Zusammenfassung und Zweck des Dokuments

Dieses Dokument stellt dar,

- welche technischen und organisatorischen Maßnahmen aus ISO 27001 Annex A die Fa. TEMA-Q umsetzt (und wieso);
- welche technischen und organisatorischen Maßnahmen aus ISO 27001 Annex A die Fa. TEMA-Q nicht umsetzt (und wieso nicht).

Das Dokument ist öffentlich und kann allen Interessenten (Kunden, Auditoren, Interessenten) bei Bedarf ausgehändigt werden. Rückfragen dazu beantwortet der Informationssicherheitsbeauftragte gerne.

Angewendete und nicht angewendete technische und organisatorische Maßnahmen

Grundsätzlich implementiert TEMA-Q alle Maßnahmen aus Annex A der ISO 27001, da sie Informationssicherheitsrisiken senken. Für den Fall, dass bestimmte Maßnahmen darüber hinaus noch aus anderen Gründen umgesetzt werden (bspw. aus vertraglichen Gründen gegenüber Kunden oder aus gesetzlichen Gründen, die in unserer Branche gelten oder aus intrinsischen Gründen), ist dies im Begründungstext vermerkt und dort zu entnehmen.

Maßnahme aus ISO 27001:2022 Anhang A	**Anwendung***	**Begründung für Anwendung oder Ausschluss***
A.5.1	Ja	Rollenspezifische Leitfäden ermöglichen ein effektives Zusammenspiel aller an der Sicherstellung der Informationssicherheit beteiligten Mitarbeiter und Externen. Regelmäßige Updates und Überprüfungen der Leitfäden sorgen dafür, dass neueste Entwicklungen und Aufgaben enthalten sind und die Leitfäden nach wie vor effektiv und angemessen sind.
A.5.2	Ja	Rollenzuweisungen helfen uns festzulegen, wer in welchen Situationen welche Verantwortlichkeiten bezüglich Informationssicherheitsmaßnahmen hat.
A.5.3	Ja	Aufgabentrennung setzen wir soweit möglich um, um dafür zu sorgen, dass ein System von gegenseitiger Absicherung bei sicherheitskritischen Aufgaben entsteht. Sie endet allerdings dort, wo sie zu Inflexibilität führt und mit der vorhandenen Personaldecke nicht geleistet werden kann.
A.5.4	Ja	Informationssicherheit wird nur dann ernst genommen, wenn die Geschäftsführung dahintersteht und die Einhaltung auch nachhaltig einfordert. Daher ist die Geschäftsführung bei uns in der Pflicht.
A.5.5	Ja	Kontakte zu relevanten Behörden versorgen uns frühzeitig mit Informationen zu Schwachstellen, Gefahren und gesetzgeberischen Entwicklungen, die für Informationssicherheit relevant sein könnten.

