



# Auditing Microsoft 365

Too big to (be) secure!?

# Agenda

**Microsoft Teams oder wie arbeite ich zusammen?**

**Microsoft Entra ID oder wie identifiziere ich mich?**

**Microsoft Power Platform oder wie verbessere ich IDV?**

# Was lässt sich am Schreibtisch prüfen?

Warum nicht nur ein Besuch in Redmond viele Risiken abdeckt...

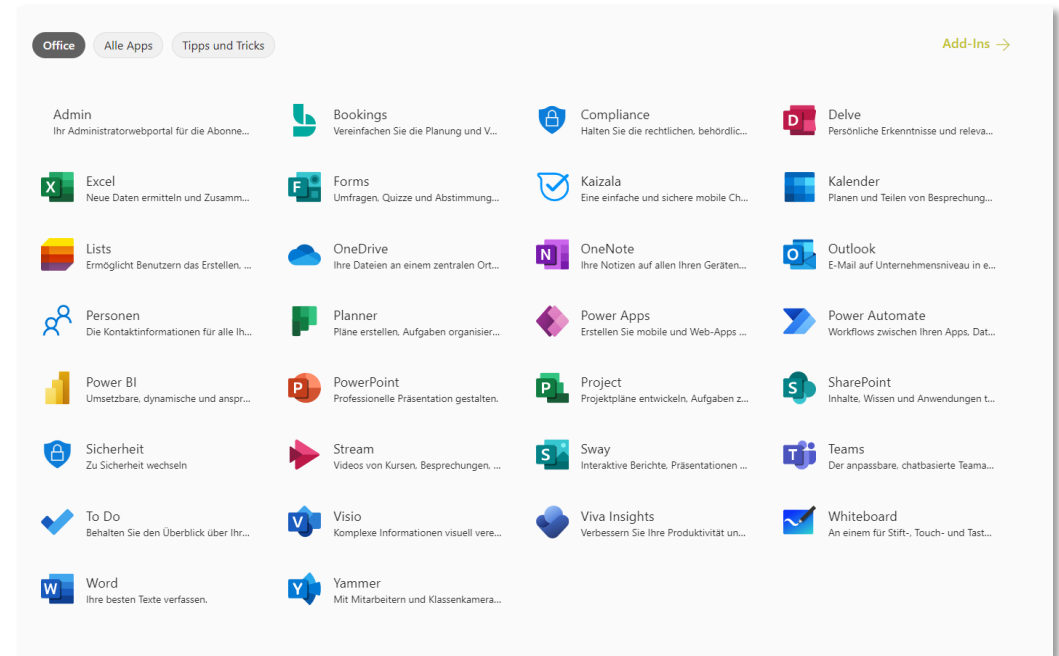
- » blaue Kästchen – Kontrollen müssen vom eigenen Unternehmen implementiert und damit von Internal Audit geprüft werden
- » geteilte Kästchen – Kontrollen müssen vom eigenen Unternehmen implementiert und damit von Internal Audit geprüft werden; zusätzlich bestehen Kontrollen von Microsoft, die innerhalb von Zertifizierungen geprüft werden
- » graue Kästchen – Kontrollen werden von Microsoft implementiert und werden im Rahmen von Zertifizierungen geprüft



# Was ist Microsoft 365? (1/2)

Namensverwirrungen und Unklarheiten...

- » „Microsoft 365-Abonnements [umfassen](#) vertraute Office-Anwendungen, intelligente Clouddienste und erstklassige Sicherheitsmerkmale – alles an einem Ort.“
- » Sammlung von Software-as-a-Service-Diensten (SaaS), die stetig erweitert wird – Überblick über den (Enterprise-)-Lizenzumfang [hier](#)
- » Früher ([Lizenzen weiterhin erwerbbar](#)) stärker unter dem Namen Office 365 vermarktet



# Was ist Microsoft 365? (2/2)

## Umfangreiche Schnittstellen zwischen den Backends

- » Diverse übergreifende Dienste, die nicht direkt für den Endbenutzer sichtbar sind
- » Beispiele:
  - › Aufbewahrungsrichtlinien, die auf Dateien in SharePoint, Anhänge in Outlook, Nachrichten in Teams etc. wirken können
  - › Geräteverwaltung, um Clients sicher für die Verbindung zu Microsoft 365 einschränken
  - › ...
- » Empfehlung: Der Scope der Microsoft-365-Prüfung sollte eher „kleiner“ gewählt werden

### – Complianceverwaltung

Compliance-Risiken bewerten, vertrauliche Daten kontrollieren und schützen sowie gesetzliche Anforderungen umsetzen

Manuelle Aufbewahrungsbezeichnungen, Inhaltssuche, Standardüberwachung

Standardrichtlinien zur unternehmens- und standortweiten Aufbewahrung, Aufbewahrungsrichtlinien in Teams, zentrale eDiscovery, Aufbewahrung für juristische Zwecke

Regelbasierte Richtlinien für die automatische Aufbewahrung, Machine Learning-basierte Aufbewahrung, Datensatzverwaltung

