

Maximale Datensicherheit bei der Nutzung von Copilot

Sie möchten [Copilot](#) in Ihrem Unternehmen einsetzen und haben spezifische Anforderungen bezüglich Datensicherheit? Mit einem ganzheitlichen 360°-Ansatz für Information Protection & Governance bilden Sie das Fundament für die Nutzung von Copilot und erfüllen zugleich Ihre Bedürfnisse.

Copilot-Ready mit Information Protection & Governance (IPG)

Unsere Lösung bietet eine umfassende Suite von Sicherheits-Tools, die es Ihnen ermöglicht, sensible Daten zu schützen, zu klassifizieren und zu verwalten. Bevor Sie Microsoft Copilot sicher nutzen und das volle Potenzial ausschöpfen können, müssen die Voraussetzungen geschaffen werden, um Ihre individuellen Sicherheitsanforderungen zu erfüllen. Durch die nahtlose Integration von Informationsschutz, Risiko- und Compliance-Management sowie Governance-Funktionen bieten wir eine ganzheitliche Lösung, um Datenschutzstandards einzuhalten und Risiken zu minimieren.

Lösungsausprägungen

Unsere Lösung ist darauf ausgerichtet, Ihre spezifischen Anforderungen im Informationsmanagement zu erfüllen, Ihre Daten sicher zu schützen, die Compliance sicherzustellen und das Risiko von Datenverlusten zu minimieren. Wir bieten Ihnen sechs konkrete Lieferobjekte, die perfekt aufeinander abgestimmt sind und das Fundament für die Nutzung von Copilot nach den Best Practices von Aveniq bilden.

1. IPG-Grundlagen

Um Ihre Organisation optimal auf die Herausforderungen vorzubereiten, erarbeiten wir folgende Grundlagen:

- MIP: Einführung in die Grundlagen der Microsoft Information Protection wie Sensitivity und Retention Labels
- DLP: Vertiefung der Grundlagen der Data Loss Prevention
- GRC: Entwicklung der Grundlagen für Governance, Risk & Compliance
- ComCom: Ausarbeitung von Grundlagen für die Communication Compliance

2. IT-Service Continuity-Katalog

Unser IT-Service Continuity-Katalog bietet eine klare Darstellung der Abhängigkeiten Ihrer IT-Services von den Business Services und legt Prioritäten fest. Sie erreichen damit, dass Ihre IT-Services die Bedürfnisse Ihres Unternehmens optimal unterstützen.

3. Cyber Security Assessment & Level Definition

Wir helfen Ihnen dabei, den richtigen Sicherheitslevel für Ihr Unternehmen zu definieren und erforderliche Massnahmen zu ergreifen. Dadurch können Sie sicherstellen, dass Ihre Daten und Systeme optimal geschützt sind.

4. Lizenzierung

Basierend auf Ihren individuellen Anforderungen ermitteln wir die benötigten Lizenzen und berechnen die Kosten. Sie haben damit die Gewissheit, dass Sie die richtigen Tools und Ressourcen haben, um Ihre Sicherheitsziele zu erreichen, ohne dabei unnötige Kosten zu verursachen.

5. Roadmap

Gemeinsam entwickeln wir eine klare Roadmap für die Umsetzung Ihrer Sicherheitsstrategie zu entwickeln. Dies ist ein wichtiger Schritt, damit Sie Ihre Ziele effizient erreichen sowie potenzielle Hindernisse frühzeitig erkennen und bewältigen können.

6. Strategie

Wir unterstützen Sie bei der Entwicklung einer ganzheitlichen Sicherheitsstrategie, die Ihre individuellen Anforderungen berücksichtigt und Ihnen dabei hilft, langfristigen Erfolg zu erzielen. Als Grundlage dafür dienen alle Lieferobjekte, welche aufeinander aufbauen.

Ihr Nutzen

Schutz und Datenklassifizierung:

Unser ganzheitlicher Ansatz im Bereich Information Protection umfasst alle relevanten Services in Microsoft 365. Wir definieren und bezeichnen Daten innerhalb von Microsoft 365 sowie anderen cloudbasierten Lösungen gemäss Ihren Anforderungen und Geschäftszielen.