A.5.6	Ja	Kontakte zu relevanten Interessenvereinigungen versorgen uns frühzeitig mit Informationen zu Schwachstellen, Gefahren und anderen Entwicklungen, die für Informationssicherheit relevant sein könnten.
A.5.7	Ja	Die Bedrohungsintelligenz ermöglicht es im Unternehmen, proaktiv und aktiv auf potenzielle Bedrohungen zu reagieren und ihre Sicherheitsstrategien zu stärken.
A.5.8	Ja	Dadurch, dass wir geplant Informationssicherheitsanforderungen in unseren Projekten betrachten, können wir diese gezielt und frühzeitig einsteuern und umsetzen. Wir analysieren, welche Informationssicherheitsanforderungen wir an die bei uns entwickelten (oder von uns zugekauften) Systeme stellen, damit wir diese umsetzen können.
A.5.9	Ja	Geräte (und andere Assets) können nur dann sicher betrieben werden, wenn sie erfasst sind. Die Pflege von Geräten (und anderen Assets) ist nur möglich, wenn sich für jedes Asset jemand verantwortlich fühlt. Daher stellen wir dies sicher.
A.5.10	Ja	Die Absicherung von Geräten (und anderen Assets) ist nur möglich, wenn für jedes Gerät klar ist, welcher Gebrauch zulässig - d.h. “sicher” ist. Daher stellen wir sicher, dass Assets nur sicher verwendet werden. Damit Geräte (und anderen Assets) so behandelt werden, wie dies vorgesehen ist (und durch unsachgemäßen Gebrauch nicht unabsichtlich die Informationssicherheit gefährdet ist), gibt es für alle wichtigen Geräte Regeln, wie diese genutzt werden dürfen.
A.5.11	Ja	Damit Geräte nicht unbeaufsichtigt sind, wenn der für sie verantwortliche Mitarbeiter das Unternehmen verlässt oder bei Änderung des Beschäftigungsverhältnisses, gibt es die Pflicht zur geregelten Rückgabe.
A.5.12	Ja	Unterschiedliche Informationsarten sind unterschiedlich kritisch. Daher haben wir die Informationsarten klassifiziert, die bei uns schutzbedürftig sind.
A.5.13	Ja	Damit jedem schnell klar ist, welche Informationen wie klassifiziert sind, sind diese Informationen festgelegt und für jeden Mitarbeiter ersichtlich.
A.5.14	Ja	Damit Mitarbeiter wissen, wie sie welche Informationen bei deren Datenübertragung schützen müssen, haben wir Übertragungsrichtlinien etabliert, auf die jederzeit zurückgegriffen werden kann. Wir treffen mit unseren Partnern Vereinbarungen, wie kritische Geschäftsinformationen übertragen werden, damit diese beim Transfer angemessen geschützt sind. Schützenswerte Informationen sichern wir auch, wenn wir diese in elektronischen Nachrichten versenden. Das tun wir, weil der

		schnelle Austausch via Nachrichten/Chats wichtig für uns ist und vielfach eingesetzt wird – und gerade deswegen sicher sein muss.
A.5.15	Ja	Eine Zugangssteuerungsrichtlinie regelt bei uns, wer aus welchem Grund auf welche Geräte und Informationen Zugriff erhalten kann. Damit stellen wir sicher, dass Zugriff auf Geräte und Informationen nicht willkürlich geschieht. Wir sichern den Zugriff auf unsere Netze ab, damit Informationen, die in diesen fließen, nicht kompromittiert werden oder die Netzwerke selbst durch zu viel Last unsere Verfügbarkeitsanforderungen nicht halten können.
A.5.16	Ja	Damit Benutzer korrekt und sauber angelegt und wieder gelöscht werden, haben wir einen Prozess, mit dessen Hilfe wir Benutzer registrieren oder deregistrieren.
A.5.17	Ja	Wir teilen geheime Authentisierungsinformationen (Passwörter u. dgl.) über einen geregelten Prozess zu, damit sichergestellt ist, dass sie während der Zuteilung auch geheim bleiben. Wir verpflichten alle Benutzer, ihre Zugangsdaten geheim zu halten, damit nicht Unbefugte diese nutzen können und damit Zugriff auf schutzwürdige Informationen haben. Damit Passworte nicht erraten oder per brute force ausgespäht werden können, stellen wir über systemseitige und organisatorische Richtlinien sicher, dass diese sicher sind (lang genug, komplex genug).
A.5.18	Ja	Damit registrierte Benutzer korrekt und sauber Rechte erhalten, haben wir einen Prozess, mit dessen Hilfe wir Rechte an Benutzer vergeben und entziehen. Alle Mitarbeiter, die bei uns für Geräte (und andere Assets) zuständig sind, überprüfen regelmäßig, ob die gewährten Zugangsrechte noch erforderlich sind. So stellen wir sicher, dass Unbefugte keinen Zugriff mehr haben. Wenn Mitarbeiter (oder Freelancer, die für uns arbeiten), ihren Aufgabenbereich wechseln oder uns verlassen, passen wir ihre Zugangsrechte an oder löschen diese, damit sie nicht unbefugt Zugriff zu schutzwürdigen Informationen haben.
A.5.19	Ja	Wenn Dienstleister von uns auf Werte unserer Organisation zugreifen müssen, so regeln wir dies vorab, um sicherstellen zu können, dass hierbei keine Sicherheitslücken entstehen.
A.5.20	Ja	Wir schließen mit allen für die Informationssicherheit relevanten Dienstleistern Verträge ab, die die Pflichten der Dienstleister bzgl. der Informationssicherheit enthalten.
A.5.21	Ja	In den Verträgen nehmen wir Regelungen auf in Bezug auf Informationssicherheitsrisiken, die bei Dienstleistern auftreten oder auftreten können, weil wir Informationssicherheitsrisiken