Advanced eDiscovery, Erweiterte Überwachung

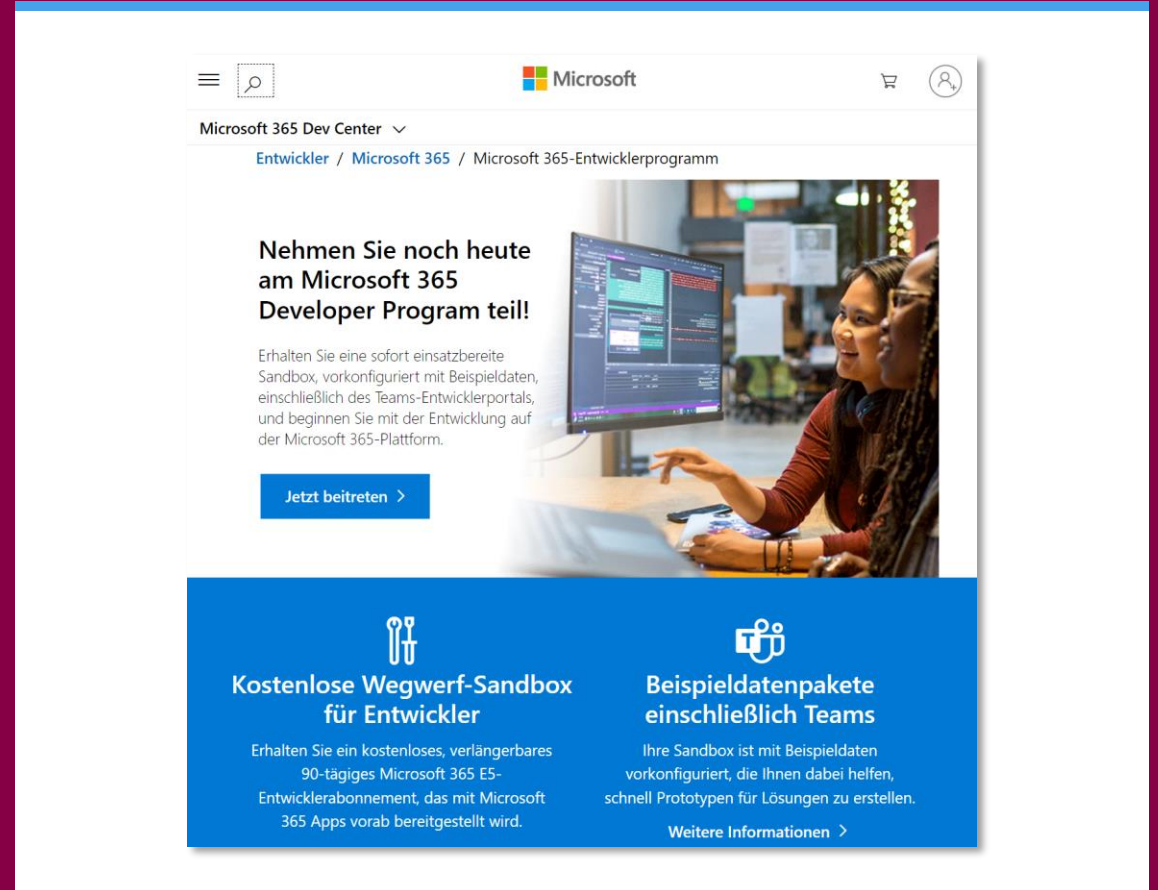
Insider-Risikomanagement, Regeln für gute Kommunikation, Informationsbarrieren, Kunden-Lockbox, Privileged Access Management

Integrierte Drittanbieter-Verbindungen

# Was findet sich in Prüfungen?

Einige Live Demos zu bad practices...

- » [Microsoft 365 Developer Program](#) – eigener Tenant, mit nahezu allen Lizenzen, Funktionalitäten und Testbenutzern
- » Halb-fiktive Ausgangslage: „Wir haben für unsere rund 15.000 Mitarbeiter eine dezentrale Benutzerverwaltung und Verantwortung bei den Teameigentümern, damit diese im Sinne ihres Bedarfs arbeiten können.“

