Informationssicherheits-, Risiko- und Compliance-Management

cirosec

Professionelles Informationssicherheits-, Risiko- und Compliance-Management

ISO 27001, Risiko- und Compliance-Management, Prozesse, Policies, Richtlinien

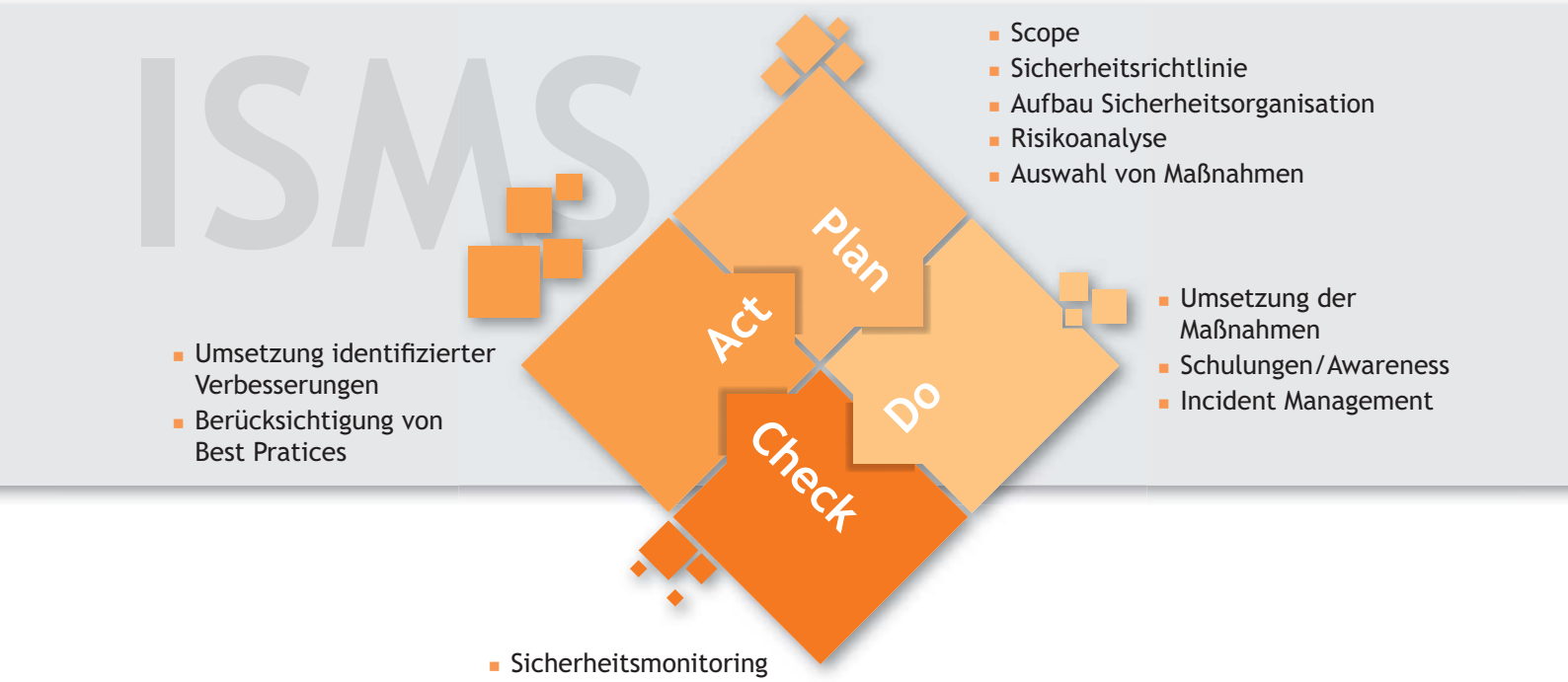
Die meisten Informationen werden heutzutage mit Mitteln der Informationstechnik verarbeitet und gespeichert. Auch die Geschäftsprozesse im Unternehmen sind heute in der Regel maßgeblich von einer funktionierenden IT abhängig.

Um die aus dem Einsatz von Informationen und IT resultierenden Risiken zu erkennen, transparent zu machen und um ein bedarfsgerechtes Schutzniveau zu erreichen, wird ein professionelles Informationssicherheits- und Risikomanagement benötigt.