		auch dann vermeiden möchten, wenn sie bei unseren Dienstleistern auftreten.
A.5.22	Ja	Wir überprüfen kontinuierlich, ob sich unsere Dienstleister an die mit ihnen vereinbarten Regelungen zur Informationssicherheit halten, damit wir uns in diesem Punkt sicher sein können. Dienstleistungen unserer Zulieferer können sich ändern: dies behalten wir im Auge, damit wir die Regelungen zur Informationssicherheit in dem Fall mit unseren Dienstleistern anpassen können.
A.5.23	Ja	Wir haben festgelegt, wie wir mit der Nutzung von Cloud-Diensten umgehen und dabei die Informationssicherheitsanforderungen zu berücksichtigen.
A.5.24	Ja	Wir haben ein Verfahren festgelegt, dass es uns ermöglicht, schnell und zuverlässig auf Informationssicherheitsvorfälle zu reagieren. Das ist uns wichtig, um Informationssicherheitsvorfälle schnell klären zu können.
A.5.25	Ja	Jedes Informationssicherheitsereignis (d.h. jeden Verdacht, dass die angestrebte Informationssicherheit kompromittiert ist), bewerten wir darauf, ob es sich um einen Vorfall handelt (d.h. die Sicherheit ist nachweislich kompromittiert worden), um adäquat darauf reagieren zu können.
A.5.26	Ja	Wir sorgen dafür, dass wir adäquat auf erkannte Informationssicherheitsvorfälle reagieren, damit diese so schnell wie möglich wieder abgestellt werden.
A.5.27	Ja	Wir sorgen dafür, dass wir gezielt aus früheren Informationssicherheitsvorfällen lernen, damit diese in der Zukunft möglichst nicht noch einmal vorkommen.
A.5.28	Ja	Bei akuten Informationssicherheitsvorfällen sind alle Mitarbeiter und auch Dienstleister angehalten, Beweismaterial zu sammeln, um die Bewertung des Vorfalls zu vereinfachen oder später rekonstruieren zu können.
A.5.29	Ja	Wir haben bestimmt, in welchen Ausnahmesituationen wir welchen Grad an Informationssicherheit aufrechterhalten wollen, damit wir dies gegenüber unseren interessierten Parteien und insb. Vertragspartnern kommunizieren können und uns auf die Aufrechterhaltung der festgelegten Informationssicherheit fokussieren können. Wir legen Verfahren fest, mit denen wir die Informationssicherheit in den festgelegten Ausnahmesituationen sicherstellen können, um bei Bedarf reagieren zu können. Wir testen die o.g. Verfahren, um sicherstellen zu können, dass diese auch funktionieren, wenn wir sie benötigen.
A.5.30	Ja	Wir haben bestimmt, in welchen Ausnahmesituationen wir welchen Grad an Verfügbarkeit der

