

Microsoft 365 IT-Sicherheitskonzept

Kai Wittenburg

Geschäftsführer, neam IT-Services GmbH

neam IT-Services GmbH

Facts

- ✓ Gegründet 1996
- ✓ Über 90 Mitarbeiter
- ✓ Paderborn, Wiesbaden & Berlin



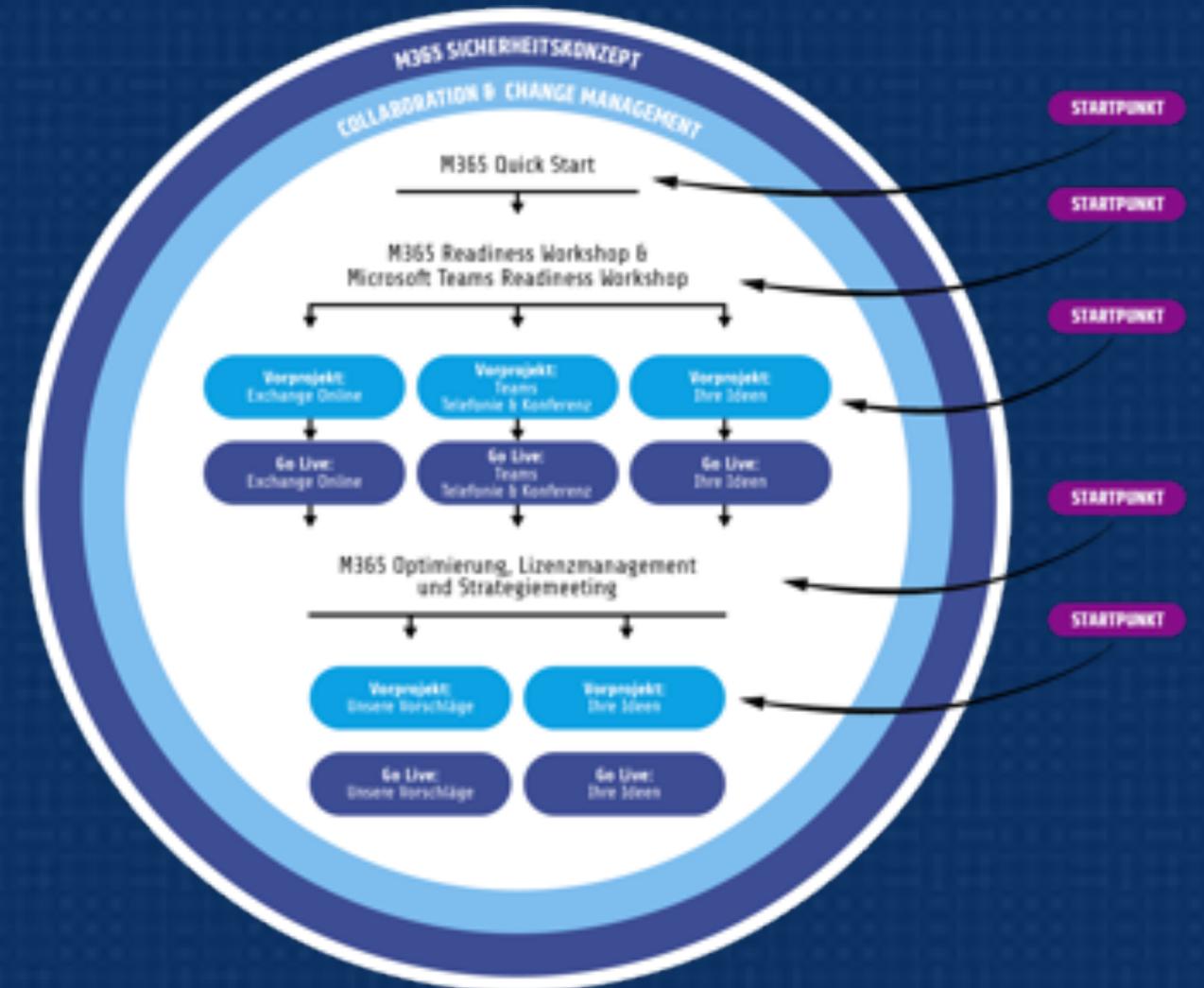
Informationssicherheit

Beratung & Schulungen

- ✓ BSI IT-Grundschutz
- ✓ ISMS nach ISO 27001
- ✓ Business Continuity Management
- ✓ Audits & Zertifizierungen
- ✓ Penetrationstest
- ✓ Social Engineering
- ✓ Incident Response

Cloud

Microsoft 365 und Azure



Microsoft Secure Score

Microsoft Secure Score

Overview Improvement actions History Metrics & trends

Microsoft Secure Score is a representation of your organization's security posture, and your opportunity to improve it.

Applied filters: Filter

Your secure score Include

Secure Score: 46%
179/320 points achieved

100%
0%
[Line chart showing score over time]

Breakdown points by: Category

- Identity: 87%
- Data: No data to show
- Device: 45%
- Apps: 100%
- Infrastructure: No data to show

■ Points achieved ■ Opportunity

Actions to review

Regressed: 0 | To address: 63 | Planned: 3 | Risk accepted: 3 | Recently added: 0 | Recently updated: 0

Top improvement actions

Improvement action	Score impact	Status	Category
Turn on Microsoft Defender Application Guard managed mode	+1.0%	<input checked="" type="radio"/> Risk accepted	Device
Block credential stealing from the Windows local security authorit...	+1.0%	<input type="radio"/> To address	Device
Use advanced protection against ransomware	+1.0%	<input type="radio"/> To address	Device
Block execution of potentially obfuscated scripts	+1.0%	<input type="radio"/> To address	Device
Block Office applications from injecting code into other processes	+1.0%	<input type="radio"/> To address	Device
Block executable content from email client and webmail	+1.0%	<input type="radio"/> To address	Device
Encrypt all BitLocker-supported drives	+1.0%	<input type="radio"/> To address	Device
Turn on PUA protection	+1.0%	<input checked="" type="radio"/> Risk accepted	Device
Block [redacted] from creating child processes	+1.0%	<input type="radio"/> To address	Device

[View all](#)

Comparison

Ihre Punktzahl 45.65%

Organisationen wie Ihre 54.75%

Benutzerdefinierter Vergleich 34.8%

Microsoft-Sicherheitsbewertung

Übersicht Verbesserungsaktionen Verlauf Metriken und Trends

Microsoft-Sicherheitsbewertung ist eine Darstellung des Sicherheitsstatus Ihrer Organisation und ihrer Möglichkeiten, ihn zu verbessern.

