InfoGuard
SWISS CYBER SECURITY

IKT-SICHERHEITS-MANAGEMENT

Automatisierung der Umsetzung und Überwachung der IKT-Sicherheitsvorgaben des Bundes

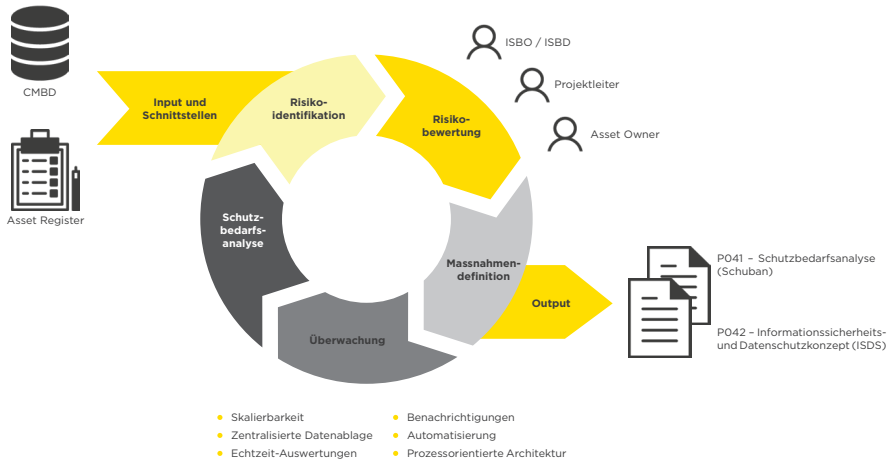
Der Bedarfsträger und Informatiksicherheitsbeauftragte eines Departements (ISBD) steht vor der schwierigen Aufgabe, die Sicherheitsvorgaben der Informations- und Kommunikationstechnik (IKT) des ISB im Rahmen eines Projekts zu erstellen und innerhalb der Organisation für deren relevante Systeme regelmässig zu überprüfen resp. zu aktualisieren. Daher sind die geltenden Sicherheitsverfahren wie die **Schutzbedarfsanalyse** (Schuban, P041) und das **Informationssicherheits- und Datenschutzkonzept** (ISDS, P042) für IKT-Schutzobjekte der Verwaltungseinheit zwingend und termingerecht zu erarbeiten. Dazu gehört die Einhaltung der Anforderungen des IKT-Grundschutzes sowie deren periodische Überarbeitung und Anpassung.

Mit einem dezentralen Ansatz sind die Sicherheitsverfahren aufwändig zu harmonisieren und ein konsolidiertes Lagebild über die gesamte Verwaltungseinheit fehlt. Oder kennen Sie zu jedem Zeitpunkt die relevanten IKT-Schutzobjekte und die akzeptierten Restrisiken, welche Sie in Ihrem Zuständigkeitsbereich tragen?

Mit Hilfe unseres toolbasierten Ansatzes unterstützen wir Sie beim Aufbau eines zentralisierten Managementsystems. Im Management Cockpit werden die wichtigsten IKT-Sicherheitsverfahren sowie der IKT-Grundschutz aufbereitet und bewirtschaftet. So kann rasch auf die wesentlichen Fragestellungen während einer Projektinitialisierung, -Aktualisierung oder bei geänderter Bedrohungslage reagiert werden.

Toolbasierte Umsetzung des IKT-Sicherheitsmanagements mittels der HiScout GRC Suite

Das spezifisch für Departemente und Organisationseinheiten der Bundesverwaltung entwickelte HiScout-Modul bietet eine zentrale Bewirtschaftung der IKT-Sicherheitsvorgaben.

