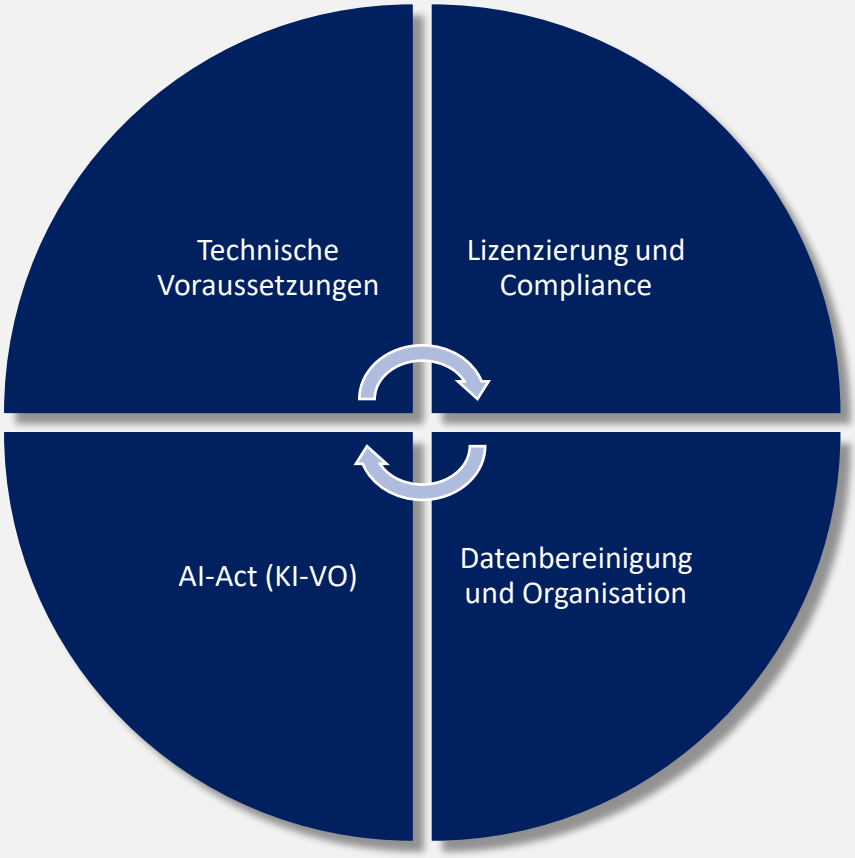
Checkliste Technical Readiness – Microsoft Copilot

Eine erfolgreiche Einführung von Microsoft 365 Copilot erfordert technische Vorbereitungen in den Bereichen Infrastruktur, Datenmigration und Berechtigungskontrolle. Eine saubere technische Umsetzung stellt nicht nur die Funktionalität sicher, sondern minimiert auch Risiken und erhöht die Benutzerakzeptanz.



Technische Voraussetzungen

1. Datenmigration

Problemstellung:
Daten aus verschiedenen Quellen (z. B. Google Drive, lokale Netzwerklaufwerke, andere Cloud-Dienste) sind nicht zentralisiert und daher für Copilot schwer zugänglich.

Lösung:
Nutzen Sie den Migration Manager, um Quellen wie File Shares / Drittanbieterdienste zu verbinden.

- ✓ Aktivieren Sie im Admin Center unter „Einstellungen > Datenmigration“ den Migration Manager. Hier können Sie Datenquellen (File Shares oder Google Drive, Box etc.) verbinden.

Wichtige Aspekte:

- ✓ Planen Sie hierfür Abstimmungen mit den betroffenen Abteilungen.
- ✓ Stellen Sie sicher, dass Dateinamen und -formate kompatibel mit SharePoint/OneDrive sind.
- ✓ Zugriffsbeschränkungen nach der Migration prüfen.

2. Netzwerk-Endpunkte

Problemstellung:
Blockierte Ports oder URLs können verhindern, dass Copilot die benötigten Dienste erreicht.

Lösung:
Öffnen Sie die Firewall-Konfiguration und fügen Sie die von Microsoft 365 genutzten URLs und Ports zur Whitelist hinzu. Die vollständige Liste finden Sie hier:
Microsoft 365-URLs und-IP-Adressbereiche - Microsoft 365 Enterprise | Microsoft Learn

- ✓ Freigabe relevanter URLs und IP-Adressen in der Firewall.
- ✓ Test der Verfügbarkeit mit PowerShell:

Test der Verfügbarkeit:

- ✓ Tools wie PowerShell oder Ping-Befehle stellen sicher, dass die URLs erreichbar sind.
- ✓ Beispiel: Test-NetConnection -ComputerName copilot.microsoft.com -Port 443

3. Update-Kanäle:

Problemstellung:
Verwendung unterschiedlicher Versionen von Office-Anwendungen => verursacht Inkompatibilitäten.

Lösung:
Setzen Sie den Update-Kanal auf „Monatlich“

- ✓ Schritte: Gehen Sie im Admin Center zu „Geräte > Update-Richtlinien“. Setzen Sie den Updatekanal auf „Monatlich (Enterprise)“.

Überprüfung der Versionen:

- ✓ Kontrollieren Sie, ob alle Nutzer dieselbe Version verwenden. Dies kann unter „Office-Installationen“ im Admin Center eingesehen werden.

Lizenzierung und Compliance

1. Lizenzen

Problemstellung: Je nach bestehendem Lizenzmodell müssen passende Lizenzen erworben werden.