Angewendete Filter:

Ihre Sicherheitsbewertung

Ein schließen

Sicherheitsbewertung:
41.29%

31.38/76 erzielte Punkte



Punkte aufgliedern nach: Kategorie

Identität	Keine anzeigenden Daten
Daten	Keine anzeigenden Daten
Gerät	Keine anzeigenden Daten
Apps	6.67%
Infrastruktur	Keine anzeigenden Daten

Erzielte Punkte Möglichkeit

Zu prüfende Aktionen



Wichtigste Verbesserungsaktionen

Verbesserungsaktion	Bewertung...	Status	Kategorie
Richtlinie zum Blockieren von Legacyauthentifizierung aktivieren	+10.53 %	<input type="radio"/> Zu behandeln	Identität
Benutzerrisiko-Richtlinie aktivieren	+9.21 %	<input type="radio"/> Zu behandeln	Identität
Anmelderisikorichtlinie aktivieren	+9.21 %	<input type="radio"/> Zu behandeln	Identität
MFA für Administratorrollen anfordern	+13.16 %	<input type="radio"/> Zu behandeln	Identität
Automatische Benachrichtigungen für neue OAuth-Anwendungen ei...	+5.26 %	<input type="radio"/> Zu behandeln	Apps
Automatische Benachrichtigungen für neue und Trend setzende Clo...	+3.95 %	<input type="radio"/> Zu behandeln	Apps
Cloud App Security zum Erkennen anomalen Verhaltens verwenden	+3.95 %	<input type="radio"/> Zu behandeln	Apps
Eine benutzerdefinierte Richtlinie zur Ermittlung verdächtiger Verwe...	+2.63 %	<input type="radio"/> Zu behandeln	Apps

[Alle anzeigen](#)

Auf einen Blick

Kategorie: Identität

Schützt vor: [Kennwortentschlüsselung](#), [Kontosicherheitsverletzung](#)

Produkt: Azure Active Directory

Benutzerauswirkungen

Wenn einige Ihrer Benutzer veraltete Client-Apps verwenden, die keine modernen Authentifizierungsmethoden unterstützen, können sie nach Aktivierung dieser Richtlinie nicht mehr auf ihre Apps zugreifen.

Betroffene Benutzer

Alle Ihre Microsoft 365-Benutzer

Implementierung

Voraussetzungen

✓ Sie haben Azure Active Directory Premium P2.

Nächste Schritte

Standardmäßige Implementierung: Wenn es in Ihrer Organisation keine komplexen Sicherheitsanforderungen gibt, können Sie die Standardsicherheitseinstellungen aktivieren, um die veraltete Authentifizierung zu blockieren und für alle Benutzer die Registrierung und die Aktivierung der mehrstufigen Authentifizierung vorgeben. [Erfahren Sie mehr darüber, wie Sie die Standardsicherheitseinstellungen aktivieren können.](#)

Benutzerdefinierte Implementierung: Wählen Sie im [Azure AD-Portal für bedingten Zugriff](#)

1. **+ Neue Richtlinie auswählen.**
2. Benennen Sie die Richtlinie. Microsoft empfiehlt Organisationen, für Richtliniennamen einen sinnvollen Standard zu etablieren.
3. Wählen Sie unter Zuweisungen die Option **Benutzer und Gruppen** aus. Wählen Sie unter Einschließen den Eintrag **Alle Benutzer** aus. Wählen Sie unter Ausschließen den Eintrag **Benutzer und Gruppen** aus und wählen Sie alle Konten aus, für die es erforderlich ist, dass die ältere Authentifizierungsform weiterhin verwendet werden kann.
4. Wählen Sie unter Bedingungen > Client-Apps aus und setzen Sie Konfigurieren auf **Ja**. Aktivieren Sie nur die Felder **Exchange ActiveSync-Clients** und **Andere Clients**. Wählen Sie nun **Fertig**.
5. Wählen Sie unter Zugriffssteuerung > Gewähren die Option **Zugriff blockieren**.
6. Bestätigen Sie Ihre Einstellungen und setzen Sie Richtlinie aktivieren auf **Ein**.
7. Wählen Sie **Erstellen** aus, um die Richtlinie zu erstellen und zu aktivieren.

Hinweis: Herkömmliche Richtlinien für bedingten Zugriff werden nicht bewertet. Verwenden Sie für eine Bewertung die empfohlenen Schritte.

Microsoft Compliance Score

Microsoft 365 compliance

Compliance Manager

Overview Improvement actions Solutions Assessments Assessment templates

Compliance Manager measures your progress in completing actions that help reduce risks around data protection and regulatory standards. Find guidance and discover

Overall compliance score

Your compliance score: 75%

14276/18301 points achieved

Your points achieved 📉
252 min

Microsoft managed points achieved 📉
14276 min

Compliance score measures your progress towards completing recommended actions that help reduce risks around data protection and regulatory standards.

