PRAXISSEMINAR

RISIKOMANAGEMENT einfach machen

für Risikomanager, CISO, ISB, DSB, IT-Leiter & Co.

13./14. März 2019 in Berlin

Angebot zum

ÖFFNE-DRINNEN-EINEN-REGENSCHIRM-TAG

Bildnachweis: ipopba (iStock)

Nutzen Sie bereits schlanke und einfache Verfahren bzw. Werkzeuge, um ihre Risiken zur Informations-, Cyber- und IT-Sicherheit zu steuern?

SEC2DO

Stand: 31.01.2019

SEC2DO

Halten Sie es für angemessen in ihrem Büro einen Regenschirm aufzuspannen?

Nein?! Wir auch nicht.

Erfahren Sie in unserem vertiefendem Praxisseminar zum Risikomanagement der Informationssicherheit eine strukturierte Vorgehensweise zur angemessenen Behandlung Ihrer Unternehmensrisiken und schaffen Sie sich eine optimale Ausganglage für Ihr Informationssicherheits-Managementsystem (ISMS).

RISIKOMANAGEMENT einfach machen

Warum sollte ich dieses Seminar besuchen?

Sie erlangen das Wissen, wie Sie Ihre Cyber- und IT-Risiken mittels effektiver Verfahren steuern können und gleichzeitig Zeit und Kosten durch einfach nutzbare Lösungen und Tools sparen.

Sie verfügen bereits über Grundkenntnisse der Informationssicherheit, aber Ihr theoretisches Wissen hilft Ihnen in der praktischen Umsetzung nicht weiter?

Sie fragen sich, was die ersten Schritte zum Risikomanagement in der Praxis sind?

Genau an dieser Stelle setzt unser praxisorientiertes Seminar an. Ein planvolles Management Ihrer Informationssicherheits-, IT- und Cyber-Risiken verhilft Ihnen zur effektiven Umsetzung und Erreichung Ihrer Unternehmensziele.

Warum brauche ich ein Risikomanagement?

Für die Vermeidung von Risiken, die Aufrechterhaltung des Geschäftsbetriebs und die Erreichung ihrer Unternehmensziele.

Wir beantworten Ihnen die Frage, warum Sie ein einfaches und strukturiertes Risikomanagement benötigen, als auch wie dieses aussehen sollte um erfolgreich zu sein.

Zum Einstieg erhalten Sie eine kurze Auffrischung worauf es gemäß IT-Grundschutz oder der DIN ISO 27001 beim Risiko- und Informationssicherheits-Management ankommt. Sie kennen die wesentlichen gesetzlichen und regulatorischen Anforderungen, erfahren wie Sie optimal den Geltungsbereich definieren, die passenden Rollen und Verantwortlichkeiten im Unternehmen bestimmten und die Dokumentation gesetzeskonform durchführen.

Ihr Schulungsleiter

MARTIN PETERS

Über 10 Jahre relevante Berufserfahrung im Bereich Informationssicherheits- und Risikomanagement

Herr Peters begleitet als Berater Unternehmen (Krankenversicherungen, Rechenzentren, Banken) und Behörden bei der Einführung und Weiterentwicklung von bedarfsgerechten IT-Risiko- und Informationssicherheitsmanagementsystemen (ISMS).

Zudem ist Herr Peters seit 2013 Lehrbeauftragter an der Hochschule für Wirtschaft und Technik in Berlin.

Im Rahmen seiner Tätigkeiten erwarb Herr Peters folgende Zusatzqualifikationen:

- Geprüfter ISO 27001 Auditor (SGS TÜV)
- Zusätzliche Prüfverfahren-Kompetenz für § 8a BSIG
- Geprüfter IT-Sicherheitsbeauftragter (SGS TÜV)
- Geprüfter Datenschutzbeauftragter (SGS TÜV)
- COBIT Practitioner (ISACA)
- Foundation in IT Service Management in FitSM
- Foundation in IT Service Management (TÜV SÜD)
- Foundation in PRINCE2 (APM Group)

+49 151 42 40 30 30
martin.peters@sec2do.com

Stand: 31.01.2019

Dieses Seminar beantwortet Ihnen folgende Fragen

1. WOHER WEIß ICH, WAS ICH SCHÜTZEN MUSS?

Es braucht eine systematische Vorgehensweise der Strukturanalyse, um die relevanten Informationen und Prozesse zu erheben.

Profitieren Sie von unserem langjährigen Praxiswissen zu einem durchdachten und planvollen Vorgehen. Sie werden erkennen, warum es wichtig ist und vor allem wie sie die relevanten Prozesse und Informationen erheben. Gemeinsam konzentrieren wir uns mit Ihnen auf das Wesentliche.

Mit unseren Werkzeugen können Sie sich selbst eine angemessene Datenbasis erstellen und kennen die wichtigsten Merkmale zur Erhebung Ihrer Werte.

