digitamondo

Stand Spätsommer 2025, Version 2.1

Digita Mondo, Inhaber Alex Schwerzmann . Schönenbergstrasse 24 . 8816 Hirzel
+41 44 520 13 89 . info@digita-mondo.ch . digita-mondo.ch

Inhaltsverzeichnis

0 Einleitung

0.1 Sinn und Zweck des Dokuments

Dieses Dokument soll dir in knappen Kapiteln Orientierung bieten, was du für eine möglichst rund laufende IT beachten kannst.

Dabei wird im ersten Teil ein kurzer Überblick über die Terminologien, Merkmale und Grundzüge von IT-Leistungen gegeben. Im zweiten Teil werden technische Merkmale festgelegt, die im Optimalfall überall erfüllt sind. Im dritten Teil findet sich eine Auflistung der Punkte, die auf Steuerungsebene beachtet werden sollten.Im vierten Teil findet sich zuletzt eine kleine Hilfestellung, wie in verschiedensten Situationen vorgegangen werden kann.

Der Anhang rundet die Sache mit dem Versuch ab, die verwirrende Vielzahl an Normen über einen Kamm zu scheren.

0.2 Nutzung

Falls du möchtest, darfst du das Dokument und die darin enthaltenen Ideen gerne selbst für private oder geschäftliche Zwecke nutzen.

Bei Fragen stehe ich gerne zu Verfügung:
Digita Mondo, Inhaber Alex Schwerzmann
Schönenbergstrasse 24
8816 Hirzel

✉ info@digita-mondo.ch +41 44 520 13 89

Bitte beachte, dass Digita Mondo sämtliche Haftung für die in diesem Dokument enthaltenen Inhalte ablehnt. Du wendest die hier aufgeführten Informationen sowie eventuell daraus gewonnen Erkenntnisse und Lehrblätze in kompletter Eigenverantwortung an.

0.3 Versionsgeschichte

Version	Bearbeitung	Datum	Autor
1	Initialversion	29.04.2025	Alex Schwerzmann
1.1	Zusammenführung mit Checkliste digitale Sicherheit	28.05.2025	Alex Schwerzmann
1.2	Erweiterung der Kapitel, Erstellung des Anhangs	04.06.2025	Alex Schwerzmann
1.3	Finalisierung der ersten zwei Kapitel	11.06.2025	Alex Schwerzmann
1.4	Finalisierung des dritten Kapitels	12.06.2025	Alex Schwerzmann
1.5	Revision bisheriger Inhalte	20.06.2025	Alex Schwerzmann
1.6	Finalisierung des vierten Kapitels, erster Version Normenmatrix	06.08.2025	Alex Schwerzmann
1.7	Zweite Version Normenmatrix, Blaupause Massnahmen ISMS	13.08.2025	Alex Schwerzmann
1.8	Aufgabe Normenmatrix (zumindest fast), Zusammenfassung der existierenden Standards	22.08.2025	Alex Schwerzmann
1.9	Erste redigierte Fassung	27.08.2025	Alex Schwerzmann
2.0	Zweite redigierte Fassung	29.08.2025	Alex Schwerzmann
2.1	**Erste Veröffentlichung**	**10.09.2025**	**Alex Schwerzmann**

1 Übersicht zu aktuellen IT-Gegebenheiten

1.1 Relevanz der Auslagerungsstufe

Heute bezieht praktisch niemand mehr seine IT-Leistungen exklusiv aus selbstverantworteten und -betriebenen Quellen.

Umso wichtiger ist es, die Art des Leistungsbezugs zu kennen, weil sich daraus Konsequenzen in der Verantwortlichkeit ergeben. Wichtig ist zu beachten, dass die Aufgaben im letzten Teil des Dokuments (Kapitel Error: Reference source not found) typischerweise nicht delegiert werden können – zumindest nicht die Verantwortung darüber.

1.2 Bezugsmodelle

Nach NIST existieren drei verschiedene „Stufen" von Service-Modellen. [Mell/Grance (2011)]

- **Infrastructure as a Service (IaaS):** Die technische Funktionsgrundlagen wie Speicher, Rechenleistung oder Netzwerke werden zu einem Lieferanten ausgelagert, damit eine Unternehmung eigene Serverbetriebssysteme, Applikationen und Services darauf aufsetzen kann.
- **Platform as a Service (PaaS):** Ein Lieferant kümmert sich um die Plattform (Betriebssystem), welche für eine Unternehmung das Ausrollen oder Installieren von eigenen Applikationen, Services oder Tools ermöglicht. Die zugrundeliegende Infrastruktur wird ebenfalls vom PaaS Lieferanten betrieben.
- **Software as a Service (SaaS):** Das „Rundum-Sorglos-Paket", welches einer Unternehmung die benötigte Software aus der Infrastruktur heraus anbietet. Typischerweise kommt diese Software mit heterogenen Client-Systemen zurecht (dank API oder Web-UI) und läuft komplett auf der Infrastruktur des Lieferanten. Der Leistungsnehmer hat keinen Einfluss auf die zugrundeliegenden Ebenen ausser bei ein paar Applikations-spezifischen Einstellungen.

Um das Konstrukt zu vervollständigen, wird in Anlehnung an swissICT noch folgendes Service-Modell hinzugefügt, welches dem gesamten Modell-Layer zugrunde liegt:

- **Facility as a Service** (**FaaS** [Hochuli u.a. (2013)], oder auch klassisches Server-Housing [Wikipedia (2025)]): Damit ist das Bedürfnis abgedeckt von Unternehmen, welche zwar eigene Hardware und eigene Komponenten betreiben wollen, aber selbst nicht das Rechenzentrum (RZ) stellen können, weil ihnen das Know-How oder die Ressourcen für beispielsweise ein FINMA- oder ISO 27001-zertifiziertes RZ fehlen.
- **Business Process as a Service (BPaaS):** Damit ist das zur Verfügung stellen von Geschäftsprozess-Anwendungen gemeint, welche komplett in der Cloud laufen und für eine Mehrkundenlandschaft erstellt wurden. [Anger u.a. (2014)]

Mit zunehmendem Funktionsumfang der Lösung werden dem Anbieter / Lieferanten immer mehr Verantwortlichkeiten übertragen und die Autonomie des Leistungsnehmers sinkt entsprechend, da die zugrundeliegenden Layer bereits integriert sind. Dies wird in der nachfolgenden Darstellung sehr schön verdeutlicht.

1.3 Verantwortlichkeiten im Outsourcing

Die nachfolgende Tabelle gibt einen Überblick über die verschiedenen Verantwortlichkeiten, welche idealerweise auch vertraglich entsprechend als ausgemacht gelten zwischen Leistungserbringer und -bezüger.

Aufgabe \ Modell	Managed Service	SaaS	PaaS	IaaS	FaaS	Lokal
Informationen und Daten (Inhalte)						
Konten und Identitäten (Erfassung der echten Personen)						
Geräte (Handy, Tablet, PC, Laptops, Drucker etc.)						
Identitätsverwaltung und Verzeichnisinfrastruktur						
Anwendungen						
Netzwerksteuerung (Durchsatz, Erreichbarkeit etc.)						
Betriebssystem (Aktualität, Sicherheit, Verfügbarkeit)						
Physische Serversysteme						
Physisches Netzwerk						
Physisches Rechenzentrum						

Quelle: Shared responsibility in the cloud - Microsoft Azure | Microsoft Learn

Leistungserbringer Leistungsbezüger Geteilt

1.4 Cloudsourcing

Von der „Cloud" haben die meisten Benutzer heute eine Vorstellung. Dennoch erstaunt es, wie unscharf Cloud oder auch SaaS auch heute noch ausgelegt wird – oft zum (verkäuferischen) Vorteil der Anbieter.

1.4.1 Definition eines Cloud-Service

Bereits vor Jahren hat das NIST einen Cloud-Dienst wie folgt definiert:

- ✓ **Auf Abruf** steht der Service bereit und erfordert keine menschliche Interaktion.
- ✓ Der Service wird über das **Internet** bereitgestellt und kann **auf beliebige Plattformen** ausgerollt werden.
- ✓ Die Ressourcen des Cloud-Lieferanten (Speicher, Rechenleistung, Arbeitsspeicher und Bandweite) können **dynamisch um- und verteilt** werden.
- ✓ Die Services **skalieren** – im Bedarfsfall automatisch – mit der Anfrage.
- ✓ Die Benutzung der Services ist **klar mess- und ausweisbar** und kann auch **überwacht** werden.