		Informationen aufrechterhalten wollen um einen störungsfreien Geschäftsbetrieb zu gewährleisten. Wir legen Verfahren fest, mit denen wir die Informationssicherheit in den festgelegten Ausnahmesituationen sicherstellen können, um bei Bedarf reagieren zu können. Wir testen die o.g. Verfahren, um sicherstellen zu können, dass diese auch funktionieren, wenn wir sie benötigen.
A.5.31	Ja	Wir sammeln alle für uns geltenden gesetzlichen, vertraglichen und regulatorischen Regelungen mit Bezug zu Informationssicherheit, damit wir wissen, welche Anforderungen wir aus dieser Sicht erfüllen müssen. Wir halten uns an alle für uns geltenden gesetzlichen, vertraglichen und regulatorischen Regelungen.
A.5.32	Ja	Es gibt Verfahren, die bei uns sicherstellen, dass wir urheberrechtlich geschützte Werke bestimmungsgemäß bzw. vertragsgemäß verwenden.
A.5.33	Ja	Dokumente werden bei uns so aufbewahrt, wie dies durch für uns geltende Gesetze, Verträge und andere regulatorische Vorgaben gefordert ist, so dass der Informationssicherheit in diesem Bereich Rechnung getragen wird.
A.5.34	Ja	Wir halten uns in Bezug auf personenbezogene Daten an die DSGVO.
A.5.35	Ja	Wir lassen unsere Regelungen zur Informationssicherheit durch unabhängige externe Stellen überprüfen (bspw. Zertifizierungsorganisationen), um sicherzustellen, dass wir nichts Wichtiges übersehen.
A.5.36	Ja	Wir überprüfen intern, ob sich alle unsere Mitarbeiter auch an die vorgegebenen Regelungen zur Informationssicherheit halten, damit diese nicht nur Lippenbekenntnisse bleiben. Wir überprüfen auch die bei uns verwendeten Informationssysteme darauf, ob diese alle Sicherheitsrichtlinien einhalten, damit hier nicht unbeabsichtigt Informationssicherheitslecks entstehen.
A.5.37	Ja	Wenn Informationssicherheit davon abhängt, dass Bedienabläufe an Geräten oder Systemen genau eingehalten werden, dann dokumentieren wir diese Bedienabläufe. Diese Dokumente stellen wir, dem Personal das sie benötigt, zur Verfügung.
A.6.1	Ja	Wir sind darauf angewiesen, dass wir nur Mitarbeiter einstellen, die in der Lage sind, unsere Sicherheitsanforderungen einzuhalten. Daher überprüfen wir genau, wen wir einstellen (oder als Freiberufler für uns arbeiten lassen).

A.6.2	Ja	Vereinbarungen zur Informationssicherheit, die Mitarbeiter einhalten müssen, sind nur dann verlässlich einhaltbar, wenn alle Seiten zu jeder Zeit Einblick nehmen können in das, worauf man sich geeinigt hat. Daher setzen wir hier auf vertragliche Regelungen.
A.6.3	Ja	Um sicherzustellen, dass unsere Mitarbeiter Informationssicherheit auch umsetzen können, setzen wir auf Schulungen in diesem Bereich und entwickeln jeden Mitarbeiter so weiter, dass er die an ihn gestellten Aufgaben bzgl. der Informationssicherheit auf sicher erfüllen kann.
A.6.4	Ja	Wenn Mitarbeiter ihren Pflichten in der Informationssicherheit nicht nachkommen, ist uns das nicht egal. Wir reden dann darüber und weisen darauf hin. Das sorgt dafür, dass die Wichtigkeit des Themas erkannt wird.
A.6.5	Ja	Da wir wissen, dass Informationssicherheit am Ende der Beschäftigung von Mitarbeitern nicht einfach aufhört. sorgen wir dafür, dass wir die über das Arbeitszeitende hinaus bestehenden Pflichten ebenfalls regeln.
A.6.6	Ja	Unsere Geheimhaltungsvereinbarungen sind immer up to date, damit wir sicherstellen, dass wir immer und aktuell das geheim halten, was uns wichtig ist.
A.6.7	Ja	Ähnlich wie Mobilgeräte sind Remote Arbeitsplätze nicht vollends “kontrollierbar” und können ein Einfallstor für Angriffe und Sicherheitslücken sein. Daher regeln wir, wie in Remote Arbeit gearbeitet werden soll, um Sicherheit zu schaffen.
A.6.8	Ja	Wir sorgen dafür, dass Informationssicherheitsereignisse und -vorfälle so schnell wie möglich über die o.g. Verfahren gemeldet und bearbeitet werden, weil das dafür sorgt, dass wir möglichst schnell Sicherheit wiederherstellen, falls sie doch einmal kompromittiert sein sollte. Unsere Mitarbeiter und Dienstleister halten wir dazu an, Informationssicherheitsvorfälle und -ereignisse zügig zu melden, damit wir diese schnell und effektiv behandeln können.
A.7.1	Ja	Wir haben bei uns physische Sicherheitszonen definiert, in denen bestimmte Regelungen zur Informationssicherheit gelten. So sorgen wir dafür, dass sicherheitskritische Informationen in unseren Räumlichkeiten nicht kompromittiert werden können.
A.7.2	Ja	Wir sorgen dafür, dass unsere Sicherheitszonen so geschützt sind, dass man nicht einfach unbefugt in sie eindringen kann. Auf diese Weise verbessern wir die Sicherheit der Informationen und Geräte in den Zonen. Wir haben Zutrittsstellen zu unseren Räumlichkeiten definiert und überwachen diese, damit keine Unbefugten an diesen Stellen