Key Improvement actions

Not completed	Completed	Out of scope
335	12	2

Improvement action	Weight
Protect Authentication Content	+17 points
Limit Conditional Logins Failure	+17 points
Implement Account Lockout	+17 points
Protect Authentication Credentials with OAuth	+17 points
Protect Wireless Access	+17 points
Protect Elements with Encryption	+17 points
Manage Authentication Lifetime and State	+17 points
Restrict Access to Private Sites	+17 points
Enforce Rules of Behavior and Acceptance Agreements	+17 points

Compliance-Manager

Ihr Kompatibilitäts Faktor: 75%

Compliance-Manager hilft Ihrer Organisation, die Compliance zu vereinfachen und Risiken im Zusammenhang mit Datenschutz und behördlichen Standards zu verringern. Ihre Punktzahl spiegelt Ihre aktuelle Compliance-Haltung wider und hilft Ihnen dabei, die Aufmerksamkeit zu erhalten.

Informationen zu Compliance-Manager

Schützen von Informationen	27 / 553
Informationen steuern	0 / 118
Steuern des Zugriffs	0 / 487
Verwalten von Geräten	0 / 756
Schutz vor Bedrohungen	0 / 274
Entdecken und Reagieren	0 / 175
Verwalten interner Risiken	0 / 56

■ Aktuelle Bewertung
 ■ Verbleibende Punktzahl

[Compliance-Manager besuchen](#)

Verbesserungsaktion

Verwalten der Authentifikator-Lebensdauer und Wiederverwendung

Implementieren von Spamfilter

Implementieren von Anti-Phishing-Richtlinien

Implementieren von DMARC für eingehende e-Mails

Anonymisieren von USA ge-Aktivitätsberichten

Ensure sufficient strength for authenticators

Einfache Kennwörter für mobile Geräte nicht zulassen

Create an iOS app protection policy

Aktivieren der Kommunikations Kompatibilität in O365

Einrichten von Sender Policy Framework zur Verhinderung von Spoofing

Create customized DLP policies for personal data

Verwalten der Freigabe von Kalender Details

Anwenden von Sensitivitäts Bezeichnungen zum Schutz vertraulicher oder kritischer Daten

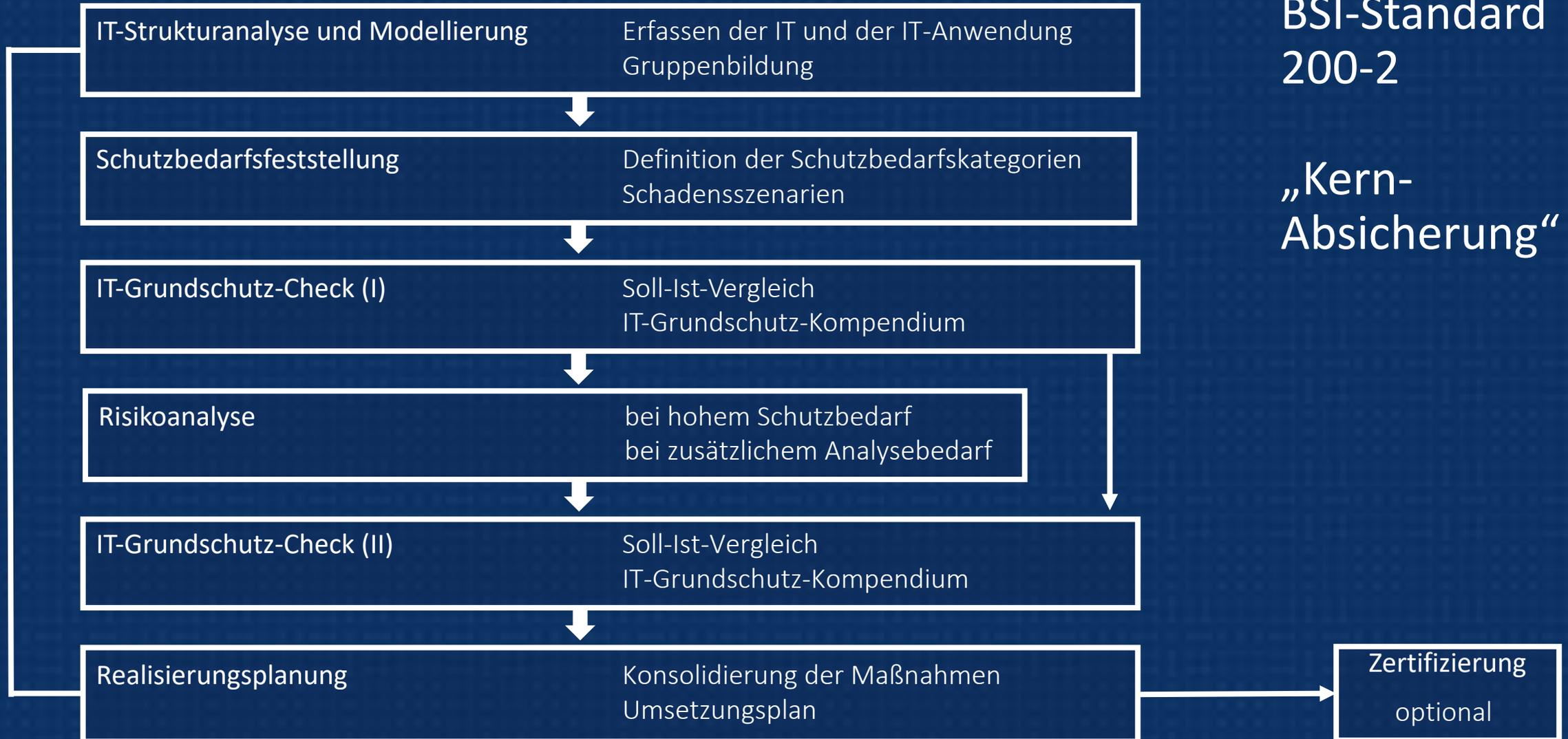
Automatisches Anwenden von Sensitivitäts Bezeichnungen

Verwenden von Grenzschutz Geräten für nicht klassifizierte nicht nationale Sicherheitssysteme