Die Definition gilt aus meiner Sicht auch heute noch uneingeschränkt, bringt aber auch im KI-Zeitalter noch einige Anbieter, die mit dem Schlagwort Cloud ihre Werbekampagnen fahren, in Verlegenheit.

1.4.2 Entstehung

Entstanden ist der Begriff des „Cloud Computing" aus einer Umschreibung des „World Wide Computers" durch Eric Schmidt, der damit die Möglichkeit des Internets beschrieb, beliebige Rechenoperationen auszuführen und auf mehrere Rechnerknoten zu verteilen. Er nannte dies „the computer in the cloud". Ein Cloudsourcing entspricht also der Auslagerung von IT-Leistungen in die (meist Public – also öffentlich erreichbare) Cloud. Natürlich können Cloud-Konzepte auch nur für sich selbst betrieben werden. Dann spricht man von Private Cloud.

1.5 Managed Services

Eine relativ junge Disziplin in der Erbringung von IT-Dienstleistungen ist die Sparte der Managed Services. In der Darstellung in Kapitel 1.3 ist die Kategorie eingebaut und fungiert als Polarität im Sinne maximal ausgelagerter Verantwortlichkeit. Typischerweise werden bei Managed Services mehrere IT-Leistungen zu einem Produkt zusammengesetzt. Der Bezüger erwartet ein jederzeit funktionierendes und nutzbares IT-Ökosystem. Folgende Gründe können für Leistungsempfänger den Bezug von Managed Services attraktiv machen.

Der Leistungserbringer

- muss jederzeit über kompetentes Personal auf dem letzten Stand der Dinge verfügen. Eigene Kompetenzaneignung beim Kunden entfällt. Dadurch wird der Leistungsbezüger auch von personellen Abhängigkeiten entlastet – oder das verfügbare Personal darf sich weniger mit technischen Herausforderungen als vielmehr mit der geschäftlichen Integration der eingekauften Technologie auseinandersetzen.
- entbindet den Bezüger von der Last, die eierlegende Wollmilchsau des EINEN IT-Verantwortlichen zu finden, der intern von Support-Anfragen bis komplexen Data Governance-Themen alles können und wissen sollte. Damit übersteigt der Leistungsumfang eine solchen Services typischerweise auch das, was eine interne IT im KMU-Umfeld zu leisten vermag.
- kümmert sich um die Partnerstati, Verträge, Absicherungen und die Einhaltung der relevanten Sicherheitsbelange (Verfügbarkeit, Integrität, Konformität).
- hat ein hohes Interesse an Standardisierung und möglichst wenigen Ausfällen oder anderen Leistungen, die er auf eigene Kosten erbringen muss. Entsprechend kann von einer hohen Stabilität und Verfügbarkeit der Leistung ausgegangen werden, weil alles andere für den Leistungserbringer ökonomisch höchst unattraktiv wäre.
- bedenkt oft den kompletten Lebenszyklus des Services. Eine Ausarbeitung und möglicherweise Überführung in ein Nachfolgeprodukt ist am Ende des Lebenszyklus' also bereits mit eingeplant und eingerechnet.
- hat bessere Chancen, die Skaleneffekte, welche von Coud-Modellen versprochen werden, auch tatsächlich zu erreichen, da er deutlich mehr Manipulationsmasse einbringen kann, weil er mehrere Kunden bedient.
- nimmt dem Bezüger überraschend auftretende Arbeiten (bspw. Ausfall eines Servers) ab und erledigt dies im Hintergrund unter Aufrechterhaltung der vertraglich vereinbarten Leistungsmerkmale.

Im obigen Sinne ist Managed Service also ein Modell, wie IT-Leistungen bezogen werden können, welches aber nicht zwingend an die Örtlichkeit der Services gebunden ist. Es wäre denkbar, Managed Services für Infrastruktur zu beziehen, die man am eigenen Standort betreibt.

1.6 IT-Mensch-Paradox

Die IT hat in den letzten 20 Jahren enorm an Bedeutung gewonnen. Entsprechend ist auch sowohl die Dominanz als auch das Mitbestimmungsrecht der IT-Themen gestiegen.
Je länger je mehr stehen aber technokratisch motivierte Entwicklungen und ureigene Interessen der Benutzerschaft im Widerspruch. Es scheint teilweise so, als ginge vergessen, dass IT nach wie vor ein Werkzeug – also ein Mittel – und kein Zweck darstellt.

Die Komplexität der mittels Managed Services ausgelieferten IT-Produkte hat in den letzten Jahren unglaublich zugenommen und führt heute zu massiven Hürden in der Nutzung dermassen ausgeklügelter IT-Lösungen, wie sie noch nie zuvor möglich waren. Dabei ändert auch die inflationäre Einführung von KI in allen Produkten und Lösungen wenig. Auch KI ist a priori ein Werkzeug, welches kompetente Benutzer um ein vielfaches beschleunigen kann, einem aber nicht von der Arbeit des Verstehens und Anwendens befreit (Stichwort Plausibilisierung).

Deshalb gilt es, folgende grundlegenden Interessenskonflikte zu erkennen und in einem partnerschaftlichen Verhältnis mit dem Leistungserbringer zu klären:

Kategorie	Interesse IT	Interesse Kunde
Genutzte Lösungen	Einsatz von Standardlösungen	Einsatz möglichst massgeschneiderter Lösungen; Bereitstellung der notwendigen Flexibilität für Profile wie SW- und HW-Entwickler, Service-Techniker, Data Scientists, Inginieure etc.
Bezugsart	**Sicheres**, mobiles Arbeiten	Ungehindertes Arbeiten
Abgrenzung	Möglichst viele Optionen und Wege, Leistungen abzugrenzen (Versicherungssyndrom)	Einfache (Pauschal-)Service- und Preisstruktur, tiefe (Sprung-)Fixkosten, hohe Absehbarkeit und damit Budgetierbarkeit der wiederkehrenden IT-Kosten
Finanzierung	Wiederkehrend abgesicherter Umsatz (Jahresverträge).	Optimales Preis-/Leistungsverhältnis über die gesamte Abschreibungsdauer / Vertragslaufzeit. Das kann bei liquiden Unternehmen auch eine einmalige Anschaffung bedeuten.
Technologie	Einführung von zentralen Paradigmen wie Single Sign-On, Geräteverwaltung, Selbstbedienung/Autonomie und technischen Standards auf aktuellen Software-Ständen.	Berücksichtigung von gesetzlichen und moralischen Verpflichtungen der eigenen Mitarbeiterschaft gegenüber; Respektieren der Privatsphäre und privater Mittel der Mitarbeitenden.
Lösungsdiversität	Konsolidierung der Anwendungslandschaft, Überführung in ein Paradigma	Betrieb von Nischenlösungen, Aufrechterhaltung von Spezialfällen aufgrund verschiedenster Gründe (strategische Erfolgsfaktoren, Mitarbeitermotivation, «es war schon immer so», Projektbudgets einsparen etc.)
Maturität der Anwender	Wenig Supportleistungen, hohe Maturität beim Anwender	Jemand, der da ist und hilft

2 Checkliste digitale Sicherheit (das T der TOM)

2.1 Zutritte und Zugriffe

Der Zugriff auf meine Daten (physisch und digital) ist geschützt durch:

- ☐ Absperrungen (Schlösser, Zäune, Firewalls etc.)
- ☐ Autorisierungsverfahren (Passwörter, Codes etc.)
- ☐ Zugriffsdokumentation (Videoüberwachung, Serverlogs etc.)
- ☐ Alarmmechanismen (virtuelle und physische) bei Nicht-Einhaltung der Vorgaben
- ☐ Individuelle Wiedererkennungsmerkmalen zwecks Erschwerung von Phishing (bspw. Branding der Loginseite etc.)