		eindringen können und die Informationssicherheit kompromittieren können.
A.7.3	Ja	Wir schützen unsere Büros, Räume und Einrichtungen, damit hier keine schützenswerten Informationen kompromittiert werden können.
A.7.4	Ja	Wir führen eine Sicherheitsüberwachung unserer Zutrittsstellen zu unseren Räumlichkeiten durch, damit keine Unbefugten an diesen Stellen eindringen können und die Informationssicherheit kompromittieren können.
A.7.5	Ja	Wir kümmern uns um einen angemessenen Schutz vor Naturkatastrophen, bösartigen Angriffen und Überfällen, damit wir durch diese Vorkommnisse keine schützenswerten Informationen verlieren.
A.7.6	Ja	Wir haben Vorgehensweisen etabliert, die für Arbeiten in Sicherheitsbereichen zur Anwendung kommen, damit wir hier nicht unabsichtlich die Sicherheit von schutzbedürftigen Informationen kompromittieren.
A.7.7	Ja	Damit schutzbedürftige Informationen nicht bei Mitarbeitern kompromittiert werden können, gilt bei uns eine “Clean Desk Policy”.
A.7.8	Ja	Damit wichtige Geräte und andere Betriebsmittel nicht ausfallen, sorgen wir dafür, dass sie sicher aufgestellt sind.
A.7.9	Ja	Wenn Geräte entfernt werden (und außerhalb ihres eigentlichen Standorts betrieben werden), haben wir Regeln, die festlegen, wie sie gesichert werden müssen, damit schutzbedürftige Informationen, die mit ihnen verarbeitet werden, nicht kompromittiert werden.
A.7.10	Ja	Wechseldatenträger können schnell verloren gehen. Daher haben wir geregelt, wie und unter welchen Bedingungen sie eingesetzt werden dürfen. Wenn Datenträger entsorgt werden, können noch kritische Informationen auf ihnen gespeichert sein. Daher haben wir geregelt, wie eine sichere Entsorgung zu geschehen hat. Wenn kritische Informationen auf transportablen Datenträgern gespeichert sind, ist das Risiko höher, dass diese kompromittiert werden als auf nicht-transportablen Datenträgern. Daher haben wir den Transport strikt geregelt. Wer Geräte oder andere Assets von ihren vorgesehenen Orten entfernen will, muss dies vorab absprechen. So stellen wir sicher, dass wir immer wissen, wo wichtige Geräte sich aufhalten und erkennen ihren Verlust frühzeitig, so dass wir reagieren können.
A.7.11	Ja	Versorgungsleitungen (Strom, Wasser etc.) konzipieren und schützen wir so, dass Ausfälle und Leckagen möglichst nicht