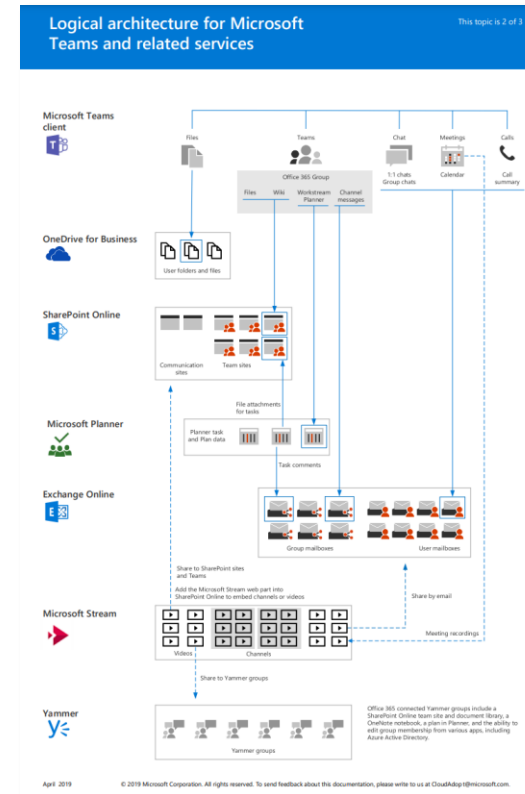


The screenshot shows the Microsoft 365 Developer Program landing page. At the top, there is a navigation bar with the Microsoft logo and a user profile icon. Below the navigation bar, the page title reads "Microsoft 365 Dev Center" and "Entwickler / Microsoft 365 / Microsoft 365-Entwicklerprogramm". The main content area features a large image of two people working at a computer. The text on the page reads: "Nehmen Sie noch heute am Microsoft 365 Developer Program teil!" followed by a description: "Erhalten Sie eine sofort einsatzbereite Sandbox, vorkonfiguriert mit Beispieldaten, einschließlich des Teams-Entwicklerportals, und beginnen Sie mit der Entwicklung auf der Microsoft 365-Plattform." Below this text is a blue button labeled "Jetzt beitreten >". At the bottom of the page, there are two blue boxes with white text. The first box is titled "Kostenlose Wegwerf-Sandbox für Entwickler" and describes a 90-day free Microsoft 365 E5 developer subscription. The second box is titled "Beispieldatenpakete einschließlich Teams" and describes pre-configured example data for Teams. Both boxes have a "Weitere Informationen >" link.

# Microsoft Teams

## Frontend für viele Backends

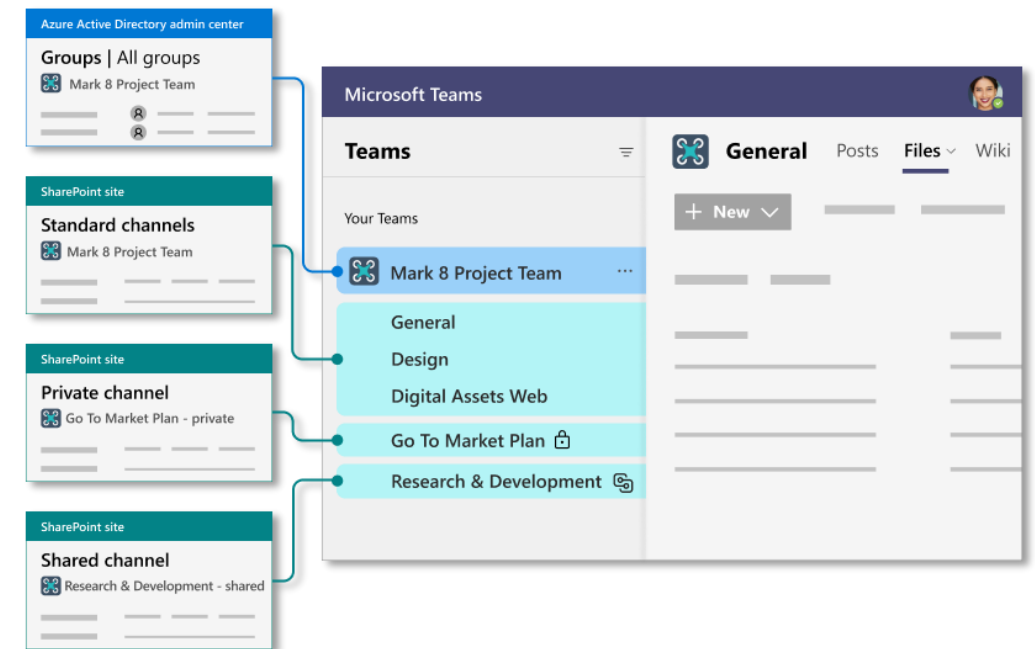
- » Bei Anlage eines Teams wird u.a. folgendes angelegt:
  - › „eine neue Microsoft 365-Gruppe
  - › eine SharePoint Online-Website und eine SharePoint Online-Dokumentbibliothek zum Speichern von Teamdateien
  - › ein freigegebenes Exchange Online-Postfach und ein Exchange Online-Kalender
  - › ein OneNote-Notizbuch
  - › Verbindungen mit anderen Microsoft 365- und Office 365-Apps wie beispielsweise Planner und Power BI“



# Microsoft Teams & SharePoint Online

## Zusammenspiel der beiden Dienste

- » SharePoint Online ist integriert in Teams und eine neue Seite wird automatisch bei Anlage eines Teams erstellt
- » Die Kanalarten führen zu unterschiedlichen Anlagen von SharePoint Sites
- » Das Teilen von Dateien ist mittels SharePoint Online möglich – übrigens OneDrive ist auch nur eine SharePoint Seite