2.2 Identitäten

- ☐ Meine Zugänge sind mit einem (ausreichend komplexen) Passwort geschützt oder es wird ein Identitätskonzept mit passwortlosem Zugriff umgesetzt.
- ☐ Ich verwende dasselbe Passwort nicht mehrmals.
- ☐ Meine Zugänge sind mit einem zweiten Faktor geschützt.
- ☐ Ich setze Phishing-resistente MFA-Methoden ein (FIDO2 Token oder Zertifikate)
- ☐ Ein Passworttreser ermöglich komplexe und geteilte Passwörter mit MFA
- ☐ *Optional: Meine Zugänge sind an meine Biometrie gebunden.*

2.3 Datenhaltung

- ☐ Meine Daten befinden sich ausschliesslich auf verschlüsselten Datenträgern.
- ☐ Meine Daten sind nicht öffentlich einsehbar.
- ☐ Meine Kommunikation und mein Zugriff auf Daten erfolgt ausschliesslich über gesicherte Verbindungen (SSL / TLS). Wo physikalische Daten «transportiert» werden, geschieht dies in abgeschlossenen Behältern.
- ☐ Meine Daten befinden sich in der Schweiz (Rechenzenter-Standort).
- ☐ Die Berechtigungsstruktur ist so gewählt, dass die Benutzer so wenig wie möglich aber so viel wie nötig (tägliche Arbeit nicht behindert) einsehen können
- ☐ Die Zugriffe auf Anwendungen und Daten werden überwacht und dokumentiert.
- ☐ *Fortgeschritten:* Weiterführende Zugriffe oder Aktivitäten mit erhöhten Rechten sind mit einem Autorisierungskonzept oder mit Siegeln (mit entsprechendem Prozess) abgesichert.
- ☐ *Fortgeschritten: Der Zugriff auf Anwendungen und Daten erfolgt über ein Zero-Trust-Konzept.*
- ☐ *Fortgeschritten: Data Loss Prevention-Systeme (DLP) verhindern ungewollten und unkontrollierten Datenabfluss aus der Unternehmung.*
- ☐ *Fortgeschritten: Meine Daten befinden sich bei Anbietern, für die der US Cloud Act sowie Safe Harbour nicht gelten.*

2.4 Integrität

Folgende Lösungskomponenten sichern die Datenintegrität ab (Stichwortartig):

- ☐ S/MIME für E-Mailverkehr
- ☐ Intrusion Detection System (IDS)
- ☐ Endpoint/Cross Detection & Response (EDR / XDR)
- ☐ Mobile Device Management (MDM)
- ☐ Mobile Application Management (MAM)
- ☐ 7/24 Security Incident & Event Management (SIEM)

2.5 Verfügbarkeit

2.5.1 Backup

- ☐ Ich habe ein Backup
- ☐ Das Backup wird in einem für mich passenden Turnus ausgeführt und regelmässig überprüft
- ☐ Das Backup befindet ist nicht direkt mit dem Speicherort der gesicherten Daten verbunden (bspw. nicht ein USB-Stick, der dauernd am Computer angeschlossen ist, an dem ich täglich arbeite)
- ☐ Das Backup befindet sich physikalisch an einem anderen Ort
- ☐ Das Backup ist verschlüsselt.
- ☐ 3-2-1-Regel erfüllt (drei Kopien auf zwei unterschiedlichen Medien, davon eine offsite).
- ☐ Das Backup kann wiederhergestellt werden.

2.5.2 Kontinuität

- ☐ Ich nutze für kritische Komponenten eine USV mit Überspannungsschutz
- ☐ Ich habe für kritische Komponenten Brandschutzmassnahmen getroffen
- ☐ Kritische Infrastruktur ist redundant ausgelegt:
  - ○ Festplatten (RAID)
  - ○ Server (Cluster)
  - ○ Georedundanz
  - ○ Verbindungsredundanz

2.6 Endpunkte

2.6.1 Schutz

- ☐ Es ist eine Antivirus installiert, welche regelmässig Updates erhält und virtual Patching unterstützt.
- ☐ Es werden regelmässig Betriebssytem-Updates gemacht.
- ☐ Das eingesetzte Betriebssytem wird vom Hersteller weiterhin unterstützt.
- ☐ Die Systeme werden überwacht und regelmässig gewartet.
- ☐ Automatisiertes Penetrationtesting rundet das Ganze ab, um Lücken zu erkennen. [Lumturo Einbruch!]
- ☐ Netzwerkknoten, über welche Daten ins System eingehen, werden mit entsprechenden Scannern geschützt (Mail-Washing, Dateiaustauschplattformen etc.).
- ☐ *Fortgeschritten: Meine Mitgliedschaft in einem Bug Bounty Programm fördert Schwachstellen frühzeitig zutage.*

2.6.2 Verwaltung

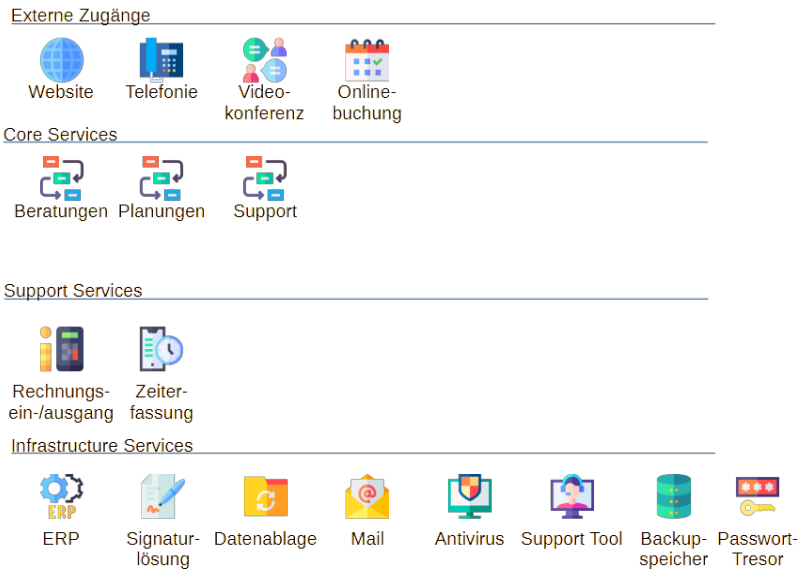
- ☐ Die eingesetzten Anwendungen schützen sich vor missbräuchlichem Zugriff mit entsprechenden Richtlinien.
- ☐ Der Geräteinventar ist jederzeit in einem kontrollierbaren Zustand.
- ☐ Geräte kommen kontrolliert hinzu und verlassen die Umgebung ebenso geordnet.
- ☐ Es werden Geräteanforderungen gestellt und automatisch überprüft, ob diese eingehalten sind.
- ☐ Bei Nichteinhaltung werden entsprechende Massnahmen ergriffen.

3 Checkliste Führung (das O der TOM)

3.1 Ökosystem / Service-Architektur [Lumturo Landkarte]

Wer einen Inventar seiner genutzten Anwendungen / IT-Services führt, dem fällt es leicht, die wichtigsten Zusammenhänge auf eine kleine Landkarte zu packen. Untenstehende Darstellung führt ein vereinfachtes Beispiel einer solchen sehr einfachen Landkarte auf:

Diese wird unterstützt von einer entsprechenden Servicelandschaft:



3.2 Realistisches Bild der eigenen Lage

Um eine realistische Einschätzung der eigenen Lage zu erhalten, helfen verschiedene Werkzeuge aus einschlägiger Fachliteratur (Suchstichwort Enterprise Architecture). Hier wird ein Maturitätsmodell von Ross et all vorgestellt [Ross et all. 2006]:

Stufe / Bereich	Geschäftssilos	Standardisierte Technologie	Optimierter Kern	Geschäftsmodularität
IT-Kapazität	Lokale IT-Anwendungen	Gemeinsam genutzte technische Plattformen	Unternehmensweit vereinheitlichte Prozesse oder Daten	«Plug-And-Play» Geschäftsprozessmodule
Geschäftsziele	ROI von lokalen Geschäftsinitiativen	Reduzierte IT-Kosten	Kosten und Qualität von Geschäftstätigkeiten	Zeit zur Marktreife; strategische Agilität
Förderschwerpunkt	Individuelle Anwendungen	Gemeinsam genutzte Infrastrukturleistungen	Unternehmensanwendungen	Wiederverwendbare Geschäftsprozesskomponenten
Schlüsselfähigkeiten im IT-Management	Technologiebasiertes Changemanagement	Standards entwerfen und aktualisieren; Finanzierung gemeinsam genutzter Leistungen	Unternehmenskritische Geschäftsprozesse definieren und messen	Verwaltung wiederverwendbarer Geschäftsprozesse
Wer definiert Anwendungen?	Leitung lokaler Geschäftseinheiten	IT und Leitung Geschäftseinheit	Geschäftsleitung und Prozessverantwortliche	IT, Geschäftsleitung und Branchenführer (ev. Konsortien)
Hauptanliegen der IT-Governance	Werte kommunizieren und messen	Lokale, regionale und unternehmensweite Verantwortlichkeiten etablieren	Projektprioritäten mit Architekturzielen abgleichen	Geschäftsmodule definieren, finanzieren und beziehen
Strategische Auswirkungen	Lokale / funktionale Optimierungen	IT-Effizienz	Operative Exzellenz	Strategische Agilität

Für jede Stufe gelten eigene Regeln und Logiken. Konsequenzen für die eigenen Möglichkeiten ergeben sich auch aus den aus der aktuellen Stufe resultierenden Beschränkungen und Eigenarten. Zu wissen, wo man als Unternehmen steht, hilft die Erwartungshaltungen und eigenen Möglichkeiten realistisch einzuschätzen.

