[Name der Organisation]

ST1 ISMS-Handbuch

Version	1.0
Eigentümer der Richtlinie	Name eintragen
Geprüft von	Name oder Rolle eintragen
Prüfdatum	Datum eintragen
Gültig ab	Datum eintragen
Nächste Überprüfung	Datum eintragen
Vertraulichkeitsklasse	INTERN

Änderungsverlauf

Datum	Version	Erstellt von	Beschreibung der Änderung
27.05.25	0.92	DataGuard	Grundstruktur des Dokuments
XX.XX.24	1.00	XX	Geprüfte Version mit geringen Änderungen

[Wie diese DataGuard Richtlinienvorlage zu verwenden ist:]

[DataGuard möchte Ihnen einige wichtige Hinweise zur Anwendung der bereitgestellten Richtlinienvorlage geben. Diese Vorlage soll Ihnen als Ausgangspunkt dienen, um eigene, auf Ihre Organisation zugeschnittene Richtlinien zu entwickeln. Bitte beachten Sie die folgenden Hinweise zur Verwendung der Vorlage sorgfältig.

Verwendung der Vorlage

- **Vorlage als Ausgangspunkt:** Diese Vorlage ist sorgfältig recherchiert und von Experten zusammengestellt worden. Sie ist als Ausgangspunkt für die Erstellung Ihrer eigenen Richtlinie gedacht und bietet eine Struktur sowie Beispiele für Ihre künftiges Dokument. Bei allen Bemühungen erhebt diese Vorlage jedoch keinen Anspruch auf Passgenauigkeit und Vollständigkeit, denn die individuellen Gegebenheiten in Ihrer Organisation können abweichen.
- **Grundsatz der Effektivität:** Eine Richtlinie soll erforderlich, angemessen, passend, aufklärend und unterstützend für Ihren individuellen Unternehmenszweck wirken. Sorgen Sie dafür, dass Ihre Richtlinien stets diesem Grundsatz entsprechen.
- **Überprüfung der Inhalte:** Gehen Sie die Inhalte der Vorlage sorgfältig durch und überprüfen Sie diese im Hinblick auf die spezifischen Bedürfnisse und Anforderungen.
- **Vollständiges Verständnis erforderlich:** Stellen Sie sicher, dass Sie als Ersteller dieses Dokuments alle beschriebenen Anweisungen und Verfahren vollständig verstehen und für Ihre Organisation als anwendbar halten. Nur so können Sie fundierte Entscheidungen über Anpassungen treffen.
- **Klärung von Unklarheiten:** Sollten Sie auf Inhalte stoßen, die Sie nicht vollständig verstehen, holen Sie unbedingt weitere Informationen ein. Dies kann durch Rücksprache mit unseren DataGuard-Experten, rechtlichen Beratern oder anderen Fachexperten außerhalb oder innerhalb Ihrer Organisation geschehen.
- **Individuelle Anpassung erforderlich:** Die in der Vorlage beschriebenen Anweisungen und Verfahren sind pauschale Beispiele oder Vorschläge ohne tiefere Berücksichtigung Ihres Unternehmenskontextes. Daher ist es erforderlich, dass Sie den Inhalt der Richtlinien an die tatsächlichen Gegebenheiten und Anforderungen Ihrer Organisation anpassen.*
- **Keine ungeprüfte Übernahme:** Übernehmen Sie keine Texte oder Anweisungen aus der Vorlage, wenn diese nicht den spezifischen Anforderungen und der tatsächlichen Situation in Ihrer Organisation entsprechen. Jede Organisation ist einzigartig, und pauschale Übernahmen können zu Fehlern oder Missverständnissen führen.
- **Verantwortung der Geschäftsführung:** Beachten Sie, dass die endgültige Verantwortung für die Gestaltung und

Umsetzung von Richtlinien bei der obersten Leitung Ihrer Organisation liegt. Es ist entscheidend, dass diese alle Inhalte kritisch überprüft und eine Korrektur von unpassenden Inhalten veranlasst.]

[*) Die in dieser Vorlage gelb hinterlegten und in eckigen Klammern gesetzten Hilfstexte und Hinweise sollen nach Kennnisnahme eliminiert oder inhaltlich angepasst werden. Beispiel: Bitte eliminieren Sie diese Seite vor Veröffentlichung der Richtlinie.]

1. Einleitung

Diese Zusammenfassung von Richtlinien dient dem Betrieb des Managementsystems für Informationssicherheit de [Name der Organisation]. Es vertieft die Vorgaben der Leitlinie für Informationssicherheit. Es stellt einen Rahmen dar, der unsere Strategie zur effektiven Verwaltung und Eindämmung von Sicherheitsbedrohungen und -vorfällen beschreibt. Dieses Dokument dient als umfassender Leitfaden, in dem detailliert beschrieben wird, wie unsere Organisation die erforderlichen Kernprozesse des Informationssicherheitsmanagementsystems (ISMS) gestaltet und umsetzt. Es beinhaltet Informationen zum normativen und organisatorischen Anwendungsbereich, sowie zu Rollen im ISMS und deren Verantwortlichkeiten.

1.1 Zweck und Umfang

Um die Wirksamkeit des ISMS zu gewährleisten, ist es unverzichtbar, klar definierte Ziele festzulegen und ein robustes Überwachungs- und Messsystem zu implementieren, um den Fortschritt in Richtung dieser Ziele zu verfolgen. Unsere Organisation legt klare Ziele der Informationssicherheit fest und stellt dafür einen effizienten Umsetzungsplan auf, um die kritischen Geschäftsaktivitäten zu schützen und Verpflichtungen gegenüber den interessierten Parteien, einschließlich Kunden, Gesellschaftern, Mitarbeitern und Lieferanten, zu erfüllen.

Diese Richtlinie gilt für alle Mitarbeiter, Auftragnehmer, Drittdienstleister und Interessengruppen, die Zugang zu den Informationsbeständen von unserer Organisation oder ihr von Dritten anvertraut wurden. Sie umfasst alle im Anwendungsbereich des ISMS festgelegten Organisationsstrukturen, physischen Bereiche, Systeme, Netzwerke und Daten, die in den Zuständigkeitsbereich von unserer Organisation fallen.

1.2 Anwendbarkeit

Diese Richtlinie gilt für alle Mitarbeiter und Beteiligten, die mit dem Betrieb des ISMS betraut sind und stellt sicher, dass sie sich an die festgelegten Richtlinien halten. Das Informationssicherheitsteam hat in Zusammenarbeit mit den zuständigen Abteilungen die Aufgabe, die Umsetzung, Pflege und kontinuierliche Verbesserung der in dieser Richtlinie beschriebenen Verfahren zu überwachen.

1.3 Normativer Verweis

[Bitte löschen Sie nicht zutreffende Angaben]

Es ist die Strategie von [Name der Organisation] ein Managementsystem für die Informationssicherheit (ISMS) zu unterhalten, das die Anforderungen der Norm: **ISO/IEC 27001 in ihrer Version 2022** erfüllt, um die primären Geschäftsziele, den Zweck und den Kontext des Unternehmens zu verfolgen.

Es ist die Strategie von [Name der Organisation] ein Managementsystem für die Informationssicherheit (ISMS) zu unterhalten, das die Anforderungen des **ISA-Katalogs (TISAX) in seiner Version 6.0** erfüllt, um die primären Geschäftsziele, den Zweck und den Kontext des Unternehmens zu verfolgen.

1.4 Aufbau des ISMS – PDCA Zyklus

Ein Managementsystem für Informationssicherheit ist ein strukturiertes Rahmenwerk, das Richtlinien, Prozesse und Verfahren definiert, um Informationssicherheitsrisiken zu identifizieren, zu bewerten, zu behandeln und zu überwachen, um die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu gewährleisten.

1.4.1 Struktur des Managementsystems

Das Managementsystem für Informationssicherheit von unserer Organisation basiert auf dem PDCA-Zyklus, auch bekannt als der Deming-Zyklus. Dieser Zyklus besteht aus den vier Phasen Plan, Do, Check und Act:

1. **Plan (Planen)**: In dieser Phase werden Ziele und Prozesse für die Informationssicherheit festgelegt bzw. bestehende angepasst. Dies umfasst die (Weiter-)Entwicklung von Richtlinien, Verfahren und Maßnahmen zur Identifikation, Bewertung und Bewältigung von Sicherheitsrisiken und die Festlegung von Zielen zur Verbesserung der Informationssicherheit.

2. **Do (Umsetzen)**: In dieser Phase werden die geplanten Maßnahmen und Prozesse implementiert. Dies beinhaltet die Schulung der Mitarbeiter, die Implementierung von konkreten Risikomanagement-, Sicherheitsmaßnahmen und -technologien sowie die Einführung von Verfahren zur Erfassung und Überwachung von Sicherheitsvorfällen.
3. **Check (Überprüfen)**: In dieser Phase wird überwacht und bewertet, wie effektiv die implementierten Maßnahmen sind. Dies beinhaltet die Durchführung von Sicherheitsaudits, Überprüfungen von Sicherheitsrichtlinien und -verfahren sowie die Analyse von Sicherheitsvorfällen und -bedrohungen.
4. **Act (Handeln)**: Basierend auf den Ergebnissen der Überprüfung werden Maßnahmen ergriffen, um die Informationssicherheit zu verbessern. Dies kann die Aktualisierung von Sicherheitsrichtlinien und -verfahren, die Implementierung zusätzlicher Sicherheitskontrollen oder die Schulung von Mitarbeitern umfassen.

Durch die kontinuierliche Anwendung des PDCA-Zyklus lässt sich das Managementsystem ständig verbessern, um sich verändernden Bedrohungen und Anforderungen gerecht zu werden und die Informationssicherheit aufrechtzuerhalten.

[Empfehlung: Recherchieren Sie den PDCA-Zyklus weiter im Knowledge Center – suchen Sie einfach nach 'Kontinuierliche Verbesserung', um mehr über den PDCA-Zyklus zu erfahren.]

1.4.2 Prozesse des Managementsystems

Alle im Rahmen des Managementsystems durchzuführenden Aufgaben sind in Managementprozesse, Kernprozesse und Unterstützungsprozesse einteilbar. Unsere Organisation beschreibt in diesem und weiteren Richtliniendokumenten Anforderungen und Verfahren, die die Prozesse des Managementsystems lenken.

