SUISSEDIGITAL
VERBAND FÜR KOMMUNIKATIONSNETZE
ASSOCIATION DES RESEAUX DE COMMUNICATION

Regionale Fachtagungen Mai 2022

Information Security Management System (ISMS)

FortIT im Auftrag von SUISSEDIGITAL

Information Security Management System

Wieso ein ISMS?

Einordnung von ISMS

Security Management ist ein Schlüsselelement im Sicherheitsdispositiv jedes Unternehmens

Was ist ein ISMS

Information Security Management System (ISMS)

Ziel

Risiko-gesteuerter und zielgerichteter Schutz der schützenswerten Informationen und der zugehörigen Informations- und Kommunikationsinfrastruktur

Fähigkeiten

- Systematische und kontinuierliche Identifikation, Analyse sowie Einschätzung von Informationssicherheitsrisiken
- Bestimmung der Risikobehandlung gemäss definierter Risikostrategie, z.B. Minimieren / Akzeptieren / Delegieren
- Ausarbeitung, Umsetzung und Überwachung von Verbesserungs- und Schutzmassnahmen
- Aktive Kommunikation und Behandlung von Restrisiken (Managementverankerung & Risikoakzeptanz)

Wieso ein ISMS

Aktives Management von Risiken und Massnahmen im Bereich Informationssicherheit

Der risiko-basierte Ansatz ermöglicht eine objektive Risiko-Übersicht und eine fundierte Priorisierung von Verbesserungs-Massnahmen

Aktuelles Fernmeldegesetz (FMG) resp. davon legitimierte BAKOM-Richtlinien empfehlen ISMS & BCM

Ausgabe 3 der „Richtlinien zur Sicherheit und Verfügbarkeit von Fernmeldeinfrastrukturen und –diensten“ vom Mai 2009:

- Jede FDA (Fernmeldedienstanbieterin) sollte ein Information Security Management System (ISMS) ausarbeiten, dokumentieren, umsetzen, nutzen, überwachen, überarbeiten und laufend verbessern, wie es in der Norm ISO/IEC 27001:2005 beschrieben ist
- Jede FDA sollte einen Kontinuitätsplan (Business Continuity Plan) und einen Wiederherstellungsplan (Disaster Recovery Plan) ausarbeiten, dokumentieren, umsetzen, überarbeiten und laufend verbessern, die namentlich auf ihrer Sicherheitspolitik und auf ihrem ISMS basieren
- Aber:
  Das BAKOM nimmt derzeit Abklärungen vor, welche sehr darauf hindeuten, zukünftig entsprechende Vorschriften zu erlassen. Die Forderung nach der Implementation einem ISMS & BCM ist durchaus als realistisch zu beurteilen.

Wieso ein ISMS

Das neue Informationssicherheitsgesetz (ISG) des Bundes betrifft (fast) alle

Das ISG verpflichtet nicht nur die Bundesbehörden, sondern auch kantonale Behörden und privatrechtliche Unternehmen, die den Bund bei der Wahrnehmung seiner Aufgaben unterstützen.

- Insb. Meldepflicht von Cyberangriffen
  (Evaluation von ggf. geforderten, adäquaten Gegenmassnahmen bedingt eine Risikobetrachtung)

Eine besondere Rolle spielen dabei die Betreiber von kritischen Infrastrukturen, für welche Art. 73a-79 gelten.

Erwähnt werden in der Botschaft zum Bundesgesetz u.a. auch Risikomanagement, Klassifizierung und Identity and Access Management als Schlüsselelemente für die Informationssicherheit.

- Zu beachten:
  Das ISG befindet sich zum 2-ten Mal in Vernehmlassung und ist dementsprechend noch nicht in Kraft.

Wieso ein ISMS

Das neue Datenschutzgesetz (DSG) tritt voraussichtlich 1. September 2023 zusammen mit der neuen Datenschutzverordnung in Kraft

Dabei sieht das nDSG keine Übergangsfristen vor und tritt somit unmittelbar in Kraft.