3.3 Kosten [Lumturo Kosten]

IT-Kosten sind so eine Sache: für den Chef immer zu hoch, aus Angestellten-Sicht «dörft's äs bizzeli meh sy».

Es macht Sinn, sich die eigenen IT-Kosten in Relation zu folgenden Ausgabeposten und in Relation zur Wichtigkeit für den Fortbestand der Unternehmung anzuschauen:

- ☐ Arbeitsplatzkosten pro Mitarbeitende/r
- ☐ Lohnkosten / Sozialabgaben pro Mitarbeitende/r
- ☐ Branchenvergleich
- ☐ Sonstige Auslagen
- ☐ Strategische Stossrichtung der Unternehmung

Mit diesem Wissen werden Diskussionen weniger emotional geführt und Finanzen effektiver eingesetzt.

3.4 Trends [Lumturo Trends]

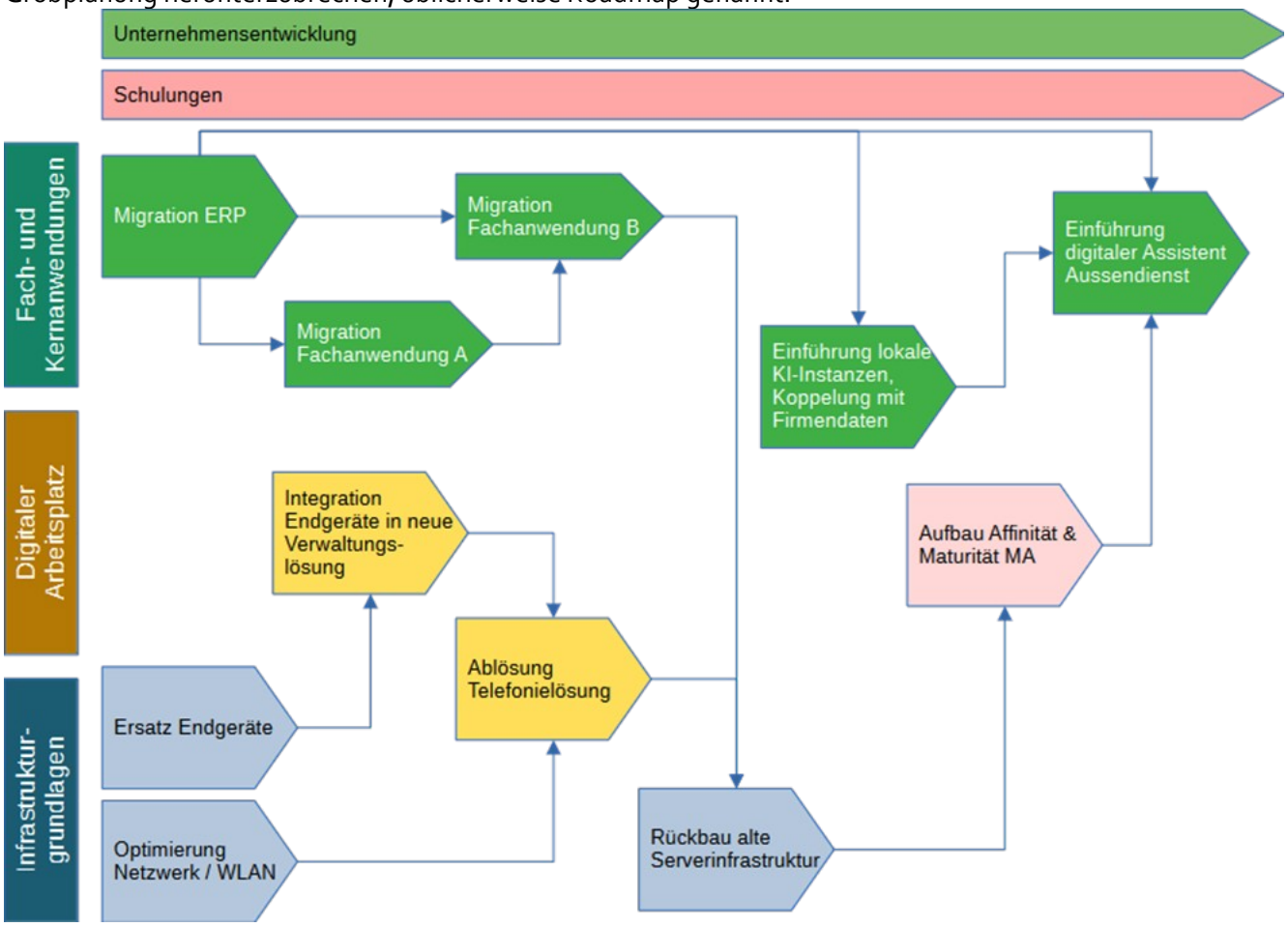
Es ist wichtig, die IT- und Branchentrends zu kennen. Diese Kenntnisse helfen, einzuordnen, was andere machen und welche Technologie eventuell das eigene Geschäftsfeld in den nächsten Jahren komplett umkrempeln wird. Dazu liefern verschiedene Hersteller aus Eigennutz bereitwillig Informationen. Beliebte Formate sind:

- ☐ Gartner Hypecycle
- ☐ IT-Trends - Capgemini
- ☐ Das Trendradar des Zukunftsinstituts resp. Die Megatrendmap des Zukunftsinstituts
- ☐ Publikationen des Gottlieb Duttweiler Instituts Creating Futures | GDI Gottlieb Duttweiler Institute
- ☐ Branchenverbände der entsprechenden Unternehmung

Tragisch aber nicht unwahr: wer wissen will, welche Technologie demnächst relevant wird, sollte schauen, was in Kriegen eingesetzt wird. Oder wie Herkaklit sagte: «Bellum pater est omnium.» (Krieg ist der Vater aller Dinge.)
Somit ist es hilfreich, einen kleinen Katalog der relevanten Veränderungen innerhalb und ausserhalb der eigenen Unternehmung zu führen und diesen regelmässig zu beraten und ggf. nachzuziehen. Daraus können spannende Geschäftsideen oder -erleichterungen entstehen oder auch Risiken frühzeitig erkannt werden.

3.5 IT-Roadmap [Lumturo Routenplanung]

Hat man sich ein Bild der Ausgangslage gemacht, lohnt es sich, die geplanten Unternehmungen auf eine Grobplanung herunterzubrechen, üblicherweise Roadmap genannt:



Diese Vorhaben gilt es dann, schrittweise und in verträglichen Einheiten umzusetzen.

3.6 Geltende Rahmenbedingungen

3.6.1 Gesetze

- ☐ DSG
- ☐ GeBüV
- ☐ OR, ZGB, Arbeitsgesetz
- ☐ Fernmeldegesetz, BÜPF
- ☐ ZertES / eIDAS
- ☐ URG / URV
- ☐ DSGVO (EU)
- ☐ […]
- ☐ Auch von Aussenstellen
- ☐ Auch von Dienstleistern / aus Verträgen

3.6.2 Interne Vorgaben

- ☐ Verträge
- ☐ Geklärte Kompetenzen und Befugnisse
- ☐ Regelungen
- ☐ Meldewege
- ☐ Vorgehen bei Vorfall X
- ☐ Unité de Doctrine bezüglich eingeforderter Dokumente, Unterlagen etc. (bspw. Auftragsdatenvereinbarung und Geheimhaltungsvereinbarungen wo nötig)

3.7 Daten / Inventar

Wichtig ist, dass du die eigenen Daten, deren Speicherorte sowie deren Klassifizierung kennst.