Dieses muss von der Unternehmensführung getragen, im gesamten Unternehmen als Prozess gelebt und in das unternehmensweite Sicherheitsmanagement verankert sein.

Für die Einführung, die Umsetzung, die Kontrolle sowie die kontinuierliche Verbesserung eines solchen Informationssicherheitsmanagementsystems (ISMS) ist es empfehlenswert, sich an anerkannten Standards wie ISO/IEC 27001 zu orientieren.

EINFÜHRUNG



Es geht in einem ISMS jedoch nicht nur darum, Sicherheitsmaßnahmen ausschließlich risikoorientiert aus IT-Bedrohungen herzuleiten, welche die Verfügbarkeit, Vertraulichkeit und Integrität von Informationen bzw. informationsverarbeitenden Systemen gefährden.

Zusätzlich ist es erforderlich, die gesetzlichen, regulatorischen und sonstigen internen und externen Anforderungen zu kennen und die daraus gegebenenfalls resultierenden Sicherheitsmaßnahmen einzuleiten, selbst wenn die herkömmliche Bedrohungs- und Risikoanalyse diese Compliance-Maßnahme möglicherweise nicht naheliegend erscheinen lässt.

In der Praxis kommt der zuletzt genannte Bereich häufig zu kurz. Oft existiert im Unternehmen nicht einmal eine nachvollziehbare Ermittlung der relevanten gesetzlichen und regulatorischen Anforderungen mit Bezug zur Informationssicherheit.

cirosec begleitet Sie bei der Einführung, Standortbestimmung, Verbesserung oder Überprüfung Ihres Informationssicherheits- und Risikomanagementprozesses unter Berücksichtigung Ihrer organisatorischen Randbedingungen, Ihrer Unternehmenskultur und vorhandenen Prozesse sowie der für Ihr Unternehmen relevanten Compliance-Anforderungen.

GRC-WERKZEUGE

Werkzeuge zur Unterstützung des Informationssicherheits-, Risiko- und Compliance-Managements

Eines der Ziele des Risikomanagements in der IT ist die transparente und nachvollziehbare Ermittlung von Risiken, welche durch den Einsatz von IT entstehen. Nur so kann dem Management eine solide Entscheidungsgrundlage geliefert werden, ob ein Risiko akzeptiert werden kann oder ob entsprechende Gegenmaßnahmen ergriffen werden müssen und wie die Umsetzung dieser Maßnahmen zu priorisieren ist. In diesem Ziel ist man sich in der Praxis überall einig.

Große Unterschiede bestehen in den Unternehmen jedoch in der Vorgehensweise bei der Maßnahmenermittlung, insbesondere wenn es um tatsächliche oder gefühlte IT-Sicherheitsrisiken geht. Häufig wird hier immer noch ohne eine vorherige und strukturierte Ermittlung der vorhandenen Bedrohungen über Sicherheitsmaßnahmen entschieden.

Leider bleibt bei dieser „bauchgetriebenen“ Vorgehensweise in der Regel unklar, ob die Maßnahmen wirklich ausreichend sind, dem Risiko angemessen entgegenzuwirken. Umgekehrt ist unklar, ob der Umfang der ergriffenen Maßnahmen tatsächlich notwendig ist und somit möglicherweise an der falschen Stelle investiert wurde. Die Umsetzung ist oft ein steiniger Weg und mit vielen Problemen behaftet. GRC-Werkzeuge versprechen hier eine Vereinfachung und Qualitätssteigerung.

Ein weiteres verbreitetes großes Problem im täglichen Risiko- und Compliance-Management ist die Verwendung von hierfür nur eingeschränkt geeigneten Werkzeugen wie zum Beispiel dem Tabellenkalkulationsprogramm Excel. Solche Tools unterstützen beispielsweise keine Workflow-gestützte Vorgehensweise mit mehreren beteiligten Gruppen und individuellen Sichten auf die Daten (von einer granularen Vergabe von Berechtigungen oder einer Nachvollziehbarkeit von Änderungen ganz zu schweigen) und führen zu einer Unmenge von Dateien, die, wenn überhaupt, nur sehr schwer übergreifend ausgewertet werden können.