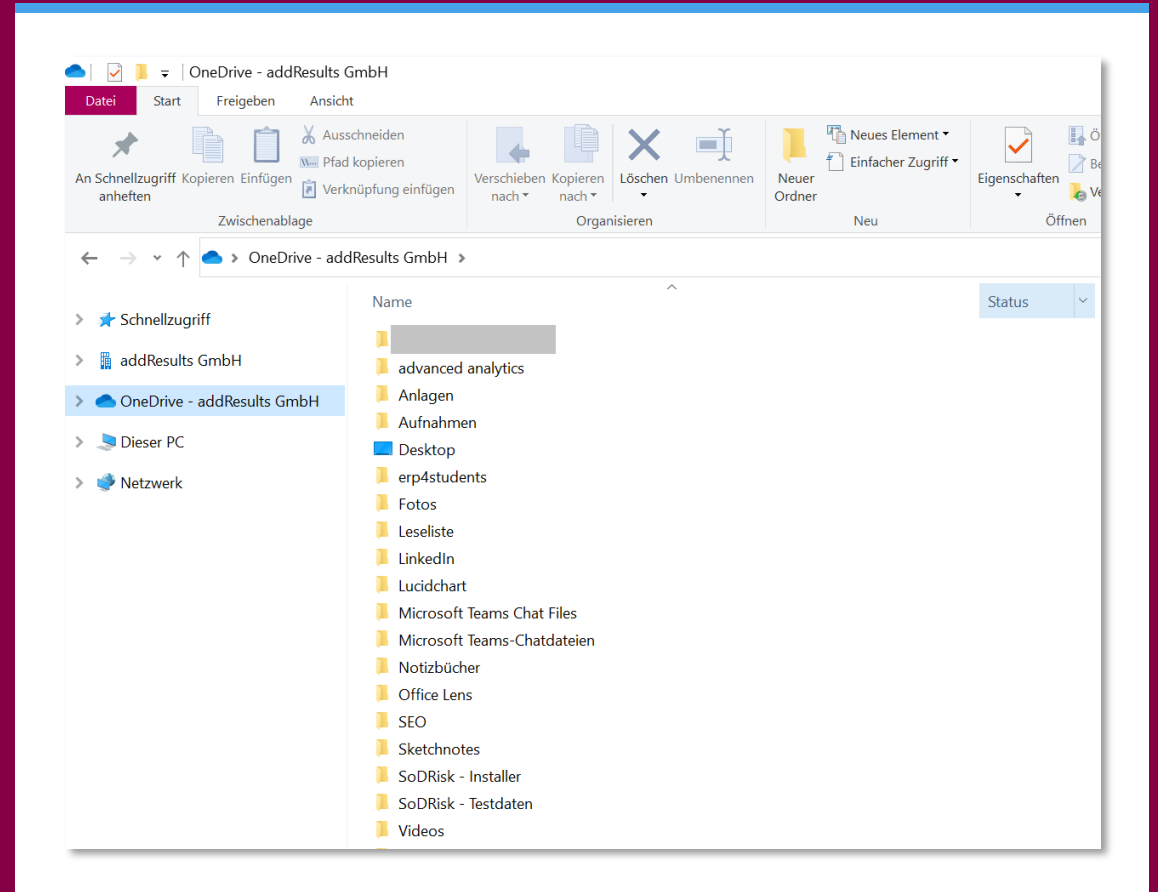




# SharePoint Online & OneDrive

## Offline-Verfügbarkeit der Daten

- » Die Benutzer können ebenfalls SharePoint-Websites offline verfügbar machen
- » Standardordner, wie ein Desktop oder Profilordner können ebenfalls automatisch synchronisiert und damit versioniert werden
- » Synchronisierung kann auf AD-Domänen eingeschränkt werden



# Microsoft Teams & die Erweiterungen

## Integration (unbekannter) Drittdienste

- » Mit Apps kann Drittanbietersoftware in Microsoft Teams integriert werden – dadurch können die Benutzer mit weniger Medienbrüchen ihrer Arbeit nachgehen
- » In der Grundeinstellung sind „alle“ Apps zugänglich und von Benutzern hinzufügb

**Microsoft Teams Admin Center** Suchen - Vorschau

### Apps verwalten

Steuern Sie, welche Apps für Benutzer in Ihrer Organisation verfügbar sind, indem Sie Apps zulassen und können auch benutzerdefinierte Apps hochladen und genehmigen. Nachdem Sie Apps auf dieser Seite v können Sie App-Berechtigungen und App-Setuprichtlinien verwenden, um zu konfigurieren, welche App Benutzer im App-Store Ihrer Organisation verfügbar sind. Weitere Informationen

**Genehmigung steht aus**

0 Benutzerdefinierte Apps übermittleit    0 Aktualisierte benutzerdefinierte Apps

**Beworbene App**

**Adobe Acrobat Sign**  
Get more done by sending documents all from within

Durchsuchen nach: Alles

+ Neue App hochladen    ✓ Zulassen    ⛔ Blockieren    ✎ Anpassen    👤 Zu Team hinzufü

✓	Name ↑	Zertifizierung ⓘ	Herausgeber
✓	1-on-1 Hub	--	Appfluence Inc
✓	1-to-1 Worldvds Comm	--	Amplitudenet LDA
✓	10xGoals	Herausgebernachweis	xto10x Technologies
✓	15Five	--	15Five, Inc.

# Microsoft Entra ID (1/2)

## Grundsätzliches zu Benutzern

- » (interaktive) Benutzertypen
  - › Mitgliedsbenutzer
  - › Gastbenutzer
- » Unterschiedliche Standardberechtigungen für Gäste und Mitglieder
- » Die Standardberechtigungen für Mitglieder sind weitreichend, z. B.
  - › Einladung von Gästen
  - › Erstellung von Sicherheits- und Microsoft 365-Gruppen
  - › Registrierung von Applikationen
  - › ...

