solbytech it-security

Einführung ISMS nach ISO 27001

Vorgehensweise, Kompetenzen & Maßnahmen

TÜV AUSTRIA

certified DATA & IT SECURITY EXPERT

AUSTRIA TECHNOLOGY WIZARDS

Einführung ISMS nach ISO 27001

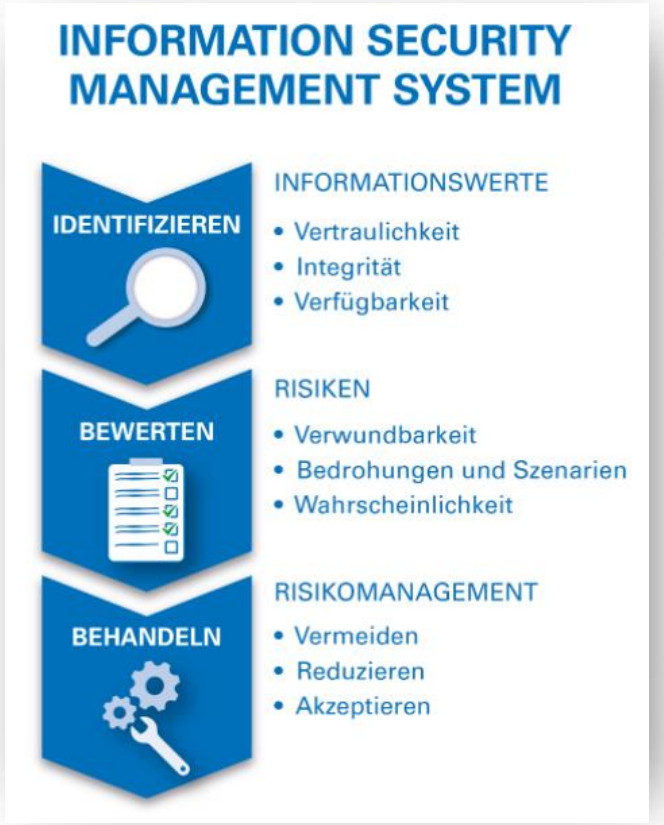
solbytech it-security

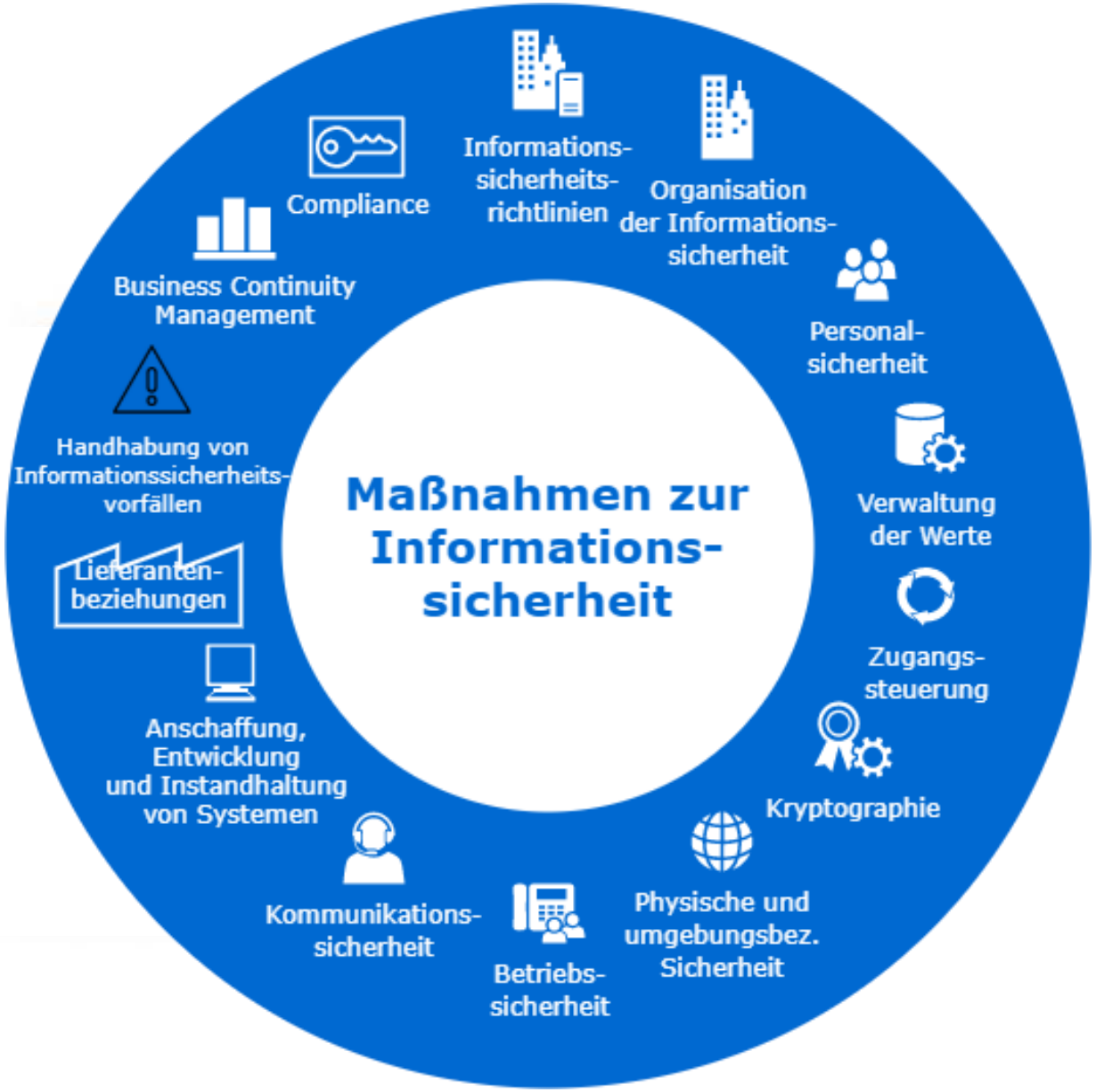
Sicherheit ist kein Produkt
→ Sicherheit kann nicht erkauft, Sicherheit muss erschaffen werden. Natürlich wird zum Schaffen von Sicherheit auch auf vorhandene Produkte zurückgegriffen.