2. WELCHE MAßNAHMEN MUSS ICH UMSETZTEN?

Die richtigen Maßnahmen erkennen Sie anhand von Schutzniveau und Schutzbedarf!

Im Risikomanagement wird auf die Unternehmenswerte und die möglichen Auswirkungen geschaut, die durch eine Verletzung der Grundwerte (Vertraulichkeit, Verfügbarkeit und Integrität) entstehen könnten. Wir geben Ihnen einfache Techniken und Werkzeuge an die Hand, mit denen Sie die Schutzbedarfsfeststellung durchführen können, um in Ihrem Unternehmen ein angemessenes Schutzniveau aufzubauen und aufrechtzuerhalten.

Neben der Business-Impact-Analyse (BIA) werden u. a. auch die Aspekte zum Verteilungs-, Kumulations- und Maximumprinzip beachtet.

3. WANN MUSS ICH RISIKOANALYSEN MACHEN?

So selten, wie möglich - so oft, wie nötig.

Wir zeigen Ihnen, wie Sie zeit- und kostenintensive Risikoanalysen vermeiden und auf bestehende Erkenntnisse zurückgreifen können. Wann reicht eine Gap-Analyse aus und wann sollten Sie eine vollständige Risikoanalyse machen?

4. WIE BEHALTE ICH DEN ÜBERBLICK UND DIE KONTROLLE?

Messen Sie mit den passenden Kennzahlen und dem richtigen Know-how fortlaufend den Erfolg und die Wirksamkeit Ihrer Maßnahmen.

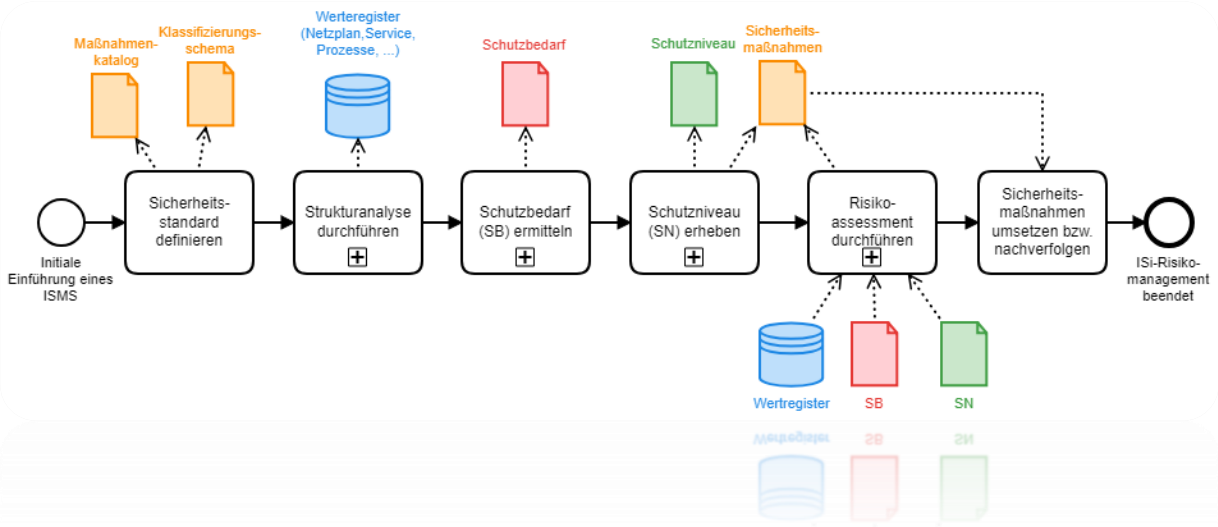
Lernen Sie, wie Sie mit einfachen und schlanken Lösungen das für Sie passende und wirksame Risiko-management für Informationssicherheits-Risiken installieren und zugleich Anforderungen an die Dokumentation erfüllen.

Überzeugen Sie sich von unseren pragmatischen Ansätzen und verständlichen Lösungen zur Risiko-berichterstattung zum erreichten Informations-sicherheitsniveau.

5. WO FANGE ICH AN?

...einfach machen.

Schaffen Sie sich die für Sie passenden Rahmen-bedingungen. Holen Sie die Fachverantwortlichen mit ins Boot und nutzen Sie individuelle Werkzeuge, um die Umsetzung zu starten. Hierzu geben wir Ihnen Tipps aus den Bereichen: Kommunikation, Security Awareness und Change-Management



Stand: 31.01.2019

Die Seminarinhalte auf einen Blick

13. MÄRZ 2019 - 10:00 BIS 18:00 UHR

EINFÜHRUNG

- Allgemeine Gefährdungslage
- Gesetzliche und regulatorische Anforderungen
- Nutzen von Standards (ISO 27001 & BSI IT-Grundschutz)
- Grundwerte der Informationssicherheit
- Geltungsbereiche; Rollen und Verantwortlichkeiten
- Überblick zur Beurteilung der Risikosituation: steuern, erheben, bewerten

