Praxisgerechte Informationssicherheit im VUCA-Zeitalter.

4 x 2 Maßnahmen
für mehr Informationssicherheit

8 Maßnahmen

Aus der IT-Praxis.
Für die Unternehmenspraxis.

Michael Bendl

Gerlinde Macho

MP2 IT-Solutions

IT-Unternehmen seit 1999 → Wien · Graz · NÖ/Zwettl

IT Services & Security

Webentwicklung & Online Shops

Digital Healthcare

Software- & App-Entwicklung

Consultings & Trainings

Gerlinde Macho
IT-Unternehmerin
Digitalisierungsberatung · Auditor ISO 27001
www.mp2.at/gerlinde.macho

Michael Bendl
COO Chief Operating Officer · Certified Data & IT Security Expert
Microsoft Certified: Azure Solutions Architect
Expert & Microsoft 365 Certified: Security Administrator Associate
www.mp2.at/michael.bendl

Moderne Business- & Arbeitswelt

Eine Herausforderung für Informationssicherheit.

- ☑ VUCA-Modell → beschreibt die zunehmende Veränderung der heutigen Welt.
- ☑ Globalisierung & Digitalisierung → KI
- ☑ Märkte & Anforderungen verändern sich rasch & New Work

⇨ agiles Management & Leadership
⇨ gesamtheitliches agiles Informationssicherheitsmanagement

⇨ Komplexität entgegenwirken
⇨ agil reagieren & handeln
⇨ Resilienz schaffen!

MP2 IT-SOLUTIONS

Informationssicherheit

Primäre Schutzziele noch wichtiger in der VUCA-Welt.

Verfügbarkeit	Informationen zur rechten **Zeit** am rechten **Ort**
Vertraulichkeit	Information nur für **Berechtigte**
Integrität	**unverfälscht** & **nachvollziehbar**

⇨ IT-Sicherheit · Datenschutz · Datensicherheit

MP2 IT-SOLUTIONS

V ⇨ VOLATILITY

Volatilität steht für Unstetigkeit & Unbeständigkeit.

VUCA

⇨ Umfeld & Rahmenbedingungen ändern sich

⇨ viele dynamische Aspekte & Themen

⇨ laufende Veränderung der Variablen

2 Maßnahmen

1) **Echtzeitüberwachung**
2) **Incident Response Plan – Notfallplan**

MP2 IT-SOLUTIONS

Echtzeitüberwachung

1

Überwachung von Netzwerkaktivitäten & Benutzerverhalten
⇨ rasche Reaktion auf ungewöhnliche Ereignisse

- ☑ **Quellen für Informationen definieren Bewertung der Bedrohungen & Maßnahmen setzen ⇨ Work-Flows definieren**
- ☑ **Monitoring, Bedrohungserkennung, Webfilter, Logs, Pentests, …**

Monitoring A.8.16

Web-Filter A.8.23 + AntiVirus A.8.7 implementieren, pflegen & Ausnahmen so gering wie möglich halten

Erkenntnisse über Bedrohungen A.5.7

ISO 27001:2022
ISO 27002

VOLATILITY

MP2 IT-SOLUTIONS

Incident Response Plan

2

Plan zur Bewältigung von Sicherheitsvorfällen
⇨ angemessene Reaktion auf unerwartete Bedrohungen

- ☑ **lebendige Notfallpläne ⇨ für alle sicherheitskritischen Dienste & Assets**
- ☑ **Asset-Liste & Infrastrukturpläne**
- ☑ **Notfallszenarien ⇨ planen, dokumentieren & überprüfen**
- ☑ **Zuständigkeiten & Kontaktpersonen ⇨ wer macht wann was? DEMI-Matrix**
- ☑ **Wiederherstellungspläne**
- ☑ **aktuelle Version des Notfallplan auch in Printform**