2. Ziele der Informationssicherheit

2.1 Zweck

Um die Wirksamkeit des ISMS zu gewährleisten, ist es unverzichtbar, klar definierte Ziele festzulegen und ein robustes Überwachungs- und Messsystem zu implementieren, um den Fortschritt in Richtung dieser Ziele zu verfolgen. Unsere Organisation legt klare Ziele der Informationssicherheit fest und stellt dafür einen effizienten Umsetzungsplan auf, um die kritischen Geschäftsaktivitäten zu schützen und Verpflichtungen gegenüber den interessierten Parteien, einschließlich Kunden, Gesellschaftern, Mitarbeitern und Lieferanten, zu erfüllen.

2.2 Zieldefinition

Es ist von entscheidender Bedeutung, dass:

- Die festgelegten Ziele im Bereich der Informationssicherheit mit der Strategie der Organisation übereinstimmen;
- Die Ziele nach Möglichkeit messbar sind;
- Sie intern (und bei Bedarf auch extern) wirksam kommuniziert werden;
- Sie im Rahmen des ISMS-Management-Review-Prozesses regelmäßig aktualisiert werden.

Die Ziele der Informationssicherheit beruhen auf einem umfassenden Verständnis der Anforderungen aus dem Kontext der Organisation und den rechtlichen, regulatorischen und vertraglichen Anforderungen der Interessengruppen Ihres ISMS festgelegten Anforderungen, und berücksichtigen die Ergebnisse der auf verschiedenen Ebenen innerhalb der Organisation durchgeführten Risikobewertungen.

2.3 Informationssicherheitsziele

Die Festlegung von Zielen der Informationssicherheit erfolgt auf drei Ebenen:

- **Strategische Ziele:** Diese müssen in der Leitlinie für Informationssicherheit formal dokumentiert sein.
- **Taktische Ziele:** Sie werden aus dem Anspruch an die kontinuierliche Verbesserung des Managementsystems und der Informationssicherheit definiert.
- **Operative Ziele:** Sie nennen die konkreten Erwartungen an die Ergebnisse der Maßnahmen im Zusammenhang mit Informationssicherheit.

Die Ziele der jeweiligen Ebenen sollen kaskadierend ineinander übergehen, bzw. aufeinander aufbauen.

[Erstellen Sie bitte ein Verzeichnis der strategischen, taktischen und operativen Ziele. Das Management der taktischen und

operativen Ziele steht in direktem Zusammengang mit den Themenbereichen zur Leistungsbeurteilung des ISMS und sollte in diesem Kontext behandelt werden.]

[Name der Organisation] verwaltet die Ziele der drei definierten Ebenen im [Bitte referenzieren Sie hier auf das Verzeichnis der Informationssicherheitsziele]. Hier erfolgt ebenfalls die Dokumentation der Messkriterien und regelmäßig der Messergebnisse.

3 Beschreibung des Kontext der Organisation

3.1 Zweck

Der Kontext der Organisation in einem ISMS ist die Beschreibung des gesamten Raums, in dem die Informationssicherheit wirkt. Dies beinhaltet die interne und externe Umgebungsstruktur der Organisation. Dazu zählen:

- Der Geschäftszweck
- Wertschöpfungsbereiche und Produktgruppen
- Quantitative Größe, sowie Bedeutung innerhalb einer Branche
- Kundensegmente und Schlüssel-Partnerschaften
- Strategische Business-Ziele, wie z.B. Wachstumspläne

Der Kontext der Organisation spielt zudem eine entscheidende Rolle bei der Festlegung der Informationssicherheitsziele, der Identifizierung von Risiken und Bedrohungen und der Wahl der geeigneten Schutzmaßnahmen.

3.2 Darstellung des Kontext der Organisation

Eine dokumentierte Beschreibung des Kontext der Organisation ist zu finden unter: [Bitte Referenz zur Dokumentation des Kontext der Organisation einfügen].

[Für die Dokumentation des Unternehmenskontexts sind oftmals bestehende Unternehmenspräsentationen z.B. für Neukunden oder neue Partner eine gute Basis, die entsprechend ergänzt werden können.]

4 Interessierte Parteien und deren Anforderungen an die Informationssicherheit

4.1 Zweck

Um alle relevanten internen und externen Erfordernisse und Erwartungen an das ISMS zu erkennen und künftig berücksichtigen zu können, bestimmt unsere Organisation Parteien, die ein berechtigtes Interesse an der Informationssicherheit der Organisation haben und pflegt ein Verzeichnis aller relevanten Anforderungen dieser Parteien. Erfordernisse oder Erwartungen können dabei einen positiven oder negativen Charakter haben.

4.2 Rechtliche, regulatorische und vertragliche Anforderungen der interessierten Parteien

Anforderungen, die interessierte Parteien an die Informationssicherheit von unserer Organisation haben, sind in anzuwendenden Gesetzen, Verordnungen, Richtlinien und Verträgen dokumentiert. Unsere Organisation führt unter dem Namen [Fügen Sie bitte den Titel und den Ablageort des genannten Verzeichnisses ein] ein Verzeichnis der zu berücksichtigenden rechtlichen, gesetzlichen, behördlichen, regulatorischen und vertraglichen Anforderungsdokumente unter Angabe der jeweiligen interessierten Partei.

Das Verzeichnis der rechtlichen, gesetzlichen, behördlichen, regulatorischen und vertraglichen Anforderung, sowie deren interessierten Parteien ist zu finden unter: [Bitte Referenz zum Verzeichnis der Interessierten Parteien einfügen]

5 Anwendungsbereich des ISMS

5.1 Zweck

Der Zweck des Anwendungsbereichs ist die eindeutige Definition der Grenzen des Informationssicherheits-Managementsystems (ISMS) unserer Organisation. Der Anwendungsbereich des ISMS definiert sich im Folgenden durch die Nennung der organisatorischen und physischen Einheiten der Organisation, sowie der IT-System-, Netzwerk- und Infrastruktur und deren Grenzen der Berücksichtigung im ISMS.

5.2 Organisatorische Grenzen

[Führen Sie die Organisationseinheiten (Wertschöpfungsbereiche) in einer angemessenen Detailtiefe in der angefügten Tabelle unter Angabe ob intern oder extern durchgeführt auf, die im Anwendungsbereich des ISMS enthalten sind. Die angegebenen Geschäftstätigkeiten der Organisation umfassen auch Produkt- & Dienstleistungsgruppen.

Bsp:

- Product Management (z.B. Software-Entwicklung)
- Marketing, Sales & Kundenservice
- Finanzen & Controlling
- Personalwesen, Schulung und Training
- IT-System-, Netzwerk- bzw. Benutzer-Administration
- Facility Management
- Informationssicherheitsmanagement
- Datenschutz
- …

Bei Bedarf können Sie die folgende Tabelle zur Gliederung und strukturierten Darstellung verwenden.]

Intern durchgeführte Tätigkeiten	Durch Dienstleister durchgeführte Tätigkeiten

5.3 Physische Grenzen

[Ergänzen Sie bitte eine Beschreibung von physischen Grenzen der Organisation wie z.B. Länder & Standorte, Rechenzentren]

5.4 IT-Systemgrenzen

[Fügen Sie hier eine grafische Darstellung Ihrer System- bzw. Netzwerkarchitektur ein.]

[Führen Sie in der angefügten Tabelle IT-Systeme, Netzwerke und Infrastrukturen in einer angemessenen Detailtiefe auf, um zu verdeutlichen, welche Elemente im Anwendungsbereich des ISMS enthalten sind, und - bei Bedarf - welche aus dem Anwendungsbereich des ISMS herausfallen.ie diese von jenen Netzwerken getrennt gehalten werden, die in den Anwendungsbereich nicht mit einbezogen sind. Unterscheiden Sie zudem zwischen intern und extern gehosteten Services.

bsp.:

- Serverarchitektur
- Datenbanksysteme
- Netzwerke

- Entwicklungs- Test- Produktivumgebung
- …]

Intern gehostet - im ISMS Anwendungsbereich	Extern gehostet - im ISMS Anwendungsbereich

Intern gehostet - außerhalb des ISMS	Extern gehostet – außerhalb des ISMS

5.5 Ausschlüsse

Die folgenden Bereiche sind aus dem Anwendungsbereich des ISMS ausgeschlossen:

[Sofern erforderlich, stellen Sie hier detailliert dar, welche der zuvor identifizierten organisatorischen, physischen und IT-Systemseitigen Einheiten aus dem ISMS ausgeschlossen sind und begründen Sie den Ausschluss. Die Begründung muss mit dem Gesamt-Sicherheitskonzept der Organisation vereinbar sein und darf die Fähigkeit des ISMS, die gewünschten Ergebnisse zu erzielen und seine Ziele zu erreichen, nicht beeinträchtigen.

5.6 [ISO27001] Erklärung zum Geltungsbereich des ISMS

[Eine Zertifizierung nach ISO27001 erfolgt auf Grundlage einer Erklärung zum Geltungsbereich des ISMS. Diese Erklärung besteht aus einer knappen, jedoch aussagefähigen Beschreibung des im vorherigen Kapitel beschriebenen Anwendungsbereichs des ISMS. Sofern sich Ihr ISMS auf die gesamte Organisation mit allen organisatorischen, physischen und System-Elementen bezieht, reicht es, wenn sie dies hier in einem Satz erwähnen (z.B. „Der Anwendungsbereich des ISMS von [Name der Organisation] bezieht sich auf alle organisatorischen, physischen und IT-Systemseitigen Elemente. Es erfolgt kein Ausschluss.) fügen Sie hier Ihre Erklärung zum Geltungsbereich des ISMS unter Angabe der genauen Firmierung und aller Standorte ein.]

6 Rollen und Verantwortlichkeiten im ISMS

6.1 Zweck

Zweck dieser Richtlinie ist die Herleitung von klaren Zuweisungen bzw. Zuständigkeiten mit jeweils definierten Verantwortlichkeiten und Befugnissen der Rollen mit Bezug zur Informationssicherheit, um sicherzustellen, dass jede innerhalb der Organisation tätige Person seine/ihre Zuständigkeit und Verantwortung bei der Aufrechterhaltung der Sicherheit von Informationswerten, für die er/sie verantwortlich ist, versteht. Eine hervorgehobene Rolle im Managementsystem für Informationssicherheit spiel die oberste Leitung der Organisation.