Data Governance & Compliance:

Durch die Festlegung des Datenlebenszyklus innerhalb von Microsoft 365 und möglicherweise weiterer Lösungen gewährleisten wir eine effiziente Data Governance, die sich am «Common Information Governance Scenario» von Microsoft nach MIP orientiert. Dadurch können Sie Compliance-Anforderungen erfüllen und den sicheren Umgang mit Daten gewährleisten.

Sensitivity & Retention Labeling:

Sensibilitätskennzeichnungen (sensitivity labels) ermöglichen die Klassifizierung und den Schutz von Daten in SharePoint und Teams, während Aufbewahrungsetiketten (retention labels) die Aufbewahrung und Archivierung von Daten regeln. Unser praxisorientierte Ansatz ermöglicht eine automatische Zuweisung von Labels basierend auf Sensitivity Information Types und suchbasierten Metadaten, ohne die Produktivität und Zusammenarbeit zu beeinträchtigen.

Transparente IT-Service-Abhängigkeiten:

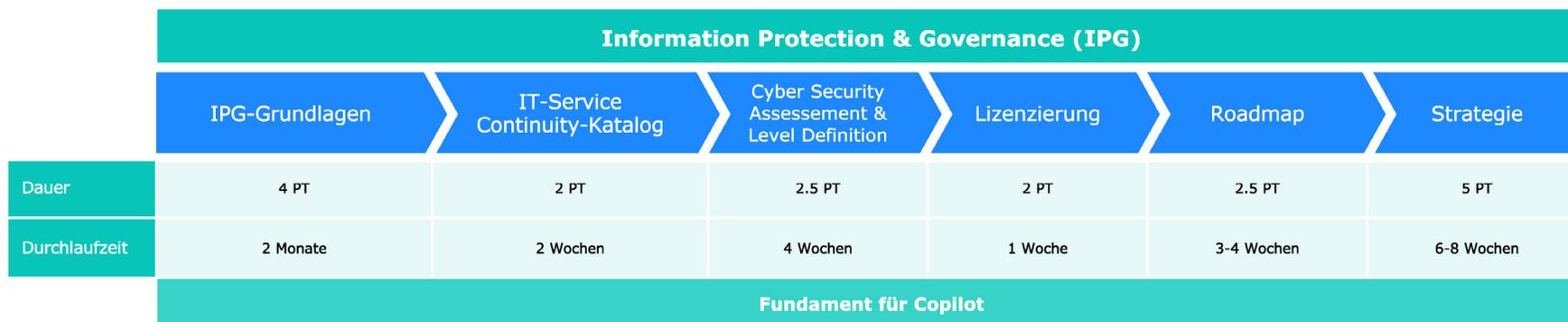
Der IT-Service Continuity-Katalog zeigt die Abhängigkeiten Ihrer IT-Services von den Business-Services auf und legt Prioritäten fest. Dies ermöglicht eine transparente Darstellung der Verknüpfungen und Interdependenzen, insbesondere im Hinblick auf bevorstehende Architektur-Anpassungen wie Exchange Online, Teams oder SharePoint Online.

Definition des Cyber Security Levels:

Wir erarbeiten und definieren den erforderlichen Cyber Security Level für Ihr Unternehmen. Basierend darauf werden die Lizenzanforderungen und Add-Ons festgelegt, um ein angemessenes Sicherheitsniveau zu gewährleisten.

Lizenzierung und Kostenanalyse:

Wir ermitteln den spezifischen Lizenzbedarf basierend auf dem Gesamtbild Ihrer Architektur und den definierten Cyber Security Levels. Die Kosten werden detailliert berechnet und dienen als Entscheidungsgrundlage, um zu gewährleisten, dass Ihre Sicherheitsziele effektiv und kosteneffizient erreicht werden.



Kontaktieren Sie uns, um gemeinsam eine Lösung zu definieren, welche Ihren aktuellen und künftigen Bedürfnissen entspricht: info@aveniq.ch