3.7.1 Ablageorte

- ☐ Physische Ablagen (Fächli, Bürotische etc.)
- ☐ Dateiablagen
- ☐ E-Mail (ACHTUNG: Der Posteingang kann durchaus heikle Informationen enthalten)
- ☐ ERP / CRM
- ☐ Austauschplattformen
- ☐ Fachanwendungen / deren Datenbanken
- ☐ …

3.7.2 Datenkategorien

- ☐ Identitätsdaten
- ☐ Kontaktdaten
- ☐ Beschäftigtendaten
- ☐ Forschungsdaten
- ☐ Finanzdaten
- ☐ Lebensgewohnheiten / Profile
- ☐ öffentliche Informationen

3.7.3 Besondere Datenkategorien

- ☐ rassische oder ethische Herkunftsdaten
- ☐ politische Meinungen
- ☐ religiöse / weltanschauliche Überzeugungen
- ☐ Sexualleben und sexuelle Orientierung
- ☐ Biometrische Daten
- ☐ Gesundheitsdaten
- ☐ Genetische Daten
- ☐ Gewerkschaftszugehörigkeit

3.7.4 Lebenszyklus von Informationen

Entsprechende Überlegungen stellen folgendes sicher:

- ☐ sichere und adäquate (ergo keine Vorratsdatenspeicherung) Aufbewahrung von Informationen
- ☐ sichere Vernichtung von Informationen am Ende des Lebenszyklus (Akten, Datenträger, Backups)
- ☐ auf welchen Geräten / an welchen Orten werden die Daten bearbeitet? Sind die Schutzmassnahmen gem. Kapitel 2 getroffen?

3.8 Lieferanten-Management

- ☐ Anwendungsinventar: Welche Anwendungen sind für die Aufrechterhaltung des IT-Betriebs relevant?
- ☐ Ist der Kontakt bekannt (kommerziell, technisch)?
- ☐ Verträge / SLA abgeschlossen und geprüft?
- ☐ Prozess klar (intern und Anlaufstellen Lieferant)?
- ☐ Datenhaltung geklärt?
- ☐ Liefermodell (BpaaS, SaaS, PaaS, IaaS)
- ☐ Normen erfüllt (Zertifizierungen, Standards, Regulatorische Bedingungen, Aussenstelle oder Hauptsitz in den USA?)

3.9 Risiken [Lumturo Risiko]

- ☐ Geschäftsrisiken erarbeitet?
- ☐ Involvierte Anwendungen / Systeme bekannt? (Organisation, Prozesse, Daten, Systeme)
- ☐ Geschäftsrisiken quantifiziert (Eintrittswahrscheinlichkeit x Schadensausmass x Gefährdung)?[1]
- ☐ Auslöser (ADE[2]) und Auswirkung auf Grundgut (CIA[3]) bekannt?
- ☐ Gefahren und mögliche Antworten bekannt (bspw. SANS CSC)?
- ☐ Verbindung zwischen IT-Gefahren und Geschäftsrisiken gemacht?
- ☐ Bewältigungsstrategien erarbeitet (Adressieren, Verlagern (Versicherung), Akzeptieren)?
- ☐ Wirksamkeit der Bewältigungsstrategien / Massnahmen überprüft?

3.10 Kontinuitätsplanung [Lumturo Geschäftskontinuität]

- ☐ Wer ein Plan hat, musste sich zumindest theoretisch mit einer Lösung eines potenziellen Problems auseinandersetzen.
- ☐ Wer sich der Situation im Rahmen eines Planspiels ausgesetzt hat, hat bessere Einsicht darin, inwiefern der Plan funktionieren könnte.

3.11 Weitere Massnahmen

- ☐ Vulnerability Disclosure Program helfen, ethischen Hackern Anreize zu geben, Lücken aufzudecken[4]
- ☐ Saubere Aufarbeitung nach dem Eintreffen eines Vorfalls hilft, die nötigen Lehren für den nächsten Vorfall zu ziehen.
- ☐ Sogenannte Security Awareness Trainings helfen, die Affinität der Angestellten auf einem zeitgemässen Niveau zu halten. Oft bieten Cybersecurity-Versicherungen ein entsprechendes Produkt kostenlos an. Dieses wird leider teilweise schlecht kuratiert, weshalb sich ein Angebot einer spezialisierten Unternehmung lohnen kann.
- ☐ Den Angestellten kommunizierte Erwartungshaltungen ermöglichen ein besseres Verständnis der benötigten Vorsicht im Umgang mit IT-Mitteln. Oft werden diese Informationen in Form von Richtlinien, Acceptable Use Policy oder IT-Sicherheitsweisungen in einem Anhang zum Arbeitsvertrag aufgeführt oder ins Mitarbeiterhandbuch integriert.

3.12 Audits

Durch eigene oder delegierte Audits (bspw. ISO-Zertifizierung des Anbieters) wird sichergestellt, dass dieser (grundlegende) Anforderungen erfüllt. Vorort-Kontrollen in beteiligten IT-Infrastrukturen können das Bild vervollständigen.

[1] Single Loss Expectancy (SLE) und Annual Loss Expectancy (ALE)
[2] A = Accidential (durch Versehen), D = (aus Absicht), E = Environmental (durch Umwelteinflüsse)
[3] C = Confidentiality (Vertraulichkeit), I = Integrität, A = Availability (Verfügbarkeit)
[4] Bspw. unter Mitwirkung bei Gemeinsam für eine sichere Schweiz - Bug Bounty Switzerland

4 Hilfestellungen und Anleitungen

4.1 Ist dies ein Phishing-Email?

Typischerweise kommen Betrugsmaschen mit einem oder mehreren der folgenden Anzeichen daher:

- **Dringlichkeit:** Oft wird aus mehr oder weniger naheliegenden Gründen Termindruck aufgebaut (Ablauf eines Kontos, unwiderbringliche Chance, nicht zustellbares Paket etc.).
- **Fordernd:** Die Art und Weise der Aufforderung lässt kein Zweifel daran, was jetzt zu tun ist. Oft ist die Ansprache auch sehr autoritär.
- **Klick:** Es wird aufgefordert, einen Link anzuklicken (beliebt sind auch Links wie www.google.ch [das L ist ein grosses I])
- **Information:** Es wird eine Eingabe / Angabe gefordert, gerne auch gerade mal eben das komplette Login durchgespielt inkl. zweitem Faktor.
- **Unüblich:** Das Vorgehen fühlt sich – offensichtlich oder nicht – irgendwie unüblich an.
- **Sensible Informationen:** Grundsätzlich gilt: Keine sensiblen Informationen wie Zugangsdaten, persönliche Daten etc. preisgeben (ganz allgemein eine gute Idee im Zeitalter von per Gesetz erlaubter Überwachung).

ACHTUNG: mit den jüngsten KI-Möglichkeiten ist es möglich, sehr passgenaue Angriffsmails zu senden. Dies, weil Angreifer sich – ähnlich einem Schneeballsystem – durch bereits gekaperte Postfächer hangeln und dort den Mailverkehr mit den nächsten Empfängern des zuvor mitlesen und analysieren kann. Du erwartest ein Handbuch zu deinem neu eingekauften CRM: hier hast du es – angereichert mit einem netten kleinen Trojaner oder verbunden mit der Aufforderung, dich bei Microsoft nochmals anzumelden.

Am einfachsten können diese Tatsachen jeweils überprüft werden, indem man das Information komplett ignoriert und den Absender kurz auf einem anderen Kanal kontaktiert oder selbstständig auf der bekannten Herstellerseite direkt anmeldet und schaut, ob dort ähnliche Information bereitliegt. Typischerweise sind bei echten Aufforderungen das Webportal und die E-Mail identisch in der Aufforderung (bspw. Überprüfung der hinterlegten Handynummer für Zweifaktorauthentifizierung).

4.2 Ist es zu spät?

Dass es bereits geschehen ist, lässt sich an folgenden Merkmalen festmachen:

- Nach dem Klicken / Eingeben von Informationen geht der Prozess nicht wie in der E-Mail angekündigt weiter (bspw. das Paket kommt nicht,)
- Das eigene Gerät verhält sich plötzlich anders:
  - Lüfter dreht voll
  - Leistung bricht ein
  - Festplatte läuft voll
  - Computer stürzt ab
  - Computer verselbstständigt sich (Fenster öffnen und schliessen, Popups tauchen auf, E-Mails werden ohne zutun versendet oder Geschäftspartner melden sich, ob die Nachricht tatsächlich von einem selbst stammt…)
- Das angekündigte Handbuch liegt nicht dort, wo die Mail versprach, es liege dort.
- Über dein (Mail-)Konto laufen plötzlich sehr suspekte Aktivitäten oder du kriegst Rückmeldungen von Empfängern, dass eine Aktivität (E-Mail, Freigabe, Zugriff, Ausdruck etc.) in deinem Namen geschah, von der du nichts weisst.