Unter der obersten Leitung unterscheiden wir drei Gruppen von Rollen:

- Organisatorische Rollen
- Rollen des ISMS
- Maßnahmenspezifische Rollen (im Rahmen z.B. von Vorfällen etc.)

Die jeweiligen Gruppen blicken aus unterschiedlichen Perspektiven auf die zugewiesenen Personen, sodass eine einzelne Person mehr als eine Rolle übernehmen kann. Die Zuweisung der Personen zu den definierten Rollen erfolgt entweder durch Benennung oder dadurch, dass eine Person bereits einer Rolle aus einer anderen Gruppe zugeordnet ist.

[Für ein besseres Verständnis der bestehenden Rollen und deren Zusammenhang empfiehlt sich ein Organigramm für die ISMS-Rollen zu erstellen. Im Kapitel "Rollen und Verantwortlichkeiten" des DataGuard Knowledge Centers finden Sie ein beispielhaftes Organigram].

6.2 Führung und Verpflichtung der obersten Leitung

Zur Erfüllung der innerhalb eines ISMS festgelegten Richtlinien und die erforderlichen Prozesse ist die Unterstützung der Leitung der Organisation zwingend erforderlich. So werden Genehmigungen für den Einsatz von Ressourcen auf allen Ebenen (Verantwortlichkeiten, Richtlinien, Personal, Technik) benötigt. Die oberste Leitung der Organisation muss daher Führung und Engagement für Belange der Informationssicherheit und deren Management demonstrieren. Hierzu zählen folgende Aspekte, zu der sich die oberste Leitung verpflichtet:

- Erstellung einer Sicherheitsleitlinie, die Informationssicherheitsziele im Einklang mit der strategischen Ausrichtung der Organisation festlegt.
- Integration der Anforderungen der Informationssicherheit in die Geschäftsprozesse der Organisation
- Bereitstellung der für die Informationssicherheit und deren Management erforderlichen Ressourcen
- Sicherstellung, dass das Managementsystem die erwartete Wirkung und Ergebnisse bringt
- Verpflichtung, Anleitung und Unterstützung von Personen in der Organisation, damit diese die Anforderungen erfüllen und zur Wirksamkeit der Informationssicherheit beitragen
- Förderung von kontinuierlicher Verbesserung
- Förderung und Forderung von Führungskräften, die Informationssicherheit in ihren Verantwortungsbereichen bestmöglich zu stärken.

Eine besonders wichtige Aufgabe fällt der obersten Leitung bei der Bildung eines allgemeinen Bewusstseins (Kultur) für existierende Risiken und Informationssicherheit zu:

- Vermittlung der Bedeutung eines wirksamen Managements der Informationssicherheit
- Erwartung der Erfüllung der definierten Richtlinien und Anforderungen

[Als dokumentierter Nachweis für die Erfüllung der Anforderungen an die oberste Leitung gilt, die im ersten Punkt erwähnte Informationssicherheitsleitlinie. Ihr Inhalt muss allen im Einflussbereich der Organisation arbeitenden Personen bewusst sein. Weitere Nachweise sind z.B. Ansprachen bzw. Mitarbeiterveranstaltungen, die insbesondere das Bewusstsein steigern.]

6.3 Organisatorische Rollen

Aus dem Kontext von unserer Organisation werden organisatorische Rollen definiert, die hierarchische Verantwortlichkeiten, Zuständigkeiten und Befugnisse abbilden. [Name der Organisation] pflegt ein entsprechendes Organigramm unter [Bitte hier auf Speicherort referenzieren oder Organigramm in dieses Dokument einbetten] aus dem die hierarchischen Verantwortlichkeiten bzw. Führungsstrukturen hervorgehen.

6.4 Rollen des ISMS

Das ISMS unserer Organisation sieht die Besetzung der folgenden Rollen vor:

[Nennen Sie hier die in Ihrem ISMS zu besetzenden Rollen und beschreiben Sie die Zuständigkeiten und Befugnisse in den angefügten Abschnitten:

- Oberste Leitung
- Informationssicherheitsbeauftragter (ISB)
- Lenkungsgruppe für Informationssicherheit (ISMS-Team)
- Asset-Eigentümer
- Risiko-Eigentümer
- Interessierte Parteien
- Datenschutzbeauftragter
- Interner Auditor für Informationssicherheit
- Externer Auditor für Informationssicherheit

Achtung: Im Verlauf der weiteren ISMS Dokumentation wird immer wieder auf die hier beispielhaft genannten ISMS-Rollen verwiesen. Wählen Sie daher zu Beginn Ihrer Dokumentation einheitlich zu verwendende Rollenbezeichnungen]

Die spezifischen Zuständigkeiten und Befugnisse jeder dieser Funktionen werden in den folgenden Abschnitten dieses Dokuments erläutert.

Die konkrete Nennung, welche Person welche Rolle übernimmt, erfolgt in[bitte hier auf ein Personenverzeichnis mit Rollenzuweisungen verweisen. Dies kann ein separates Verzeichnis sein, oder ergänzende Rolleninformationen in einem Personal-Verwaltungssystem.].

6.4.1 Klassifizierung des erforderlichen Kompetenzniveaus

Zudem werden in den folgenden Abschnitten die erforderlichen Kompetenzen genannt und das erforderliche Kompetenzniveau nach dem folgenden Schema beziffert:

- Kompetenzniveau 1: Erfordert fundierte Kenntnisse inkl. Umsetzungserfahrung
- Kompetenzniveau 2: Erfordert gute Kenntnisse inkl. Möglichkeiten der Umsetzung
- Kompetenzniveau 3: Erfordert grundlegende Kenntnisse

6.4.2 Oberste Leitung

ROLLENBEZEICHNUNG	Oberste Leitung
KURZBESCHREIBUNG	Die Oberste Leitung ist die gesetzliche Vertretung der Organisation und Initiator von Informationssicherheitsmanagement.
DER ROLLE ZUGEORDNET	Geschäftsführer A …
ZUSTÄNDIGKEITEN	• Beauftragung und Genehmigung zur Schaffung und Aufrechterhaltung eines ISMS • Festlegung der Sicherheitsziele im Einklang mit den strategischen Zielen der Organisation • Festlegung einer Informationssicherheits-Leitlinie • Bereitstellung der erforderlichen Ressourcen • Zuweisung von Verantwortlichkeiten und Sicherstellung, dass die Anforderungen des ISMS in die Geschäftsprozesse der Organisation integriert werden • Förderung einer positiven organisatorischen Einstellung zur Informationssicherheit (Awareness). • Anleitung und Unterstützung der Führungskräfte in ihren Führungsrollen und deren Mitarbeiter, damit diese zur Wirksamkeit des ISMS beitragen können (enablement). • Sicherstellung, dass das ISMS ein beabsichtigtes Ergebnis erzielt (inspect) • Förderung der fortlaufenden Verbesserung (adapt)
BEFUGNISSE	Im Rahmen der allgemeinen Compliance besteht keine explizite Einschränkung der Befugnisse.

KOMPETENZ	**ERFORDERLICHES KOMPETENZ-NIVEAU**
ISMS-Konzepte, Planung und Kontrolle	3
Risikomanagement im Bereich der Informationssicherheit	3
Richtlinien zur Informationssicherheit	3
Durchführung von Managementprüfungen	3
Kontinuierliche Verbesserung	2

Management von Informationssicherheitsvorfällen	2

6.4.3 Informationssicherheitsbeauftragter (ISB)

ROLLENBEZEICHNUNG	Informationssicherheitsbeauftragter (ISB)
KURZBESCHREIBUNG	Der Koordinator für Informationssicherheit oder auch Informationssicherheitsbeauftragter (ISB) genannt, übernimmt die koordinierende Funktion innerhalb des Managementsystems. Er steuert die Management-, Kern- & Unterstützungsprozesse des ISMS und verbindet als Kommunikator die Rollen der Informationssicherheit.
DER ROLLE ZUGEORDNET	Formal Benannter und nachweislich kompetenter und erfahrener Koordinator für Informationssicherheit [oft auch als Information Security Officer (ISO). Wenn erforderlich, kann die übergeordnete Verantwortung für die generelle Informationssicherheit zusätzlich an eine entsprechend kompetente und erfahrene Führungsrolle übergeben werden. Diese wir dann meist als Chief Information Security Officer (CISO) bezeichnet.]
ZUSTÄNDIGKEITEN	• Sicherstellung, dass die Anforderungen an die Informationssicherheit festgelegt und erfüllt werden, um Risiken zu minimieren und die Informationssicherheitsziele wirksam zu erreichen. • Koordination der Management-, Kern- & Unterstützungsprozesse des ISMS. • Ansprechperson bei Informationssicherheitsvorfällen. • Quantifizierung und Überwachung von Art, Umfang und Auswirkungen von Sicherheitsvorfällen und Störungen. • Erstellung des Management Review und Berichterstattung. • Initiierung der kontinuierlichen Verbesserung des ISMS. • Kontaktperson bei Belangen der Informationssicherheit zu externen speziellen Interessengruppen und Behörden.
BEFUGNISSE	• Beratend und koordinierend • Direktes Vortragsrecht bei der obersten Leitung • Zutrittsrecht zu allen Standorten und Bereichen • Informationsrecht bezüglich Informationssicherheitsrelevante Prozesse und Verfahren.

KOMPETENZ: Die Rolle des Koordinators für Informationssicherheit erfordert eine formale Benennung durch die oberste Leitung der Organisation und einen entsprechenden formalen Kompetenznachweis, meist in Form eines Schulungsnachweises bzw. eines entsprechenden Personenzertifikats.	**ERFORDERLICHES KOMPETENZ-NIVEAU**
ISMS-Konzepte, Planung und Kontrolle	1
Organisation der Informationssicherheit	1
Risikomanagement im Bereich der Informationssicherheit	1
Vorbereitung von Management-Reviews	1
Kontinuierliche Verbesserung des ISMS	1
Kalkulation der für Informationssicherheit benötigten Ressourcen	2
Überwachung der Informationssicherheit und Berichterstattung an die oberste Leitung	1
Grundsätze der Auditierung der Informationssicherheit	2

Einhaltung der Compliance	2

6.4.4 Lenkungsgruppe für Informationssicherheit

ROLLENBEZEICHNUNG	Lenkungsgruppe für Informationssicherheit
KURZBESCHREIBUNG	Die Lenkungsgruppe für Informationssicherheit unterstützt und beaufsichtigt den Betrieb des ISMS in Ergänzung zur Obersten Leitung und trägt somit wesentlich zur Wirksamkeit des ISMS bei.
DER ROLLE ZUGEORDNET	• Oberste Leitung • Koordinator für Informationssicherheit • Vertreter der Asset-Eigentümer • Datenschutzbeauftragter • [z.B. Vertreter Interessierter Parteien] …
ZUSTÄNDIGKEITEN	Sicherstellen, dass die Anforderungen an die Informationssicherheit festgelegt und erfüllt werden, um Risiken zu minimieren und die Informationssicherheitsziele wirksam zu erreichen.
BEFUGNISSE	• Identifikation von Änderungen im Kontext der Organisation • Identifikation von Änderungen in Assets und Risiken • Beratung in der Identifikation und Bewertung von Risiken, sowie Priorisierung der Behandlung • Beratung und Unterstützung bei der Definition von Richtlinien, Prozessen und Verfahren des ISMS • Beratung und Unterstützung bei der Umsetzung der ISMS Management-, Kern- & Unterstützungsprozesse.