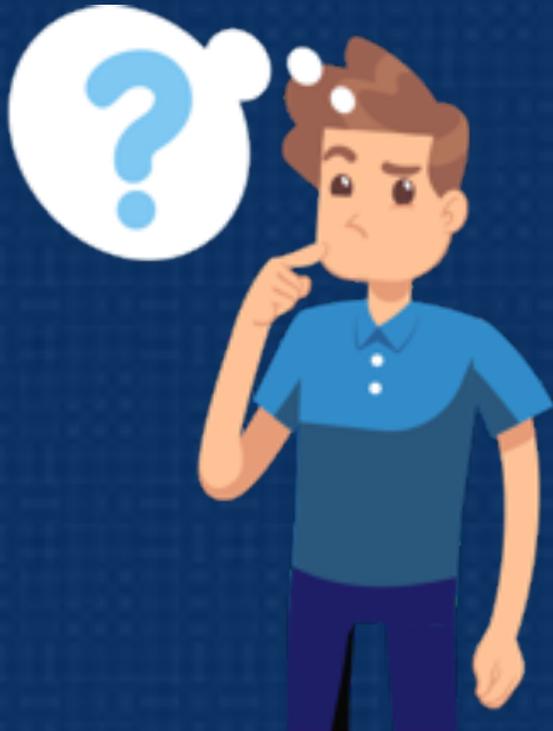
Create a device configuration profile for Andoid devices

Erfordern von mobilen Geräten zum Verwalten der e-Mail Profile

IT-Sicherheitskonzept



Bausteine & Profil?



Bringt neam
mit.



- 🏢 Geschäftsprozesse
 - 🏢 GP-01 Kommunikation
- 📁 Anwendungen
 - 📁 A-01 Microsoft 365
 - ▶ OPS.2.2 Cloud-Nutzung
 - ▶ APP.1.4 Mobile Anwendungen (Apps)
 - ▶ bB-M365 Microsoft365
 - ▶ Datenschutz-Gefährdungen
 - ▶ Elementare Gefährdungen
- 🏢 IT-Systeme
 - 📁 Clients
 - ▶ C-01 Desktop-PCs (Arbeitsplätze)
 - ▶ C-02 Laptops
 - ▶ M-01 Smartphones & Tablets Apple iOS
 - ▶ M-02 Smartphones & Tablets Android
- 🏢 Kommunikationsverbindungen
- 🏢 Räume
 - ▶ R-01 Büroraum (Standort)
 - ▶ R-02 HomeOffice
 - ▶ R-03 Mobiler Arbeitsplatz
- 👤 Personen
 - ▶ OPS.1.2.4 Telearbeit
 - ▶ bCON.2 Datenschutz
 - ▶ Elementare Gefährdungen

benutzerdefinierter
Baustein M365

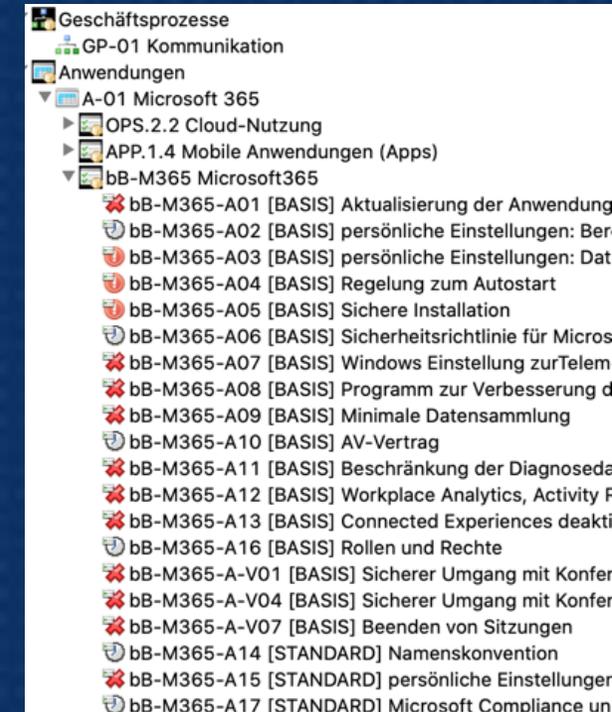
Cloud
Nutzung

Mobile
Anwendungen
(Apps)