		passieren oder wenn doch, dass diese dann die Sicherheit der schutzbedürftigen Informationen nicht kompromittieren.
A.7.12	Ja	Kabel die Strom, Daten oder unterstützende Informationsdienste transportieren, schützen wir, um sicherzustellen, dass diese nicht unterbrochen oder angezapft werden und somit schutzbedürftige Informationen nicht kompromittiert werden.
A.7.13	Ja	Damit Geräte, die für die Informationssicherheit wichtig sind, nicht ausfallen, sorgen wir dafür, dass diese gem. der vorgesehenen Intervalle fachkundig gewartet werden.
A.7.14	Ja	Geräte und Betriebsmittel, die Speichermedien enthalten, löschen wir, bevor wir sie entsorgen oder recyclen. Dadurch stellen wir sicher, dass keine schutzbedürftigen Informationen (inkl. urheberrechtlich geschützt) auf ihnen gespeichert sind.
A.8.1	Ja	Endpunktgeräte stellen ein leicht zu nutzendes Einfallstor für Angriffe und Sicherheitslücken dar. Daher regeln wir, wie sie eingesetzt werden dürfen und wie nicht. Damit Unbefugte nicht Zugriff zu unbeaufsichtigten, für die Informationssicherheit wichtigen Geräten nehmen können, schützen wir solche Geräte, wenn sie nicht durch Mitarbeiter beobachtet werden, auf angemessene Weise: Durch Wegschluss, durch Sperren und durch andere angemessene Maßnahmen.
A.8.2	Ja	Damit nicht absichtlich oder unabsichtlich durch privilegierte Zugänge (Admin-Accounts) die Informationssicherheit kompromittiert wird, schränken und verwalten wir solche Zugänge auf diejenigen Personen, die sie benötigen.
A.8.3	Ja	Wir beschränken nach dem Need-to-know-Prinzip den Zugang zu Informationen auf diejenigen Mitarbeiter, die zur Ausübung ihrer Tätigkeit zu diesen Informationen Zugang haben müssen – alle anderen bekommen keinen Zugang. Damit stellen wir so gut wie möglich sicher, dass niemand, der eigentlich keinen Zugriff zu schutzwürdigen Informationen braucht, diese unabsichtlich oder absichtlich unsicher behandelt.
A.8.4	Ja	Unser Sourcecode-Repository ist ebenfalls ein System, auf das wir nur gem. unserer Zugangssteuerungsrichtlinie Zugriff gewähren, damit keine Unbefugten Sourcecode zweckentfremden oder verändern können.
A.8.5	Ja	Damit geheime Authentisierungsinformationen nicht nach deren Eingabe in Informationssysteme kompromittiert werden, nutzen wir ausschließlich sichere Anmeldeverfahren, in denen die Authentisierungsinformationen sicher transportiert werden.