In jedem Fall ist es nie zu spät, entsprechend zu reagieren. Je eher und je offener ein Vorfall kommuniziert wird, je besser kann Schaden abgewendet werden. Jede Fachperson weiss: es kann jeden treffen, die Angriffsmethoden werden je länger je ausgefeilter.

4.3 Ich bin darauf reingefallen

Und wenn ich geklickt habe?

- ☐ Tief durchatmen und bitte keine Selbstvorwürfe
- ☐ Betroffenen Computer vom Internet trennen
- ☐ Passwort wechseln (auch überall dort, wo dasselbe Passwort eingesetzt wird), Zweifaktormethoden prüfen, alle bestehenden Sitzungen zentral trennen
- ☐ Virenscanner laufen lassen
- ☐ Im Zweifelsfall Computer zurücksetzen (oder aufbewahren für die forensische Untersuchung, falls Strafanzeige gemacht wird)
- ☐ Logs prüfen
- ☐ Eventuelle weiterführende Schritte:
  - ☐ Meldung bei der Plattform/dem Anbieter, auf der/bei dem der Vorfall geschah
  - ☐ Meldung beim BACS
  - ☐ Anzeige erstatten

4.4 Risikomatrix

Entsteht gerade 😉

4.5 Incident Response Plan[5]

Aufgabe	Teilschritte
Organisation	
Ruhe bewahren und Überblick gewinnen	1. Situation erfassen 2. Sich an die eigenen Pläne und Überlegungen erinnern! 3. Sich in Gelassenheit und «Es ist keine Schande» üben 4. Vertuschung verhindern
Krisenstab einrichten	1. Wer wirkt in einer Delegation mit? Mit welcher Aufgabe/Verantwortlichkeit? 2. Braucht's externe Unterstützung? 3. Welche Aufgaben aus dem Tagesgeschäft können stattdessen liegengelassen werden? 4. Wer trifft Entscheidungen auf Basis welcher Quelle/Gremium? 5. Wer kommuniziert an wen wann?
Kriminalistische Fragen klären	1. Müssen Spuren gesichert werden (digitale Forensik) oder werden die Systeme schnell wieder aufgesetzt und in Betrieb genommen? 2. Anzeige erstatten (Achtung eventuelle Meldepflicht): 1. https://www.report.ncsc.admin.ch/de/ 2. https://www.suisse-epolice.ch/home
Kosten und Unternehmensfortführung	Es gibt zahlreiche Berichte, die davon erzählen, dass Unternehmen sich nach einem Sicherheitsvorfall nicht mehr erholt haben. Schnellstmöglich ist entsprechend eine wirtschaftliche Prüfung der Lage mit eventueller Äuffnung von Notbudgets zu starten.
Nachbereitung	Das Ereignis sollte – je nach Belastung auch zwecks «Psychohygiene der Betroffenen» – nachbesprochen werden. Fragen können sein: 1. Wie konnte es soweit kommen? Möglichst als sachliche Feststellung und ohne unterschwellige Schuldzuweisung. 2. Was ist noch ausstehend? Wie können künftig ähnliche Situationen verhindert werden? Dies muss aufgegleist werden, solange der Schmerz noch präsent ist. Kommt Zeit, kommt Relativierung. 3. Was lief gut, was kann verbessert werden? 4. Dank und Kompensation (Ausschlafen! Fein go Ässe? Prämien?) für die an der Vorfallsbewältigung Beteiligten.
Technik	
Isolation	1. Sicherstellen, dass keine Anmeldungen mit privilegierten Konten (Admins) erfolgt, solange das System noch online ist 2. Betroffene Systeme offline nehmen (Netzwerkkabel ziehen) aber laufen lassen zwecks Möglichkeit für ein Speicherabbild für eine spätere forensische Untersuchung. 3. Betroffene Netze / Standorte vom Rest der Infrastruktur trennen.

[5] In Anlehnung an Erste Hilfe bei einem schweren IT-Sicherheitsvorfall

Abgrenzung (rotes / grünes Netz)	1. Welche Systeme/Abteilungen/Aussenstellen sind nicht betroffen und können aufrecht erhalten werden? 2. Kann auf einer (read-only) Datenbasis eingeschränkt weitergearbeitet werden? 3. Gab es Mitarbeitende im Urlaub oder solche, die zum fraglichen Zeitpunkt gerade offline und deshalb (noch) nicht betroffen waren? Dies insbesondere zwecks Garantie eines «sauberen Datenbestandes». 4. Netzwerkverkehr beobachten 5. Aggressive Scans von Antivirusprogrammen laufen lassen.
Identifikation	1. Um welches Schadprogramm handelt es sich? Welcher Art? 1. Erpressung? 2. Zerstörung? 3. Diebstahl von Daten / Identitäten?
Identitäten schützen / wiederherstellen	1. Passwörter zurücksetzen 2. Konten revozieren (erfordert erneute Anmeldung auf allen Geräten) 3. Alle MFA-Methoden zurücksetzen 4. Gilt auch für Service- und Admin-Konten (vor allem für die)
Wiederherstellung vorbereiten und durchführen	1. Alle Systeme neu aufsetzen (tendenziell muss davon ausgegangen werden, dass unerkannte Modifikationen auf den betroffenen Systemen gemacht wurden, weshalb sich ein Reset der Systeme aufdrängt) 2. Wiederherstellung planen: 1. Mit welchem System wird begonnen / Abhängigkeiten? 2. Mit welchem Datenstand (nicht kompromittierte Backups) wird gearbeitet? 3. Gibt es Systeme, wo eine Bereinigung vorerst genügt und deren komplette Neuaufsetzung auch später erfolgen kann? Gibt es Systeme, die vorerst ein Offline-Dasein fristen können und so als Informationsquelle dienen, ohne online ins Geschehen eingreifen zu können? 4. Ab wann kann mit einem System (in Wiederherstellung) bereits wieder gearbeitet werden? Minimalbetrieb? 5. Gab es während dem Ausfall Notsysteme, deren Daten zurück ins Hauptsystem integriert werden müssen?
Auf allfällige Erpressung nicht eingehen	1. Falls Daten verschlüsselt wurden, sollte auf die Erpressung nicht eingegangen werden. 2. Im Zweifelsfall dringend den Austausch mit Spezialisten von der Polizei suchen und auf deren Erfahrung bauen.

4.6 Ideen zur Absicherung der technischen Geschäftskontinuität

Entsteht gerade 😉

5 ANHANG

5.1 EXEMPLARISCHE ANWENDUNG ISO27001:2022 IN EINEM ISMS

Dieses Kapitel beschreibt interessante Lösungsansätze für die Umsetzung der ISO27001:2022 Norm. Anschliessend werden unter Mapping die Ideen dann mit den ISO Controls in Verbindung gebracht.

Schnelle Erfolge können insbesondere mit technischen Massnahmen (T 01…) erzielt werden. Deren Auswirkungen auf die Mitarbeiter(-zufriedenheit) sind allerdings nicht zu missachten und müssen dennoch sorgfältig vorbereitet und adressiert werden.

