Microsoft 365 IT-Sicherheitskonzept

Kai Wittenburg
Geschäftsführer, neam IT-Services GmbH

neam IT-Services GmbH

Facts

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

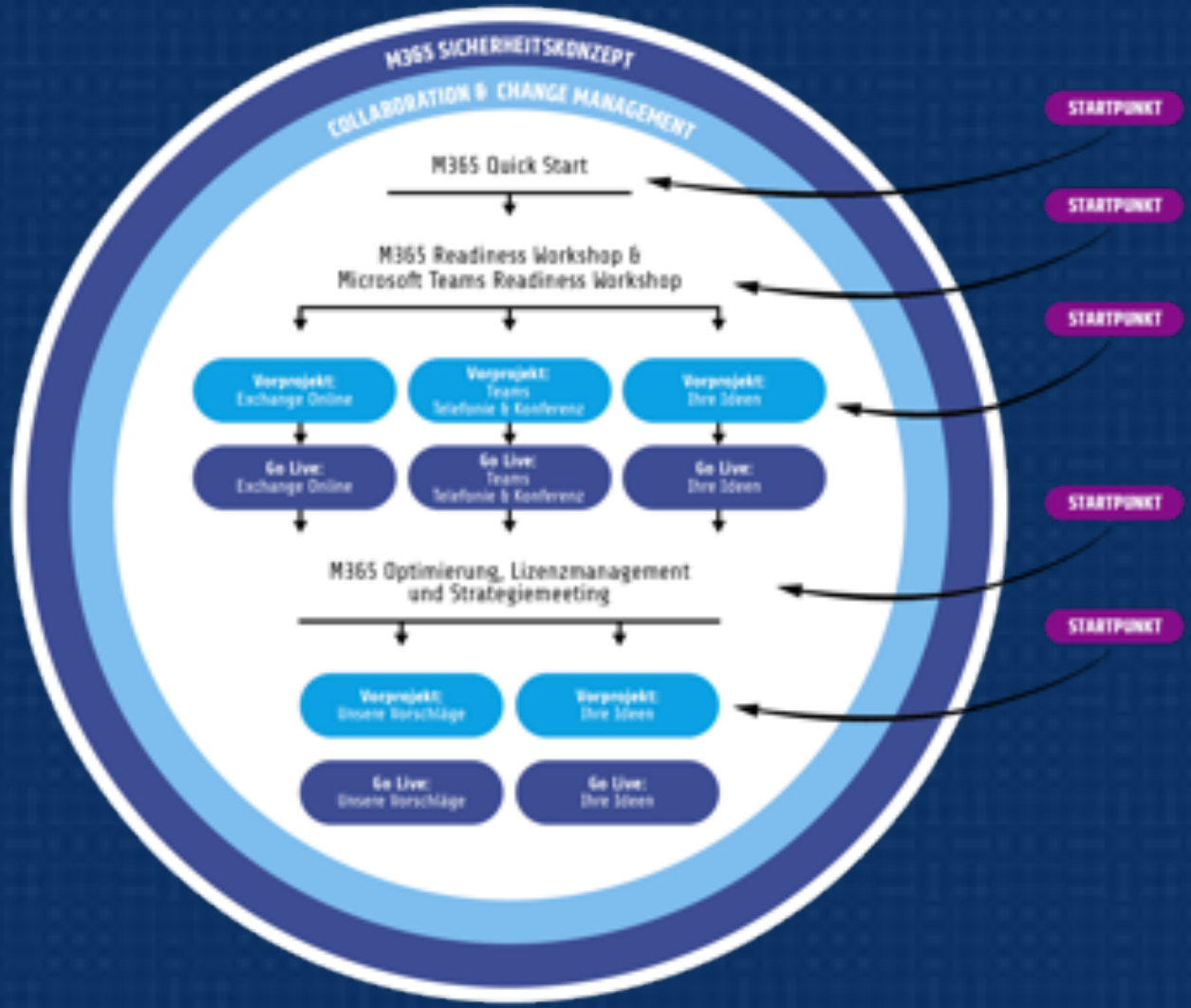
Informationssicherheit

Beratung & Schulungen

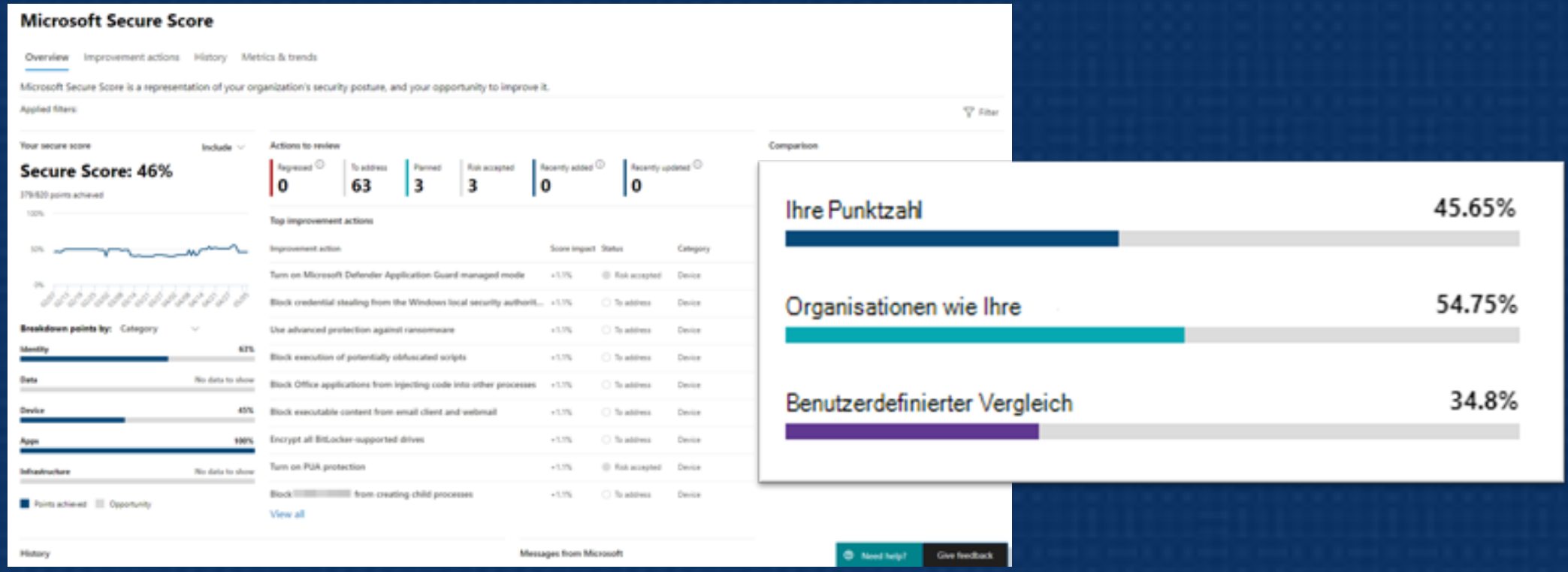
- BSI IT-Grundschutz
- ISMS nach ISO 27001
- Business Continuity Management
- Audits & Zertifizierungen
- Penetrationstest
- Social Engineering
- Incident Response

Cloud

Microsoft 365 und Azure



Microsoft Secure Score