Windows/ Linux/
MacOS-Clients

Android/ iOS
Smartphones und
Tablets

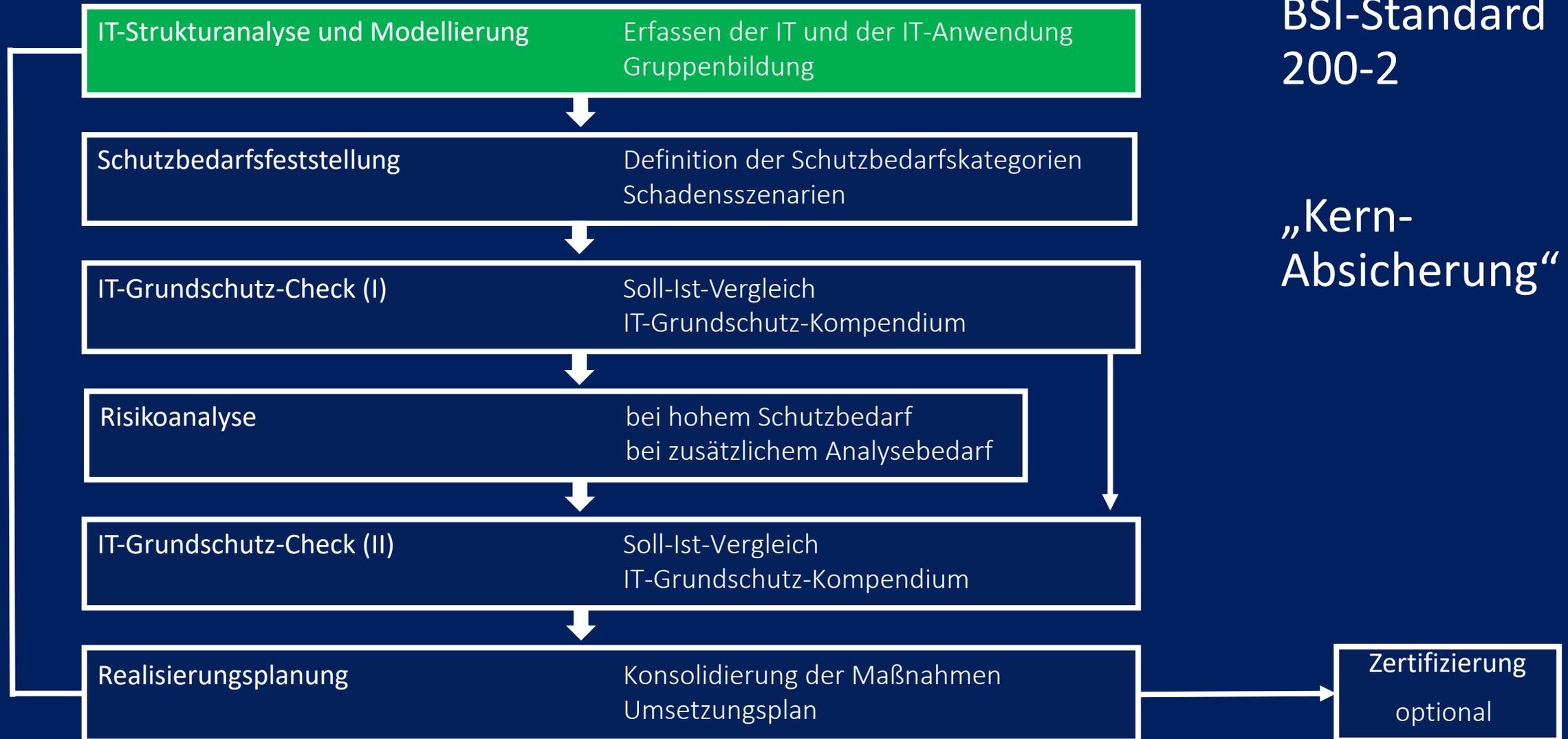
Telearbeit



The screenshot shows a list of business processes (Geschäftsprozesse) in Windows Task Manager. The list is organized into a tree structure:

- GP-01 Kommunikation
- Anwendungen
 - A-01 Microsoft 365
 - OPS.2.2 Cloud-Nutzung
 - APP.1.4 Mobile Anwendungen (Apps)
 - bB-M365 Microsoft365
 - bB-M365-A01 [BASIS] Aktualisierung der Anwendung
 - bB-M365-A02 [BASIS] persönliche Einstellungen: Ber...
 - bB-M365-A03 [BASIS] persönliche Einstellungen: Dat...
 - bB-M365-A04 [BASIS] Regelung zum Autostart
 - bB-M365-A05 [BASIS] Sichere Installation
 - bB-M365-A06 [BASIS] Sicherheitsrichtlinie für Micros...
 - bB-M365-A07 [BASIS] Windows Einstellung zurTelem...
 - bB-M365-A08 [BASIS] Programm zur Verbesserung d...
 - bB-M365-A09 [BASIS] Minimale Datensammlung
 - bB-M365-A10 [BASIS] AV-Vertrag
 - bB-M365-A11 [BASIS] Beschränkung der Diagnosedat...
 - bB-M365-A12 [BASIS] Workplace Analytics, Activity F...
 - bB-M365-A13 [BASIS] Connected Experiences deakti...
 - bB-M365-A16 [BASIS] Rollen und Rechte
 - bB-M365-A-V01 [BASIS] Sicherer Umgang mit Konfer...
 - bB-M365-A-V04 [BASIS] Sicherer Umgang mit Konfer...
 - bB-M365-A-V07 [BASIS] Beenden von Sitzungen
 - bB-M365-A14 [STANDARD] Namenskonvention
 - bB-M365-A15 [STANDARD] persönliche Einstellungen
 - bB-M365-A17 [STANDARD] Microsoft Compliance un...