DURCHFÜHRUNG EINER STRUKTURANALYSE

- Erstellung der Datenbasis
- Erhebung der Prozesse und Informationen
- Identifikation der Auslagerungen
- Komplexitätsreduktion durch Gruppierung
- Übungen & Diskussion

14. MÄRZ 2019 - 09:00 BIS 17:00 UHR

RISIKOASSESSMENT

- Gap-Analyse vs. Risikoanalyse
- Eintrittswahrscheinlichkeiten und Schadenspotenzial
- Bedrohungen- und Schwachstellen-Analyse Gefährdungsbewertung
- Risikoklassen/ Risikomatrix
- Restrisikoanalyse
- Umgang mit Risiken
- Maßnahmenplanung Risikobehandlungsplan
- Übungen & Diskussion

Mittagspause

BESTIMMUNG DER SCHUTZBEDARFSANFORDERUNGEN

- Business-Impact-Analyse
- Verteilungs-, Kumulations- und Maximumprinzip
- Übungen & Diskussion

ERMITTLUNG DES ERREICHTEN SCHUTZNIVEAUS

- Ermittlung des erreichten Schutzniveaus
- Unterscheidung Schutzniveau in fachlicher und technischer Sicht
- Prüfung und Bewertung von Konzepten Maßnahmenerhebung
- Übungen & Diskussion

BERICHTERSTATTUNG & KONTROLLE

- Anforderungen an die Dokumentation
- Erklärung zur Anwendbarkeit (SOA – Statement of Applicability)
- Wesentliche Risikoinformationen
- Kennzahlen für die Erfolgsmessung
- Management-Übersicht

PRAKTISCHE HINWEISE: NÄCHSTE SCHRITTE

- Rahmenbedingungen schaffen
- Werkzeuge auswählen
- Erstellung der Vorgehensweise
- Wertvolle Tipps aus den Bereichen: Change Management, Security Awareness und Unternehmenskommunikation

Stand: 31.01.2019

Unser Angebot

TEILNAHMEGEBÜHREN

Early-Bird-Ticket

Zum Öffne-drinnen-einen-Regenschirm-Tag

Zahlen Sie bis zum 8. März 2019 und erhalten Sie rund **33% Rabatt** auf die Standard-Teilnahmegebühr

997 €
zzgl. MwSt

Standard-Ticket

Standard-Teilnahmegebühr bei Buchung ab dem 08.03.2019

1.490 €
zzgl. MwSt

Sie-kommen-nicht-alleine-Ticket

Jede weitere Person erhält **50% Rabatt** auf die von Ihnen gezahlte Teilnahmegebühr für ein Early-Bird- oder Standard-Ticket

ab 498,50 €
zzgl. MwSt

Buchen Sie jetzt Ihre Weiterbildung!
Senden Sie hierzu das Anmeldeformular per Mail an team@sec2do.com

Die Teilnahmegebühr stellen wir ab Buchung mit sofortigem Zahlungsziel in Rechnung. Die Teilnahmegebühr beinhaltet ein gemeinsames Mittagessen pro vollem Seminartag, Pausenverpflegung und Arbeitsunterlagen. In unseren AGBs finden Sie Informationen bezüglich anfallender Kosten bei Stornierung, Umbuchung und Ersatzteilnehmer.

TERMIN UND ORT

Am 13. und 14. März 2019 in Berlin (*Seminarort wird noch bekannt gegeben*)

TEILNEHMERKREIS UND TEILNAHMEVORAUSSETZUNGEN

Beauftragte im Informationssicherheits-Management (CISO, ISB, DSB, Risikomanager) sowie Führungskräfte, Projektleiter mit Grundkenntnissen zum Risikomanagement in der Informationssicherheit.

Ihr Nutzen auf einen Blick

- Sie kennen zwar die Theorie zum Informationssicherheits-Risikomanagement, aber können das Erlernte nicht richtig in die Praxis umsetzen? Sie brauchen eine Anleitung für die ersten Schritte? Wir verraten es Ihnen!
- Erwarten Sie Praxiswissen und Übungen anstatt langweilige Theorie und PowerPoint. Wir zeigen auf wie die Prinzipien des Informationssicherheits-Risikomanagement auch für Sie funktionieren können!
- In der Schulung geht es in die Tiefe. Schritt-für-Schritt lernen Sie die Fähigkeiten, Strategien und Techniken, um die Steuerung ihrer Risiken zu meistern!
- Sie erhalten ein Arbeitsbuch (Leitfaden, Checklisten etc.). Darin stehen alle wichtigen Fakten aus den Schulungsinhalten sowie Fragen zur Reflexion und Übungen. Es unterstützt Sie dabei, den größten Mehrwert für Sie herauszuholen und das neugewonnene Wissen wirklich zu verinnerlichen!

WIR FREUEN UNS, MIT IHNEN INS GESPRÄCH ZU KOMMEN!

www.sec2do.com
+49 30 68 40 30 30

Stand: 31.01.2019