Microsoft-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 — Einschließen

Sicherheitsbewertung: 41.29%

31.38/76 erzielte punkte

Punkte aufgliedern nach: Kategorie

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

Erzielte Punkte | Möglichkeit

Zu prüfende Aktionen

Verschlechtert	Zu behandeln	Geplant	Risiko akzeptiert	Zuletzt hinzugefügt	Kürzlich aktualisiert
0	12	0	0	0	0

Wichtigste Verbesserungsaktionen

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

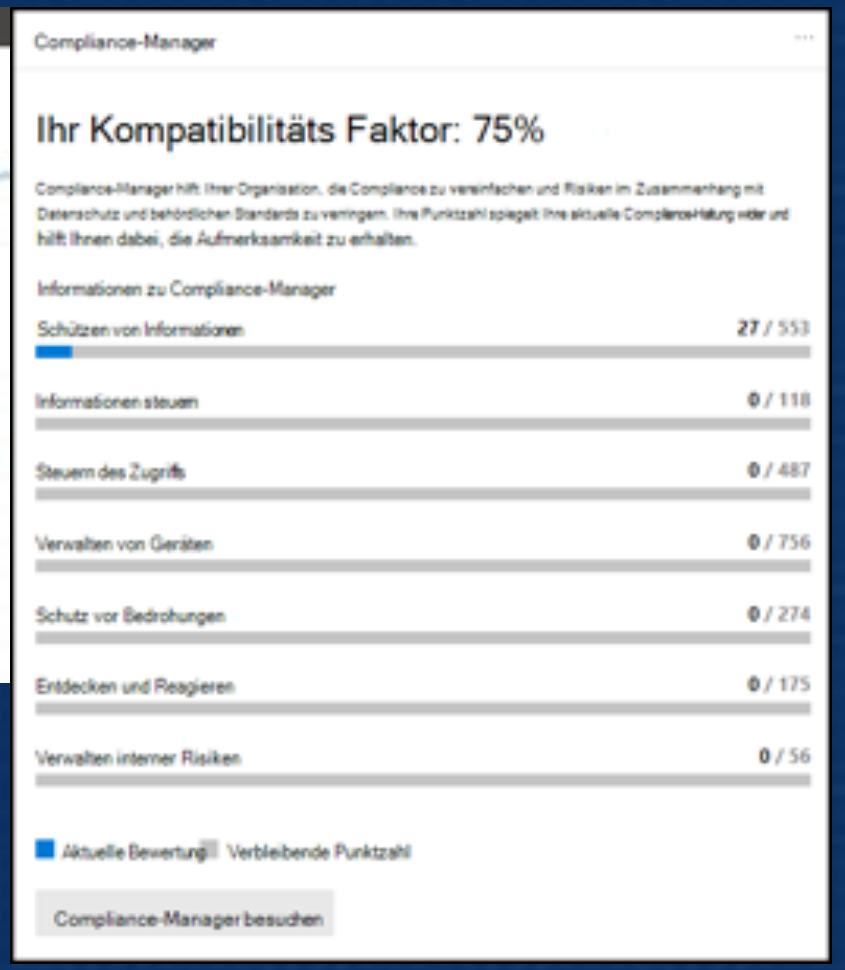
Voraussetzungen
✓ Sie haben Azure Active Directory Premium P2.