IT-Sicherheitskonzept



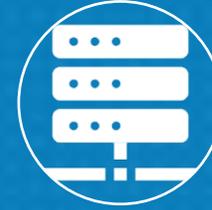
Strukturanalyse



Geschäftsprozesse



Anwendungen



IT-Systeme

Sind untereinander und mit ihren jeweils passenden Bausteinen „verknüpft“

Strukturanalyse

- + Geschäftsprozess
- + Anwendung
- + IT-Systeme

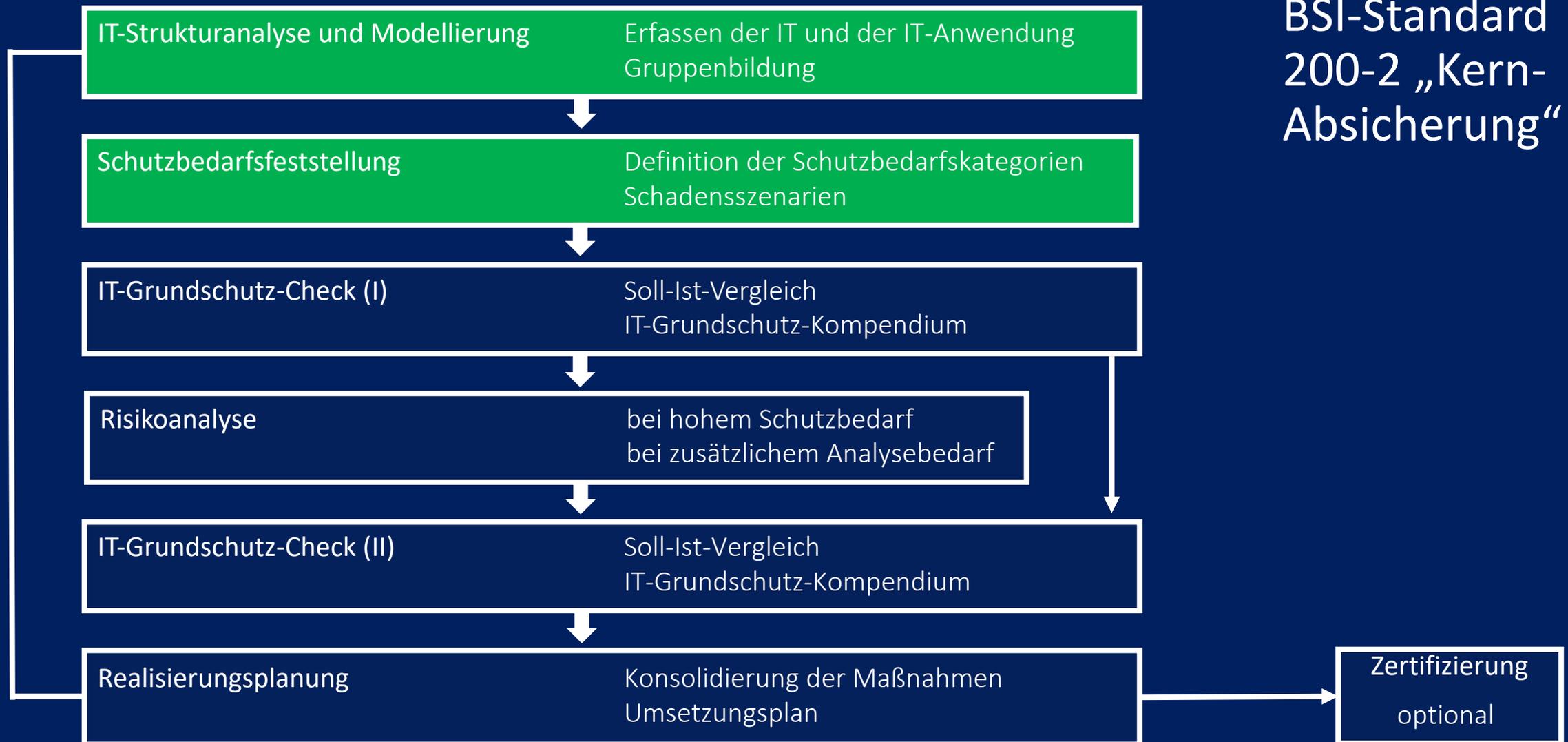
	Verknüpfung		Titel
	nötig für		GP-01 Kommunikation
	benötigt		C-01 Desktop-PCs (Arbeitsplätze)
	benötigt		C-02 Laptops
	benötigt		M-01 Smartphones & Tablets Apple iOS
	benötigt		M-02 Smartphones & Tablets Android

- C-01 Desktop-PCs (Arbeitsplätze)
- C-02 Laptops
 - ▶ SYS.2.1 Allgemeiner Client
 - ▶ SYS.2.2.3 Clients unter Windows 10
 - ▶ SYS.3.1 Laptops
 - ▶ Elementare Gefährdungen
 - ▶ SYS.2.1 Allgemeiner Client
 - ▶ SYS.3.1 Laptops
- M-01 Smartphones & Tablets Apple iOS
 - ▶ SYS.3.2.1 Allgemeine Smartphones und Tablets
 - ▶ SYS.3.2.3 iOS (for Enterprise)
 - ▶ Elementare Gefährdungen
 - ▶ SYS.3.2.3 iOS (for Enterprise)
- M-02 Smartphones & Tablets Android

- ▼ A-01 Microsoft 365
 - ▶ OPS.2.2 Cloud-Nutzung
 - ▶ APP.1.4 Mobile Anwendungen (Apps)
 - ▶ bB-M365 Microsoft365
 - ▶ Elementare Gefährdungen

IT-Sicherheitskonzept

BSI-Standard
200-2 „Kern-
Absicherung“



Schutzbedarfsfeststellung

normal

- Schadensauswirkungen begrenzt und überschaubar

hoch

- Schadensauswirkungen können beträchtlich sein

sehr hoch

- Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen

Schutzbedarfsfeststellung

- ✓ Geschäftsprozess
 - ✓ Anwendung
 - ✓ IT-Systeme

GP-01

Kommunikation

Der Geschäftsprozess umfasst die elektronischen Kommunikationsformen und -wege von bremenports mittels eMail, Chat, Telefon- und Videokonferenzen. Technische Basis bildet dafür Microsoft365 u.a. mit den Anwendungen TEAMS, genutzt auf Desktopsysteme, Laptop Smartphones und Tablets

Ja

Unterstützender Prozess

Ändern...

Ändern...

Kumulationseffekt

Normal

aufgrund der verarbeiteten Informationen wurde ein normaler Schutzbedarf in Bezug auf die Vertraulichkeit festgestellt