KOMPETENZ	**ERFORDERLICHES KOMPETENZ-NIVEAU**
ISMS-Konzepte, Planung und Kontrolle	3
Risikomanagement im Bereich der Informationssicherheit	2
Durchführung von Management Reviews	3
Kontinuierliche Verbesserung des ISMS	2
Management von Informationssicherheitsvorfällen	2

6.4.5 Asset Eigentümer

ROLLENBEZEICHNUNG	Asset Eigentümer
KURZBESCHREIBUNG	Übernahme der Verantwortlichkeit für Primär- & Sekundär Assets bzw. Asset-Gruppen der eigenen Organisation oder von interessierten Parteien.

DER ROLLE ZUGEORDNET	• [Organisatorische Rollen, denen die Verantwortung für Assets zugeteilt wurde • z.B. Geschäftsführer • z.B. Personalleiter • z.B. IT-Leiter • z.B. …].
ZUSTÄNDIGKEITEN	Sicherstellen, dass die individuellen Anforderungen der Assets an die Informationssicherheit festgelegt und erfüllt werden. Definition des Schutzbedarfs bzw. der Schutzklasse der Assets bzw. der Asset-Gruppen. Aufrechterhaltung und Überprüfung der Sicherheitskontrollen für zugewiesene Vermögenswerte. Freigabe von Zugriffsrechten auf die zugeteilten Assets.
BEFUGNISSE	• Definition des Schutzbedarfs • Zuteilung von Schutzklassen • Vergabe bzw. Genehmigung von Zugriffsrechten

KOMPETENZ	**ERFORDERLICHES KOMPETENZ-NIVEAU**
ISMS-Konzepte, Planung und Kontrolle	2
Asset-Management	1
Klassifizierung von Informationen	1
Risikomanagement im Bereich der Informationssicherheit	2
Grundsätze der Kontrolle der Informationssicherheit	2

6.4.6 Risiko Eigentümer

ROLLENBEZEICHNUNG	Risiko Eigentümer
KURZBESCHREIBUNG	Übernahme der Verantwortlichkeit für identifizierte bzw. nach einer Behandlung verbliebene Informationssicherheitsrisiken.
DER ROLLE ZUGEORDNET	• [Organisatorische Rollen, denen die Verantwortung für Risiken zugeteilt wurde • z.B. Leiter IT • z.B. Facility Manager • z.B. IT-Leiter • z.B. …].
ZUSTÄNDIGKEITEN	Verantwortlich für die Überwachung und das Management von spezifischen Risiken für die Informationssicherheit. Sicherstellen, dass Risiken in angemessenem Maße behandelt (Gemindert, vermieden, geteilt, akzeptiert) werden. Aufrechterhaltung und Überprüfung von Sicherheitskontrollen, die das/die verwaltete(n) Risiko(e) behandeln. Teilnahme an den Bewertungen der zugeteilten Risiken. Kontaktaufnahme mit dem/den Eigentümer(n) der von dem/den Risiko(s) betroffenen Informationswerte(n).

BEFUGNISSE	• Beratend bei der Bewertung von Risiken • Beratend und unterstützend bei der Behandlung von Risiken. • Eskalation an das Management, wenn Risiken nicht angemessen behandelt werden. • Genehmigung der Höhe des Restrisikos, nachdem im Risikobehandlungsplan Behandlungsmaßnahmen festgelegt wurden.

KOMPETENZ	**ERFORDERLICHES KOMPETENZ-NIVEAU**
ISMS-Konzepte, Planung und Kontrolle	2
Risikomanagement im Bereich der Informationssicherheit	2
Behandlung von Informationssicherheitsrisiken	1
Grundsätze der Kontrolle der Informationssicherheit	2

6.4.7 Interessierte Partei

ROLLENBEZEICHNUNG	Interessierte Partei
KURZBESCHREIBUNG	Bestimmte interne und externe Interessensgruppen einer Organisation in Bezug auf Informationssicherheit.
DER ROLLE ZUGEORDNET	Siehe separates Verzeichnis “Interessierte Parteien“ [Bitte referenzieren Sie hier zum Verzeichnis „Interessierte Parteien“]
ZUSTÄNDIGKEITEN	Nennung und Vertretung der Interessen von Interessierten Parteien im Allgemeinen und speziellen.
BEFUGNISSE	Einfordern der gesetzlich, regulativ oder vertraglich zugesicherten Vorgaben in der Informationssicherheit (Compliance).
KOMPETENZ Keine expliziten Anforderungen an KOMPETENZ	

6.4.8 Datenschutzbeauftragter

ROLLENBEZEICHNUNG	Datenschutzbeauftragter
KURZBESCHREIBUNG	Der Datenschutzbeauftragte schützt die personenbezogenen Daten.
DER ROLLE ZUGEORDNET	Vom Verantwortlichen für den Datenschutz (Oberste Leitung) formal Benannter und nachweislich kompetenter und erfahrene interne oder externe Person.
ZUSTÄNDIGKEITEN	Das Hinwirken auf die Einhaltung aller relevanten Datenschutzvorschriften, die Überwachung bestimmter Prozesse, wie Datenschutz-Folgenabschätzung, Sensibilisierung und Schulung der Mitarbeiter. Kontaktperson zu interessierten Parteien des Datenschutzes, sowie Aufsichtsbehörden.
BEFUGNISSE	• Beratend und koordinierend • Direktes Vortragsrecht gegenüber der Obersten Leitung • Zutrittsrecht zu allen Bereichen • Informationsrecht bezüglich Datenschutzrelevanter Prozesse und Verfahren.

KOMPETENZ	**ERFORDERLICHES KOMPETENZ-NIVEAU**
ISMS-Konzepte, Planung und Kontrolle	3

Rechtsvorschriften zum Datenschutz	1
Datenschutz-Folgenabschätzungen	1
Risikomanagement im Bereich der Informationssicherheit	2
Grundsätze der Kontrolle der Informationssicherheit	2

6.4.9 Interner Auditor für Informationssicherheit

ROLLENBEZEICHNUNG	Interner Auditor für Informationssicherheit
KURZBESCHREIBUNG	Durchführende Person eines systematischen, unabhängigen und dokumentierten internen Prozesses zur Erlangung objektiver Nachweise und Bewertung, inwieweit die Auditkriterien erfüllt sind.
DER ROLLE ZUGEORDNET	Unabhängige, nicht mit der Definition oder operativen Umsetzung der auditierten Richtlinien, Verfahren und Prozesse beteiligt sind/waren.
ZUSTÄNDIGKEITEN	Planung, Einführung, Umsetzung und Aufrechterhaltung eines Auditprogramms, einschließlich der Häufigkeit, Methoden, Zuständigkeiten, Planungsanforderungen und Berichterstattung. Festlegung der Prüfungskriterien und des Prüfungsumfangs für jede Prüfung. Durchführung von internen Audits in geplanten Abständen. Sicherstellen, dass der Prüfungsprozess objektiv und unparteiisch ist. Sammlung von Nachweisen und Bewertung, inwieweit die Umsetzung im Einklang mit rechtlichen, regulativen und vertraglichen Anforderungen steht. Dokumentation der Ergebnisse und Berichterstattung über die Ergebnisse der Prüfungen an das zuständige Management.
BEFUGNISSE	• Informationsrecht bezüglich Informations- & Datenschutzrelevanter Prozesse und Verfahren. Untersuchung von Verfahren und Kontrollen im Zusammenhang mit der Informationssicherheit, um ihre Eignung und Wirksamkeit zu bewerten. • Meldung der Ergebnisse an das zuständige Management. • Zutrittsrecht zu allen relevanten Bereichen • Bewertung der Einhaltung der rechtlichen, regulativen und vertraglichen Anforderungen.

KOMPETENZ	**ERFORDERLICHES KOMPETENZ-NIVEAU**
ISMS-Konzepte, Planung und Kontrolle	1
Planung, Einführung, Umsetzung und Pflege eines Auditprogramms	1
Risikomanagement im Bereich der Informationssicherheit	1
Grundsätze der Kontrolle der Informationssicherheit	1

6.4.10 Externer Auditor für Informationssicherheit

ROLLENBEZEICHNUNG	Externer Auditor für Informationssicherheit
KURZBESCHREIBUNG	Durchführende Person eines systematischen, unabhängigen und dokumentierten Prozesses zur Erlangung objektiver Nachweise und Bewertung, inwieweit die Auditkriterien erfüllt sind.
DER ROLLE ZUGEORDNET	Vertreter einer beauftragten unabhängigen und akkreditierten Zertifizierungsgesellschaft, die nicht an der Definition, Implementierung oder Durchführung des ISMS beteiligt ist/war.
ZUSTÄNDIGKEITEN	Sammlung von Nachweisen, was die auditierte Organisation machen möchte, was sie macht und wie. Bewertung, inwieweit die Umsetzung im Einklang mit rechtlichen, regulativen und vertraglichen Anforderungen steht. Dokumentation der Ergebnisse.

BEFUGNISSE	• Zutrittsrecht zu allen relevanten Bereichen • Informationsrecht bezüglich Informations- & Datenschutzrelevanter Prozesse und Verfahren. • Bewertung der Einhaltung der rechtlichen, regulativen und vertraglichen Anforderungen.