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.

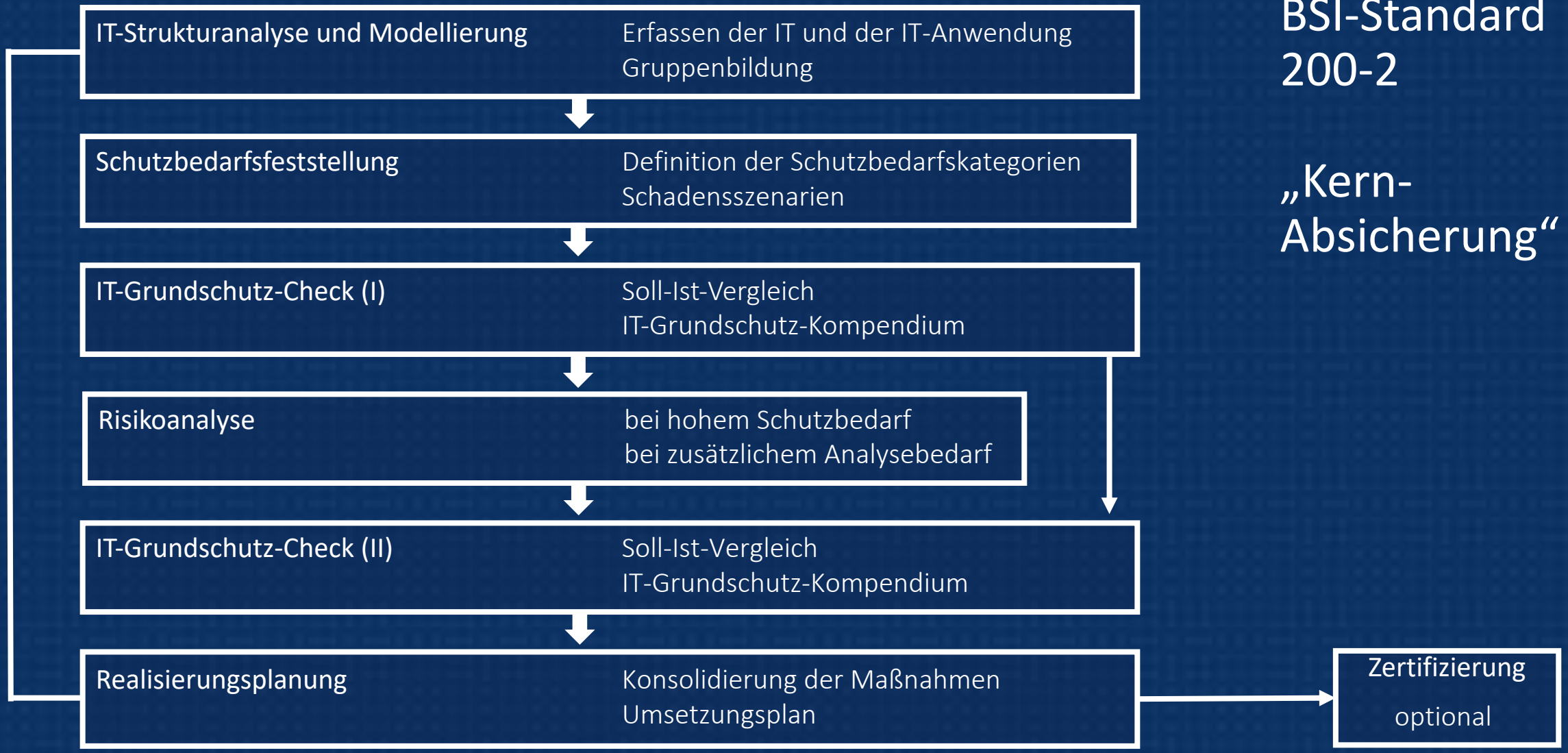
Microsoft Compliance Score



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 des e-Mail-Profils

IT-Sicherheitskonzept



BSI-Standard 200-2

„Kern-Absicherung“

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

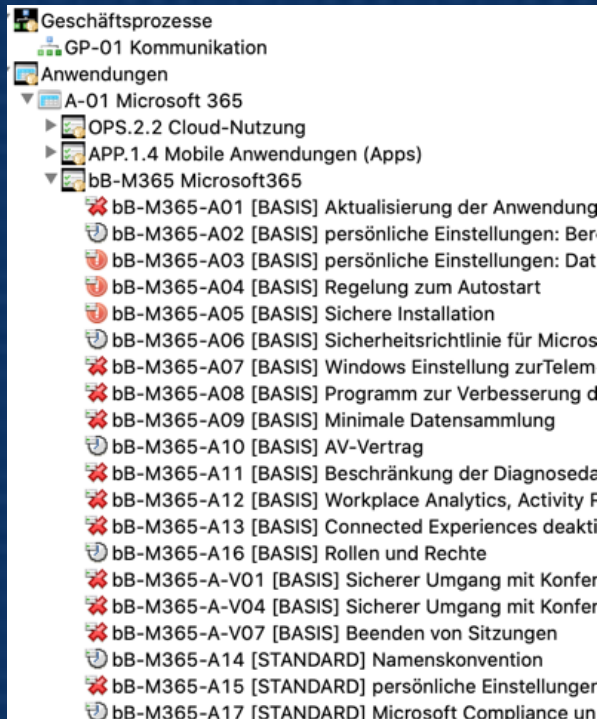
Cloud Nutzung

Mobile Anwendungen (Apps)