Sicherheit ist kein Projekt
→ Es genügt nicht, Sicherheit einmal zu schaffen, sondern Sicherheit muss aufrecht erhalten werden. Aufbau und Aufrechterhaltung von Sicherheit wird auch teilweise in Projekten abgewickelt.

Informationssicherheit ist ein Prozess!

Überblick ISMS





Roadmap Einführung ISMS nach ISO 27001

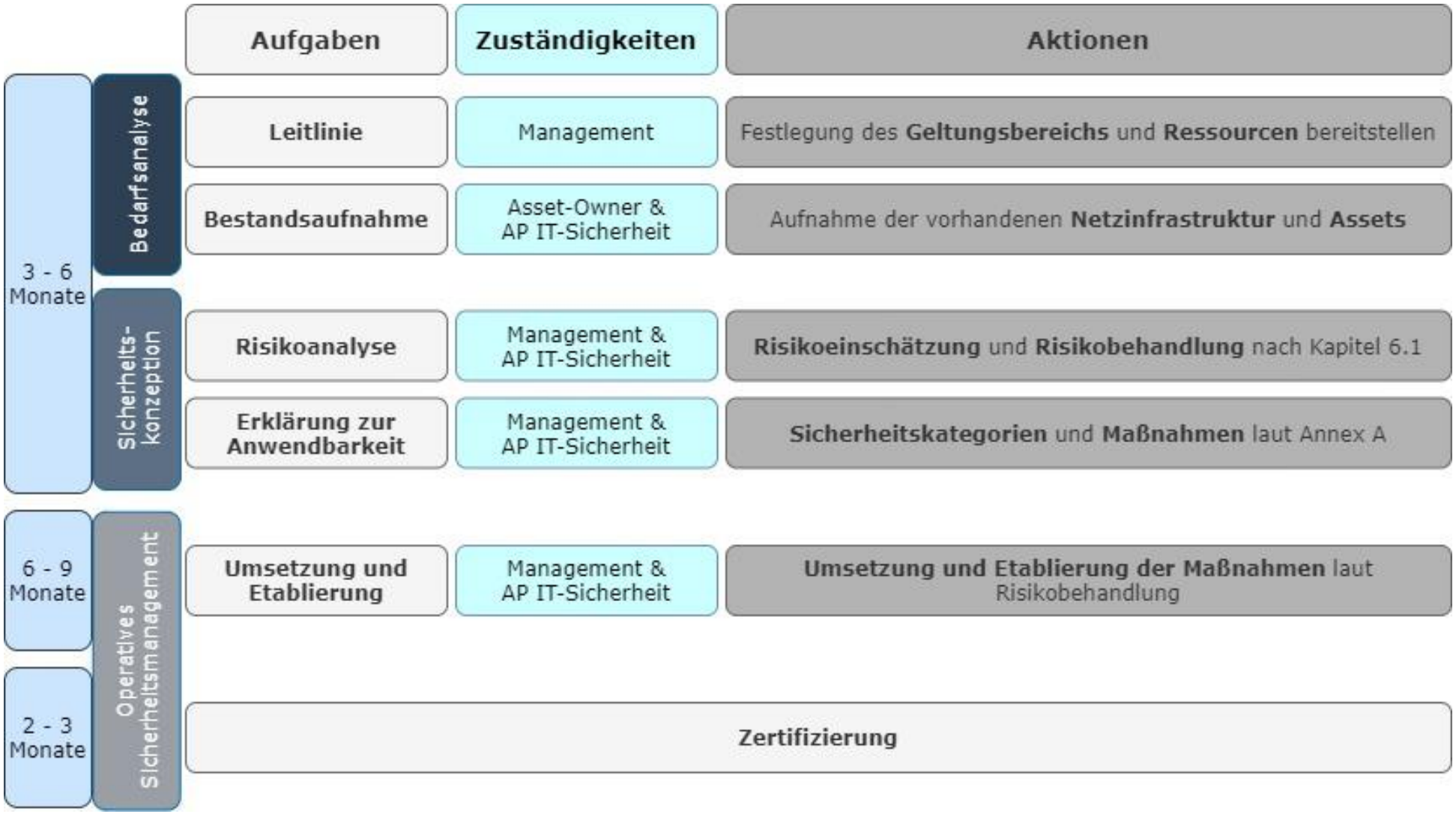
solbytech it-security

Bedarfsanalyse | **Sicherheitskonzeption** | **Operatives Sicherheitsmanagement**

IST-Aufnahme	Definition Anwendungsbereich	Definition Sicherheitsziele und Policy	Risiko-Management	Festlegung Maßnahme	Umsetzung IS-Maßnahme	Überwachung & Verbesserung
•Sicherheitsleitlinie erstellen •Verantwortlichkeiten •Richtlinien •Risikosituation •Ressourcen, Kompetenzen •Erfassung physischer und technischer Maßnahmen •Bestandsaufnahme Netzinfrastruktur •Prozesse zur Messung und Überwachung	•Identifikation der Assets/Werte •Identifikation der relevanten internen/externen Aspekte •Identifikation der Anforderungen Dritter •Identifikation der Schnittstellen zwischen internen und extern ausgeführten Aufgaben	•Identifikation von Sicherheitszielen aus Prozessen •Festlegung der Organisationsstruktur des Sicherheits-managements •Ermittlung der benötigten Ressourcen •Definition von Verantwortlichkeiten •Definition von Messmethoden •Definition von Kommunikations-strukturen	•Festlegung eines Risikomanagement-prozesses •Festlegung von Risikokategorien und –kriterien •Definition des Risiko-Owners •Durchführung von Risikoanalysen •Festlegung angemessener Maßnahmen zur Risikobehandlung •GAP-Analyse bestehendes ISMS •Erstellung SoA	•Festlegung der notwendigen Ressourcen •Personalanforderung