Hotline ☎

A.5.24 – A.5.29 Controls hinsichtlich Informationssicherheitsvorfälle

A.6.8 Meldung von Informationssicherheitsereignisse

A.5.9 – A.5.10 Werte & zulässiger Gebrauch

VOLATILITY

MP2 IT-SOLUTIONS

Incident Response Plan

Auszug als Beispiel

2

	Asset	Szenario	Vorgehen	D	E	M	I	Kontaktdaten
#72	**IT**	**Verschlüsselungsvirus**	1. Isolieren der infizierten Systeme	IT	AL		GF	GF-DW 100
			2. Zusammenarbeit mit Cyber-Security-Experten	AL		EX		IT-Leitung -DW 300
			3. Identifikation des Virus und seiner Auswirkungen	IT	AL	EX		"Externe Expert:innen
			4. Entfernung / Isolierung des Viruses	IT	AL	EX		Gmbh":+43 720 555955
			5. Notfallwiederherstellung der betroffenen Systeme einleiten	IT	AL	EX		support@externe-
			6. Kommunikation an betroffene Abteilungen	AL		EX		experten.at
			7. Fortschritt verfolgen und überwachen					
			8. Detailanalyse des Vorfalls					
			9. Lessions Learned					
#73	**Notebook**	**Notebook-Verlust**	1. Meldung über Teams Informationssicherheits					
			2. Überprüfung, welche Daten betroffen sind					
			3. Kommunikation mit Datneschutzbeauftragter					
			4. Aktivierung von Remote-Löschfunktion					
			5. Erstellung von Verlustdokumentation					
			6. Fortschritt verfolgen und überwachen	DS				

Legende

AL	Abteilungsleitung
DS	Datenschutzbeauftragte
EX	Externe Firma
MA	Mitarbeiter:innen
IT	IT-MA

⇨ Detaillierungsgrad definieren

⇨ klare Vorgehensweise

⇨ DEMI hilft dabei

A.5.24 – A.5.29 Controls hinsichtlich Informationssicherheitsvorfälle

A.6.8 Meldung von Informationssicherheitsereignisse

A.5.9 – A.5.10 Werte & zulässiger Gebrauch

VOLATILITY

mp2 IT-SOLUTIONS

U ⇨ UNCERTAINTY

New Work bringt oftmals Unsicherheiten mit sich.

- ⇨ verschiedene Szenarien
- ⇨ Ungewissheit und Unbekanntheit führt zu Unvorhersagbarkeit
- ⇨ Erfahrungswerte gelten nicht (mehr)

2 Maßnahmen

3) **Awareness & Schulungen**
4) **Ausfallssicherheit**

MP2 IT-SOLUTIONS

Awareness & Schulung

3

Mensch ist Angriffsziel & Sicherheitsfaktor #1 zugleich ⇨
Investitionen in Awareness & Sicherheitstrainings lohnen sich.

- ☑ **Schaffung von Bewusstsein von Informationssicherheit → NIS2**
- ☑ **Webinare, Trainings & Know-how-Check → Maßnahmen setzen & Wirksamkeit überprüfen!**
- ☑ **wichtig: richtige Entscheidungen bei unklaren Situationen**
- ☑ **Informationssicherheit für jene ohne digitalen Arbeitsplatz**

- *A.7.7 Aufgeräumte Arbeitsplatzumgebung & Bildschirmsperren*
- *A.6.3 Informationssicherheitsbewusstsein, -ausbildung und -schulung*
- *A.6.4 Maßregelungsprozess*

MP2 IT-SOLUTIONS

Ausfallssicherheit

4

Implementieren Sie redundante Systeme und Backup-Pläne!
⇨ inkl. Cloud-Dienste

☑ **redundante Systeme**
- ✓ jede Komponente eines wichtigen Systems
- ✓ Überprüfung diverser Ausfallszenarien
- ✓ lagernde Ersatzteile

A.8.13 Sicherung von Informationen → Backup & Wiederherstellung(stests)