Folgende (neue) Herausforderungen sind zu meistern:

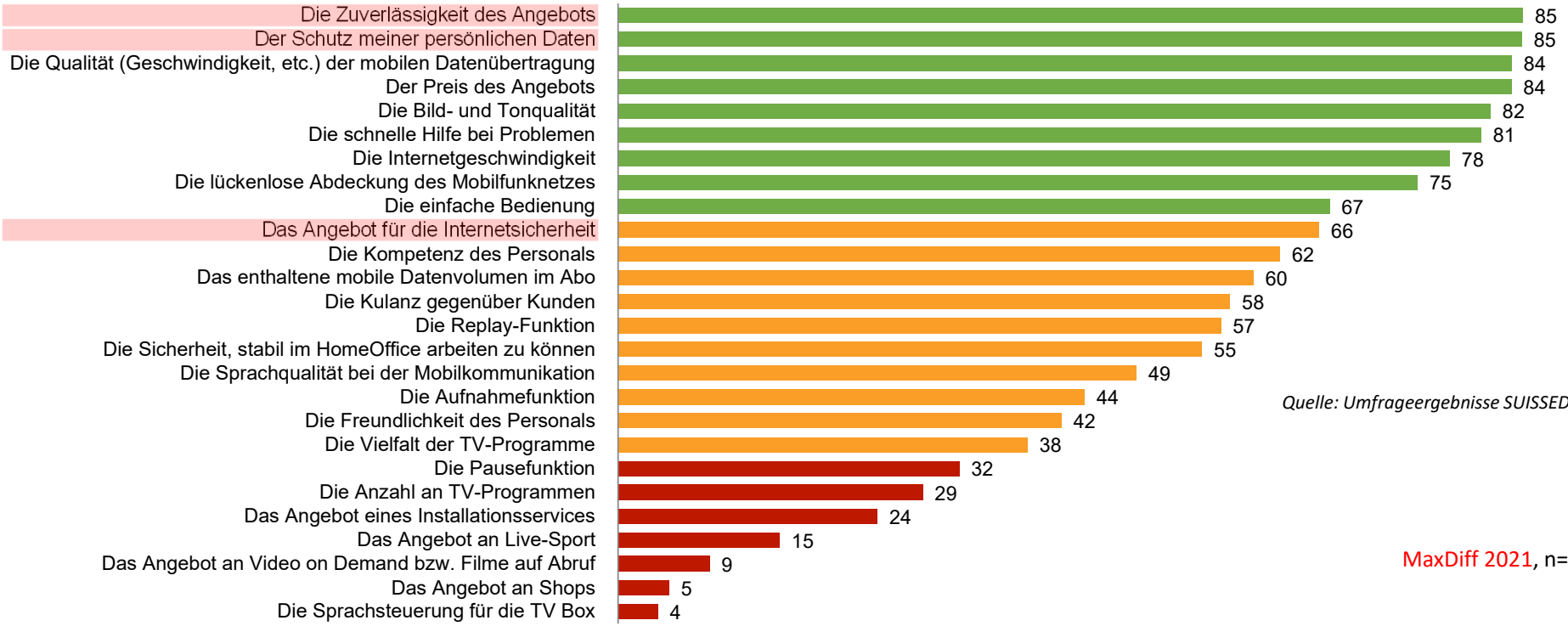
- Erweiterte Informationspflichten (Art. 24, Art. 25): z.B. Meldung Verletzung Datensicherheit
- Die Pflicht zur Erstellung eines Bearbeitungsverzeichnisses (Art. 12): z.B. Zweck, Quelle, Empfänger der Daten gemäss Auskunftsrecht
- Ausbau der Rechte der betroffenen Person (Art. 28): z.B. Datenherausgabe /-übertragung
- Datenschutz durch Technik und Voreinstellungen (Art. 7): z.B. „Privacy by Design / by Standard“ : Datenminimierung, Löschkonzepte, Pseudonymisierung
- Datenschutz-Folgeabschätzung (Art. 22): z.B. Risikobasiertes Sicherheits-/Datenschutzmanagement

Wieso ein ISMS

Im Eigeninteresse für das Unternehmen, dieses vor Gefahren für die Informationssicherheit zu schützen…

Wieso ein ISMS

… und die Bedürfnisse der Kunden zu respektieren.