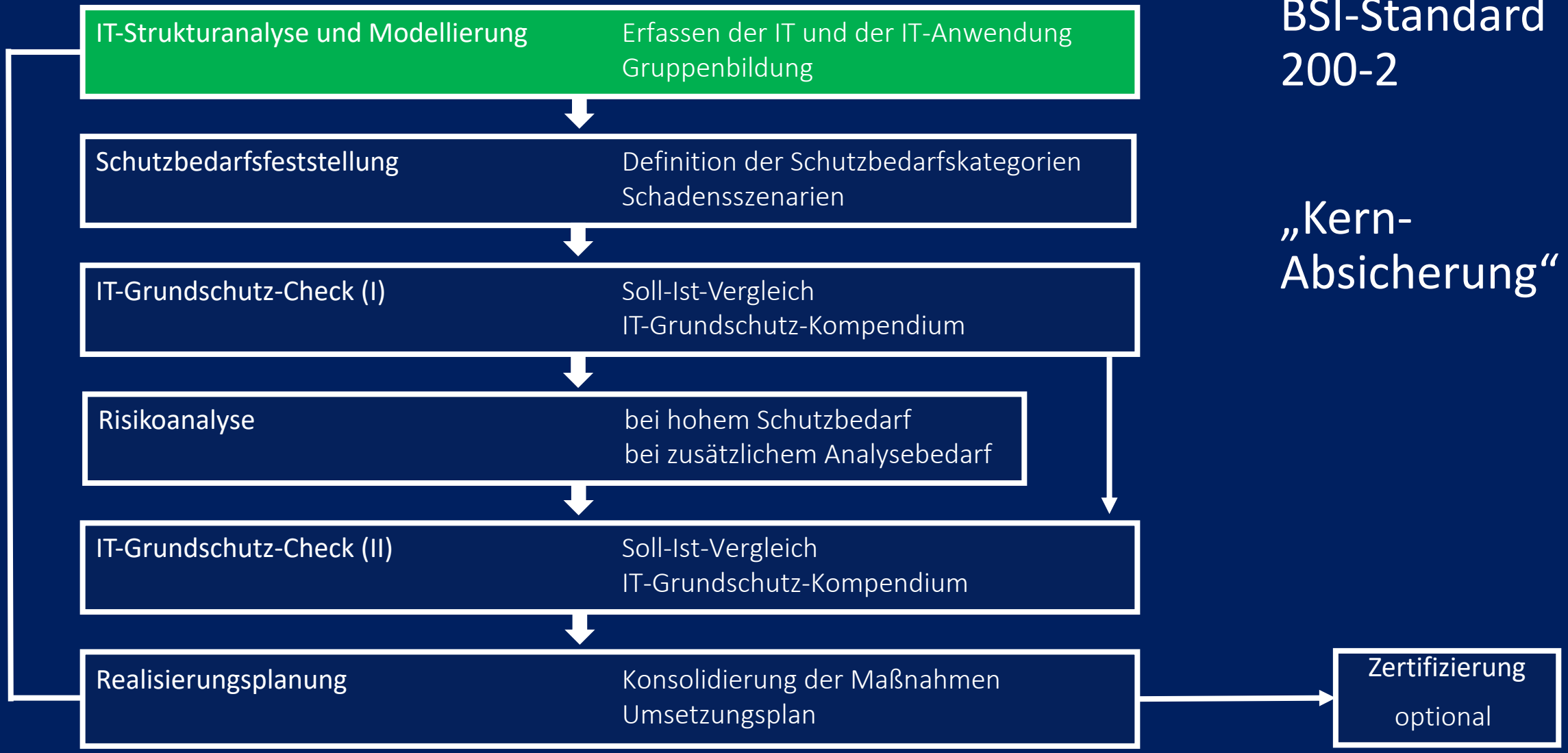
Windows/ Linux/ MacOS-Clients

Android/ iOS Smartphones und Tablets

Telearbeit



IT-Sicherheitskonzept



BSI-Standard 200-2

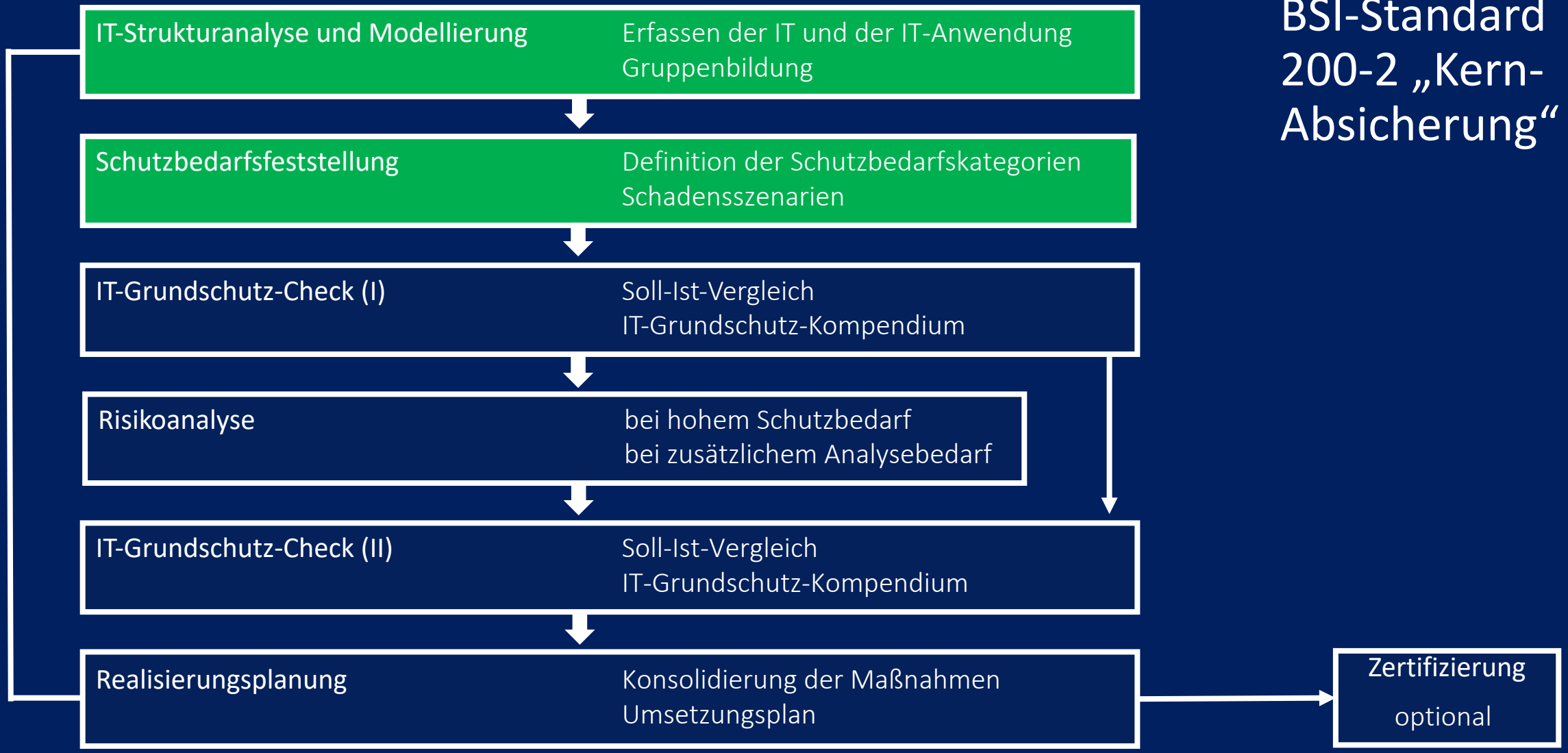