A.5.30 IKT-Bereitschaft für Business Continuity

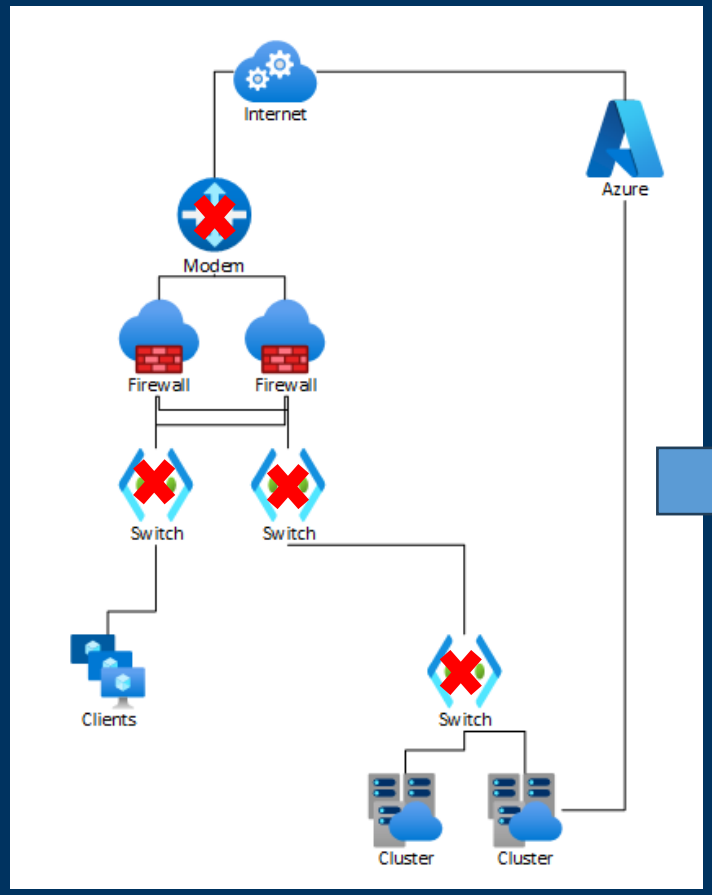
A.5.23 Informationssicherheit für die Nutzung von Cloud-Diensten