KOMPETENZ	**ERFORDERLICHES KOMPETENZ-NIVEAU**
Akkreditierter Auditor	1
Planung, Einführung, Umsetzung und Pflege eines Auditprogramms	1
Risikomanagement im Bereich der Informationssicherheit	1
Grundsätze der Kontrolle der Informationssicherheit	1

[Ergänzen Sie bitte bei Bedarf weitere Profile von Ihnen eingesetzte ISMS-Rollen.]

6.5 Maßnahmenspezifische Rollen

Einzelne im Geltungsbereich des ISMS befindliche Maßnahmen erfordern die Benennung von weiteren Rollen, um Zuständigkeiten, Verantwortlichkeiten und Befugnisse festzulegen. Diese Rollen werden in den themenspezifischen Dokumenten der Maßnahmen näher beschrieben.

[Bsp:

- Personal-Sicherheits-Manager
- Lieferanten-Manager (SCM)
- Anwendungs- & Entwicklungsmanager
- Projekt-Manager
- Liegenschafts-Manager
- Netzwerk-Manager
- Identitäts- & Zugangsmanager (IAM)
- Geschäftskontinuitätsmanager (BCM)
- Vorfall-Reaktions-Team (IRT)
- ...

Achtung: Im Verlauf der weiteren ISMS Dokumentation wird immer wieder auf die hier beispielhaft genannten Maßnahmenspezifischen-Rollen verwiesen. Sollten Sie diese Rollen hier ändern, ergibt sich an zahlreichen weiteren Stellen der ISMS-Dokumentation weiterer Änderungsbedarf.]

6.6 Trennung von Verantwortlichkeiten

Im Rahmen der Rollenaufteilung und Zuordnung muss sichergestellt werden, dass Verantwortlichkeiten so verteilt sind, dass objektive Prüfmechanismen bestehen und Interessenskonflikte vermieden werden. Dies trägt dazu bei, Manipulationen, Fehler oder unbefugte Änderungen zu verhindern.

6.7 ISMS-Verantwortungsmatrix

Es muss sichergestellt werden, dass alle beauftragten Personen und Gruppen ihre Aufgaben und Verantwortlichkeiten im Rahmen des ISMS und ihre Rolle bei der Sicherung der Informationsbestände verstehen. Verantwortlich hierfür ist die Oberste Leitung der Organisation.

Eine Übersicht der Zuordnungen von Rollen und deren Verantwortlichkeiten und Befugnisse zu den ISMS-Prozessen und den Maßnahmen im Geltungsbereich des ISMS erfolgt in einer innerhalb der Organisation zu kommunizierenden ISMS-Verantwortungsmatrix (RASCI-Matrix).

Die Zuständigkeiten, Verantwortlichkeiten und Befugnisse der im Zusammenhang mit Informationssicherheit stehenden Rollen sind in der RASCI-Matrix dargestellt. Darin wird je Bereich die Art der Zuständigkeit jeder Rolle nach dem folgenden Schema definiert:

- **R: (Responsible)** Verantwortlich, d.h. diese Rolle trägt die Hauptverantwortung für

die Durchführung der Aktivitäten in diesem Abschnitt.

- **A: (Accountable)** Rechenschaftspflichtig, d. h. diese Rolle wird zur Rechenschaft

gezogen, wenn die Risiken eintreten (normalerweise, weil präventive Kontrollen

versagen): Dies ist im Allgemeinen der Budgetverantwortliche.

- **S: (Supported)** Unterstützend, d. h. diese Rolle hilft aktiv bei der Gestaltung, Umsetzung oder Verwaltung der Aktivitäten in diesem Abschnitt.
- **C: (Consulted)** Konsultiert, d.h. dies ist eine praktische Rolle, die den aktiven Beteiligten Anleitung bietet.
- **I: (Informed)** Informiert, d. h. diese Rolle hat ein Interesse am Status der Risiken in diesem Bereich und sollte über die Situation auf dem Laufenden gehalten werden.

[Fügen Sie hier eine Verlinkung bzw. Referenzangabe zum Verzeichnis RASCI-Matrix ein]

6.8 ISMS Ressourcen

Um die Informationssicherheitsziele der Organisation zu erreichen, ist die Bereitstellung der erforderlichen zeitlichen sowie finanziellen Ressourcen erforderlich. Diese müssen ermittelt, kalkuliert und dauerhaft bereitgestellt, bzw. genehmigt werden. Hierzu zählen einerseits Ressourcen, die für den Aufbau und Betrieb des Managementsystems für Informationssicherheit entlang des kontinuierlichen Verbesserungsprozesses erforderlich sind (u.A. Personal, Prozesse, Expertisen, Aus- und Fortbildung, Test- und Uberprüfungsverfahren). Andererseits sollen alle zeitlichen und finanziellen Ressourcen identifiziert werden, die für die Erreichung der taktischen und operativen Ziele der Informationssicherheit erforderlich sind, wie zum Beispiel noch nicht umgesetzte Maßnahmen aus der Risikobehandlung. Der Koordinator (ISB) für Informationssicherheit muss einen Überblich der erforderlichen Ressourcen erstellen und diesen regelmäßig mit der obersten Leitung der Organisation abstimmen.

[Erstellen Sie bitte einen entsprechenden Personal- & Finanzmittelbedarf, der im Rahmen des Management-Reviews besprochen und genehmigt wird. Dokumentieren Sie darin die im Management-Review getroffenen Ressourcen-Entscheidungen].

7. Kommunikation

7.1 Zweck

Dieses Dokument beschreibt die Methoden, mit denen die Kommunikation in Bezug auf die Informationssicherheit sowohl mit internen als auch mit externen Parteien, die mit unserer Organisation verbunden sind, hergestellt wird. Es legt die Mittel zur Einrichtung effektiver Kommunikationskanäle fest:

- Identifizikation des Empfängerkreises von Kommunikation (Interessierte Parteien)
- Definition geeigneter Kommunikationsthemen für jede interessierte Partei
- Einigung auf die am besten geeigneten Methoden für Engagement und Kommunikation
- Umsetzung des Kommunikationsprogramms
- Einholung und Berücksichtigung von Rückmeldungen zur Wirksamkeit der Kommunikation, die in den Plan zur kontinuierlichen Verbesserung einfließen werden.

Diese Schritte werden in separaten Abschnitten behandelt, die jeweils detaillierte Anleitungen und Verfahren enthalten.

7.2 Empfängerkreis

Das Ziel dieses Kommunikationsprogramms ist es, sowohl interne als auch externe interessierte Parteien einzubeziehen, die zum Funktionieren und Wachstum des ISMS beitragen. Zur genaueren Betrachtung des Empfängerkreises soll das Verzeichnis der interessierten Parteien unserer Organisation hinzugezogen werden.

7.3 Themen

Das Kommunikationsprogramm soll die wesentlichen Faktoren in den folgenden Hauptbereichen erläutern:

- Das geschäftliche Umfeld, in dem das ISMS betrieben wird, einschließlich wesentlicher Änderungen, sobald diese auftreten
- Der Gesamtrahmen des ISMS, einschließlich der Vision, der Richtlinien, Pläne und Ziele, die erreicht werden sollen
- Wie sich die Etablierung des ISMS auf bestimmte Geschäftsprozesse im Unternehmen auswirkt
- Wie sich die vorhandenen Informationssicherheitsmaßnahmen (Controls) auf die Bedürfnisse und die Geschäftsziele des Unternehmens beziehen
- Wie das ISMS die geschäftlichen Anforderungen erfassen und erfüllen soll, um die Geschäftsziele der Organisation zu unterstützen
- Die gesetzlichen, regulatorischen und vertraglichen Anforderungen und Einschränkungen, unter denen das ISMS arbeiten muss
- Aktualisierungen der Fortschritte bei der Erreichung der festgelegten ISMS-Ziele
- Bewusstsein für Fragen der Informationssicherheit, für Risiken und für die Vorgehensweise bei deren Bewältigung.

7.4 Kommunikationsmethoden

Die im folgenden Abschnitt beschriebenen Kommunikationsmethoden verwendet die Organisation. Dazu gehören regelmäßige Teamsitzungen, Briefings, Newsletter und jährliche Veranstaltungen. Darüber hinaus werden zusätzliche Methoden eingeführt, entweder vorübergehend oder dauerhaft, um die bestehenden Kanäle zu ergänzen.

Workshop
Das ISMS Team präsentiert der gesamten Belegschaft – den internen wie externen Mitarbeitern – die Anforderungen an die Umsetzung eines dokumentierten ISMS und die Auswirkungen auf die Geschäftsprozesse des Unternehmens.

Management-Briefings
Das ISMS Team bietet dem Führungsteam regelmäßige Briefings zu vorrangigen Angelegenheiten im Zusammenhang mit dem Informationssicherheitsmanagement.

Sicherheitsschulung
Alle Mitarbeiter müssen mindestens einmal jährlich eine Sicherheitsschulung absolvieren. Diese Schulung umfasst für das ISMS relevante Themenbereiche.

Wöchentliche Team-Runden
Ein Mitglied des ISMS Teams informiert anlassbedingt die Runde über spezielle Sicherheitsthemen, Geschäftsprozessen, Veränderungen, etc.

Briefing-E-Mails
Je nach Bedarf informiert das ISMS Team alle Mitarbeiter über notwendige Änderungen im Zusammenhang mit den Betriebsverfahren zur Unterstützung des ISMS.

Persönliches Einzelgespräch
Die Geschäftsleitung führt nach Bedarf mit einem Mitarbeiter ein Einzelgespräch zwecks Aufklärung, Ermahnung, Verwarnung, Maßregelung oder anderer disziplinarischen Maßnahmen.

[Bitte passen Sie die Beschreibung der Kommunikationsmethoden an Ihre Organisation an.]

7.5 Kommunikationsplan

Unsere Organisation bestimmt in einem Kommunikationsplan

- Wann kommuniziert wird
- Mit wem kommuniziert wird
- Wie und worüber kommuniziert wird

[Nennen Sie hier bitte den Dokumentennamen des zu erstellenden Kommunikationsplans. Der Kommunikationsplan kann auch aus einer Zusammenstellung von verschiedenen Kommunikationselementen in Ihrem ISMS Aufgabenmanagement bestehen und als filterbare Aufgaben für mindestens ein Jahr im Voraus terminiert werden.]

8 Dokumentenlenkung

8.1 Zweck

Diese Richtlinie soll die angemessene Erstellung, Genehmigung, Verteilung, Verwendung und Aktualisierung von Dokumenten und Aufzeichnungen (auch dokumentierte Informationen genannt) sicherstellen, die im Informationssicherheitsmanagementsystem (ISMS) unserer Organisation verwendet werden.

