INFORMATIONSSICHERHEITSMANAGEMENT

NACH ISO/IEC 27001

Stepping Stone – Information Security Event

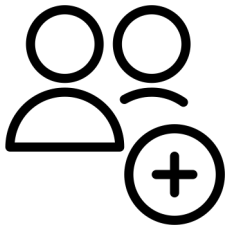
REDGUARD
SECURING YOUR ASSETS

Agenda

- Einleitung & Vorstellung Redguard AG
- Intro - Informationssicherheitsmanagement
- Erläuterung zur Norm
- Schlüsselfaktoren für die erfolgreiche Umsetzung
- Rolle bei der Begleitung zur ISO/IEC 27001-Zertifizierung

EINLEITUNG & VORSTELLUNG REDGUARD AG

Fakten



Wir sind aktuell
39 Team Member.

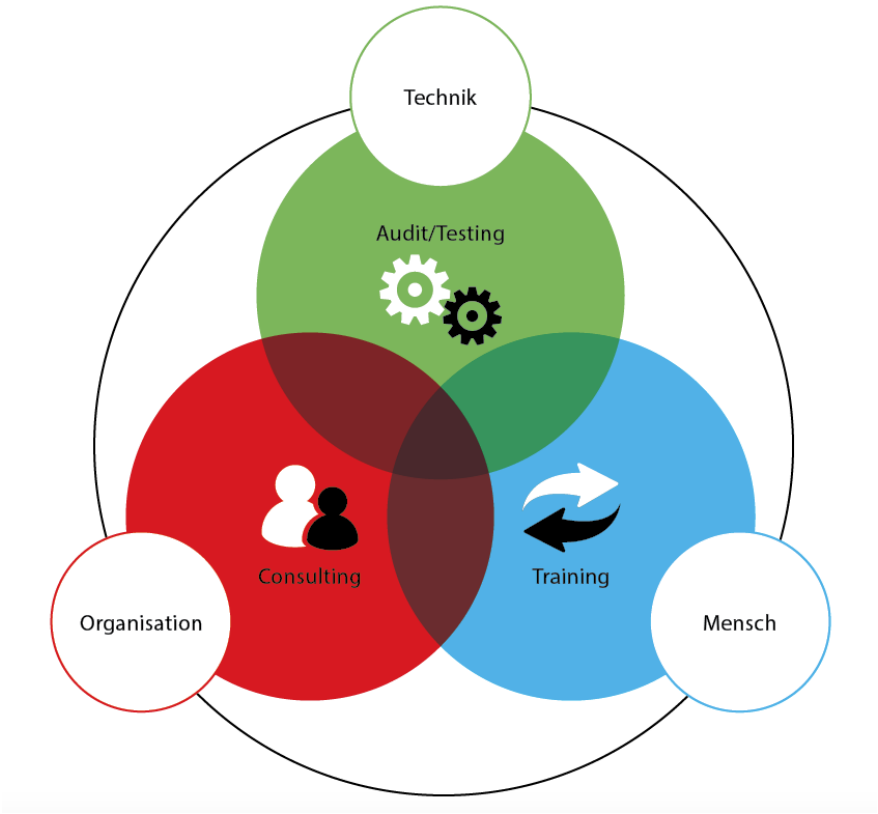
Der Frauenanteil bei
Redguard beträgt: 20 %

Standorte in Bern
und Zürich.

Seit 2012 im Bereich
Informationssicherheit tätig.

Jährlich 300+
Projekte.

DIENSTLEISTUNGEN



CONSULTING

Die komplexe Vernetzung von Prozessen und Funktionen wirken sich auf sämtliche Geschäftsvorhaben aus. Redguard unterstützt die Kunden bei der Informationssicherheit vollumfänglich: von der Konzeption bis zur Umsetzung.

AUDIT / TESTING

Wir überprüfen das ICT-Umfeld Kunden nach Schwachstellen und Risiken und die ICT-Infrastruktur aktiv angegriffen oder technische Tests auf sämtliche Systeme oder Anwendungen werden durchgeführt. Unabhängige Prüfungen auf Basis von internationalen Standards umfassen technologische, organisatorische sowie menschliche Aspekte. Sämtliche Audits können mit den obengenannten technischen Prüfungen erweitert werden.

TRAINING

Die Redguard-Kurse und Trainings umfassen alle Aspekte aus den Leistungsschwerpunkten und werden spezifisch auf die Bedürfnisse der Kunden zusammengestellt und durchgeführt.

INTRO - INFORMATIONSSICHERHEITS-MANAGEMENT

Intro - Informationssicherheitsmanagement

Informationssicherheit ist gewährleistet, wenn die **Informationen** ausschliesslich dem **autorisierten** Personenkreis zugänglich sind, in einer **kontrollierten, konsistenten und nachvollziehbaren Art und Weise erzeugt, mutiert** oder **ergänzt** werden und innerhalb **nützlicher Frist** zur Verfügung stehen.