Viele dieser Probleme können heute mit dem Einsatz von IT-GRC-Werkzeugen gemindert oder gar vollständig beseitigt werden.

cirosec zeigt Ihnen die Möglichkeiten, Einsatzbereiche, aber auch Grenzen solcher Governance-, Risk-Management- und Compliance-Werkzeuge in Ihrem Unternehmensumfeld auf, ermittelt gemeinsam mit Ihnen Ihre Anforderungen und unterstützt Sie als herstellerunabhängiger Berater bei der Auswahl der für Sie am besten geeigneten Lösung.

ANGEBOT

Leistungen von cirosec im Einzelnen

Planung und Einführung des ISMS

Wir unterstützen Sie bei folgenden Aktivitäten:

- Erstellung bzw. Optimierung der Leitlinie und von Sicherheitsrichtlinien
- Aufbau bzw. Optimierung Ihrer Sicherheitsorganisation
- Einführung bzw. Verbesserung der operativen ISMS-Prozesse, z. B. Incident Management, Schwachstellenmanagement oder Policy-Management
- Ausgestaltung des Risikomanagementprozesses
- Durchführung von Bedrohungs- und Risikoanalysen
- Ermittlung von Messgrößen zur Messung der Effizienz des ISMS und der getroffenen Maßnahmen
- Durchführung von Trainings- und Awareness-Maßnahmen.

Dabei richten wir uns an internationalen Standards wie ISO/IEC 27001 aus und berücksichtigen selbstverständlich Ihre individuellen Rahmenbedingungen und Compliance-Anforderungen.

ISMS-Standortbestimmung und -Überprüfung

Sie möchten in Erfahrungen bringen, ob Ihr ISMS als Prozess funktioniert und alle wichtigen und im ISO/IEC-Standard 27001 geforderten Aspekte abdeckt?

Hier unterstützen wir Sie bei folgenden Aktivitäten:

- Ist-Analyse des ISMS
- Gap-Analyse (Soll-Ist-Vergleich)
- Definition und Abarbeitung von Arbeitspaketen zum Schließen erkannter Lücken
- Ermittlung der Effizienz des ISMS und der ergriffenen Maßnahmen.

Vorbereitung zur Zertifizierung nach ISO/IEC 27001

Falls Sie Ihr ISMS nach ISO/IEC 27001 zertifizieren lassen möchten, begleiten wir Sie auf dem Weg dorthin. Im Rahmen eines Pre-Zertifizierungsaudits („27001-Compliance-Audit“) ermitteln unsere ISMS-Lead-Auditoren mögliche Handlungsbedarfe und helfen Ihnen anschließend, etwaige Lücken zu schließen.

IT-Risikomanagement

Ein strukturiertes Risikomanagement ist der Schlüssel für ein erfolgreiches ISMS. Wir begleiten Sie zum Beispiel bei folgenden Aktivitäten:

- Erarbeitung einer Methodik zur Ermittlung, Bewertung und Behandlung von Risiken
- Beschreibung der Schnittstelle zum Unternehmens-risikomanagement
- Durchführung von Business-Impact-Analysen und Schutzbedarfsermittlungen
- Durchführung von Schwachstellen- und Bedrohungsanalysen zur Ermittlung Ihrer Risiken
- Entscheidung über den weiteren Umgang mit identifizierten Risiken, z. B. bei der Auswahl geeigneter Maßnahmen und deren Priorisierung.

Werkzeuge zur Unterstützung des Informationssicherheits-, Compliance- und Risikomanagements

Wir zeigen Ihnen die Möglichkeiten, Einsatzbereiche, aber auch Grenzen so genannter Governance-, Risikomanagement- und Compliance-Werkzeuge in Ihrem Unternehmensumfeld auf und unterstützen Sie als herstellerunabhängiger Berater bei der Auswahl der für Sie am besten geeigneten Lösung mit folgenden Dienstleistungen:

- Potentialanalyse zur Ermittlung des zu erwartenden Mehrwerts eines GRC-Werkzeugs
- Anforderungsermittlung und -analyse
- Produktvorauswahl
- Produktevaluierung anhand eines Prototyps
- Produkteinführung.

IT-Grundschutz

Wendet Ihr Unternehmen die IT-Grundschutz-Vorgehensweise des BSI an, unterstützen wir Sie bei allen Schritten der Sicherheitskonzeption nach IT-Grundschutz:

- Strukturanalyse
- Schutzbedarfsermittlung
- Modellierung des IT-Verbunds
- Basis-Sicherheitscheck (Soll-Ist-Vergleich)
- Ergänzende Sicherheitsanalyse
- Realisierungsplanung.