Lösung:
- ✓ Überprüfen Sie im Admin Center unter „Abrechnung > Dienste kaufen“, ob Copilot verfügbar ist.
- ✓ Nutzen Sie PowerShell für Massenzuweisung von Lizenzen: Connect-MsolService Set-MsolUser License -UserPrincipalName "user@domain.com" -AddLicenses "tenant:ENTERPRISEPREMIUM"

2. Berechtigungen

Problemstellung: Zu breite Freigaben gefährden die Sicherheit.

Lösung:
- ✓ In SharePoint und OneDrive anonyme Links deaktivieren.
- ✓ Sensible Dokumente (z. B. aus dem HR-Bereich) nur für Mitglieder freigeben.

Datenbereinigung

1. Datenbereinigung organisieren

Problemstellung: ROT-Daten (Redundant, Obsolete, Trivial)
- ✓ Abstimmung mit Abteilungen bzgl. Datenbereinigung & Wissensaufbau für zukünftige Arbeitsweise.
- ✓ Veraltete oder doppelte Daten erschweren die Arbeit und belasten den Speicher.

Lösung:
- ✓ Bereinigen Sie Daten im SharePoint Admin Center unter „Speicherberichte“.
- ✓ Automatisieren Sie den Prozess mit Tools wie Microsoft Purview.

2. Monitoring und Analysen

Problemstellung: Keine Transparenz über die Nutzung von Copilot.

Lösung:
- ✓ Datenschutzbeauftragte oder Betriebsräte hinzuziehen für datenschutzkonforme Berichte.
- ✓ Erstellen Sie Nutzungsstatistiken im Admin Center unter „Berichte > Nutzungsstatistiken“.

Ergebnisanalyse:
- ✓ Identifizieren Sie Schulungsbedarf basierend auf den Nutzungszahlen.

Problemstellung: Es gibt keine Kontrolle über kritische Zugriffe.

Lösung:
- ✓ Überwachungsprotokolle im Compliance Center zum Verfolgen von Zugriffen und Änderungen.

KI-VO: Technical Readiness Check

1. Datenschutz

Problemstellung: Keine ausreichender Datenschutz und Schutz der Privatsphäre der Nutzer.

Lösung:
- ✓ DSGVO-Konformität sicherstellen.
- ✓ Datenminimierung und Zweckbindung beachten.
- ✓ Transparenz gegenüber Nutzern gewährleisten.

2. Sicherheitsmaßnahmen

Problemstellung: Unzureichender Schutz vor unbefugtem Zugriff und Cyberangriffen auf KI-Systeme.

Lösung:
- ✓ Verschlüsselung und Zugriffskontrollen implementieren.
- ✓ Regelmäßige Sicherheitsaudits durchführen.
- ✓ Cybersecurity-Tools (z. B. Microsoft Defender) nutzen..

3. Technische Dokumentation

Problemstellung: Fehlende oder unvollständige technische Dokumentation

Lösung:
- ✓ Vollständige und aktuelle Dokumentation erstellen, die den Anforderungen der KI-VO genügt
- ✓ Standardisierte Formate verwenden.
- ✓ Dokumentation für Audits und Behörden bereitstellen..

4. Daten- und Modellnutzung

Problemstellung: Unkontrollierte Nutzung von Daten und Modellen (ohne rechtliche Vorgaben).

Lösung:
- ✓ Nur autorisierten Datenzugriff erlauben.
- ✓ Sensible Daten besonders schützen und Einwilligungen einholen.
- ✓ Tenant-bezogene Datenbeschränkungen einhalten.

5. Mitarbeiterschulung

Problemstellung: Mangelnde Schulung und Sensibilisierung derBelegschaft für den verantwortungsvollen Umgang mit KI-Systemen.

Lösung:
- ✓ Regelmäßige Schulungen zu KI-VO und Datenschutz durchführen.
- ✓ Bewusstsein für Compliance und ethischen KI-Einsatz fördern.
- ✓ Best Practices und Erfahrungen intern teilen..
- ✓ Der KI Führerschein® von soluzione

Link Sammlungen

Diese Link Sammlung hilft Ihnen, die richtige Anleitung sowie Information zur Abarbeitung der Checkliste zu finden.

- Datenmigration: https://learn.microsoft.com/de-de/sharepointmigration/mm-get-started
- Netzwerk-Endpunkte prüfen: Prüfen Sie die Erreichbarkeit von copilot.microsoft.com und anderen relevanten URLs. https://learn.microsoft.com/de-de/microsoft-365/enterprise/urls-and-ip-address-ranges
- Updatekanäle optimieren: https://learn.microsoft.com/de-de/deployoffice/overview
- Lizenzanforderungen überprüfen: https://learn.microsoft.com/de-de/microsoft-365/admin/manage/assign-licenses-to-users
- Berechtigungen prüfen: https://learn.microsoft.com/de-de/sharepoint/sharing-permissions
- ROT-Daten entfernen: https://learn.microsoft.com/de-de/sharepoint/manage-site-collection-storage-limits
- Daten konsolidieren: https://learn.microsoft.com/de-de/onedrive/plan-onedrive-migration
- Aufbewahrungsrichtlinien: https://learn.microsoft.com/de-de/microsoft-365/compliance/retention-policies
- Vertraulichkeitslabels: https://learn.microsoft.com/de-de/microsoft-365/compliance/sensitivity-labels
- Nutzungsberichte: https://learn.microsoft.com/de-de/microsoft-365/admin/activity-reports/activity-reports
- Zugriff überwachen: https://learn.microsoft.com/de-de/microsoft-365/compliance/audit-log-search