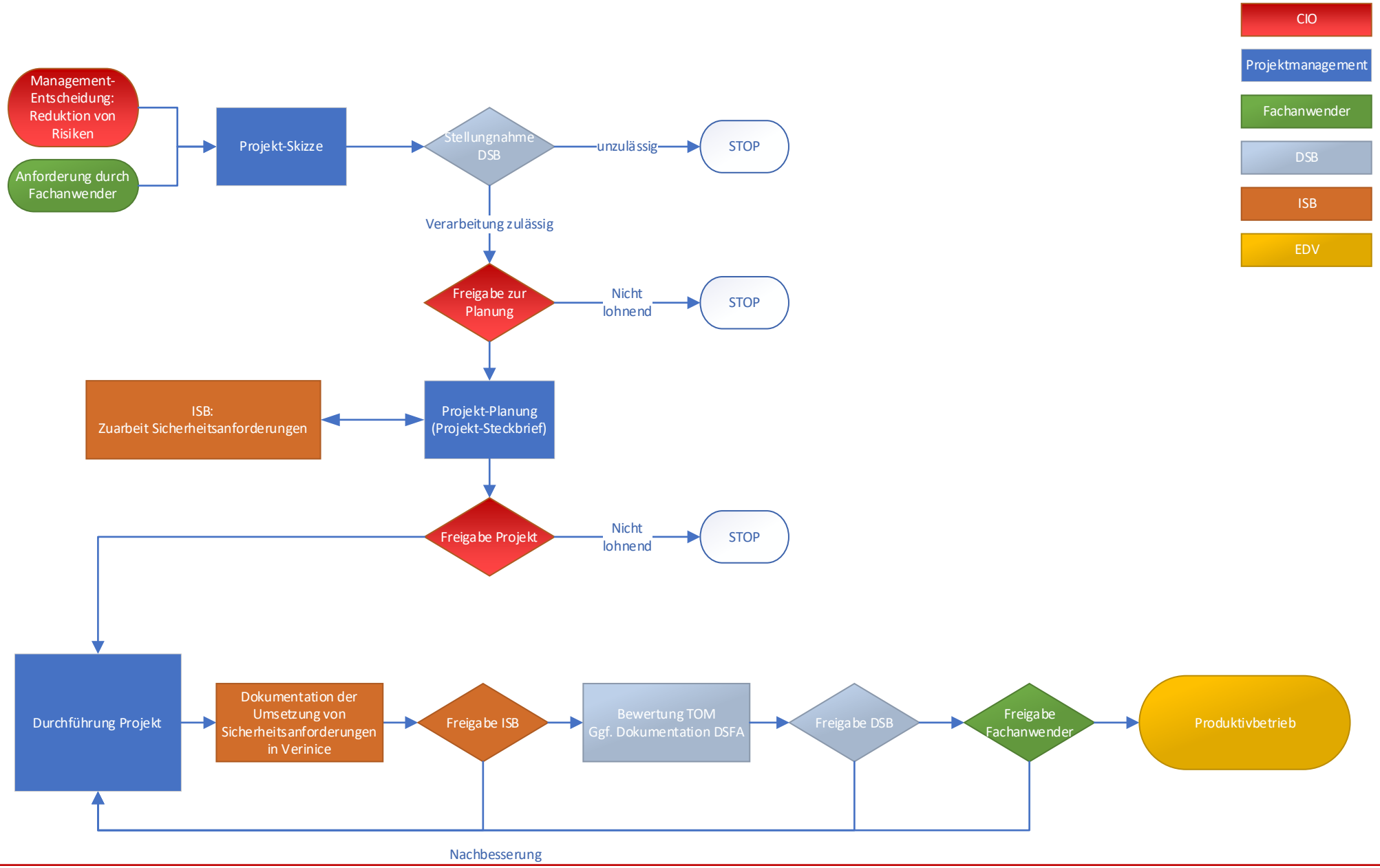
- Lenkungsausschuss (gibt Phasenübergänge frei)
  - Auftraggeber (Kosten/Nutzen)
  - Benutzervertreter (Qualität)
  - Lieferantenvertreter (Machbarkeit)
- Projektmanager (Steuerung mit Plänen)
- Teammanager (Lieferung von Produkten)

Projektphasen

- Projektinitiierung
- Projektfreigabe (Lenkungsausschuss bzw. Programm- oder Projektportfolio-Management)
- Projektphase(n) mit Arbeitspaketen (Produktlieferung)
- Projektabschluss

ISB in Projekten

- ISB sollte bei Informationssicherheits-Projekten „Benutzervertreter“ sein
- ISB ist bei allen anderen Projekten „Stakeholder“
- ISB ist bei jedem Phasenübergang ins Benehmen zu setzen
- Spätestens zum Projektabschluss erfolgt die Aufnahme der gelieferten Produkte ins ISMS


