



Wahlweise als Inhouse-Seminar oder Webinar buchbar

Risikoanalyse M365 für Banken und Versicherungen

Zielgruppe: Cloud Use Case Owner, Cloud Manager, IT-Leiter, IT-Projektleiter, IT-Provider-Manager, Beauftragte für IT-Outsourcing, Beauftragte für Datenschutz, Informationssicherheit und IT-Risiko-Management, IT-Revision, IT-Betrieb und Rechtsabteilung, Betriebs- und Personalrat

Dauer: Empfohlen als 1-tägiges Seminar (ca. 6 h) oder Webinar in 2 Einheiten (ca. 2x 3 h)

Preis: Bis 4 Personen: EUR 650,- p. P., ab der 5. bis zur 8. Person: EUR 500,- p. P. zzgl. MwSt. und bei Vor-Ort-Seminaren Reisekosten für die ReferentInnen. Im Preis enthalten sind die Vorbereitung (Briefing-Telko) und Durchführung des Seminars bzw. Webinars inkl. Unterlagen. Mindestteilnehmerzahl: 4 Personen. Bei Gruppen mit mehr als 8 Personen Preis auf Anfrage

Kurzbeschreibung:

Banken, Finanz- und Zahlungsdienstleister sowie Versicherungen stehen bei der Nutzung cloudbasierter Lösungen „unter Aufsicht“. Wie im traditionellen IT-Outsourcing gilt bei Vorliegen der entsprechenden Voraussetzungen auch bei Cloud-Diensten wie M365 die zwingende Notwendigkeit zur Analyse der damit verbundenen Risiken in der Nutzung (u.a. MaRisk, Solvency II). Dabei stoßen diese Unternehmen vielfach an die Grenzen der Komplexität der individuell zu prüfenden Anforderungen wie sie u.a. aus dem Datenschutz, der Informationssicherheit, dem IT-Risikomanagement erwachsen – nicht zuletzt, weil jede der in Frage stehenden M365-Apps wie Exchange, SharePoint, Teams etc. einzeln aufgrund der unterschiedlichen Anwendungsfälle auf ihre jeweilige Risikobehaftung zu prüfen sind.

Das Seminar/Webinar gibt einen umfassenden Einblick in den Ablauf solcher Risikoanalysen und zeigt die von Microsoft standardmäßig ergriffenen technischen und organisatorischen Maßnahmen auf, die es zu bewerten gilt. Die ReferentInnen der ISW und microfin geben vor dem Hintergrund ihrer einschlägigen Erfahrung aus der Begleitung solcher Risikoanalysen Beispiele weiter, die sich in der Praxis bei der Risikobeurteilung der M365-Apps bislang bewährt haben. Die TeilnehmerInnen erhalten zugleich Orientierung, welche einschlägigen Dokumentationen, Nachweise, Zertifikate etc. hierzu auf der Webseite von Microsoft ausgewiesen werden und im Rahmen der Risikoanalyse herangezogen werden sollten.

Übersicht der Module und Inhalte:



Regulatorische Notwendigkeit zur Durchführung von Risikoanalysen der M365-Apps bei Banken, Finanz- und Zahlungsdienstleistern sowie Versicherungen



Übersicht der an der Risikoanalyse der M365-Apps üblicherweise zu beteiligten Funktions- und Organisationseinheiten im Unternehmen einschließlich der damit verbundenen, jeweiligen Prüf- und Verantwortungsbereiche



Praxistipps zur Entflechtung der M365-Apps in sinnvolle Anwendungsfälle bei der Risikoanalyse („Produkte“/Services, Abhängigkeiten und mögliche Optionen bei den verschiedenen Produkten)



Praxistipps zum – möglichst „schlanken“ – Vorgehen in der M365-Risikoanalyse (von der Anforderungsdefinition bis zur Entscheidungsvorlage)



Übersicht zu prüfungsrelevanten (Microsoft-) Dokumenten wie Zusatzvereinbarungen, Testatsberichte, Prüfkataloge wie BSI C5 oder andere Standards

Stimmen Sie Ihren individuellen Bedarf in einem persönlichen Gespräch mit uns ab



Irina Shapiro
microfin

T +49 6172 / 177 63 - 175
E anfrage@microfin.de



Praxiseinblick zu technischen Risiken in der Nutzung der M365-Online-Dienste (fehlende Verschlüsselung, mangelhafter Verschlüsselungsstandard, fehlende Hoheit über die Schlüssel, Verfügbarkeitsabhängigkeiten von Internetzugang und Kundeneinstiegspunkt bei MS, Wiederherstellungszeiten und Integrationsverlust mit/ohne O365-Backup, Berechtigungszuweisungen durch CSP, Availability Key, Angriff über Lizenz-Provider etc.)



Exit-Plan für M365
(Anforderungen, Konzept und Vorgehen)



Praxisbewährte Hilfsmittel zur „handhabbaren“ und zugleich revisionssicheren Durchführung und Dokumentation der M365-Risikoanalyse



Nach der Erstanalyse: Revalidierung der identifizierten Risiken während der Nutzung von M365 (Rhythmus, Wiedervorlagen Nachweise der Kontrollen und Garantien etc.)



Exkurs: O365-Backup und Notfallplan als Einflussfaktoren auf die Risikoanalyse?

IT-Security@Work (ISW)

ISW unterstützt ihre Kunden dabei, aktuelle Entwicklungen und Trends, Aspekte der IT-Security, IT-Risikomanagement, Compliance und des Datenschutzes mit ihrem Business in Einklang zu bringen. Insbesondere kümmern wir uns darum, Business- und Betriebsprozesse so zu kombinieren, dass ein Optimum im Spannungsfeld Business, Betrieb (Work) und IT-Security erreicht wird.

Hierbei legen wir großen Wert auf nachhaltige und systemische IT-Beratung, mit Blick auf alle Umstände beim Kunden, gemäß unserem Slogan: „Mit Sicherheit ein Blick fürs Ganze“.

microfin Unternehmensberatung

microfin bringt Unternehmen in der Digitalisierung voran – durch Cloud Services, Managed Services oder in hybriden Sourcing-Modellen. Als Sourcing-Experten realisieren wir Strategien, Ausschreibungen sowie Transitionen und setzen Provider- und Cloud-Management-Organisationen auf. Die Durchführung von Benchmarks sowie die Planung und Umsetzung von IT-Kostenoptimierungen ergänzen unser Leistungsportfolio.

Unsere agilen Teams aus Informatikern, Juristen und Betriebswirten gestalten und integrieren IT- und Business-Services – mit Herz und Verstand seit 2002.

Sie haben Fragen? Wir haben Antworten!

Gerne stellen wir unser Angebot vor und beantworten Ihre Fragen in einem persönlichen Gespräch.



Dirk Rauschenbach
ISW

T +49 6103 / 37416 00
E dirk.rauschenbach@isw-online.de



Irina Shapiro
microfin

T +49 6172 / 177 63 175
E i.shapiro@microfin.de