Das Verfahren wird auf alle intern oder extern erstellte Dokumente und Aufzeichnungen im Zusammenhang mit dem ISMS angewandt, unabhängig von der Form, in der sie gespeichert sind.

8.2 Dokumentierte Information

8.2.1 Dokumenteninformationen

Alle Dokumente, die innerhalb der Organisation für das ISMS erstellt werden, müssen zudem die folgenden Dokumenteninformationen geben:

- Name der Organisation
- Titel des Dokuments
- Eigentümer des Dokuments
- Geprüft von
- Prüfdatum
- Gültig ab
- Nächste Überprüfung
- Vertraulichkeitsklasse
- (sofern in DIN formatiert) Seiten-Nummer

8.2.2 Versionshistorie

Zur Nachverfolgbarkeit der Änderungen im Dokument werden Änderungen mit Versionsnummer, Datum der letzten Änderung, Bearbeiter und Beschreibung der Änderung.

- Datum
- Version
- Erstellt von
- Beschreibung der Änderung

8.2.2 Dokumentenablage

[Bitte beschreiben Sie hier die Ablage und den Ablageort der ISMS-Dokumente]

8.2.3 Veröffentlichung von relevanten Dokumenten

Eine Veröffentlichung der Dokumente erfolgt im Anwendungsbereich des ISMS und an die Personengruppen, für die eine Kenntnisnahme zur Erfüllung ihrer Rolle erforderlich ist

Sobald ein neues Dokument oder eine neue Version eines Dokuments veröffentlicht wird, hat eine Information an alle als Nutzer des Dokuments festgelegten Personen zu erfolgen.

Wenn eine ältere Version des Dokuments existiert, muss dieses aus dem Ordner für gültige Dokumente gelöscht und in den Archivordner verschoben werden.

8.2.4 Dokumente mit hoher Vertraulichkeitsstufe

[Bitte beschreiben Sie hier die Verfahren zum Schutz von Dokumenten mit hoher Vertraulichkeitsstufe (z.B. besonders reglementierter Speicherort, Zugriffsrechte, Verschlüsselungsmaßnahmen, etc.)]

8.2.5 Überprüfung und Aktualisierung

Die Person, die als Dokumenten-Eigentümer benannt ist, ist für eine regelmäßige Überprüfung und ggf. eine Aktualisierung des Dokuments verantwortlich. Die Überprüfung erfolgt in den für jedes Dokument festgelegten Abständen, mindestens jedoch einmal pro Jahr.

[Bitte berücksichtigen Sie die Überprüfungen in Ihrem ISMS Aufgabenmanagement]

Die Änderungen gegenüber der Vorgängerversion sind in der "Versionshistorie", die jedem Dokument beigefügt werden muss, kurz zu beschreiben.

8.2.6 Aufzeichnungen zu Dokumenten

Schutz von Aufzeichnungen

Aufzeichnungen, wie z.B. dokumentierte Protokolle können mit personenbezogenen Daten Aufschluss auf Verhaltensmuster und persönliche Präferenzen geben und bieten besonderes Risikopotential in Bezug auf Vertraulichkeit. Um potenzielle Risiken für die Privatsphäre zu erkennen und zu minimieren, soll daher für jedes interne Dokument des ISMS festgelegt werden, wie die aus seiner Verwendung resultierenden Aufzeichnungen zu behandeln sind. Diese Definition muss folgendes beinhalten:

- Titel der Aufzeichnung
- Ort der Speicherung/Aufbewahrung
- Die für die Aufbewahrung verantwortliche Person
- Maßnahmen zum Schutz der Aufzeichnungen
- Aufbewahrungsfrist.

Der Zugang zu den archivierten Aufzeichnungen (Loggs) ist für die Mitarbeiter der Organisation nur mit Genehmigung der Person möglich, die für die Aufbewahrung der jeweiligen Aufzeichnungen verantwortlich ist.

Wenn Unterlagen so sensible Informationen enthalten, dass die Erlaubnis für den Zugang von einer anderen Person erteilt werden muss, muss dies in dem entsprechenden internen Dokument in dem Kapitel, das beschreibt, wie Unterlagen kontrolliert werden, angegeben werden.

Die Befugnisse für den Zugang zu und die Einsicht in Unterlagen werden vom Eigentümer der jeweiligen Unterlagen (Asset-Eigentümer) festgelegt.

Die für die Aufbewahrung der Aufzeichnung benannte Person ist für die Vernichtung aller Unterlagen verantwortlich, deren Aufbewahrungsfrist abgelaufen ist.

Verwaltung der Aufzeichnungen

Alle aus der Verwendung eines Dokuments resultierenden Aufzeichnungen müssen in das zentrale Verzeichnis der Aufzeichnungen der Organisation unter Angabe folgender Informationen aufgenommen werden:

- Name der Aufzeichnung
- Aufbewahrungsort
- Für Aufbewahrung verantwortliche Person
- Sicherheitsmaßnahmen zum Schutz der Aufzeichnungen
- Aufbewahrungsfrist
- Inhalt personenbezogener Daten
- Vertraulichkeitsklassifizierung

9. Inventar der Informationswerte

9.1 Zweck

Für jede Organisation ist es wichtig, die Informationen zu kennen, die einen wesentlichen Wert für sie darstellen (z. B. Geschäftsgeheimisse, kritische Geschäftsprozesse, Know-How, Patente). Ebenso wichtig ist zu identifizieren, welche informationsverarbeitenden und informationsunterstützenden Einrichtungen, Infrastrukturen und Geräte die Organisation benötigt, um die Vertraulichkeit, Verfügbarkeit und den beabsichtigten Betrieb der Informationswerte zu gewährleisten. Unsere Organisation pflegt ein Inventar in [bitte nennen Sie den Ort Ihres Asset Inventars, z.B. die DataGuard Plattform] die Aufschluss über folgende Informationen gibt:

9.2 Verzeichnisinformationen

- Asset Typ (Primär- oder Sekundär-Asset Unterscheidung z.B. von TISAX verlangt)
- Asset Name
- Asset-ID
- Asset-Owner (z.B. Business-Rolle)
- Asset Beschreibung (z.B. Charakter des Assets, Angabe des Orts des ursprünglichen Verzeichnisses, ...)
- Asset-Kategorie (hilfreich zur Bündelung von einzelnen Assets in Gruppen)
- Personenbezogene Daten (Ja/Nein)
- Sensible Kundendaten (Ja/Nein)
- Vertraulichkeit (Hoch, Mittel, Niedrig, Keine)
- Integrität (Hoch, Mittel, Niedrig, Keine)
- Verfügbarkeit (Hoch, Mittel, Niedrig, Keine)
- Überprüfungsintervall (monatlich, alle 3; bzw. 6; bzw. 12 Monate)
- Datum letzte Überprüfung
- Datum nächste Überprüfung
- Bei Bedarf weitere individuelle Felder zum Management von Assets

[Sofern die Verfügbarkeit Ihrer digitalen Assets eine besondere Rolle spielt, ergänzen Sie Felder aus Ihrer Business Impact Analyse zur Behandlung im Business Continuity Management hinzu:

- RTO (Recovery Time Objective) in Std.
- RPO (Recovery Point Objective) in Std.
- MTD (Maximal tolerierbare Ausfallzeit) in Std.
- Existiert ein Notfall-Wiederherstellungsplan (Ja/Nein)
- Backup-Intervall
- Lizenz-Erneuerungsintervall]

Diese werden als Informationswerte bezeichnet. Durch eine Inventarisierung wird sichergestellt, dass die Organisation einen Überblick über ihre Informationswerte erhält. Darüber hinaus ist es wichtig, die Informationsträger (z. B. IT-Systeme, Services/IT-Dienste, Mitarbeiter) zu kennen, welche diese Informationswerte verarbeiten.

10. Risikomanagement

10.1 Zweck

Zweck dieser Richtlinie ist es, die Methodik für die Beurteilung, Bewertung und Behandlung von

Informationssicherheitsrisiken in der [Name der Organisation] klar zu definieren und das akzeptable Risikoniveau standardisiert festzulegen, um so die Konsistenz, Gültigkeit und Vergleichbarkeit von Informationssicherheitsbeurteilungen sicherzustellen. Ziel ist, dass ein wiederholter Bewertungsprozess zu vergleichbaren Ergebnissen führt.

Die Anwendung eines dokumentierten Verfahrens des Risikomanagements innerhalb der DataGuard Plattform[ggf. abweichenden Risiko-Management Ort nennen] erfordert eine entsprechende Qualifizierung der durchführenden Personen, sowie eine Überwachung durch interne Audits. Ein kontinuierlicher Verbesserungsprozess soll eine dauerhaft hohe Qualität von Informationssicherheits-Risikobeurteilungen sicherstellen.

Die Methodik wird auf den gesamten Geltungsbereich des Informationssicherheits-Managementsystems (ISMS) angewandt, d.h. auf alle Szenarien und Informationswerte, die innerhalb der Organisation vorkommen oder verwendet werden.

[Bitte ändern Sie die folgenden Abschnitte, sofern Sie ein anderes Verfahren in Ihrer Organisation praktizieren. Beachten Sie, dass ein Auditor nach dokumentierten Nachweisen für den beschriebenen Prozess verlangen wird. Seien Sie daher für ein Audit entsprechend vorbereitet und in der Lage, dokumentierte Nachweise für die Durchführung eines solchen Prozesses in einem Audit vorzuzeigen].

10.2 Risikobewertung

10.2.1 Bestimmung der Chancen und Risiken im ISMS

Basis einer Risikobewertung ist die Identifikation von zu behandelnden Aspekten aus dem Kontext der Organisation und aus den Interessierten Parteien, sowie deren rechtlichen, regulatorischen und vertraglichen Anforderungen an die Informationssicherheit unserer Organisation. Solche Aspekte können sowohl Chancen als auch Risiken darstellen und müssen bestimmt werden. Da sich im Laufe der Zeit diese so identifizierten Chancen und Risiken verändern, sind diese regelmäßig vor einer Risikobewertung zu bestimmen und im Bewertungsprozess zu berücksichtigen.