The screenshot shows the Microsoft Azure portal interface for managing users. The top navigation bar includes the Microsoft Azure logo and a search bar. The main content area is titled 'Benutzer' and displays a list of 20 users. The list has two columns: 'Anzeigename' and 'Benutzerprinzipalname'. The users listed are:

Anzeigename	Benutzerprinzipalname
Diego Siciliani	DiegoS@devaddresults.onmicrosoft.com
Evi's Eishütte	EvisEishtte@dev.addresults.de
Grady Archie	GradyA@devaddresults.onmicrosoft.com
Henrietta Mueller	HenriettaM@devaddresults.onmicrosoft.com
Isaiah Langer	IsaiahL@devaddresults.onmicrosoft.com
Jackmuth, Stefa...	stefan.jackmuth_addrresults.de#EXT#@devaddresults.onmicrosoft.com
Johanna Lorenz	JohannaL@devaddresults.onmicrosoft.com
Joni Sherman	JoniS@devaddresults.onmicrosoft.com
Lee Gu	LeeG@devaddresults.onmicrosoft.com
Lidia Holloway	LidiaH@devaddresults.onmicrosoft.com
Lynne Robbins	LynneR@devaddresults.onmicrosoft.com

# Microsoft Entra ID (2/2)

## Grundsätzliches zu Gruppen

- » Sicherheitsgruppen
  - › „nur“ eine Bündelung von Benutzern, Geräten, Gruppen und Service Principals
  - › Gruppen des on-Premise AD DS
- » Microsoft 365-Gruppen
  - › Gruppe zur Zusammenarbeit, gleichzeitig wird ein Postfach, SharePoint-Seite, Kalender etc. erstellt
  - › kann nur Benutzer aufweisen
- » Zwei Arten von „Berechtigungen“:
  - › Besitzer
  - › Mitglieder

### Types of groups and where they are created

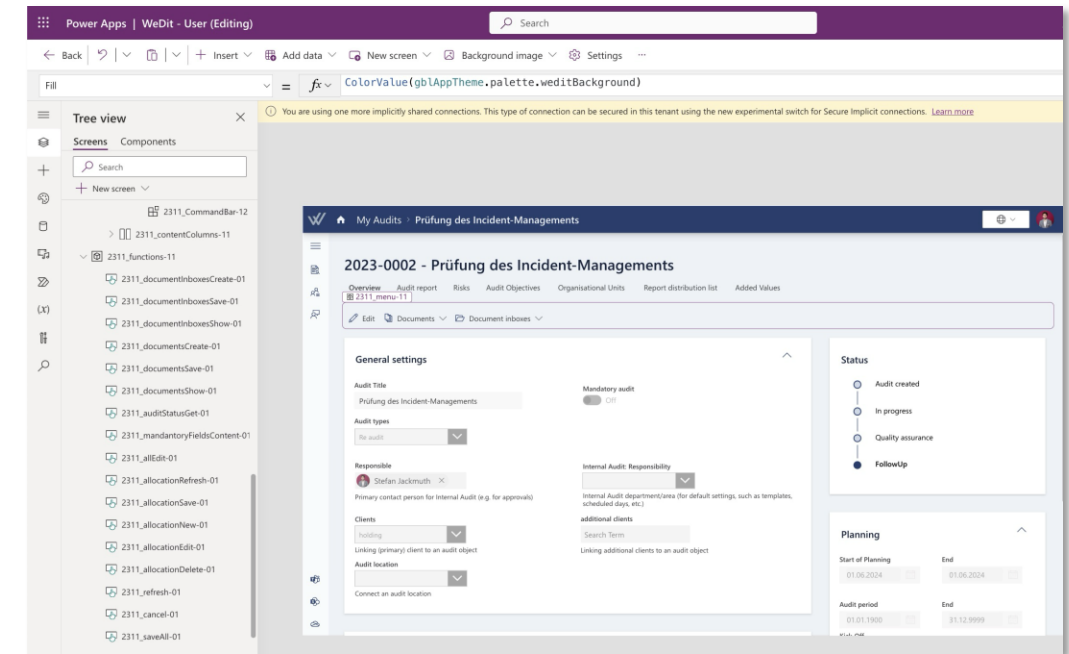
Groups can be created in several of the admin centers and by users from within apps.

Type of group	Security group	Microsoft 365 group	Mail-enabled security group	Distribution group	Shared mailbox
	Used for granting access to resources and for managing devices.	Used for collaboration. Includes a group email and shared workspaces.	Includes the ability to send mail to a group. Cannot be dynamically managed. Cannot contain devices.	Used for sending notifications to a group of people.	Used when multiple people need to access the same mailbox, such as a support email address.
Where groups can be created	Azure AD	Microsoft 365 admin center	Exchange admin center		
			Outlook		
			Teams		
			SharePoint		
			Planner		
			Yammer		
			Stream		
			Power BI (classic)		
			Roadmap		
			Project for the web		