„Kern-Absicherung“

Strukturanalyse

Strukturanalyse

- Geschäftsprozess
- Anwendung
- IT-Systeme

IT-Sicherheitskonzept



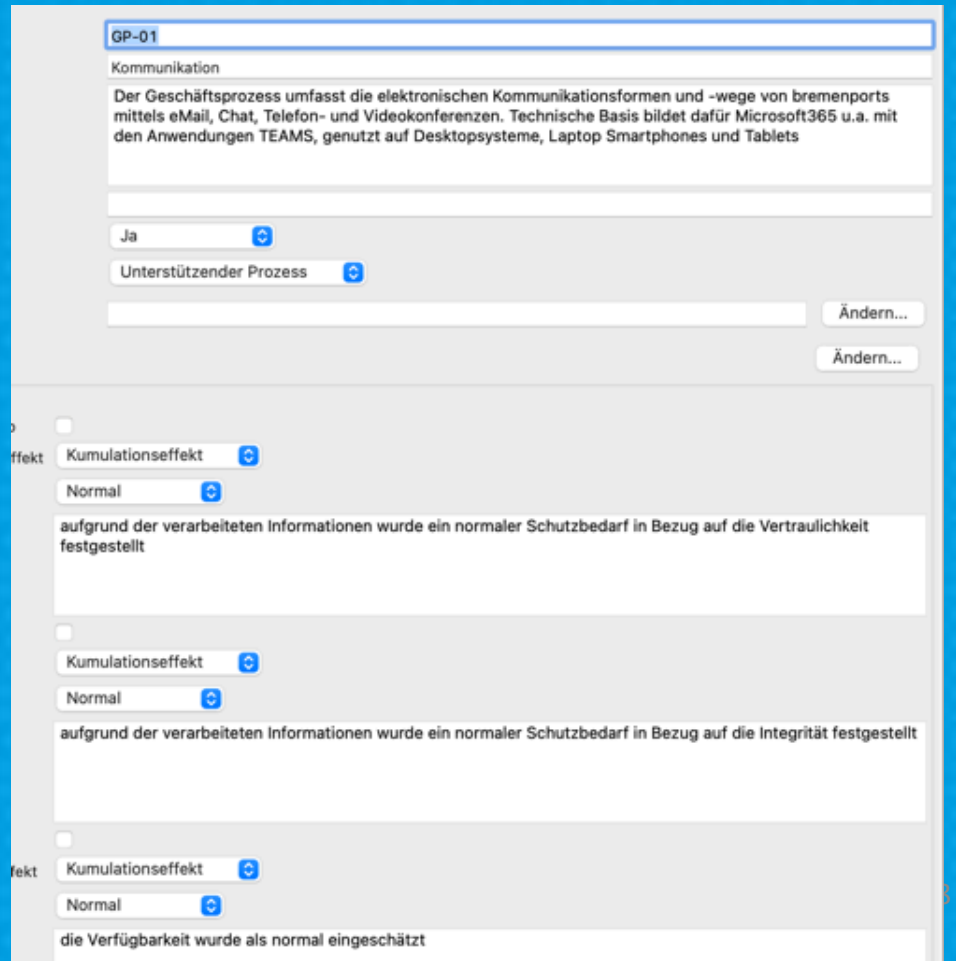
BSI-Standard 200-2 „Kern-Absicherung“

Schutzbedarfsfeststellung