CIO
Projektmanagement
Fachanwender
DSB
ISB
EDV
Management-Entscheidung: Reduktion von Risiken
Anforderung durch Fachanwender
Projekt-Skizze
Stellungnahme DSB
unzulässig
STOP
Verarbeitung zulässig
Freigabe zur Planung
Nicht lohnend
STOP
ISB: Zuarbeit Sicherheitsanforderungen
Projekt-Planung (Projekt-Steckbrief)
Freigabe Projekt
Nicht lohnend
STOP
Durchführung Projekt
Dokumentation der Umsetzung von Sicherheitsanforderungen in Verinice
Freigabe ISB
Bewertung TOM Ggf. Dokumentation DSFA
Freigabe DSB
Freigabe Fachanwender
Produktivbetrieb
Nachbesserung

Incident Management

Definitionen

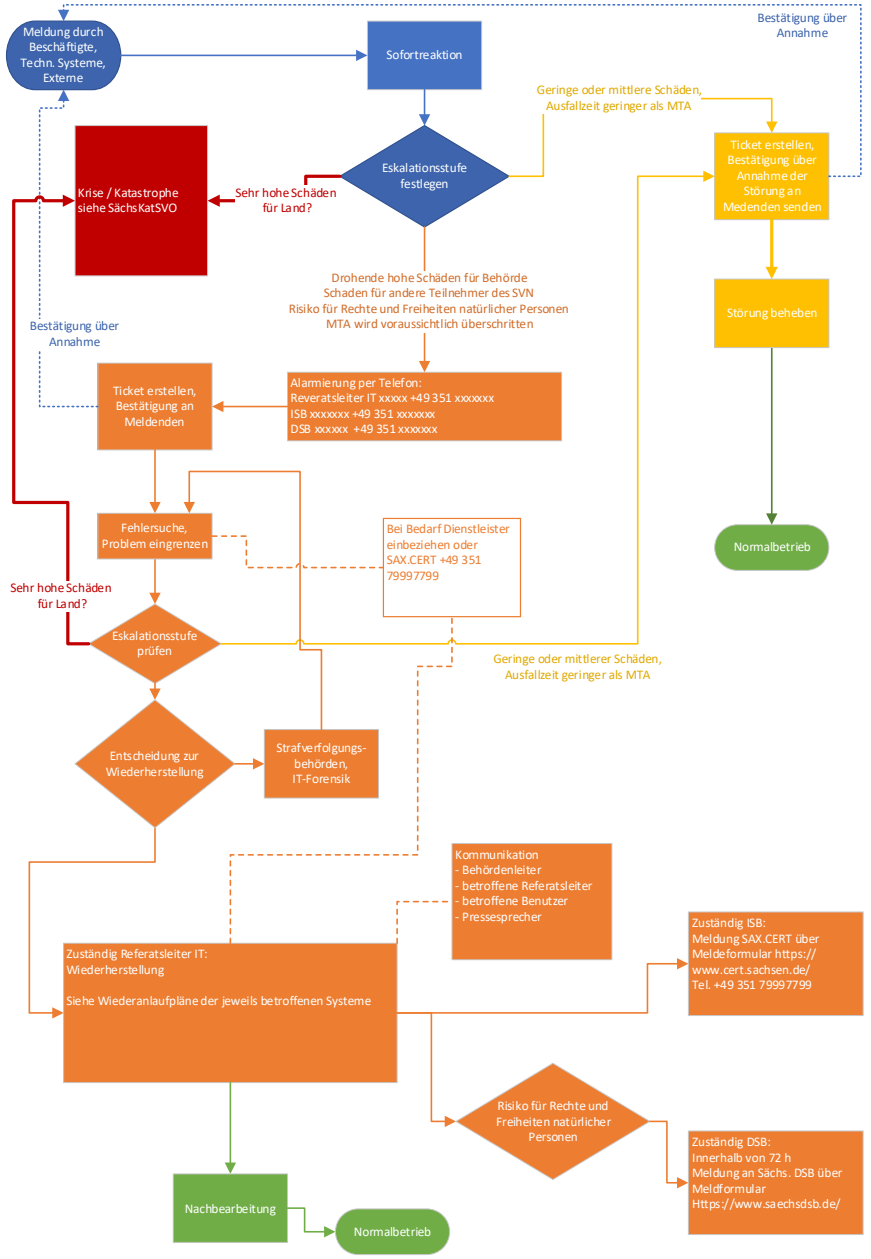
- Krise / Katastrophe
  - Schaden „sehr hoch“
- Notfall, schwerwiegender Sicherheitsvorfall
  - Schaden „hoch“
- Störung, Sicherheitsvorfall
  - Schaden „gering“ bis „mittel“
- Datenpanne
  - Personenbezogene Daten betroffen, Risiko für die Rechte und Freiheiten natürlicher Personen

Einbeziehung ISB

- KRITIS: ISB meldet an BSI, wenn kritische Dienstleistung beeinträchtigt war oder beeinträchtigt werden könnte
- ISB sollte Mitglied im Krisenstab sein (bei Schaden „hoch“)
- Meldung von Sicherheitsvorfällen an den ISB
  - „hoch“ sofort
  - „gering“ bis „mittel“ wöchentlich
- Sicherheitsvorfälle sind ein Indiz für unzureichend behandelte Risiken

Alarmierungsplan

- BSI-Standard 200-4
- Umsetzungs-Rahmenwerk



Fragen?

ulf@riechen.consulting

+49 170 2467199