Trainings und Awareness-Maßnahmen

Trainings und Awareness-Maßnahmen sind ein wesentlicher Teil eines ISMS, weil ein Sicherheitsprozess nur dann funktionieren und gelebt werden kann, wenn die Notwendigkeit für Sicherheitsmaßnahmen auf allen Ebenen im Unternehmen erkannt und akzeptiert worden ist. Hier unterstützt Sie cirosec unter anderem bei:

- Entwicklung des übergreifenden Awareness-Konzepts
- Durchführung von Awareness-Maßnahmen, z. B. in Form von Vorträgen oder Live-Hacking-Vorführungen
- Durchführung von Schulungen, z. B. die Trainings aus unserer Hacking-Extrem-Serie
- Messung der Wirksamkeit durchgeführter Awareness- und Schulungsmaßnahmen.

Ausbildung zum Certified ISO 27001 Lead Implementer

Dieser fünftägige Intensiv-Kurs vermittelt den Teilnehmern die nötigen Fachkenntnisse, um ein Unternehmen bei der Implementierung und beim Management eines Informationssicherheits-Managementsystems (ISMS) nach ISO/IEC 27001 zu unterstützen.

Die Teilnehmer erwerben in diesem zertifizierten Training außerdem umfassende Kenntnisse über die Best-Practices bei der Implementierung von Kontrollmechanismen für die Informationssicherheit aus allen Bereichen des Standards ISO 27002.

Ausbildung zum Certified ISO/IEC 27001 Lead Auditor

Dieses zertifizierte fünftägige Intensivtraining versetzt die Teilnehmer in die Lage, durch die Anwendung anerkannter Auditierungsprinzipien, -prozeduren und -techniken ein Informationssicherheitsmanagementsystem (ISMS) zu auditieren, sowie ein Team von Auditoren zu führen.

Die Teilnehmer erlangen im Laufe des zertifizierten Trainings das Wissen und die Fertigkeiten, um ein solches Audit kompetent und konform zum Zertifizierungsprozess des Standards ISO/IEC 27001 zu planen und durchzuführen.

CIROSEC – IHR PARTNER IN DER IT-SICHERHEIT

Wir sind ein spezialisiertes Unternehmen mit Fokus auf IT- und Informationssicherheit und beraten unsere Kunden im deutschsprachigen Raum.

Das cirosec-Team zeichnet sich dabei durch seine zahlreichen Experten aus, die als Buchautoren oder Referenten internationaler Kongresse bekannt sind und den Kunden individuell mit technischem und strategischem Sachverstand beraten.

Darüber hinaus verfügen wir über langjährige Erfahrung in der Konzeption und Integration von Sicherheitsprodukten in komplexen Umgebungen. Bekannt sind einige der Mitarbeiter auch durch erfolgreiche Research-Tätigkeit, da sie immer wieder neue, noch nicht gemeldete Schwachstellen in Standardsoftwareprodukten finden.

Das Leistungsspektrum umfasst die Bereiche:

- Konzepte, Reviews und Analysen
- IT-Sicherheitsmanagement-beratung (ISO 27001, Risikomanagement, Erstellung von Prozessen, Policies, Richtlinien)
- Durchführung von Audits und Penetrationstests
- Incident Response und Forensik
- Trainings
- Konzeption, neutrale Evaluationen und Implementation von Produkten und Lösungen.

Typische Themen im Umfeld von Produkten und Lösungen sind:

- Moderne Schutzmaßnahmen für Unternehmen (z. B. WAFs, Schutz vor DDoS und gezielten Angriffen)
- Sicherheit im internen Netz (z. B. LAN-Zugangskontrolle, 802.1x, NAC/NAP, IPS)
- Bring your own Device, Mobile/ Wireless Security
- Werkzeuge für ISMS, Verwundbarkeits- und Risikomanagement
- Nachvollziehbarkeit administrativer Zugriffe.

cirosec GmbH
Edisonstraße 21 | 74076 Heilbronn | Deutschland
T +49 7131 59455-0 | F +49 7131 59455-99 | www.cirosec.de

v01CRS-13-1927-DE130624 · Bildquellen: istockphoto, shutterstock