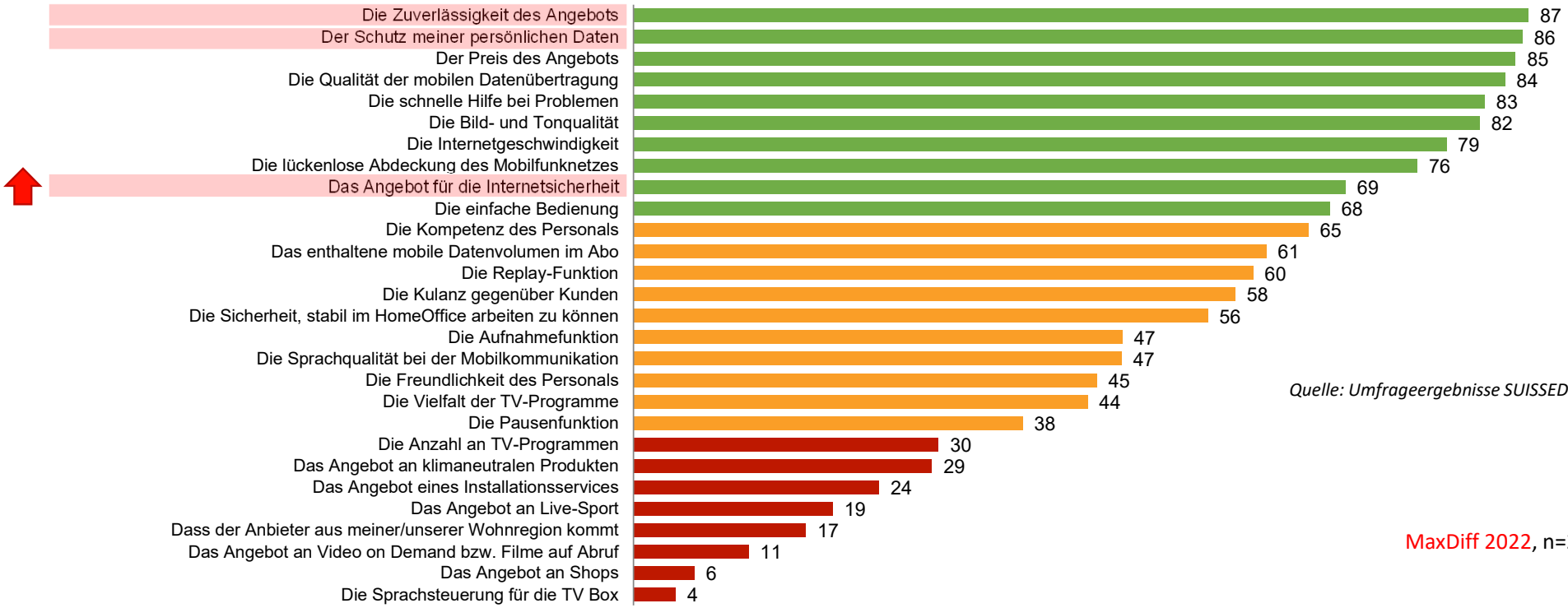


Quelle: Umfrageergebnisse SUISSEDIGITAL

MaxDiff 2021, n=2’050

Wieso ein ISMS

… und die Bedürfnisse der Kunden zu respektieren.



Quelle: Umfrageergebnisse SUISSEDIGITAL

MaxDiff 2022, n=2'040

Information Security Management System

Handlungsempfehlung

Handlungsempfehlung ISMS

Aufbau Kernfähigkeiten

A Systematische Risikobewirtschaftung
- Klare Verantwortlichkeiten
- Objektive Risikoeinschätzung

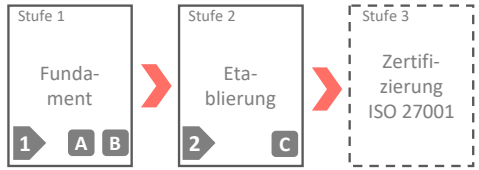
B Kontinuierliche Verbesserung
- Priorisierte Massnahmen

C Aktive Berichterstattung
- Systematische Überprüfung Security Controls über 3 Jahre
- Jährliches Management Review

Vorgehen

1 Fundament
- Verantwortlichkeiten
- Hauptverfahren

2 Etablierung
- Nebenverfahren
- Verankerung & Systematisierung



Empfehlung

Erfolgsfaktoren

- Etablierung Top Down
- Iteratives Vorgehen – Umsetzbarkeit steht im Vordergrund
- Awareness und Verständnis schaffen
- Integration mit bestehenden ISO-Standards wie Qualitätsmanagement (ISO 9001), Umweltmanagement (ISO 14000) oder IT-Service-Management (ISO 20000)