und erforderliche Kompetenzen festlegen •Konzeption der Prozesse (Incident-Behandlung, Dokumentation, interne Audits etc.) •Maßnahmen laut Risikoanalyse priorisieren, planen und konzeptionieren	•Umsetzung der Maßnahmen und Prozesse laut Risikoanalyse •Erkennung und Analyse von Sicherheitsvorfällen •Durchführung von Sensibilisierungs- und Schulungsmaßnahmen •Regelmäßige Durchführung von Risikoanalysen und Anpassung des Risiko-behandlungsplans	•Wirksamkeit der Maßnahmen und Prozesse messen •Durchführung von internen Sicherheits- und Lieferantenaudits •Durchführung von Management-bewertungen •Abweichungen korrigieren •Verbesserungs-möglichkeiten umsetzen
Ergebnis → Dokumentierter IST-Zustand	**Ergebnis →** Geltungsbereich ist definiert und klar abgegrenzt	**Ergebnis →** Sicherheitsrichtlinie und Policy sind erstellt und veröffentlicht	**Ergebnis →** Risikoanalyse erstellt und Risiko-behandlungsplan definiert	**Ergebnis →** Geplante und konzeptionierte Maßnahmen	**Ergebnis →** Unternehmenseigene Sicherheitskonzeption ist umgesetzt	**Ergebnis →** Gemäß PDCA-Zyklus wird das ISMS überwacht und verbessert

Kommunikation und Changemanagement

Ablauf ISMS nach ISO 27001



Das Team

DI Manuel Dorfer, BSc

ZERTIFIZIERTER DATA & IT-SECURITY EXPERT

Florian Dodegge, MSc

ZERTIFIZIERTER ISMS MANAGER & AUDITOR NACH ISO 27001 TÜV®

DI Gerald Eder, BA

IT-SECURITY BERATER

KONTAKT solbytech

solbytech it-security

Schlossallee 7 | 5412 Puch/Hallein

Gewerbezeile 68 | 4202 Sonnberg

Zederhaus 155 | 5584 Zederhaus

www.solbytech-security.at

+43 660 5584007

security@solbytech.at

TÜV AUSTRIA

certified DATA & IT SECURITY EXPERT

AUSTRIA TECHNOLOGY WIZARDS