5.1.1 IDEENSKIZZEN

Nr.	Bezeichnung	Beispiele
Vertragliche Mittel		
V 01	Vertragliche und schriftliche Anweisungen an MA	Arbeitsvertrag, AUP, Mitarbeiterhandbuch
V 02	Vertragliche Absicherungen mit (IT-)Dienstleistern	SLA, Servicebeschreibungen, (Dienstleistungs-)Verträge
V 03	Vertraglich abgesicherte Zusammenarbeit	Bspw. in einem Bug Bounty Programm (Gemeinsam für eine sichere Schweiz - Bug Bounty Switzerland) oder mit PenTestings
V 04	Entsprechend aufbereitete Verträge mit Lieferanten und Kunden	Datenschutzerklärung, Auftragsdatenverarbeitung, Geheimhaltungsvereinbarungen etc.
Technische Mittel		
T 01	Technische Richtlinien, auf alle Geräte angewendet	Technische Richtlinien im Umgang mit Informationen und Geräten, Konformitätsanforderungen an zugreifende Systeme
T 02	Anwendung von erhöhten Sicherheitsrichtlinien	Zero Trust, XDR etc.
T 03	Automatische Sicherheitsmassnahmen	DLP, Impossible Travel, Risky Sign In etc.
T 04	Technisches MA Monitoring	Insider Risk Score etc.
T 05	Anschluss / Integration der Fachanwendungen und bestehenden Lösungen in Security Monitoring	Single Sign-On, Automatisierung und Konsolidierung in einer entsprechenden Governance-, Risk- und Compliance-Lösung
T 06	Technische Abos zwecks relevanter Information	CVEs, Scans, Automatisierte technische Audits
T 07	Klassische Mittel des IT Servicemanagements	Incident Management, Change Management, Problem Management, Service Level Management, Capacity Management, KVP etc.
T 08	Aufbau entsprechender Schutzmassnahmen	Schliesssysteme, Firewalls, Netzwerksegmentierung, PIM / PAM
T 09	Aufbau oder Einforderung moderner Entwicklungsstandards	Release- und Change Management, (Biz-)DevOps, Desired State, Continuous Integration
Organisatorische Mittel		
O 01	AKV	Rollen, Verantworlichkeiten, Job Profile, MA-Zielsteuerung
O 02	Offenlegung von Mitgliedschaften und Beteiligungen	Interne Anweisung, Integration in Arbeitsvertrag
O 03	MA Monitoring	Strafregisterauszug, Betreibungsregisterauszug etc.
O 04	Netzwerk etablieren	Präventiver Aufbau einer Beziehung mit Strafverfolgungsbehörden und Regulierungsbeauftragten
O 05	Mitgliedschaften und Vertretung in Interessensgruppen	Branchenverbände, Interessensgemeinschaften
O 06	Etablierung eines entsprechenden Prozesses	Generischer Platzhalter für beliebige betriebliche und/oder ISMS-relevante Prozesse
O 07	Regelmässige Prüfung	Im Rahmen regelmässiger Checks sowie der jährlichen Audits

Nr.	Bezeichnung	Beispiele
O 08	Audits bei Lieferanten	Einforderung von Normen, Audits, Klärung der vertraglichen Grundlagen und bestehenden Zertifizierungen
O 09	Aufbau eines Notfallorganisation	Incident Management, Business Continuity Managements
O 10	Regelmässige Schulungen und Trainings	Security Awareness Training, Social Engineering Pen Tests, Planspiele etc.

5.1.2 Mapping (exemplarisch, Basis ISO 27001:2022)

Nr.	Massnahme	Kurzbeschreibung	Mögliche Mittel
Organisatorische Massnahmen (37 Controls)			
A 5.1	Richtlinien zur Informationssicherheit	Festlegung und Pflege von Sicherheitsrichtlinien	V 01, T 01
A 5.2	Rollen und Verantwortlichkeiten	Klare Zuweisung von Sicherheitsaufgaben	O 01
A 5.3	Funktionstrennung	Vermeidung von Interessenskonflikten	O 02, O 03
A 5.4	Verantwortung des Managements	Führungskräfte müssen Sicherheitsziele unterstützen	O 01-03
A 5.5	Kontakt zu Behörden	Kommunikation mit zuständigen Stellen	O 04, O 05
A 5.6	Kontakt zu Interessengruppen	Austausch mit externen Fachkreisen	O 05
A 5.7	Bedrohungsaufklärung	Sammlung und Analyse von Bedrohungsinformationen	O 03-05, T 06
A 5.8	Sicherheit im Projektmanagement	Integration von Sicherheitsaspekten in Projekte	O 06, T05
A 5.9	Inventarisierung von Informationen	Übersicht über alle Informationswerte	O 06, O 07, T05
A 5.10	Zulässige Nutzung	Regeln zur Nutzung von Informationen und Assets	V 01, T 03
A 5.11	Rückgabe von Assets	Rückgabe bei Austritt oder Rollenwechsel	O 06, T 01-03
A 5.12	Klassifizierung von Informationen	Einstufung nach Schutzbedarf	T 03
A 5.13	Kennzeichnung von Informationen	Sichtbare Markierung sensibler Daten	T 03
A 5.14	Informationsübertragung	Sicherer Austausch intern und extern	T 01-03
A 5.15	Zugriffskontrolle	Steuerung von Zugriffsrechten	O 01
A 5.16	Identitätsmanagement	Verwaltung von Benutzeridentitäten	O 02
A 5.17	Authentifizierungsinformationen	Schutz von Passwörtern und Zugangsdaten	V 01-02, T 01-03
A 5.18	Zugriffsrechte	Vergabe und Kontrolle von Berechtigungen	O 01
A 5.19	Sicherheit bei Lieferantenbeziehungen	Schutz bei Zusammenarbeit mit Dritten	T 01-03
A 5.20	Sicherheitsanforderungen in Verträgen	Sicherheitsklauseln in Lieferverträgen	V 04
A 5.21	Sicherheit in der ICT-Lieferkette	Kontrolle über IT-Dienstleister	V 04, O 08
A 5.22	Überwachung von Lieferantenservices	Regelmässige Prüfung externer Leistungen	V 04, O 08
A 5.23	Cloud-Sicherheit	Schutz bei Nutzung von Cloud-Diensten	V 04, O 08
A 5.24	Planung für Sicherheitsvorfälle	Vorbereitung auf Zwischenfälle	O 04, O 05, O 09
A 5.25	Bewertung von Sicherheitsereignissen	Einschätzung von Vorfällen	T 05, O 06
A 5.26	Reaktion auf Sicherheitsvorfälle	Massnahmen zur Schadensbegrenzung	T 05, O 06, O 09
A 5.27	Lernen aus Vorfällen	Analyse und Verbesserung nach Vorfällen	T 05, O 06, O 09
A 5.28	Beweissicherung	Dokumentation für rechtliche Zwecke	O 09
A 5.29	Sicherheit bei Störungen	Schutz bei Betriebsunterbrechungen	O 09
A 5.30	IT-Notfallbereitschaft	Vorbereitung auf IT-Ausfälle	O 09

Nr.	Massnahme	Kurzbeschreibung	Mögliche Mittel
A 5.31	Gesetzliche Anforderungen	Einhaltung von Vorschriften und Gesetzen	V 01-04
A 5.32	Schutz geistigen Eigentums	Wahrung von Urheberrechten	V 01-04
A 5.33	Schutz von Aufzeichnungen	Integrität und Verfügbarkeit von Dokumenten	T 07
A 5.34	Datenschutz	Schutz personenbezogener Daten	V 02, V 04, T 01-03, T 07
A 5.35	Unabhängige Sicherheitsprüfung	Externe Kontrolle der Sicherheitsmassnahmen	O 07, O 08
A 5.36	Einhaltung interner Regeln	Kontrolle der Umsetzung interner Vorgaben	O 07, O 08
A 5.37	Dokumentierte Betriebsverfahren	Standardisierte Abläufe für Sicherheit	V 01, O 06
Personelle Massnahmen (8 Controls)			
A 6.1	Hintergrundüberprüfung	Prüfung vor Einstellung	T 04, O 03
A 6.2	Arbeitsbedingungen	Sicherheitsrelevante Vertragsinhalte	V 01
A 6.3	Schulung und Sensibilisierung	Förderung des Sicherheitsbewusstseins	O 10
A 6.4	Disziplinarverfahren	Sanktionen bei Verstössen	V 01
A 6.5	Verantwortung nach Austritt	Regelungen für ehemalige Mitarbeitende	O 06
A 6.6	Vertraulichkeitsvereinbarungen	Schutz durch NDAs	V 01
A 6.7	Mobiles Arbeiten	Sicherheitsregeln für Homeoffice	V 01
A 6.8	Melden von Vorfällen	Pflicht zur Meldung von Sicherheitsproblemen	O 06
Physische Massnahmen (14 Controls)			
A 7.1	Sicherheitszonen	Abgrenzung sensibler Bereiche	T 08
A 7.2	Zugangskontrollen	Kontrolle physischer Zutritte	T 08, T 05
A 7.3	Sicherung von Räumen	Schutz von Büros und Serverräumen	T 08
A 7.4	Überwachung	Einsatz von Kameras und Sensoren	T 08
A 7.5	Schutz vor Umweltgefahren	Massnahmen gegen Feuer, Wasser, Stromausfall	T 08
A 7.6	Arbeiten in sicheren Bereichen	Regeln für Hochsicherheitszonen	T 08, O 06
A 7.7	Clean Desk & Screen	Keine sensiblen Daten offen liegen lassen	V 01, O 06, T 01
A 7.8	Geräteschutz	Physische Sicherheit von Hardware	T 01
A 7.9	Schutz ausserhalb des Standorts	Sicherheit bei mobilen Geräten	T 01, T 02
A 7.10	Speichermedien	Umgang mit USB-Sticks, Festplatten etc.	T 01, T 02
A 7.11	Versorgungseinrichtungen	Absicherung von Strom, Wasser, Klima	T 08
A 7.12	Kabelsicherheit	Schutz vor Manipulation und Schäden	T 08
A 7.13	Wartung von Geräten	Regelmässige technische Pflege	T 01
A 7.14	Entsorgung oder Wiederverwendung	Sichere Löschung vor Weitergabe	O 06
Technologische Massnahmen (34 Controls)			
A 8.1	Endgeräte	Schutz von Laptops, Smartphones etc.	T 01
A 8.2	Privilegierte Zugriffe	Kontrolle über Admin-Rechte	T 08
A 8.3	Zugriffsbeschränkung	Begrenzung auf notwendige Daten	O 01, T 08
A 8.4	Quellcodezugriff	Schutz von Softwarecode	T 08, T 09
A 8.5	Sichere Authentifizierung	Mehrfaktor, starke Passwörter etc.	T 02
A 8.6	Kapazitätsmanagement	Vermeidung von Systemüberlastung	T 07
A 8.7	Schutz vor Malware	Virenschutz und Anti-Malware	T 02
A 8.8	Schwachstellenmanagement	Patchen und Absichern von Systemen	T 01-03, T 06