# Microsoft Power Platform

Low-/No-Code für die Business User

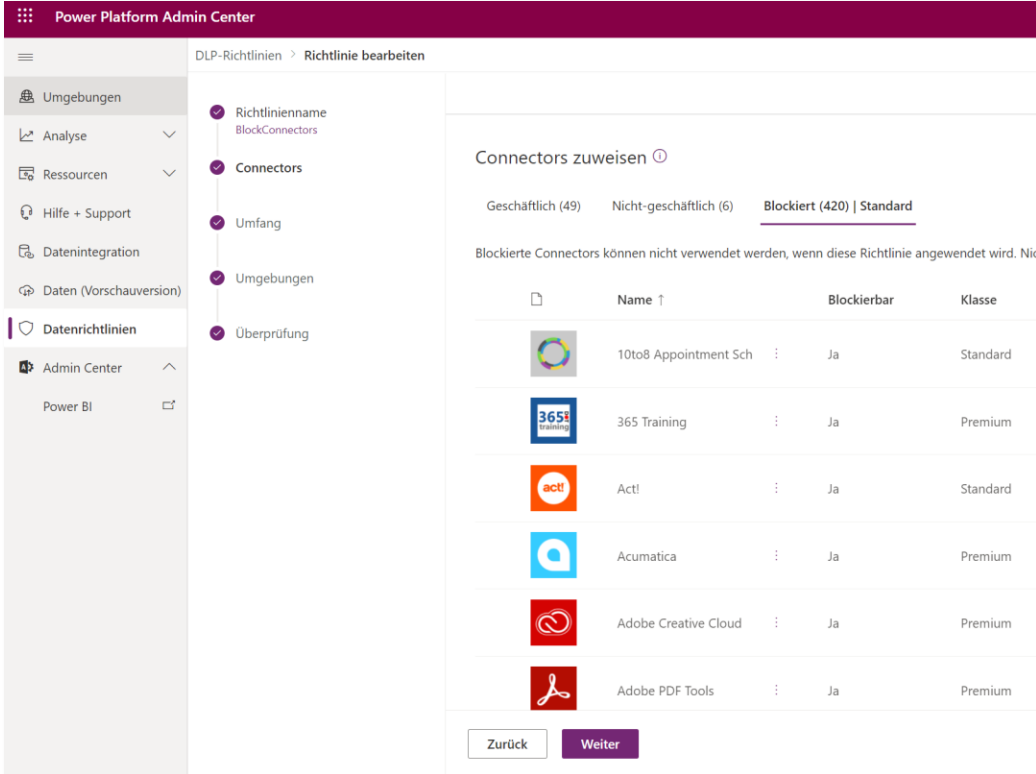
- » Citizen Development via Low-Code – Fachbereiche sollen in die Lage versetzt werden, einfach Applikationen und Automatisierungen zu entwickeln
- » Die IT ist potenziell an dieser dezentralen Entwicklung nur im Betrieb beteiligt
- » Klarer Entwicklungsprozess möglich – IDV kann leichter prozessual begrenzt werden, aber nicht per „eingebautem“ Application Lifecycle Management



# Microsoft Power Automate

## Automatisieren mit Vor- und Nachteilen

- » Erstellung von Workflows, die APIs aufrufen und JSONs übergeben
- » Die Automatisierungen können von einfachen Unterstützungen a la „lege mir Dateien ab, wenn eine Mail ankommt“ zu komplexen Programmierungen gehen
- » „Lege mir jede Datei, die per Mail kommt, in meiner privaten Dropbox ab.“



The screenshot shows the Power Platform Admin Center interface for editing a DLP policy. The left sidebar contains navigation options like Umgebungen, Analyse, Ressourcen, Hilfe + Support, Datenintegration, Daten (Vorschauversion), Datenrichtlinien, Admin Center, and Power BI. The main area is titled 'DLP-Richtlinien > Richtlinie bearbeiten' and shows a configuration tree with 'Connectors' selected. The 'Connectors zuweisen' section displays a table of connectors with their status and classification.

Name ↑	Blockierbar	Klasse
10to8 Appointment Sch	Ja	Standard
365 Training	Ja	Premium
Act!	Ja	Standard
Acumatica	Ja	Premium
Adobe Creative Cloud	Ja	Premium
Adobe PDF Tools	Ja	Premium

# Change Management (1/2)

## Roadmap für die großen Schritte

- » Laufend Entwicklung und Veröffentlichung von neuen Funktionalitäten
- » Schrittweises Ausrollen der Funktionen – manchmal nicht genau erkennbar, wann das eigene Unternehmen davon profitiert
- » Phasen:
  - › Private Preview
  - › Public Preview
  - › General Availability

The screenshot shows the Microsoft 365 Roadmap website. The header includes the Microsoft logo and navigation links for 'Microsoft 365', 'Produkte', 'Ressourcen', 'Vorlagen', 'Support', and 'Jetzt kaufen'. The main heading is 'Microsoft 365-Roadmap' with a sub-heading: 'Finden Sie die neuesten Updates zu unseren erstklassigen Produktivitätsanwendungen und intelligenten Clouddiensten. Erleben Sie Produktivität in einer neuen Dimension, vereinfachen Sie Geschäftsprozesse, und schützen Sie Ihr Unternehmen mit Microsoft 365.' Below this are two buttons: 'Roadmap verwenden' and 'Roadmapverbesserungen'.

The main content area features a search section with the text 'Nach einem bestimmten Element suchen:' and a search input field. To the right, there are filters for 'Produkt', 'Freigabezeitraum', 'Plattform', and 'Cloudinstanz'. Below these are buttons for 'Neu oder aktualisiert' and 'Alle löschen'.

The section 'Wird angezeigt 1709 Updates¹:' includes three summary cards: '486 Entwicklung' (Updates in development), '133 Rollout' (Updates in rollout), and '1080 Freigegeben' (Fully released updates). At the bottom, there is a list of updates with columns for product name and general availability date (GA).