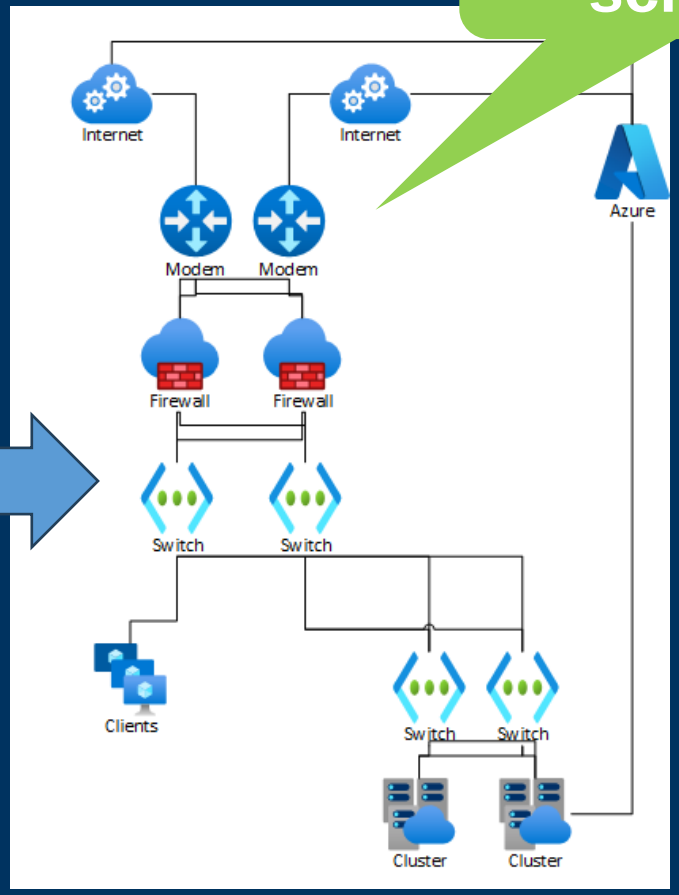
MP2 IT-SOLUTIONS

Ausfallssicherheit

Redundanz schaffen

4





- *A.8.13 Sicherung von Informationen → Backup & Wiederherstellung(stests)*
- *A.5.30 IKT-Bereitschaft für Business Continuity*
- *A.5.23 Informationssicherheit für die Nutzung von Cloud-Diensten*

UNCERTAINTY

MP2 IT-SOLUTIONS

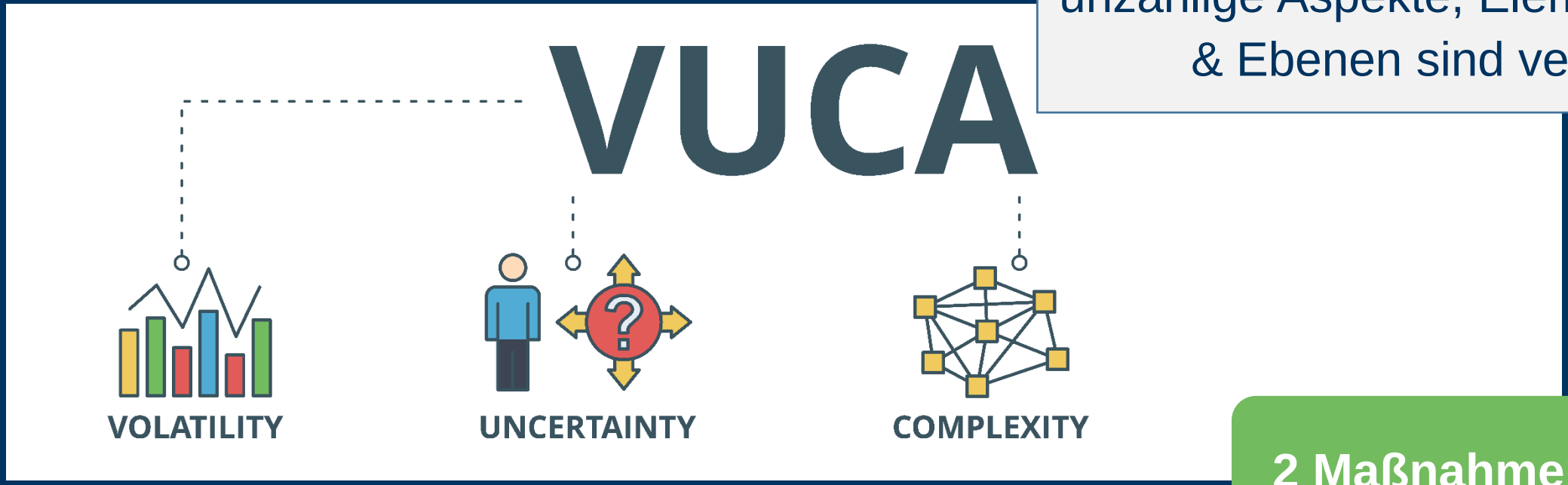
C ⇨ COMPLEXITY

New Work erhöht die Komplexität.

verschiedene Systeme ⇦

Abgrenzung kaum möglich ⇦

unzählige Aspekte, Elemente & Ebenen sind vernetzt ⇦



2 Maßnahmen

5) **interdisziplinäre Zusammenarbeit**
6) **Sicherheitsautomatisierung**

MP2 IT-SOLUTIONS

Interdisziplinäre Zusammenarbeit

5

Internes & externes fachübergreifendes Zusammenarbeiten ist in der VUCA-Welt ein entscheidender Faktor.