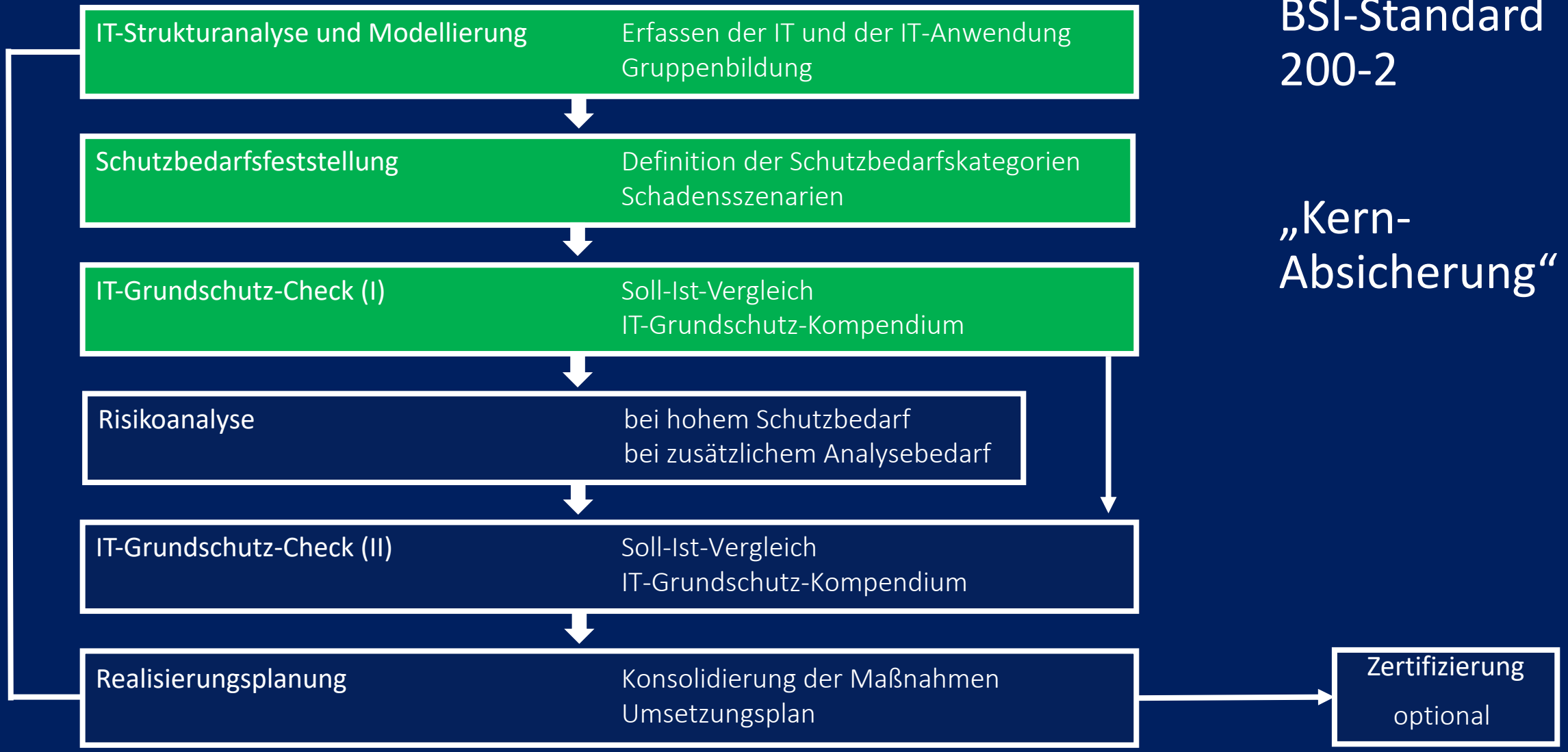
normal	hoch	sehr hoch
▪ Schadensauswirkungen begrenzt und überschaubar	▪ Schadensauswirkungen können beträchtlich sein	▪ Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen

Schutzbedarfsfeststellung

- Geschäftsprozess
  - Anwendung
    - IT-Systeme



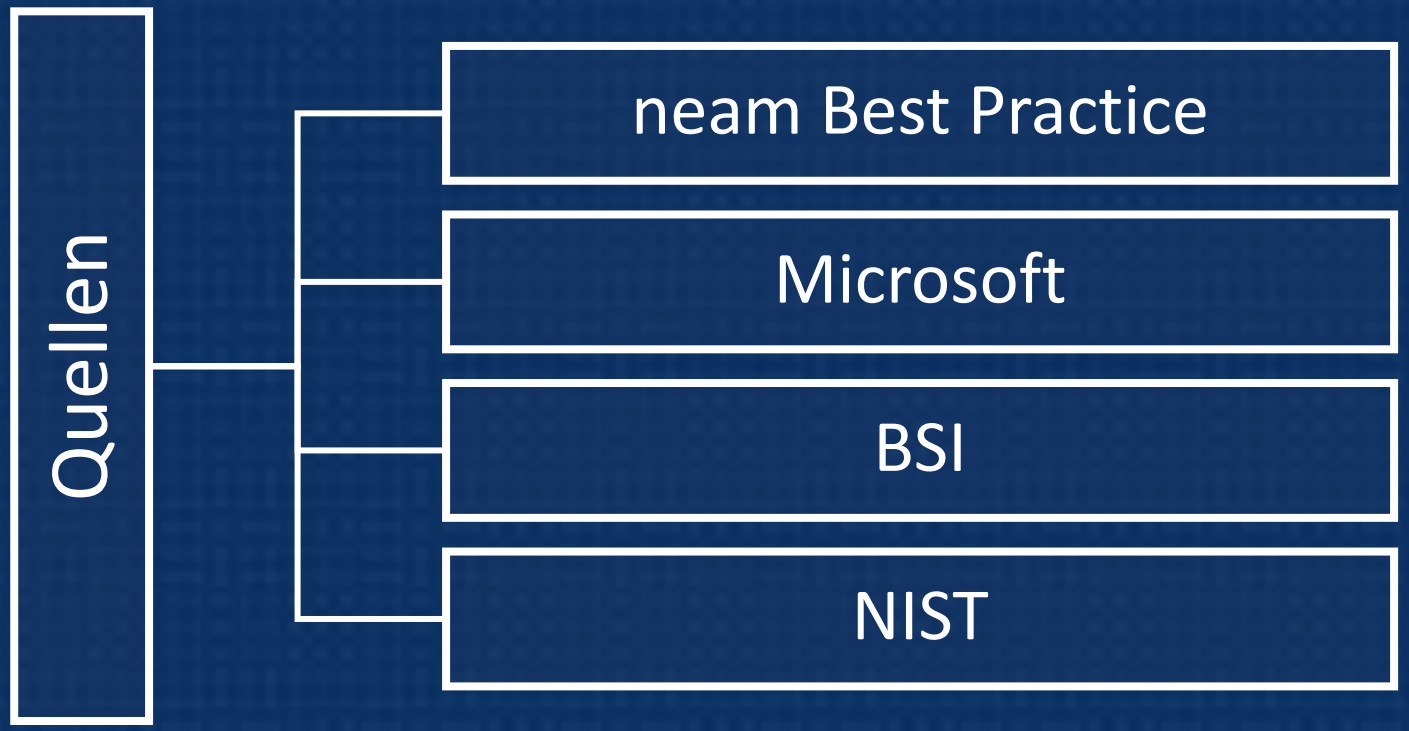
IT-Sicherheitskonzept

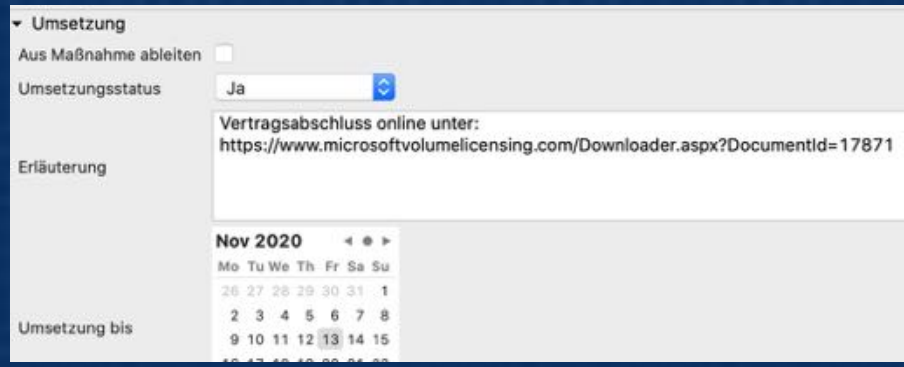


BSI-Standard 200-2

„Kern-Absicherung“

Umsetzungsstatus der Anforderungen





Risikoanalyse

1. Gefährdungen	2. Gefährdungsbewertung