Product Name	GA Date
Microsoft 365 admin center: Groups - Group Driven Membership Management	GA: December 2022
Microsoft Teams: Adobe Sign Integration in Approvals for GCC-High and DoD	GA: December 2022
Microsoft Teams Rooms Managed Services: Device Portfolio - Teams Rooms (Android)	GA: December 2022
Outlook for Windows: Signature cloud settings	Preview: Sep

# Change Management (2/2)

## Message Center für die detaillierten Änderungen

- » „Um bevorstehende Änderungen, einschließlich neuer und geänderter Features, geplanter Wartung oder anderer wichtiger Ankündigungen, nachzuverfolgen, wechseln Sie zum Nachrichtencenter.“
- » „das Nachrichtencenter ist die primäre Art und Weise, wie wir den Zeitpunkt einzelner Änderungen in Microsoft 365 kommunizieren“
- » „Wichtige Updates werden mindestens 30 Tage im Voraus mitgeteilt, wenn eine Aktion erforderlich ist [...]“

The screenshot shows an email notification from the Microsoft 365 Message Center. The subject is "Major update from Message center". The sender is "Microsoft 365 Message center <o365mc@microsoft.com>" and the recipient is "An: Stefan Jackmuth". The email content is in German and discusses the deprecation of Basic Authentication in Exchange Online. The main heading is "Basic Authentication Deprecation in Exchange Online – May 2022 Update". The email ID is "MC375736 - DEVADDRESSRESULTS". The body text states: "In about 150 days from today, we're going to start to turn off Basic Auth for specific protocols in Exchange Online for those customers still using it." It also includes a "Timeline and Scope" section: "As we communicated last year in [blog posts](#) and MC286990, we will start to turn off Basic Authentication in our worldwide multi-tenant service on October 1, 2022. To clarify, we will start on October 1; this is not the date we turn it off for everyone. We will randomly select tenants, send 7-day warning Message Center posts (and post Service Health Dashboard notices), then we will turn off Basic Auth in the tenant. We expect to complete this by the end of this year. You should therefore be ready by October 1." It lists the protocols affected: "We're turning off Basic Auth for the following protocols: MAPI, RPC, Offline Address Book (OAB), Exchange Web Services (EWS), POP, IMAP, Exchange ActiveSync (EAS) and Remote PowerShell." Finally, it notes: "We are not turning off SMTP AUTH. We have turned off SMTP AUTH for millions of tenants not using it, but if SMTP AUTH is enabled in your tenant, it's because we see usage and so we won't touch it. We do recommend you disable it at the tenant level and re-enable it only for those user accounts that still need it."



# Welche Berechtigungen für ein Audit?

Problem: Großer, multinationaler Tenant

- » Einfachste Lösung – Zuweisung der Rolle „globaler Leser“
  - › Zugang zu allen Admin Centern in Microsoft 365
  - › Zugang zu allen Daten in den Admin Centern
- » Mögliches Problem: Eingeschränkter Prüfungsumfang bzgl. der Gesellschaft/juristischen Person
  - › Ggf. nicht möglich, da Datenbestand nicht „klar“ getrennt – ggf. über „Administrative Units“ realisiert, dann zu teilen umsetzbar

ADD  
RESULTS

Blog



20. August 2021

## Microsoft Azure - Welche Rollen brauche ich zum Prüfen?



Stefan Jackmuth

Heute ein kurzer Blogbeitrag zu Berechtigungen. Nicht nur, weil diese gut und einfach zu prüfen sind, sondern weil wir ohne die richtigen Berechtigungen selbst nicht zum Prüfen kommen. Welche Berechtigungen brauche ich also für ein Audit von Microsoft Azure?

Die Antwort ist auf den ersten Blick simpel und dann leider doch komplexer. Was in SAP das Profil SAP\_ALL ist, entspricht im Microsoft Azure AD der Rolle „Globaler Administrator“. Diese würde für die Nutzung innerhalb einer Prüfung ausscheiden, da in dieser auch Änderungsberechtigungen enthalten sind. Es gibt aber die lesende Entsprechung „Globaler Leser“.

Diese Rolle ist perfekt für ein Audit von Microsoft 365 geeignet, jedoch nicht von Microsoft Azure. Ich habe ein kleines GIF erstellt, um den Effekt zu demonstrieren. Zuerst ist der Benutzer, inkl. der zugewiesenen Rolle zu sehen, den ich zur Demonstration nutze. In Microsoft 365 erhalte ich Zugriff auf alle Admin-Center. Im Beispiel wähle ich das Teams-Admin-Center aus, um eine Richtlinie anzusehen.

# Fazit

- » Dienste hängen zusammen – Scope klein halten, er vergrößert sich automatisch
- » Stetige Änderungen – nur weil die Administration vor zwei Jahren gute Kontrollen erstellt hat, sind diese nicht noch immer gut
- » Neugierig bleiben – irgendwelche neue Risiken ergeben sich immer – Was ist eigentlich der Microsoft Copilot?



# WeDit

Audit... aber digital!  
mit Microsoft 365

The screenshot shows a Microsoft Teams chat window. On the left is the Teams navigation pane with icons for Activity, Chat, Teams, Calendar, Calls, OneDrive, Approvals, and Power Apps. The main chat area shows a conversation with a team named 'WeDit-Dev-00'. The selected chat is titled 'General' and contains a list of audit reports: '2024-0005\_Geman...', '2024-0006\_Geman...', '2024-0009\_Geman...', and '2024-0007\_Implem...'. The '2024-0007\_Implem...' chat is selected, displaying a detailed audit report for 'Implementierte Unternehmensarchitektur'.