- ☑ **Synergien nutzen und Know-how weitergeben**
- ☑ **andere Perspektiven in die Planung des Konzeptes miteinbinden**

→ **Informationssicherheitsteam**
→ **Arbeitsgruppen, Boards**
→ **Jourfixe**

- *A.5.5 Kontakt mit Behörden*
- *A.5.6 Kontakt mit speziellen Interessensgruppen*
- *A.5.19-5.22 Lieferantenbeziehung*
- *A.5.2 Rollen & Verantwortlichkeiten*
- *A.6.3 Informationssicherheitsbewusstsein, -ausbildung & -schulung*

COMPLEXITY

MP2 IT-SOLUTIONS

Sicherheitsautomatisierung

6

Setzen Sie auf Automatisierung von Aufgaben und Prozesse, um Fehler zu minimieren!

- ☑ **Was tut sich in meiner Infrastruktur?**
- ☑ **regelmäßige Infrastruktur-Scans ⇨ Geräte, Zugriffe, Berechtigungen**
  - ☑ **Thema Schatten-IT**
- ☑ **Update-Management**
- ☑ **aktives Schwachstellen-Management (intern & extern)**
  - ☑ **Vulnerability Scans & Pentests**

A.5.7 Erkenntnisse über Bedrohungen

A.8.8 Handhabung von technischen Schwachstellen

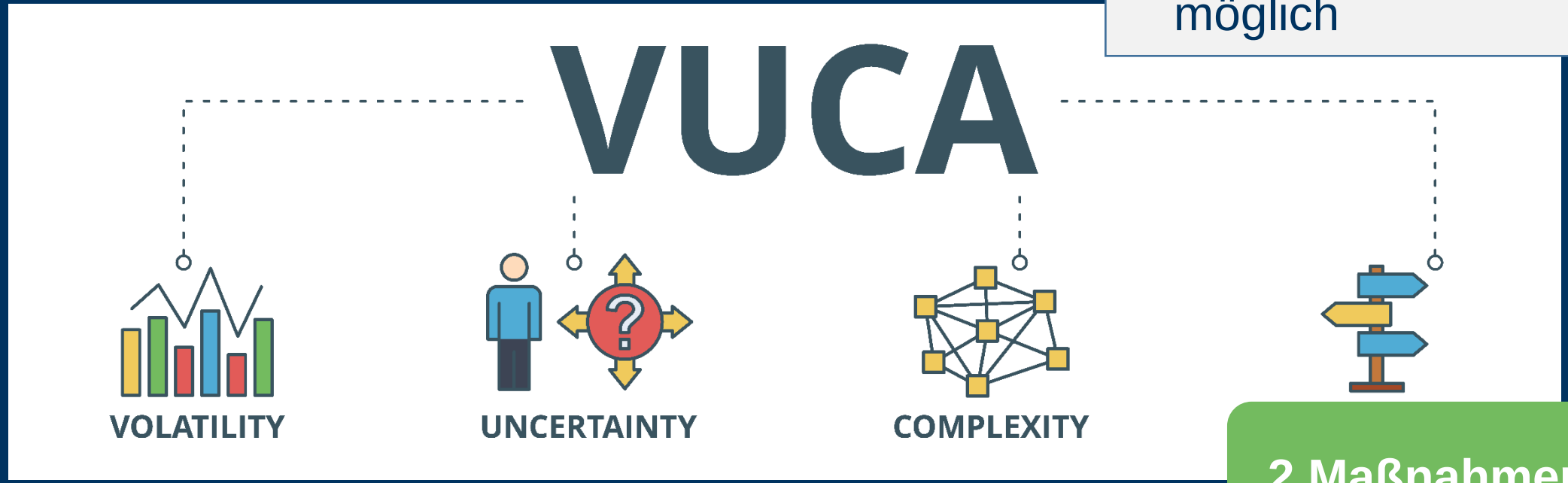
COMPLEXITY

MP2 IT-SOLUTIONS

A ⇨ AMBIGUITY

Mehrdeutigkeit in der Welt von New Work.