Information Security Management System

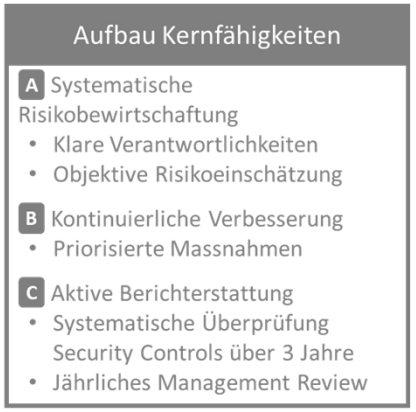
Einfacher zum ISMS mit fortControl

Schlankes ISMS mit fortControl Security Management

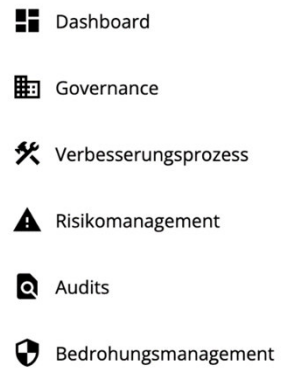
fortControl ist eine von FortIT entwickelte und betriebene Webapplikation für Sicherheitsmanagement.

fortControl unterstützt insbesondere kleinere und mittlere Unternehmen im Aufbau eines schlanken ISMS:

- Einfache Umsetzung der benötigte ISMS Kernfähigkeiten durch entsprechende Systemunterstützung
  - ✓ Risikobewirtschaftung
  - ✓ Kontinuierliche Verbesserung
  - ✓ Aktive Berichterstattung



Kernfähigkeiten für ein ISMS

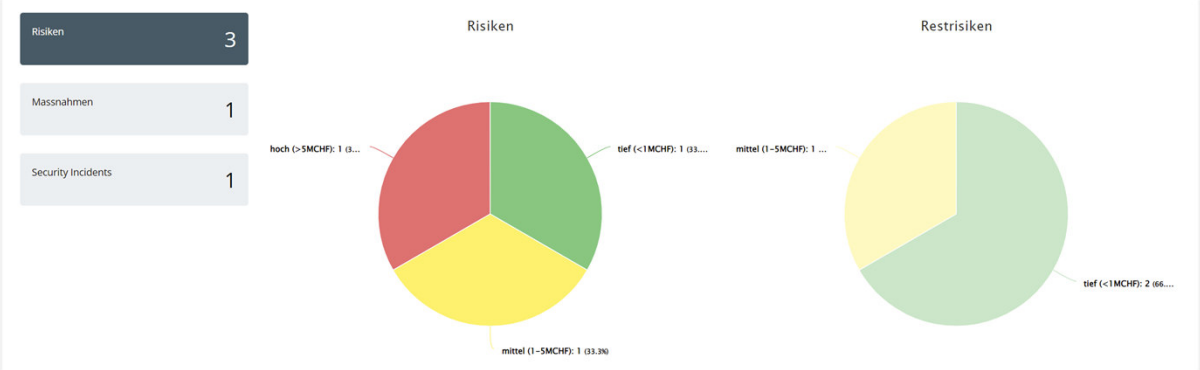


Auszug Menu fortControl

Weitere Module ab Q3/22 verfügbar:

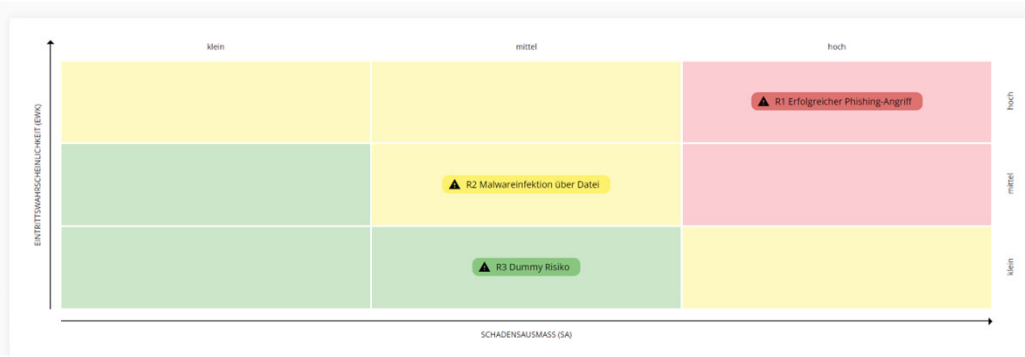
- Datenschutzmanagement konform zu nDSG
- Lieferantenmanagement