The audit report interface includes a search bar at the top, a navigation bar with 'General', 'Posts', 'Files', 'Notes', and 'WeDit - User'. The report title is '2024-0007 - Implementierte Unternehmensarchitektur'. Below the title are tabs for 'Overview', 'Audit report', 'Times', 'Costs', 'Risks', 'Audit Objectives', 'Organisational Units', 'Report distribution list', and 'Added Values'. The 'Audit report' tab is active, showing a 'Result' section with the following data:

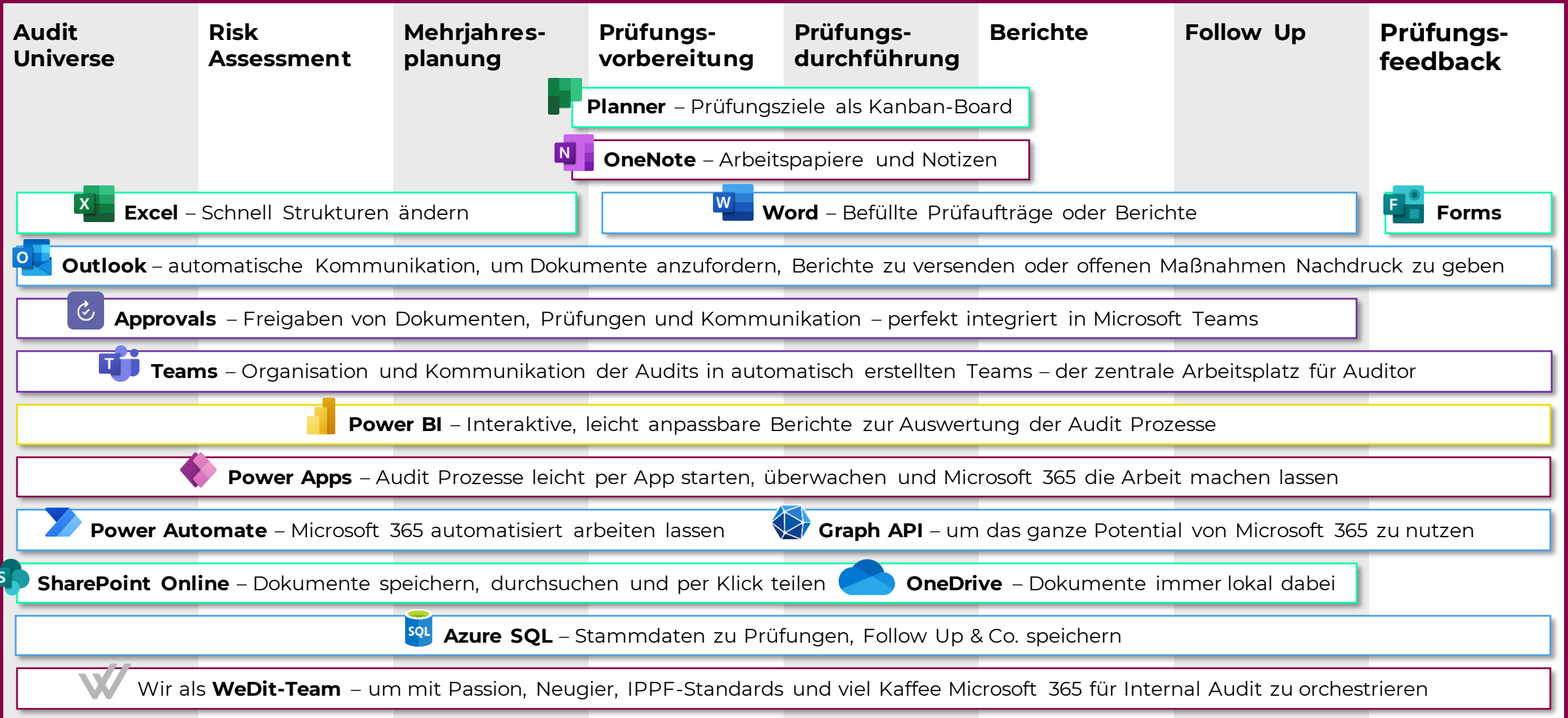
Field	Value
Result	sufficient
Report Date	15.03.2024
Overall judgement: Risk	medium
Overall judgement: Control	unsuitable
Overall judgement: Actions	necessary

Below the result section is a 'Findings' section with a table of audit findings:

↑	Finding Title	Condition	Assessment
1	Fehlende Nutzung von Standard...	Aktuell werden keine konsistenten Standards g...	B
2	Unklare Verantwortung	Die für den Prozess Verantwortliche Person hat ...	A

On the right side of the report, there is a 'Status' section with a vertical progress indicator and labels: 'Create report', 'Report created', 'Quality assurance', 'Department', and 'Final version'.

# Warum WeDit?



# LASSEN SIE UNS REDEN

WEIL JEDER INDIVIDUELLE IDEEN BESITZT

+49 162 70 70 466  
[stefan.jackmuth@addResults.de](mailto:stefan.jackmuth@addResults.de)

addResults GmbH  
Schulweg 17a  
51503 Rösrath

**TERMIN  
BUCHEN**



**Stefan  
Jackmuth**



geht den Dingen auf den Grund. Wenn es sinnvoll ist, zeigt er neuartige, kreative Lösungen auf. Aber, was im Leben gilt, gilt auch für Unternehmen: Free Jazz ist nicht für jeden Ort gedacht.