⇨ Situationen unterschiedlich beurteilbar
⇨ keine einfache Erklärung möglich



2 Maßnahmen

7) **agiles Sicherheitskonzept & Risikomanagement**
8) **Audits & Checks**

MP2 IT-SOLUTIONS

Agiles Sicherheitskonzept

volatilen Umgebung, wie ändernde Bedrohungen, Technologien
⇨ Sicherheitsmaßnahmen müssen laufend angepasst werden.

- ☑ **regelmäßiges Überprüfen, Herausfordern & Adaptieren**
- ☑ **Analyse der aktuellen Gegebenheiten ⇨ intern & extern**
- ☑ **physische Sicherheit → Homeoffice, Teleworking, Remote**
- ☑ **agiles Risikomanagment**

⇨ ISO 27001 Kapitel 4 Kontext der Organisation

A.5.1 Informationssicherheitsrichtlinien

A.6.7 Telearbeit

A.7.9 Sicherheit von Werten außerhalb der Räumlichkeiten

AMBIGUITY

MP2 IT-SOLUTIONS

Flexibles Risikomanagement

7

Das Risikomanagement muss an die volatilen und unsicheren Umstände der VUCA-Welt an gepasst werden.

- ☑ **Risikoanalysen & -bewertungen → Informationsgrundlage für Sicherheitsmaßnahmen**
- ☑ **Bewertung von Risiken → proaktive Anpassung → Schutz vor Unvorhergesehenem.**
- ☑ **BIA Business Impact Analyse**

! **Einbeziehung aller Stakeholder & Themen**

⇨ ISO 27001 6.1 Maßnahmen zum Umgang mit Risiken und Chancen

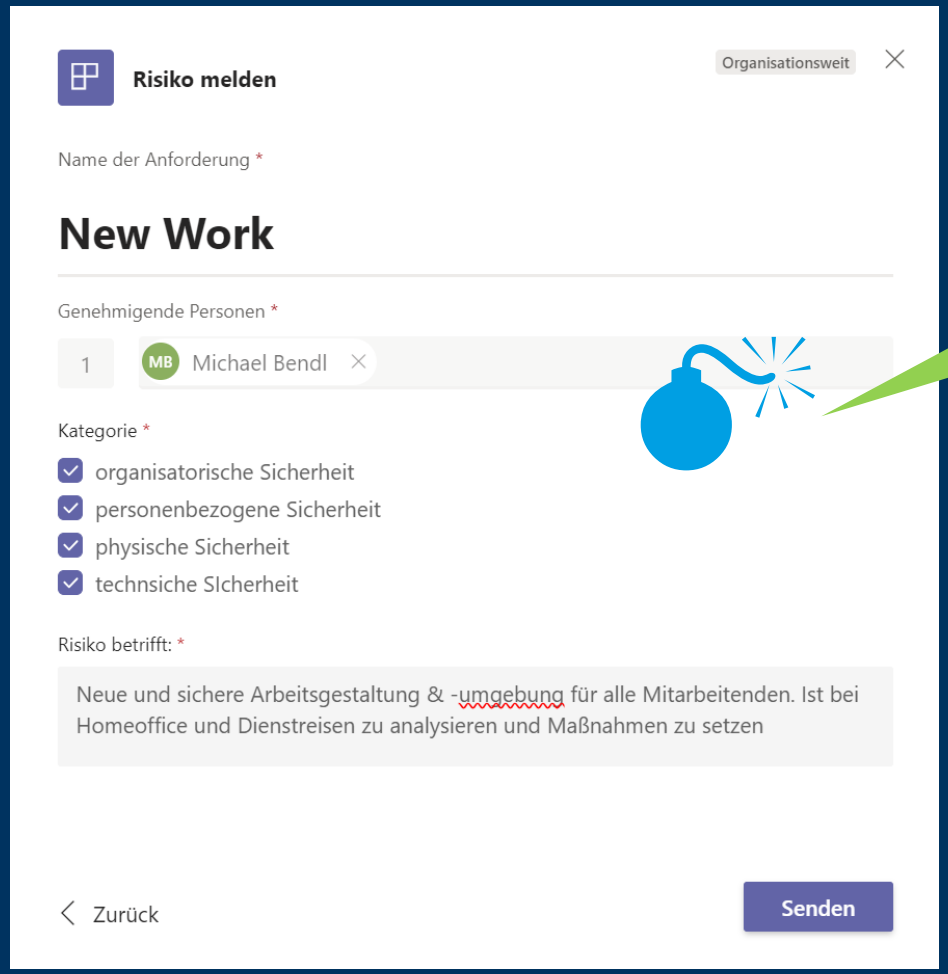
A.5.30 IKT-Bereitschaft für Business Continuity