A.8.6	Ja	Wenn die Auslastung bestimmter Ressourcen (Systeme, Mitarbeiter) wichtig für die Informationssicherheit sind, so monitoren wir diese, um frühzeitig Trends zu Überlastungen erkennen und diesen entgegen wirken zu können.
A.8.7	Ja	Wir setzen auf allen Systemen, auf denen dies angemessen möglich ist, Maßnahmen gegen Schadsoftware um, damit die Systeme gegen böswillige Angriffe gehärtet sind und die Informationssicherheit aufrechterhalten können. Durch Mitarbeiterschulungen unterstützen wir dieses.
A.8.8	Ja	Wir holen Informationen zu technischen Schwachstellen der bei uns verwendeten Systeme ein, damit wir diese zügig abstellen können und schützenswerte Informationen nicht kompromittiert werden. Wir überprüfen und bewerten auch die bei uns verwendeten Informationssysteme darauf, ob diese alle Sicherheitsrichtlinien einhalten, damit hier nicht unbeabsichtigt Informationssicherheitslecks entstehen.
A.8.9	Ja	Wir verwenden ein Konfigurationsmanagement, um die Konsistenz, Kontrolle und Qualität von IT-Systemen, Software und anderen technischen Assets sicherzustellen.
A.8.10	Ja	Sensible Informationen werden bei uns nicht länger gespeichert als für den Zweck erforderlich oder rechtliche Aufbewahrungsfristen bestehen. Durch die Löschung von Informationen vermeiden wir unnötige Preisgabe sensibler Informationen und halten rechtliche und vertragliche Anforderungen zum Löschen ein.
A.8.11	Ja	Wir schützen vertrauliche Informationen durch die Maskierung der Daten, ohne den Betrieb oder die Analysefähigkeit zu beeinträchtigen.
A.8.12	Ja	Durch die Vermeidung von Datenlecks auf Systemen, Netzwerke und anderer Systeme die sensible Informationen verarbeiten, speichern oder übertragen gewährleisten wir die Sicherheit und Integrität vertraulicher Informationen.
A.8.13	Ja	Damit wichtige Informationen nicht verloren gehen, haben wir eine Backuprichtlinie für alle Informationen, deren Verfügbarkeit schutzbedürftig ist.
A.8.14	Ja	Wir planen diejenige Infrastruktur, die wir benötigen, so redundant, dass die Risiken, die durch Ausfall entstehen, auf ein akzeptables Maß gesenkt werden können.
A.8.15	Ja	Um entweder im Vorfeld oder forensisch auswerten zu können, welche Ereignisse auf unsere Systeme einwirken, loggen wir alle wichtigen Ereignisse. Die Log-Informationen werden wiederum gesichert, damit diese nicht bewusst oder unbewusst verfälscht, gelöscht oder offengelegt werden

		können. Dasselbe gilt auch für die Log-Informationen, die sich aus Admintätigkeiten ergeben.
A.8.16	Ja	Wir überwachen Aktivitäten, um Sicherheitsbedrohungen zu minimieren, die Einhaltung von Vorschriften zu gewährleisten Ressourcen zu optimieren und die Effizienz sowie die Stabilität von Systemen zu verbessern.
A.8.17	Ja	Um Log-Informationen zur Analyse korrekt verwenden zu können, synchronisieren wir die Uhren aller Systeme, die Log-Informationen erzeugen.
A.8.18	Ja	Wir schränken die Verwendung von privilegierten Hilfsprogrammen („Ausführen als…“) so stark wie möglich ein, denn diese Programme können ein Einfallstor für Angriffe sein, wenn Schadsoftware plötzlich mit Admin-Rechten arbeiten kann.
A.8.19	Ja	Damit kritische Informationssysteme nicht unvermittelt ausfallen oder nicht so arbeiten wie benötigt, sorgen wir dafür, dass auf ihnen nicht einfach so neue oder geänderte Software installiert wird. Eine softwareseitig und organisatorisch umgesetzte Installationsrichtlinie sorgt dafür, dass das Risiko eines unbewussten Installierens von Schadsoftware sinkt.
A.8.20	Ja	Wir konzipieren und verwalten die von unseren Systemen verwendeten Netzwerke, damit diese nicht unvermittelt ausfallen oder dem zu erwartenden Verkehr nicht gewachsen sind.
A.8.21	Ja	Wir überlegen uns, welche Netzwerkleistung wir (intern wie extern) benötigen und sorgen dafür, dass diese zur Verfügung stehen, um nicht überrascht zu werden. Dieses überwachen wir weil wir sicherstellen wollen, dass die Systeme sicher sind.
A.8.22	Ja	Wir trennen, soweit nötig, diejenigen Netzwerke, in denen unsere Mitarbeiter arbeiten und diejenigen Netzwerke, in denen unsere produktiven Systeme operieren, damit sich diese nicht gegenseitig stören können.
A.8.23	Ja	Durch den Einsatz von Webfiltern schützen wir das Unternehmensnetzwerk und minimieren die Risiken.
A.8.24	Ja	Wir haben Richtlinien, nach der wir Informationen verschlüsseln – sowohl bei der Speicherung als auch beim Versand. Darüber stellen wir sicher, dass wir kritische Informationen geeignet gegen Ausspähen schützen. Und für den Gebrauch von kryptographischen Schlüsseln, denn verschlüsselte und authentifizierte Informationen sind nur so sicher wie die Aufbewahrung und Verwendung ihrer Schlüssel.