10.2.2 ISMS-Lenkungsgruppe (ISMS-Team) und Risiko-Eigentümer

Der Koordinator für Informationssicherheit (ISB) initiiert und steuert den Risikobewertungsprozess und führt diesen gemeinsam mit dem ISMS-Team durch.

Das ISMS-Team legt für jedes identifizierte Risiko einen Risiko-Eigentümer fest. Die Festlegung und Bestimmung des Risikoeigentümers erfolgt nach den folgenden Kriterien:

- **Verantwortlichkeiten und Befugnisse:** Der Risikoeigentümer soll über die erforderliche Autorität und Befugnis verfügen, um Entscheidungen hinsichtlich des Risikomanagements treffen zu können.
- **Geschäftsziele und -Interessen:** Der Risikoeigentümer soll ein Verständnis der Geschäftsziele und der Geschäftsinteressen haben, die von den zu schützenden Prozessen, Informationen und Systemen abhängen.
- **Kenntnisse und Erfahrung:** Der Risikoeigentümer soll über ausreichende Kenntnisse und Erfahrungen im Bereich der Informationssicherheit und des Risikomanagements verfügen.
- **Verfügbarkeit und Ressourcen:** Der Risikoeigentümer soll die notwendigen personellen, finanziellen oder technologischen Ressourcen und Unterstützung erhalten, um seine Aufgaben effektiv wahrnehmen zu können.
- **Kommunikationsfähigkeiten:** Der Risikoeigentümer soll über gute Kommunikationsfähigkeiten verfügen, um innerhalb der Organisation effektiv zu interagieren.

10.2.3 Auslöser der Durchführung von Risikobewertungen

Neben einem geplanten regelmäßigen (mindestens einmal im Jahr) Risiko-Bewertungstermin[Bitte berücksichtigen Sie die regulären Risiko-Bewertungstermine in Ihrem ISMS-Aufgabenmanagement.] sollen folgende Auslöser im Geschäftsbetrieb zu weiteren Bewertungen der Risiken führen:

- Initial bei Einführung des ISMS
- Bei wesentlichen Änderungen
- In der Design-Phase von Projekten
- Bei Änderungen in Projekten
- Wenn Ausnahmen von getroffenen Regelungen erfolgen

- Bei Bekanntwerden von neuen Bedrohungen
- Bei Bekanntwerden von neuen Schwachstellen
- Bei Bekanntwerden von Informationssicherheitsvorfällen in der Organisation
- Nach Durchführung von Ursachenanalysen im Rahmen des Verfahrens zur Behandlung von Informationssicherheitsvorfällen
- Nach Durchführung von Ursachenanalysen im Rahmen des Verfahrens zur Behandlung von Nichtkonformitäten
- Vor dem Abschluss von Verträgen mit Lieferanten und Service Providern gemäß den Vorgaben der Sicherheitsrichtlinie für Lieferantenbeziehungen (z.B. Cloud Dienste)
- Bei Bekanntwerden von Änderungen an ausgelagerten Diensten
- Bei Bekanntwerden von Informationssicherheitsvorfällen bei Kunden, Lieferanten und Service-Providern
- Bei wesentlichen Risiken (Risiken, die das Potential haben, bei näherer Betrachtung als inakzeptabel eingestuft zu werden. Davon ist auszugehen, wenn der Wert der betroffenen Informationswerte als kritisch für das Unternehmen anzusehen ist oder ein hohes Risiko für Betroffene im Sinne der DSGVO vorliegt.)

10.2.4 Prozess der Risikobewertung

Unsere Organisation wendet im Risikomanagement der DataGuard-Plattform ein szenarien-basiertes Risikobewertungsschema an, das sich auf die Eintrittswahrscheinlichkeit und die Auswirkungen von Risikoszenarien konzentriert. Das bedeutet, dass sich die beschriebenen Risiken jeweils auf spezifische Gefahren- oder Schwachstellenszenarien beziehen, die innerhalb des ISMS-Anwendungsbereichs der Organisation auftreten können. Jedes Risikoszenario wird separat betrachtet und bewertet, um eine detaillierte Einschätzung zu ermöglichen.

Der Prozess zur Risikobewertung besteht aus den folgenden Schritten:

1. Risikoidentifikation und Analyse:
   - Risikobeschreibung
   - Bestimmung möglicher Risikoursachen
   - Bestimmung möglicher Risikobedingungen
   - Bestimmung möglicher Risikofolgen
   - Identifikation der betroffenen Geschäftsfunktion
   - Zuweisung eines Risikoverantwortlichen (Risiko-Eigentümer)
2. Risiko-Bewertung:
   - Risikobeurteilung der Auswirkung auf die Organisation
   - Risikobeurteilung der Wahrscheinlichkeit des Eintritts
3. Begründung der Bewertung
4. Berechnung des Risiko-Niveaus

10.2.5 Risikobewertungsschema

[Bitte wählen Sie das von Ihnen in der DataGuard-Plattform verwendete Bewertungsschema (3x3; 4x4; 5x5) aus und löschen Sie die zwei nicht zutreffenden Beschreibungen im folgenden Abschnitt]

10.2.5 a 3-stufiges Risikobewertungsschema **[Wenn nicht zutreffend, bitte Abschnitt löschen]**

Im auf der DataGuard-Plattform durchgeführten Risikomanagement werden die Auswirkungen auf die Organisation und die Eintrittswahrscheinlichkeit des jeweiligen Szenarios gemäß einer festgelegten Bewertungsskala in jeweils drei Stufen definiert.

Bewertungsskala der Auswirkungen auf die Organisation:

RISIKONIVEAU	BEWERTUNG	DEFINITION DER MÖGLICHEN AUSWIRKUNGEN
Ertragbar	1 (grün)	Die Konsequenzen des Ereignisses haben geringe Auswirkungen und führen zu ertragbaren Störungen der Organisation.
Schwerwiegend	2 (gelb)	Die Konsequenzen des Ereignisses verursachen beträchtliche Störungen und gefährden die Geschäftsziele und/oder Reputation der Organisation.
Existenzgefährdend	3 (rot)	Die Konsequenzen des Ereignisses verursachen immense Störungen und können die Existenz der Organisation gefährden.

Bewertungsskala der Eintrittswahrscheinlichkeit:

RISIKONIVEAU	BEWERTUNG	DEFINITION DER MÖGLICHEN WAHRSCHEINLICHKEIT
Selten	1 (grün)	Das Ereignis tritt voraussichtlich wenige male innerhalb von 5 Jahren ein.
Häufig	2 (gelb)	Das Ereignis tritt voraussichtlich wenige male pro Jahr ein.
Sehr häufig	3 (rot)	Das Ereignis tritt voraussichtlich mindestens einmal monatlich ein.

Durch Eingabe der Auswirkungs- und Wahrscheinlichkeitswerte in die Plattform wird das Risikoniveau automatisch durch Multiplikation der beiden Werte berechnet.

RISIKOMATRIX		WAHRSCHEINLICHKEIT		
		Selten	Häufig	Sehr häufig
AUSWIRKUNGEN	Ertragbar	1 (grün)	2 (grün)	3 (gelb)
	Schwerwiegend	2 (grün)	4 (gelb)	6 (rot)
	Existenzgefährdend	3 (gelb)	6 (rot)	9 (rot)

10.2.5 b 4-stufiges Risikobewertungsschema [Wenn nicht zutreffend, bitte Abschnitt löschen]

Im auf der DataGuard-Plattform durchgeführten Risikomanagement werden die Auswirkungen auf die Organisation und die Eintrittswahrscheinlichkeit des jeweiligen Szenarios gemäß einer festgelegten Bewertungsskala in jeweils vier Stufen definiert.

Bewertungsskala der Auswirkungen auf die Organisation:

RISIKONIVEAU	BEWERTUNG	DEFINITION DER MÖGLICHEN AUSWIRKUNGEN
Unbedeutend	1 (grün)	Die Konsequenzen des Ereignisses haben unmerkliche Auswirkungen und haben geringe Bedeutung für die Organisation.
Ertragbar	2 (gelb)	Die Konsequenzen des Ereignisses haben geringe Auswirkungen und führen zu ertragbaren Störungen der Organisation.
Schwerwiegend	3 (gelb)	Die Konsequenzen des Ereignisses verursachen beträchtliche Störungen und gefährden die Geschäftsziele und/oder Reputation der Organisation.

Existenzgefährdend	4 (rot)	Die Konsequenzen des Ereignisses verursachen immense Störungen und können die Existenz der Organisation gefährden.

Bewertungsskala der Eintrittswahrscheinlichkeit:

RISIKONIVEAU	BEWERTUNG	DEFINITION DER MÖGLICHEN WAHRSCHEINLICHKEIT
Sehr selten	1 (grün)	Das Ereignis tritt voraussichtlich maximal alle 5 Jahre einmal ein.
Selten	2 (gelb)	Das Ereignis tritt voraussichtlich wenige male innerhalb von 5 Jahren ein.
Häufig	3 (gelb)	Das Ereignis tritt voraussichtlich wenige male pro Jahr ein.
Sehr häufig	4 (rot)	Das Ereignis tritt voraussichtlich mindestens einmal monatlich ein.

Durch Eingabe der Auswirkungs- und Wahrscheinlichkeitswerte in die Plattform wird das Risikoniveau automatisch durch Multiplikation der beiden Werte berechnet.

RISIKOMATRIX		WAHRSCHEINLICHKEIT			
		Sehr selten	**Selten**	**Häufig**	**Sehr häufig**
AUSWIRKUNGEN	**Unbedeutend**	1 (grün)	2 (grün)	3 (gelb)	4 (gelb)
	Ertragbar	2 (grün)	4 (gelb)	6 (gelb)	8 (gelb)
	Schwerwiegend	3 (gelb)	6 (gelb)	9 (gelb)	12 (rot)
	Existenzgefährdend	4 (gelb)	8 (gelb)	12 (rot)	16 (rot)

10.2.5 c 5-stufiges Risikobewertungsschema [Wenn nicht zutreffend, bitte Abschnitt löschen]

Im auf der DataGuard-Plattform durchgeführten Risikomanagement werden die Auswirkungen auf die Organisation und die Eintrittswahrscheinlichkeit des jeweiligen Szenarios gemäß einer festgelegten Bewertungsskala in jeweils fünf Stufen definiert.