AMBIGUITY

MP2 IT-SOLUTIONS

Flexibles Risikomanagement

7



Risiken rasch aufnehmen
⇨ für alle zugänglich machen

⇨ ISO 27001 6.1 Maßnahmen zum Umgang mit Risiken und Chancen

A.5.30 IKT-Bereitschaft für Business Continuity

AMBIGUITY

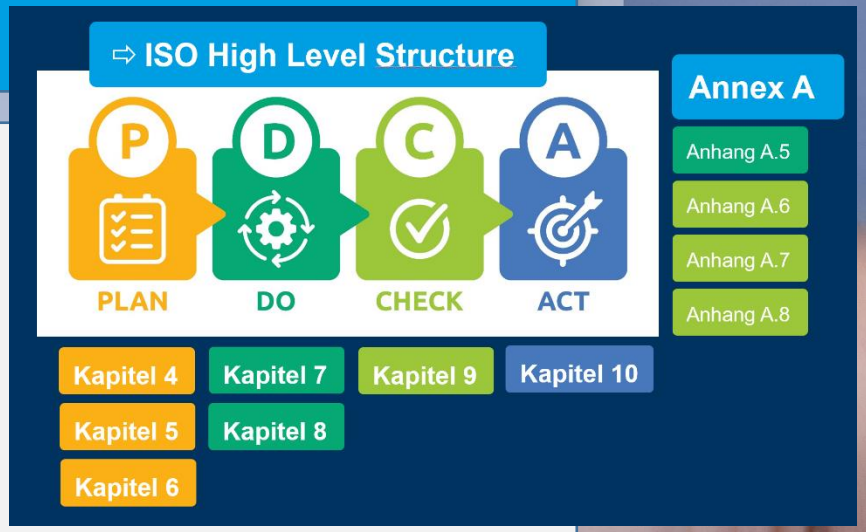
MP2 IT-SOLUTIONS

Audits & Checks

8

Systeme regemäßig checken → intern & extern

- ☑ **Simulationen durchführen**
- ☑ **interne & externe Checks**
- ☑ **interne Audits & externe Audits ⇨ Zertifizierungen**
- ☑ **Maßnahmen setzen zur laufenden Verbesserung**



- *A.8.34 Schutz der Informationssysteme während der Überwachungsprüfung*
- *⇨ ISO 27001 Kap. 9+10 Bewertung der Leistung + Verbesserung*
- *Informationssicherheitsrollen und -verantwortlichkeiten A.5.2*
- *Aufgabentrennung A.5.3*

AMBIGUITY

MP2 IT-SOLUTIONS

MP2 IT-Solutions

Wir sind für Sie da.

✉ mp2@mp2.at ☎ 0720 555 955 www.mp2.at

IT Services & Security

Webentwicklung & Online Shops

Digital Healthcare

Software- & App-Entwicklung

Consultings & Trainings

- ⇨ gesamtheitliche Informationssicherheit
- ⇨ Resilienz stärken!

Michael Bendl & Gerlinde Macho

MP2 auf LinkedIn

MP2 IT-SOLUTIONS