fortControl – Einfacher Überblick über relevante Sicherheitsmetriken

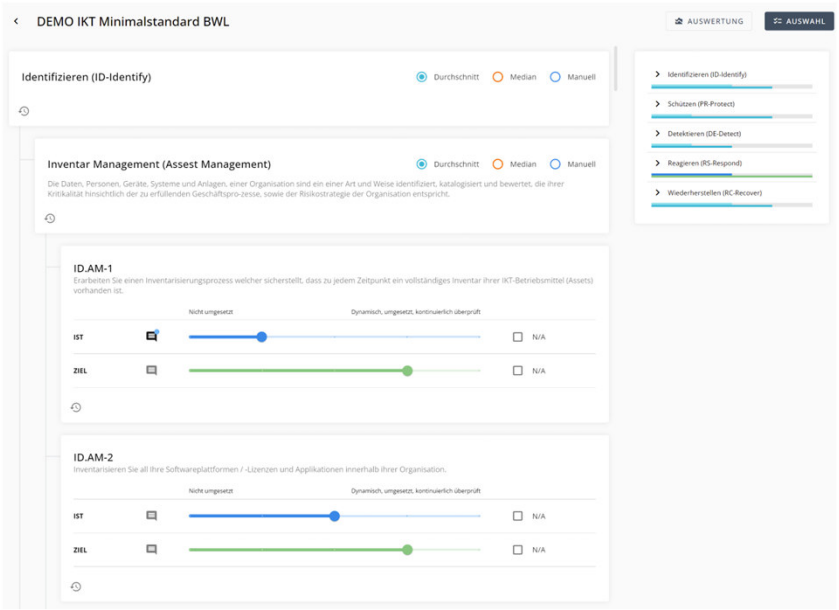


Risiken, pendente Massnahmen und aktive Security Incidents auf einen Blick

Risikodarstellung auf Basis der eigenen Metrik für Eintrittswahrscheinlichkeit und Schadensausmass