▪ Elementare Gefährdungen BSI ▪ Spezifische Gefährdungen neam ▪ Mögliche Folgen eines Datenschutzverstoßes	▪ 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

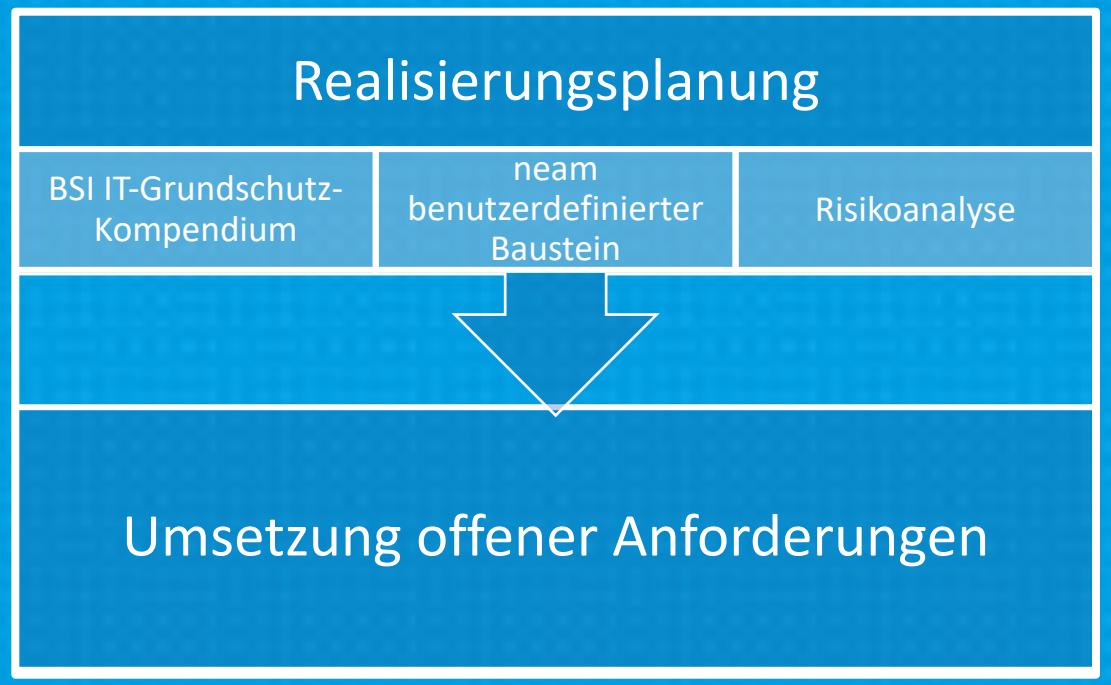
- Risiko akzeptabel
- Risiko durch Informationseigentümer
  … durch Geschäftsführung akzeptabel
- Maßnahmen müssen gefunden werden

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