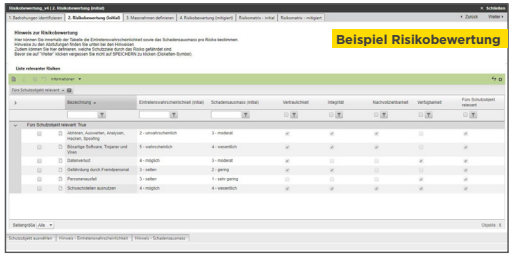


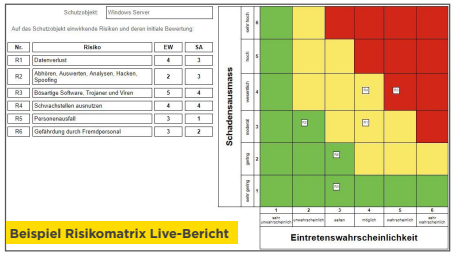
Funktionen für Verantwortliche / Inhaber von IKT-Schutzobjekten:

- Identifikation und Bewirtschaftung von IKT-Schutzobjekten
- Durchführung der Schutzbedarfsanalyse (Schuban)
  - Feststellung des Schutzbedarfs
  - Werkzeuge zum Erstellen und automatisierten Aktualisieren der erforderlichen Dokumentation
- Durchführen der Risikobeurteilung
  - Identifikation von Bedrohungen
  - Bewerten von Risiken
  - Definieren von Massnahmenplänen und Verfolgen der wirksamen Umsetzung
  - Ausweisen von Restrisiken
- Identifikation und Dokumentation zur Umsetzung der minimalen Sicherheitsvorgaben gemäss IKT-Grundschutz
- Werkzeuge zur Erstellung des Informationssicherheits- und Datenschutzkonzepts (ISDS)

Funktionen für Informatiksicherheitsbeauftragte:

- Definition und Verwaltung von (Standard-)Bedrohungen und Massnahmen
- Festlegen der Risikopolitik (Risikotoleranz)
- Bewirtschaftung des IKT-Grundschutzes
- (Periodisches) Prüfen von Schutzbedarfsanalysen und ISDS-Konzepten
- Zentralisiertes Reporting über sämtliche IKT-Schutzobjekte
  - Ausweisen von Restrisiken
  - Identifikation besonders schützenswerter Objekte
  - Benutzerdefinierte Berichtsabfragen in Echtzeit





Ergänzende Funktionen für den Betrieb des Managementsystems

- Konfigurierbare Anpassung des Datenmodells
- Revisionssichere Einbindung und Referenzierung externer Dokumente
- Rollenspezifische Zugriffsrechte
- Automatisierung wiederkehrender Aktionen (mit Hilfe der Business Logic Engine)
- Workflows zur Freigabe und Versionierung
- Frei konfigurierbare Ansichten
- Texteditor und Berichtsvorschau
- Adaptierbare und erweiterbare Daten-Schnittstellen

SICHERHEITSKOMPETENZ AUS DER SCHWEIZ

Zahlreiche nationale und internationale Richtlinien, das Datenschutzgesetz sowie die IKT-Sicherheitsvorgaben des Bundes fordern verschiedenste Sicherheitsmassnahmen, welche Ihre Organisation, Prozesse und Ihre Infrastruktur betreffen. Mit Hilfe des Toolsets unterstützen wir Sie in der zentralen Bewirtschaftung der wesentlichen Fragestellungen.

Wir stellen sicher, dass die IKT-Sicherheitsvorgaben des Bundes korrekt umgesetzt werden:

- Digitalisierung des ISDS-Prozesses
- Medienbruchfreie Integration von Dokumenten in das Managementsystem
- Benutzerfreundliche, webbasierte Oberfläche
- Workflow basiert
- Effizient und effektiv
- Mandantenfähigkeit – Rollenspezifische Rechtevergabe für übergreifende Zusammenarbeit

System Voraussetzungen (für vor Ort Installation)**:**

Server Software
Windows 2012 (64 Bit); 2012 R2 (64 Bit); 2016 (64 Bit)
.NET Framework 4.5.2

Server Hardware
CPU: min 4, 6 physische Kerne (empfohlen)
RAM: 8 GB (mindestens), 32 GB (empfohlen)
Applikation: 10 GB freie Speicherkapazität
Daten-Ablage: Empfohlen ab 100 GB (abhängig von der Anzahl importierter Dokumente)

InfoGuard AG
Lindenstrasse 10
6340 Baar/Schweiz
Telefon +41 41 749 19 00

Office Bern
Stauffacherstrasse 141
3014 Bern/Schweiz
Telefon +41 31 556 19 00

ISO 27001
ZERTIFIZIERT

INFOGUARD.CH