- angemessener **Schutz von Informationen**
- umfasst die **Sicherung längerfristiger Geschäftstätigkeiten** und den **Schutz** von **nicht elektronisch verarbeiteten Informationen**
- Ist eine **strategische** und **keine reine technische Frage**, somit umfassender als der Begriff IT-Sicherheit

Intro – Primäre Schutzziele der Informationssicherheit

CIA-Prinzip

- **C**onfidentiality - *Vertraulichkeit*
- **I**ntegrity - *Integrität*
- **A**vailability – *Verfügbarkeit*

CIA ist das Gegenteil von **DAD**:

- **D**isclosure – *Offenlegung*
- **A**lteration – *Änderung*
- **D**istruction - *Zerstörung*

ERLÄUTERUNG ISO/IEC 27001

Erläuterung ISO/IEC 27001

- Normenreihe ISO/IEC 2700x geht auf ältere britische Standards zurück – BS7799
- Durchgängiges Thema ist die Informationssicherheit, d.h. die Sicherheit (bei) der Informationsverarbeitung von Organisationen
- Beschreibt die Anforderungen für das Einrichten, Realisieren, Betreiben und Optimieren eines dokumentieren Informationssicherheits-Managementsystems (ISMS)
- ISO/IEC 27001 übergeordneter und zentraler Teil der Normenreihe, da das Management der Informationssicherheit behandelt wird

REDGUARD
SECURING YOUR ASSETS

Weitere Standards der ISO/IEC 2700x-Reihe

- ISO/IEC 27002 – Handlungsanweisungen
- ISO/IEC 27005 – Risiko-Management
- ISO/IEC 270017 – Informationssicherheitskontrollen für Cloud-Computing-Dienste
- ISO/IEC 270018 – Schutz von Personendaten, die in öffentlichen Cloud-Computing-Diensten verarbeitet werden
- ISO/IEC 27799 – Sicherheitsmanagement im Gesundheitswesen

REDGUARD
SECURING YOUR ASSETS

Weitere Standards

- BSI – Bundesamt für Sicherheit in der Informationstechnik
- NIST – National Institute of Standards and Technology
- COBIT – Control Objectives for Information and Related Technology

REDGUARD
SECURING YOUR ASSETS

Warum eine ISO/IEC 27001-Zertifizierung?

- Bedeutung der kontinuierlicher Informations- und Datensicherheit im Unternehmen
- Geschäftliche Risiken reduzieren
- Anforderung seitens bestehender oder potentiellen Geschäftspartnern
- Image- und Wettbewerbssteigerung

SCHLÜSSELFAKTOREN FÜR DIE ERFOLGREICHE UMSETZUNG

Schlüsselfaktoren – Management-Unterstützung

- Unterstützung durch das Top-Management
  - *wirkungsvolle und nachhaltige Umsetzung*
  - *fester Bestandteil der Unternehmenspolitik*
  - *organisatorische Einbindung des Sicherheitsmanagements im Unternehmen*

Schlüsselfaktoren – Sicherheitsbewusstsein

- Sicherheitsbewusstsein als Bestandteil der Unternehmenskultur
  - *Bewusstsein über die Bedeutung von Informationen im eigenen Geschäftsumfeld*
  - *Einbindung der Mitarbeitenden in den Sicherheitsprozess*
  - *Sinn und Zweck von Sicherheitsmassnahmen vermitteln*

Schlüsselfaktoren – Ressourcen

- Ressourcen
  - *Finanziell*
  - *Personell*
  - *Zeitlich*

ROLLE BEI DER BEGLEITUNG ZUR ISO/IEC 27001-ZERTIFIZIERUNG

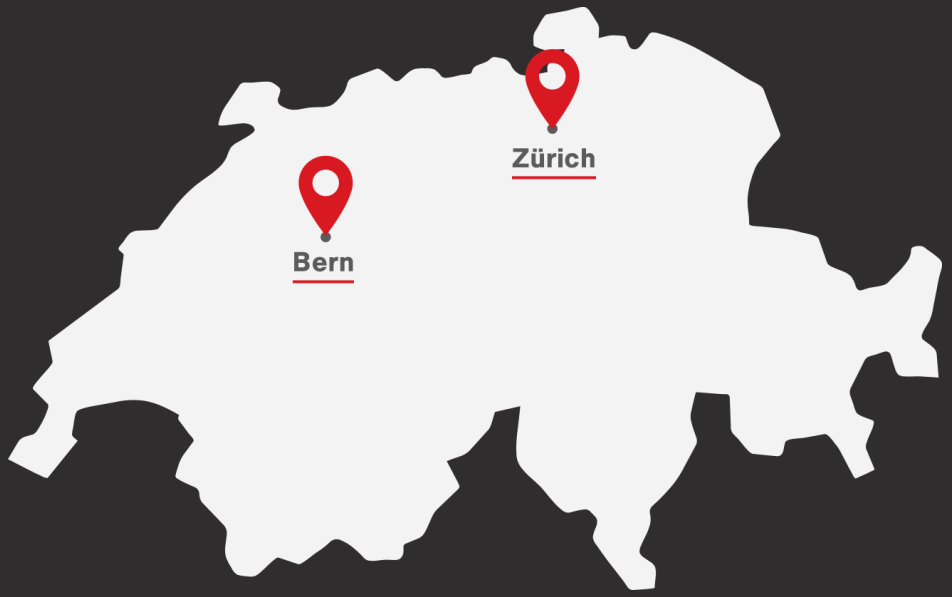
REDGUARD
SECURING YOUR ASSETS

Rolle bei der Begleitung zur ISO/IEC 27001-Zertifizierung

- Unternehmensanalyse
- Standortbestimmung
- Roadmap mit Massnahmen und Handlungsempfehlungen
- Unterstützung bei der Erstellung von relevanten Dokumenten (Richtlinien, Checklisten, etc.)
- Durchführen von Vor-Audits nach ISO 27001
- Begleitung Zertifizierung ISO 27001
- Durchführen von internen Audits im Rahmen des Re-Zertifizierungsprozess ISO 27001

FRAGEN?

Herzlichen Dank



BERN
Redguard AG
Eigerstrasse 60
CH-3007 Bern

ZÜRICH
Redguard AG
Thurgauerstrasse 36/38
CH-8050 Zürich

Phone: +41 (0)31 511 37 50
contact@redguard.ch
www.redguard.ch