fortControl – Nutzung von vordefinierten Assessments

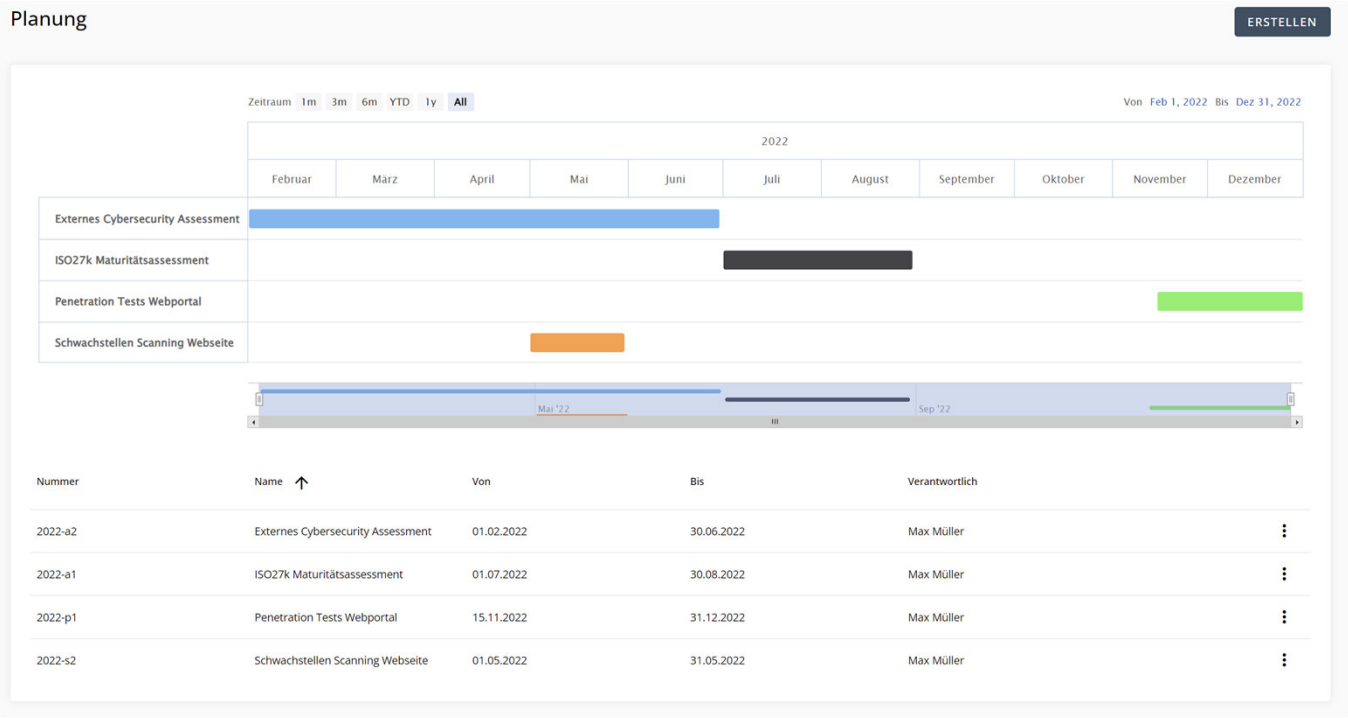


Geführte Sicherheitsbeurteilung auf Basis von vordefinierten Assessments (inkl. Kommentarmöglichkeiten)

Gezielte Auswertungs- und Reportingmöglichkeiten der Resultate (inkl. Thrill-Down)

fortControl – Nahtlose Planungsinstrumente

Jahresplanungen für die Umsetzung, Audits und Verbesserungen mit wenigen Mausklicks



Wie weiter?

Informationen & Ausprobieren

Weitere Informationen zu fortControl sind auf https://fort-it.ch/fortControl zu finden.
Jeder kann sich bei fortControl registrieren und dieses gratis ausprobieren: https://control.forthub.io

Unterstützung vom Verband

Der Verband SUISSEDIGITAL koordiniert Fragen und Interesse rund um fortControl.
Bei breitem Interesse ist angedacht, dass der Verband zentrale Dienstleistungen für ihre Mitglieder erbringt wie z.B.:

- Unterstützung beim initiales Setup von fortControl und bei inhaltlichen Fragen im Betrieb
- Regelmässiges Update und Interpretation der externen Abhängigkeiten: z.B. Anforderungen aus dem neuen ISG

Information Security Management System

Fragen?

Anhang

Zusätzliche Informationen (wird nicht präsentiert)

Verantwortlichkeiten

Wie auch das Enterprise Risikomanagement, die Finanzkontrolle oder die Compliance, ist das Informationssicherheitsmanagement in der Verantwortung der Geschäftsleitung: Mindestens einmal jährlich muss im Rahmen des Management Reviews das Thema Informationssicherheit aktiv behandelt werden.

Für die Weiterentwicklung und den Betrieb des ISMS, ist meistens der CISO (Chief Information Security Officer) verantwortlich.

Empfehlung

Jedes Unternehmen hat andere Rollen oder Verantwortlichkeiten im Bereich Security. Initiale Workshops zu den wesentlichen Verantwortlichkeiten in einem ISMS bringen Klarheit.

ISMS – Empfohlene Ausbaustufe ohne Zertifizierung

Hauptverfahren

- Verbesserungsprozess
- Risikoerhebung
- BIA

①

Diese drei Hauptverfahren nach ISO 27000 stellen das Rückgrat des Informationssicherheits-Managementsystems dar.
Der **Verbesserungsprozess** stellt die risikobasierte Verbesserung der Informationssicherheit sicher.
Der **Risikoerhebungsprozess** definiert eine systematische und nachvollziehbare Risikobeurteilung.
Mittels **Business Impact Analyse (BIA)** werden die kritischsten Geschäftsprozesse analysiert.

Nebenverfahren

- KPI & Berichterstattung
- Sicherheit in Projekten
- Auditverfahren & Konformitätsprüfung

②

Mittels einer standardisierten **Berichterstattung** (inkl. KPIs) werden Risiken und empfohlene Massnahmen transparent kommuniziert.
Es wird definiert, wie die **Sicherheit in Projekten** frühzeitig im ISMS behandelt wird.
Das **Auditverfahren und die Konformitätsprüfung** stellen sicher, dass Abweichungen vom IST zum SOLL systematisch identifiziert werden.

Berichte, Aufzeichnungen

- SoA (Statement of Applicability) ①
- Risikoliste ①
- Verbesserungsprogram ①
- Auditprogramm & -berichte ②

Das «Statement of Applicability» stellt eine wichtige Grundlage dar: Welche Informationssicherheitsbereiche sind für die Organisation relevant und wie werden diese angegangen.

Die weiteren Berichte und Aufzeichnungen dienen der Nachvollziehbarkeit der Haupt- und Nebenverfahren.

Risikoanalyse - Zusammenhänge