Kumulationseffekt

Normal

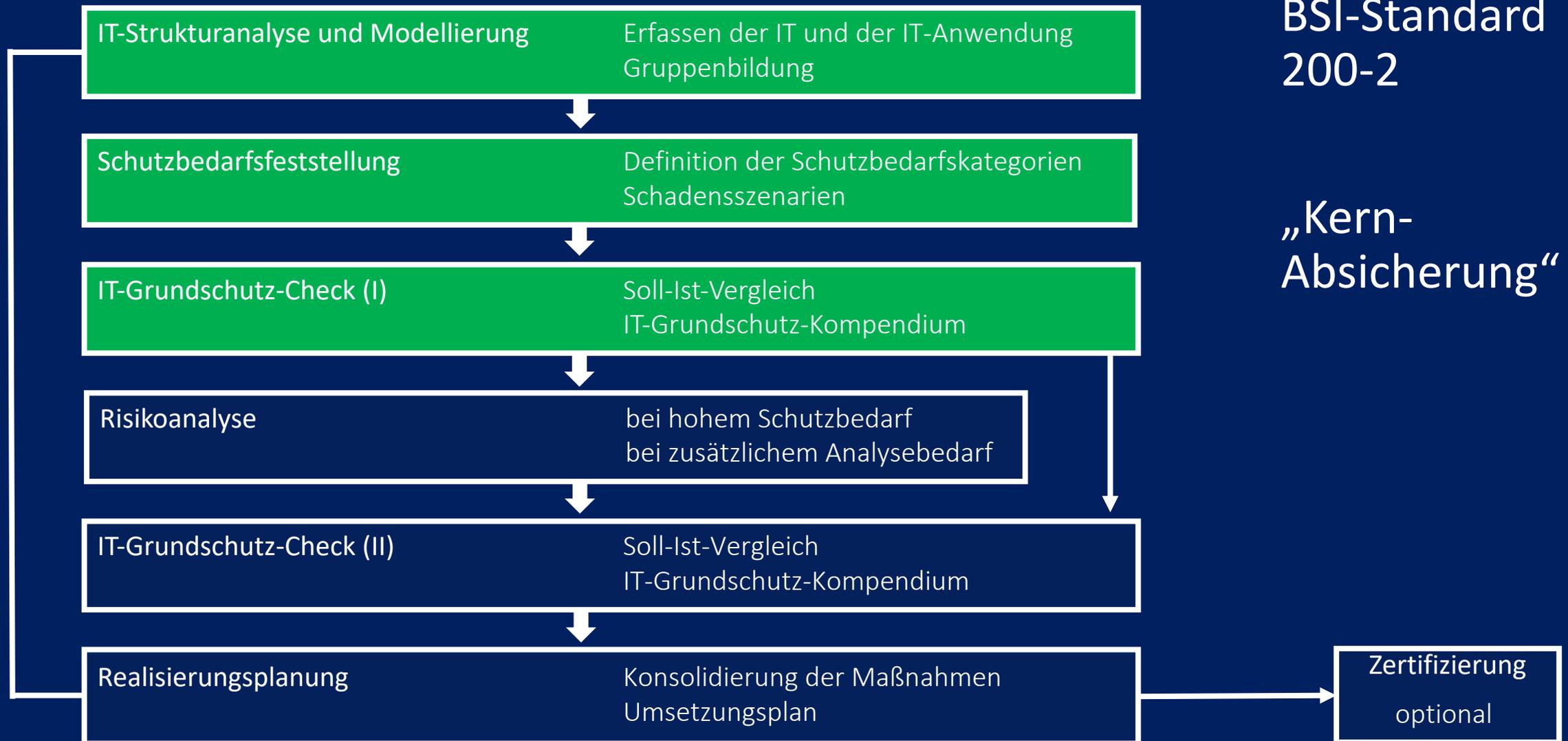
aufgrund der verarbeiteten Informationen wurde ein normaler Schutzbedarf in Bezug auf die Integrität festgestellt

Kumulationseffekt

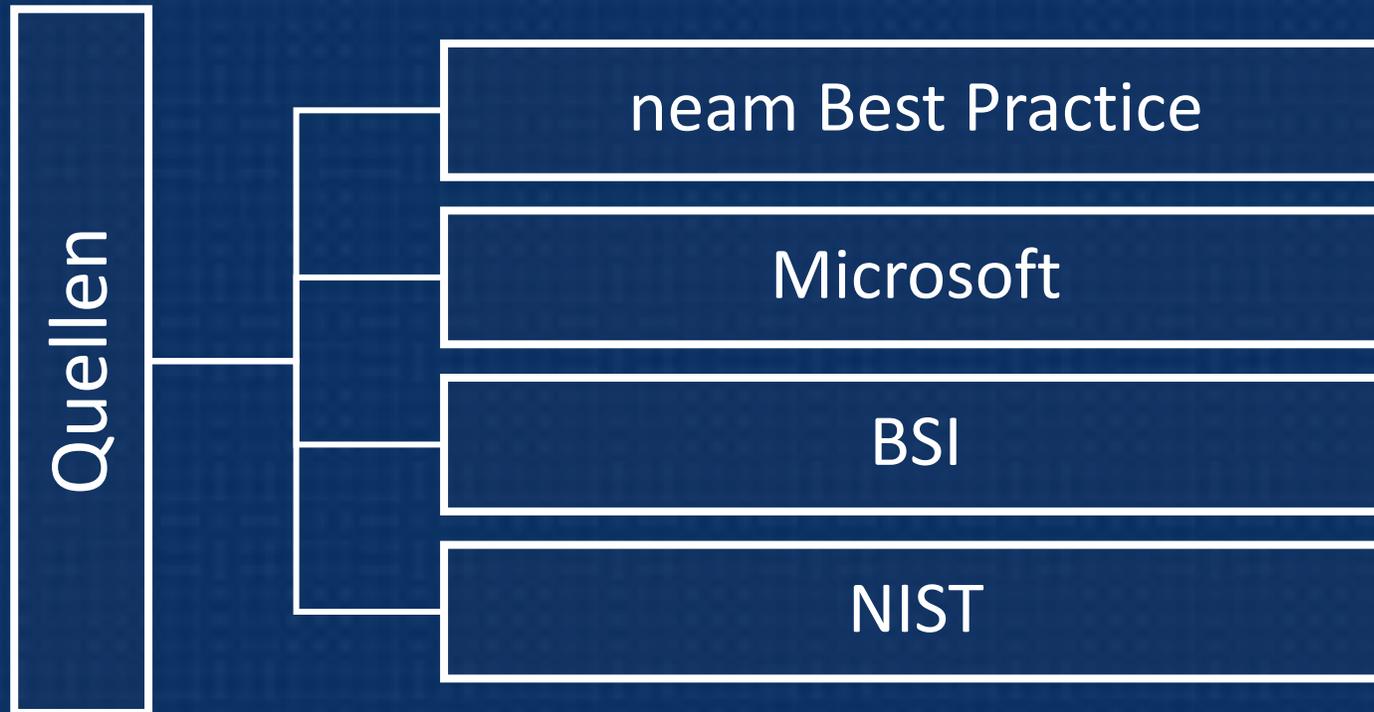
Normal

die Verfügbarkeit wurde als normal eingeschätzt

IT-Sicherheitskonzept



Umsetzungstatus der Anforderungen



▼ Umsetzung

Aus Maßnahme ableiten

Umsetzungstatus

Erläuterung
Vertragsabschluss online unter:
<https://www.microsoftvolumelicensing.com/Downloader.aspx?DocumentId=17871>

