Risk Management & Information Security (IS) Teil 1 und Teil 2

Kennen Sie Ihr volles Risiko?

Ein Risk & Security Check zeigt, wo Sie stehen …

Wir leben im Zeitalter einer sich rasant weiterentwickelnden Technik – beispielsweise in der Telekommunikation, IT und Medizintechnik. Dies stellt Unternehmen und Organisationen strategisch und systemtechnisch vor große Herausforderungen. Durch die Komplexität steigen die Risikopotentiale, so auch die Risiken hinsichtlich Datenmissbrauch und Systemausfall.

Entsprechende Rahmenbedingungen werden u. a. per Gesetze oder Standards vorgegeben und sind von den Unternehmen einzuhalten. Standards geben genau vor, „WAS" im Rahmen der Planung, Beschaffung, Entwicklung, Implementierung, Betrieb, Support und Verbesserung von IT-Services für Unternehmensbedürfnisse zu tun ist. Best Practices, Frameworks, Prozess-Assessment-Modelle (PAM) und Prozess-Referenz-Modelle (PRM) unterstützen bei der Umsetzung, dem „WIE".

Dieses Training vermittelt Anforderungen seitens Risk und Information Security Management für Unternehmen. Es wird u. a. gezeigt, wie in einem Self-Assessment eine Standortbestimmung erstellt werden kann. Dieses Ergebnis kann als Basis für ein externes Assessment herangezogen werden, um im nächsten Schritt eventuell einem Audit unterzogen werden zu können.

Nutzen

- ☐ Gute Gründe für Risk Management und Information Security Management
- ☐ Bedürfnisse, Maßnahmen und Konsequenzen kennen lernen
- ☐ Kenntnisse über ÖNORM EN 31010 - Risk Management – Risk Assessment Techniques
- ☐ Kenntnisse über ISO 27001 - Information Security Management
- ☐ Wie kann ich in ein Self-Assessment durchführen?

Zielgruppe

GeschäftsführerInnen, VerwaltungsdirektorInnen öffentlicher Organisationen, kaufmännische und technische Leitung von Unternehmen und Non-Profit-Organisationen, IT-ManagerInnen, Business Excellence ManagerInnen;

Generell all jene Personen, die sich mit Information Security Management und Risk Management Agenden auseinandersetzen oder einfach mehr darüber wissen möchten.

Stragere Management Consulting e.U.
Am Kirchenweg 8 I A-3071 Böheimkirchen
+43 664 5324685 I office@stragere.at
www.stragere.at

© Stragere Management Consulting e.U.

Voraussetzungen

Teil 1: Keine besonderen Voraussetzungen
Teil 2: Besuch von Risk Management & Information Security Management Teil 1 empfohlen

Inhalt

TEIL 1

- ☐ Warum Risk Management und Information Security Management?
- ☐ Bedürfnisse - Maßnahmen - Konsequenzen
- ☐ Überblick über Standards und Frameworks
- ☐ Einführung Risk Management Prozess & Methoden zur Risiko Identifizierung und Analyse
- ☐ Risk Management – Risk Assessment Techniques: Einführung in die ÖNORM EN 31010
- ☐ Information Security Management: Einführung in den Standard ISO 27001
- ☐ Praktische Beispiele

TEIL 2 (Aufbauseminar)

- ☐ Risk Management Prozess & Methoden zur Risiko Identifizierung und Analyse
- ☐ Anforderungen der EN 31010 und ISO 27001
- ☐ Mapping beider Normen – Wo gibt es Zusammenhänge?
- ☐ Self-Assessment – Wie Sie eine Standortbestimmung durchführen können
- ☐ Praktische Beispiele

Seminardauer

Dauer: Teil 1 und Teil: je 2 Tage
Abschluss: Teilnahmebestätigung / Zertifikat

Allgemeine Informationen

Weitere Informationen (Teilnahmebedingungen, Veranstaltungsort, Termine und Dauer, usw.) finden Sie in unseren Informationsbroschüren sowie auf unserer Homepage www.stragere.at.

Für weitere Fragen und Informationen über spezielle Angebote und Pakete für firmeninterne Seminare stehen wir gerne zur Verfügung.
Kontaktieren Sie uns unter office@stragere.at oder rufen Sie uns einfach an: +43 664 5324685.

Stragere Management Consulting e.U.
Am Kirchenweg 8 I A-3071 Böheimkirchen
+43 664 5324685 I office@stragere.at
www.stragere.at

Juni 2016
© Stragere Management Consulting e.U.