accuris®
Informationssicherheit & Datenschutz

Security Compliance

(Ausgewählte Aspekte)

Dr. Christian Scharff

BSI Certified ISO 27001 Lead Auditor
Information Security Revisor (BSI)
TÜV-zertifizierter Datenschutzauditor

Security Compliance

- Nationale und internationale Standards zur IT-Sicherheit (BSI-Standards 100-1 bis 100-4, ISO 27001 und folgende) bilden die Grundlage zur Minimierung der IT-Risiken
- Vorgaben aus Telekommunikationsgesetz (TKG) und Bundesdatenschutzgesetz (BDSG)
- Arbeitsrechtliche Aspekte (BetrVG) bei der arbeitnehmerseitigen Nutzung der IT
- Einhaltung der Vorgaben aus den Standards sind Teil der Risikomanagementpflichten der Geschäftsführung/des Vorstands (KonTraG)
- Verstöße können Schadensersatzforderungen, Rechtsverlust, persönliche Haftung des Managements oder strafrechtliche Verfolgung bewirken

Welche Gesetze/Normen sind relevant?

accuris®
Informationssicherheit & Datenschutz

ISO 27001: 2005	*Information Security Management System, Requirements*
ISO 27002:2005	*Code of practice for Information Security Management System*
ISO 27003 (Draft)	*ISMS Implementation Guidance*
ISO 27004 (Draft)	*Information security management measurements*
ISO 27005: 2008	*Information Security Risk Management*
Cobit	*Control Objectives for Information and Related Technology, Framework for IT-Governance*
SOX	*IT-control objectives for Sarbanes Oxley, The Role of IT in the design and implementation of internal control over financial reporting*
EU-DSRL	*EU-Datenschutzrichtlinie 95/46/EG und 2002/58/EG*
E-Commerce-R	*EU-Richtlinie 2000/31/EG zum elektronischen Geschäftsverkehr*
BDSG	*Bundesdatenschutzgesetz, Schutz von personenbezogenen Daten*
KonTraG	*Gesetz zur Kontrolle und Transparenz im Unternehmensbereich, Errichtung eines Risikomanagements*
AktG	*Aktiengesetz § 91 Abs. 2 und § 93 Abs. 2*
HGB	*Handelsgesetzbuch § 317, Abs. 2 und 4*
TKG	*Telekommunikationsgesetz*
TMG	*Telemediengesetz*
UrhG	*Urheberrechtsgesetz*

Checkliste für Einführung eines Sicherheitsmanagementsystems (ISMS)

accuris®
Informationssicherheit & Datenschutz

1. Sicherheit der Unternehmensdaten ist Chefsache!
2. Vergewissern Sie sich, wie der Stand der Sicherheit im eigenen Unternehmen ist (IT-Sicherheitsanalyse, Basic Check-Up) und wo Handlungsbedarf besteht!
   - Risiken identifizieren
   - Wie wirksam sind die vorhandenen Maßnahmen zur Abdeckung der Risiken?
   - Wo sind Sicherheitslücken, wo besteht Handlungsbedarf?
3. Entwicklung einer Information Security Policy/IT-Sicherheitsleitlinie und -Strategie unter Berücksichtigung der rechtlichen Aspekte der IT-Nutzung
4. Benennung eines IT-Sicherheitsbeauftragten und eines IT-Sicherheitsmanagementteams

accuris AG, Agnes-Pockels-Bogen 1, 80992 München, Tel. + 49 (0) 89.903.40 00 Fax. +49 (0) 89.900.19 373, office@accuris.de, www.accuris.de

Checkliste für Einführung eines Sicherheitsmanagementsystems (ISMS)

accuris®
Informationssicherheit & Datenschutz

5. Entwicklung eines Konzepts zur Sicherheit der Unternehmens daten und der personenbezogenen Daten, bestehend aus:
   - Organisatorischen Maßnahmen
   - Personellen Maßnahmen
   - Technischen Maßnahmen
   - Baulichen und infrastrukturellen Maßnahmen
6. Vertragliche Regelungen mit den Mitarbeitern (Betriebsvereinbarung, Geheimhaltungsverpflichtung als Bestandteil des Anstellungsvertrags
7. Vertragliche Regelungen zur Vertraulichkeit mit Partnerunternehmen und Dienstleistern
8. Umsetzung der spezifizierten Maßnahmen (Investitionsplanung!)
9. Aufrechterhaltung des Sicherheitsprozesses (Audits, Reviews, Revision)
10. Überprüfung und permanente Verbesserung des Sicherheitsprozesses

accuris AG, Agnes-Pockels-Bogen 1, 80992 München, Tel. + 49 (0) 89.903.40 00 Fax. +49 (0) 89.900.19 373, office@accuris.de, www.accuris.de

Checkliste für organisatorische und personelle Maßnahmen

accuris®
Informationssicherheit & Datenschutz

- Informationssicherheit als Unternehmensziel festlegen (Security Policy)
- Sicherheitsstrategie (Policy) festlegen und IT-Sicherheitsbeauftragten benennen
- IT-Sicherheitskonzept entwickeln
- Informationssicherheit in die Geschäftsprozesse implementieren
- Schulung und Sensibilisierung der Mitarbeiter
- Vertraulichkeitsvereinbarungen
- Aufklärung über die Methoden des Social Engineerings
- Eingehende Überprüfung von Kandidaten vor der Neueinstellung
- Sicherheit von Unternehmensdaten und Geheimhaltung auch nach der Kündigung sicherstellen
- Disziplinarische Maßnahmen bei Verstößen gegen die IT-Sicherheitsrichtlinien

accuris AG, Agnes-Pockels-Bogen 1, 80992 München, Tel. + 49 (0) 89.903.40 00 Fax. +49 (0) 89.900.19 373, office@accuris.de, www.accuris.de

Checkliste für technische Maßnahmen
(ausgewählte Maßnahmen)

accuris®
Informationssicherheit & Datenschutz

- Absicherung des Unternehmens netzes durch z.B.
  - Firewall
  - Intrusion Detection und Intrusion Prevention
  - Sichere Authentifizierung der Benutzer (sichere Anmeldung im Netzwerk)
  - Zwei-Faktor-Authentifizierung bei hohem Schutzbedarf
  - Sichere Remote-Verbindungen, Remote-Zugang restriktiv handhaben
  - Schließen aller unkontrollierbarer Netzzugänge (z.B. Web-Mail)
  - Netzwerk-Monitoring
- Absicherung der Clients durch z.B.
  - Device Management (kontrollierte Rechtezuweisung von Schnittstellen = USB-Port-Kontrolle)
  - Restriktive Benutzerrechte
  - Festplatten-Verschlüsselung (Notebook-Sicherheit)
- Content Security Konzeption für Internetnutzung

Ich bedanke mich für Ihre Aufmerksamkeit!

Kontakt:

Dr. Christian Scharff
c.scharff@accuris.de
Tel. 089-903 4000