Nr.	Massnahme	Kurzbeschreibung	Mögliche Mittel
A 8.9	Konfigurationsmanagement	Standardisierte Systemkonfiguration	T 09
A 8.10	Datenlöschung	Sichere Entfernung sensibler Daten	O 06
A 8.11	Datenmaskierung	Verbergen sensibler Informationen	T 02
A 8.12	Schutz vor Datenabfluss	DLP-Systeme zur Verhinderung von Leaks	T 03
A 8.13	Datensicherung	Backup und Wiederherstellung	O 06
A 8.14	Redundanz	Ausfallsicherheit durch doppelte Systeme	T 07, V 02, V 03
A 8.15	Protokollierung	Logging sicherheitsrelevanter Aktivitäten	T 01, T 08
A 8.16	Überwachung	Monitoring von Systemen und Netzwerken	T 08
A 8.17	Zeitabgleich	Synchronisierung von Systemuhren	T 08
A 8.18	Kryptografie	Verschlüsselung von Daten	T 03, T 08
A 8.19	Schlüsselmanagement	Verwaltung von Verschlüsselungsschlüsseln	T 08
A 8.20	Netzwerksicherheit	Schutz vor Angriffen auf Netzwerke	T 08
A 8.21	Sicherheit von Netzwerkdiensten	Absicherung externer Dienste	T 08
A 8.22	Netzwerktrennung	Segmentierung zur Risikominimierung	T 08
A 8.23	Webfilterung	Blockieren gefährlicher Webseiten	T 02, T 08
A 8.24	Mobile Geräte	Sicherheitsrichtlinien für Smartphones etc.	T 01
A 8.25	Telearbeit	Schutz bei Remote-Zugriffen	T 01-04
A 8.26	Sicherer Entwicklungsprozess	Sicherheitsanforderungen in der Softwareentwicklung	T 09
A 8.27	Sicherheitsanforderungen für Anwendungen	Definition sicherer Softwarefunktionen	T 09, O 06
A 8.28	Sicherheitsarchitektur	Design sicherer IT-Systeme	T 08, T 09, O 06
A 8.29	Sicheres Programmieren	Vermeidung von Schwachstellen im Code	T 09
A 8.30	Sicherheitstests	Prüfung vor Produktivsetzung	T 06, T 09
A 8.31	Ausgelagerte Entwicklung	Kontrolle über externe Entwickler	V 02, T 09, O 08
A 8.32	Änderungsmanagement	Kontrolle über Systemänderungen	T 07, T 09
A 8.33	Testdaten	Schutz sensibler Testinformationen	T 08
A 8.34	Testumgebungen	Absicherung von Entwicklungsumgebungen	T 08

5.2 Betrieb ISMS

#	Titel	Inhalt	Verantwortlich	
Kapitel 4 – Kontext der Organisation				
4.1	Verstehen der Organisation und ihres Kontextes	Analyse interner und externer Faktoren, die das ISMS beeinflussen	Kunde ✅	DM ✅
4.2	Verstehen der Bedürfnisse und Erwartungen interessierter Parteien	Identifikation relevanter Stakeholder und ihrer Anforderungen	Kunde ✅	DM ✅
4.3	Festlegen des Anwendungsbereichs des ISMS	Definition, welche Teile der Organisation vom ISMS abgedeckt sind	Kunde ✅	DM ❌
4.4	ISMS / KVP	Aufbau, Umsetzung und kontinuierliche Verbesserung des ISMS	Kunde ✅	DM ✅
Kapitel 5 – Führung				
5.1	Führung und Engagement	Top-Management muss das ISMS aktiv unterstützen und Ressourcen bereitstellen	Kunde ✅	DM ❌
5.2	Informationssicherheitspolitik	Festlegung und Kommunikation einer geeigneten Sicherheitsrichtlinie	Kunde ✅	DM ✅
5.3	Rollen, Verantwortlichkeiten und Befugnisse	Klare Zuweisung von Aufgaben und Verantwortlichkeiten im ISMS	Kunde ✅	DM ✅
Kapitel 6 – Planung				
6.1	Massnahmen zum Umgang mit Risiken und Chancen	Identifikation und Behandlung von Risiken für das ISMS	Kunde ❌	DM ✅
6.2	Informationssicherheitsziele und Planung zu deren Erreichung	Festlegung messbarer Ziele und deren Umsetzung	Kunde ❌	DM ✅
6.3	Planung von Änderungen	Strukturierte Planung bei Änderungen am ISMS	Kunde ❌	DM ✅
Kapitel 7 – Unterstützung				
7.1	Ressourcen	Bereitstellung notwendiger Mittel für das ISMS	Kunde ✅	DM ❌
7.2	Kompetenz	Sicherstellung der Qualifikation beteiligter Personen	Kunde ✅	DM ❌
7.3	Bewusstsein	Förderung des Sicherheitsbewusstseins im Unternehmen	Kunde ✅	DM ✅
7.4	Kommunikation	Effektive interne und externe Kommunikation zum ISMS	Kunde ✅	DM ✅
7.5	Dokumentierte Information	Erstellung, Pflege und Kontrolle relevanter Dokumente und Nachweise	Kunde ❌	DM ✅
Kapitel 8 – Betrieb				
8.1	Betriebliche Planung und Steuerung	Umsetzung geplanter Massnahmen zur Risikobehandlung	Kunde ✅	DM ✅
8.2	Bewertung von Informationssicherheitsrisiken	Systematische Risikoanalyse und -bewertung	Kunde ✅	DM ✅
8.3	Behandlung von Informationssicherheitsrisiken	Auswahl und Umsetzung geeigneter Controls zur Risikominimierung	Kunde ✅	DM ✅
Kapitel 9 – Bewertung der Leistung				
9.1	Überwachung, Messung, Analyse und Bewertung	Prüfung der Wirksamkeit des ISMS anhand definierter Kennzahlen	Kunde ❌	DM ✅
9.2	Internes Audit	Regelmässige interne Überprüfung des ISMS	Kunde ❌	DM ✅
9.3	Managementbewertung	Bewertung durch das Management zur Sicherstellung der Eignung und Wirksamkeit	Kunde ✅	DM ✅

#	Titel	Inhalt	Verantwortlich	
Kapitel 10 – Verbesserung				
10.1	Nichtkonformität und Korrekturmassnahmen	Behandlung von Abweichungen und deren Ursachen	Kunde ☑	DM ☑
10.2	Kontinuierliche Verbesserung	Fortlaufende Optimierung des ISMS zur Steigerung der Wirksamkeit	Kunde ☑	DM ☑

5.3 Im Dschungel der Standards

Folgende Normen und Standards drehen sich alle um mehr oder weniger um Themen, die auch in ISO 27001 adressiert werden. Viele bieten öffentlich einsehbare Umsetzungsmittel, Normen, Checklisten und «Controls» und sind mehr oder weniger austauschbar:

- Empfehlungen IKT-Minimalstandards (die Schweizer Lösung)
- BSI - IT-Grundschutz (die Deutsche Ausführung)
- Cybersecurity Framework | NIST (die US-amerikanische Variante mit strategischem Fokus)
- CIS Critical Security Controls (auch von den Amis, aber eher konkreterer Checklistencharakter)

5.4 Ein Versuch, dies alles zu verbinden

Eine Tabelle, die versucht eine Gegenüberstellung all dieser Standards zu wagen, ist aktuell in Bearbeitung.