A.8.25	Ja	Wir haben eine Richtlinie für Softwareentwicklung und verpflichten alle, die für uns Software entwickeln, diese anzuwenden, damit Software sicher entwickelt wird.
A.8.26	Ja	Wir schützen unsere Onlinesysteme so, dass sie sicher sind vor betrügerischen Angriffen, die dazu führen, dass wir unsere Verträge mit unseren Kunden nicht einhalten können. Wir schützen alle Transaktionen, die unsere Kunden mit unseren Anwendungen durchführen, damit diese vollständig, unverfälscht, authentisch und vertraulich bleiben.
A.8.27	Ja	Wir haben Grundsätze für die Entwicklung sicherer Systeme. Diese wenden wir an, damit die von uns entwickelten Systeme auch sicher sind.
A.8.28	Ja	Durch sichere Programmierung stellen wir sicher, dass die Anzahl potenzieller Sicherheitsschwachstellen in der Software reduziert wird.
A.8.29	Ja	Wir testen alle Sicherheitsfunktionen der Systeme, die wir entwickeln, damit wir sicher sind, dass sie auch funktionieren wie gedacht. Wir führen darüber hinaus Abnahmetests für alle Systeme durch, die wir anschaffen oder entwickeln, damit wir sicherstellen können, dass deren Sicherheitsfunktionen nicht nur im Einzelfall, sondern auch im Gesamtkontext funktionieren.
A.8.30	Ja	Wir lagern Entwicklungstätigkeiten an Partner aus. Diese überwachen wir, weil wir sicherstellen wollen, dass die dort entwickelten Systeme so sicher sind, wie wir sie benötigen.
A.8.31	Ja	Wir trennen Entwicklungs-, Staging- und Produktivsysteme bewusst, damit nicht Änderungen an dem einen unvermutete Konsequenzen auf die Informationssicherheit der jeweils anderen haben können. Da auch über Entwicklungsumgebungen Sicherheitsrisiken in entwickelte Systeme eingeschleust werden können, sorgen wir dafür, dass wir die von uns verwendeten Entwicklungsumgebungen so gut wie möglich absichern.
A.8.32	Ja	Wir sorgen dafür, dass wichtige Prozesse, Informationssysteme o.ä. nicht “mal eben so” geändert werden, weil dies die Informationssicherheit gefährden kann. Wir ändern weder die Systeme, mit deren Hilfe wir Software entwickeln, noch unsere entwickelten Softwareprodukte „einfach so“, sondern nur nach gründlicher Prüfung dessen, was wir ändern – weil wir wissen, dass Änderungen auch Informationssicherheitslecks bedeuten können. Und das wollen wir vermeiden. Wenn wir die in der Entwicklung verwendeten Betriebssysteme updaten, überprüfen wir, ob unsere Entwicklungssysteme danach noch fehlerfrei funktionieren – weil wir wissen, dass nicht

		fehlerfreies Verhalten zu Informationssicherheitslecks führen kann. Wir updaten Softwarepakete nicht deswegen, „weil es geht“, sondern weil wir die Notwendigkeit sehen. Wir prüfen die neuen Pakete vorab.
A.8.33	Ja	Da wir wissen, dass Testdaten manchmal aus Produktivdatenbanken entstammen, sorgen wir dafür, dass unsere Testdaten sorgfältig geschützt sind.
A.8.34	Ja	Wenn unsere Produktivsysteme auditiert werden sollen, werden wir dafür sorgen, dass dies nicht in den Hauptgeschäftszeiten geschieht, so dass wir die Verfügbarkeit unserer Systeme für unsere Kunden auch während des Audits sicherstellen können.

* **Anwendung:** Ja, wenn die Annex A-Maßnahme angewendet wird. Nein, wenn nicht.
Begründung für Anwendung oder Ausschluss: Der Grund, aus dem die Maßnahme angewendet wird oder nicht ausgeschlossen wird.