Umsetzung bis

Nov 2020						
Mo	Tu	We	Th	Fr	Sa	Su
26	27	28	29	30	31	1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22

Risikoanalyse

1. Gefährdungen

- Elementare Gefährdungen
BSI
- Spezifische Gefährdungen
neam
- Mögliche Folgen eines
Datenschutzverstoßes

2. Gefährdungsbewertung

- Eintrittswahrscheinlichkeit
- Auswirkungen

Risikoanalyse

Informationssicherheit

- Sicht der Organisation
- ISO 27005, BSI Standard 200-3

Datenschutz

- Sicht der Betroffenen
- DSGVO Art 32 (TOMs), 35 (DSFA)
- Standarddatenschutzmodell (SDM)

Risikoanalyse

-  Risiko akzeptabel
-  Risiko durch Informationseigentümer ... durch Geschäftsführung akzeptabel
-  Maßnahmen müssen gefunden werden

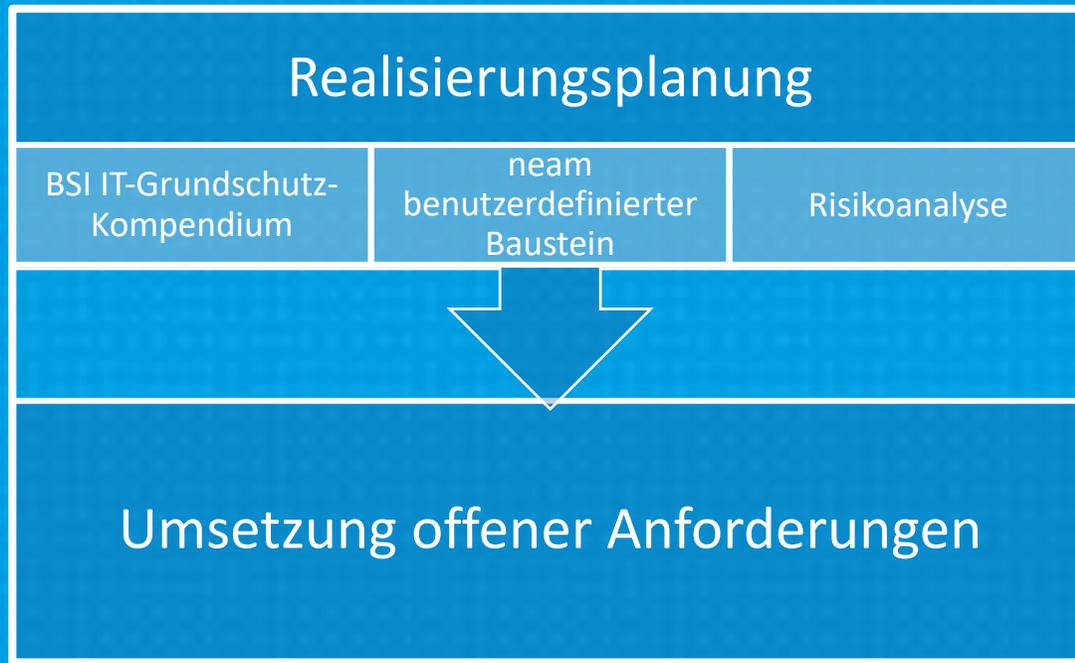
Auswirkung				
existenzbedrohend	mittel	hoch	sehr hoch	sehr hoch
beträchtlich	mittel	mittel	hoch	sehr hoch
begrenzt	gering	gering	mittel	hoch
vernachlässigbar	gering	gering	gering	mittel
	selten	mittel	häufig	sehr häufig
	Eintrittshäufigkeit			

Risikoanalyse

- ✓ Erweiterter Gefährdungskatalog
- ✓ Maßnahmenempfehlungen für erhöhten Schutzbedarf

bB-M365-A18 [ERHÖHT] Anwendung des BSI C5-Anforderungskatalog durch Microsoft
bB-M365-A19 [ERHÖHT] Kunden-Lockbox
bB-M365-A-20 [ERHÖHT] Sichere Administration durch 4-Augen-Prinzip
bB-M365-A-21 [ERHÖHT] Service-Reviews
bB-M365-A-22 [ERHÖHT] Verschlüsselte Datenablage
bB-M365-A-23 [ERHÖHT] Messung der Microsoft 365 Nutzung
bB-M365-A-24 [ERHÖHT] Planung und Durchführung von Audits der Microsoft 365 - N
bB-M365-A-V50 [ERHÖHT] Keine Aufzeichnung von Konferenzinhalten
bB-M365-A-V52 [ERHÖHT] Einschränkung von KI-Funktionen
bB-M365-A-V54 [ERHÖHT] Verzicht auf Konferenzen in Großraumbüros
bB-M365-A-V55 [ERHÖHT] Verzicht auf Sprachsteuerung/ Sprachassistenten
bB-M365-A-V59 [ERHÖHT] Ausschließliche Datenablage innerhalb der Europäischen U.

Individuelle Anpassung



Sicherheit als Prozess

-  Messung der Zielerreichung in die IT-Sicherheitsstrategie integrieren
-  Realisierung der beschlossenen Maßnahmen überprüfen
-  Wirksamkeit und Effizienz der beschlossenen Maßnahmen überprüfen

VIELEN DANK
für Ihre Aufmerksamkeit