Bewertungsskala der Auswirkungen auf die Organisation:

RISIKONIVEAU	BEWERTUNG	DEFINITION DER MÖGLICHEN AUSWIRKUNGEN
Unbedeutend	1 (grün)	Die Konsequenzen des Ereignisses haben unmerkliche Auswirkungen und haben geringe Bedeutung für die Organisation.
Ertragbar	2 (gelb)	Die Konsequenzen des Ereignisses haben geringe Auswirkungen und führen zu ertragbaren Störungen der Organisation .
Störend	3 (gelb)	Die Konsequenzen des Ereignisses sind spürbar und können unangenehme Störungen in der Organisation und/oder Reputation verursachen.
Schwerwiegend	4 (gelb)	Die Konsequenzen des Ereignisses verursachen beträchtliche Störungen und gefährden die Geschäftsziele und/oder Reputation der Organisation.

Existenzgefährdend	5 (rot)	Die Konsequenzen des Ereignisses verursachen immense Störungen und können die Existenz der Organisation gefährden.

Bewertungsskala der Eintrittswahrscheinlichkeit:

RISIKONIVEAU	BEWERTUNG	DEFINITION DER MÖGLICHEN WAHRSCHEINLICHKEIT
Extrem selten	1 (grün)	Das Ereignis tritt voraussichtlich maximal alle 10 Jahre einmal ein.
Sehr selten	2 (gelb)	Das Ereignis tritt voraussichtlich maximal alle 5 Jahre einmal ein.
Selten	3 (gelb)	Das Ereignis tritt voraussichtlich wenige male innerhalb von 5 Jahren ein.
Häufig	4 (gelb)	Das Ereignis tritt voraussichtlich wenige male pro Jahr ein.
Sehr häufig	5 (rot)	Das Ereignis tritt voraussichtlich mindestens einmal monatlich ein.

Durch Eingabe der Auswirkungs- und Wahrscheinlichkeitswerte in die Plattform wird das Risikoniveau automatisch durch Multiplikation der beiden Werte berechnet.

RISIKOMATRIX		WAHRSCHEINLICHKEIT				
		Extrem selten	**Sehr selten**	**Selten**	**Häufig**	**Sehr häufig**
AUSWIRKUNGEN	**Unbedeutend**	1 (grün)	2 (grün)	3 (grün)	4 (gelb)	5 (gelb)
	Ertragbar	2 (grün)	4 (grün)	6 (gelb)	8 (gelb)	10 (gelb)
	Störend	3 (grün)	6 (gelb)	9 (gelb)	12 (gelb)	15 (rot)
	Schwerwiegend	4 (gelb)	8 (gelb)	12 (gelb)	16 (rot)	20 (rot)
	Existenzgefährdend	5 (gelb)	10 (gelb)	15 (rot)	20 (rot)	25 (rot)

10.2.6 Begründung der Risikobewertung

Zur Nachvollziehbarkeit von Risikobewertungen sollen die Gründe für die jeweilige Bewertung im Prozess dokumentiert werden. Dies kann entweder in einem separaten Gesprächsprotokoll unter Angabe des bewerteten Risikos oder in den entsprechenden Freitextfeldern der DataGuard Plattform erfolgen. Als Gründe können Auditergebnisse, Beobachtungen, Messungen, Vorfälle oder ähnliche Informationen beschrieben werden.

10.3 Risikobehandlung

10.3.1 Zweck

Die Behandlung von Risiken hat zum Ziel, hohe bzw. inakzeptable Risiken innerhalb des ISMS unserer Organisation durch geeignete Maßnahmen auf ein akzeptables Maß zu reduzieren. Dabei wurde durch den Risiko-Bewertungsprozess bereits eine Priorisierung der zu behandelnden Risiken vorgenommen. Die Organisation soll im Risikobehandlungsprozess Maßnahmen planen, um Risiken zu akzeptieren, zu vermeiden, zu transferieren oder zu mitigieren (verringern).

10.3.2 Priorisierung der Risikobehandlung

Im Rahmen der Risikobewertung auf der DataGuard-Plattform wird in der Matrix das Risikoniveau berechnet. Das ermittelte Risikoniveau ist die Basis für eine Einstufung der Risikopriorität und wird in der DataGuard-Plattform mit den drei Farben grün, gelb und rot dargestellt.

Das Risiko-Niveau dient so als eines von mehreren Kriterien für eine mögliche Akzeptanz von Risiken. Im roten Bereich bewertete Risiken werden als inakzeptabel festgelegt. Die Schwelle oberhalb des roten Bereichs und unterhalb des grünen Bereichs ist die Risikoakzeptanzschwelle (auch als ALARP „as low as reasonable“ bezeichnet), der grüne Bereich stellt das akzeptable Niveau dar.

- **Grün:** geringe Risikopriorität, Risiko erfordert wenig Aufmerksamkeit, kann formlos akzeptiert werden.
- **Gelb:** normale Risikoprioriät, Risiko erfordert angemessene Aufmerksamkeit zur Risikominimierung und muss überwacht werden.
- **Rot:** hohe Risikopriorität, Risiko erfordert dringende und umfassende Risikobehandlung zur Vermeidung von schwerwiegenden Schäden.

Als weitere Kriterien für die Akzeptanz von Risiken müssen die persönlichen Einschätzungen von Fachexperten, der Asset- und Risiko-Eigentümer oder der obersten Leitung der Organisation (ISMS-Team) einbezogen werden. Bewertete Risiken müssen durch die Organisation behandelt werden. Risikobehandlungsoptionen sind: Akzeptieren, Vermeiden, Transferieren oder Mitigieren.

10.3.3 Risikobehandlungsprozess

Die Schritte des Risikobehandlungsprozesses sind:

1. Auswahl der angemessenen Risikobehandlungsoption
2. Bestimmung der anzuwendenden Schutzmaßnahmen (Controls), um die Risikobehandlungsoption zu implementieren.
3. Benennung einer Person/Rolle, die die Risiko-Verantwortlichkeit übertragen bekommt
4. Erneute Analyse und Bewertung des Risikoniveaus von Ziel Auswirkung und Ziel Wahrscheinlichkeit nach Auswahl der Maßnahmen (Bewertung des Restrisikos)
5. Dokumentation des Maßnahmenplans (Risikobehandlungsplan)
6. Überprüfung und Bestätigung des Restrisikos

Auswahl der angemessenen Risikobehandlungsoption
Die benannten Risiko-Eigentümer entscheiden mit Unterstützung des ISMS-Teams die jeweils angemessene Behandlungsoption des Risikos. Sie orientieren sich dabei an dem in der Risikobewertung berechneten Risiko-Niveau.

Risiken mit entsprechend gering bewertetem Risiko-Nivea (grün markiert) werden in der Organisation – wenn nicht anders im Gremium entschieden - so lange akzeptiert, bis sich bei einer Neubewertung das Niveau in einen inakzeptablen Bereich verschiebt.

Für Risiken, die als mittel (gelb markiert) oder hoch (rot markiert) bewertet wurden, ist die Behandlungsoption im ISMS-Team oder vom Risiko-Eigentümer zu bestimmen. Bei nicht akzeptablen Risiken wählt die Organisation eine der folgenden drei Behandlungsoptionen:

- Vermeiden: Gänzliche Beseitigung der Risiko-Quelle
- Transferieren: Verlagerung durch Outsourcing oder Versicherung auf Drittanbieter
- Mitigieren: Verringerung durch Maßnahmen zur Senkung der

Eintrittswahrscheinlich und/oder der Schadenshöhe

Die oberste Leitung kann nach erfolgter reiflicher Abwägung und schriftlicher Begründung die Akzeptanz von gelb oder rot bewerteten Risiken vollständig oder auf einen bestimmten Zeitraum begrenzt (temporär) genehmigen. [Das kann das erfolgen, wenn z.B. die Kosten für die Implementierung von Risikobehandlungsmaßnahmen unverhältnismäßig hoch wären. Eine temporäre Akzeptanz von Risiken kann ebenfalls durch die oberste Leitung genehmigt werden, wenn z.B. die Organisation für einen definierten Zeitraum nicht über ausreichende Finanz- und/oder Personalressourcen verfügt, um eine erforderliche Maßnahme umzusetzen.]

Bestimmung der anzuwendenden Maßnahmen
Umzusetzende Sicherheitsmaßnahmen (Controls) werden entweder in der Plattform aus dem Maßnahmenkatalog des Annex A der ISO 27001 (automatische Vorbelegung), den anzuwendenden Kapiteln anderer Rahmenwerke oder individuell bestimmt.

Erneute Analyse und Bewertung des Risikoniveaus von Ziel Auswirkung und Ziel Wahrscheinlichkeit
Nach Auswahl der Risiko-Behandlungsmaßnahmen muss das Risikoniveau des verbleibenden neuen Restrisikos erneut analysiert und bewertet werden. Ist das verbleibende Risiko trotz der festgelegten Maßnahmen noch immer oberhalb des Risikotoleranzniveaus, müssen weitere Maßnahmen festgelegt werden. Dieser Prozess muss so lange durchgeführt werden, bis ein akzeptables Risikoniveau erreicht wird, oder die oberste Leitung das Restrisiko wie beschrieben akzeptiert.

Dokumentation des Maßnahmenplans (Risikobehandlungsplan)
Alle Entscheidungen im Rahmen des Risikobehandlungsprozesses über durchzuführende Sicherheitsmaßnahmen getroffen wurden, müssen protokolliert und aufbewahrt werden. Zudem müssen die verabschiedeten Maßnahmen terminiert und in

das allgemeine Aufgaben- bzw. Projektmanagement der Organisation übernommen und gesteuert werden.

Überprüfung und Bestätigung des Restrisikos
Im letzten Schritt des Prozesses muss die Wirksamkeit des Risikobehandlungsplans durch die als Risiko-Eigentümer benannte Person/Rolle überprüft und bestätigt werden. Durch diese Überprüfung soll sichergestellt werden, dass alle Risiken angemessen behandelt werden und dass die Restrisiken im angemessenen Rahmen liegen. Die Überprüfungen der Restrisiken muss regelmäßig entsprechend dem Risikomanagement-Intervall überprüft werden, um sicherzustellen, dass alle Maßnahmenanforderungen auf einem aktuellen und angemessenen Stand sind und die Organisation auf neue oder entstehende Risiken angemessen reagieren kann.

10.4. Planung der Prozesse und Planung von Änderungen

Die Organisation muss zum einen die Prozesse zur Durchführung der im Zusammenhang mit dem Risikomanagement bestimmten Maßnahmen planen. Das geschieht, indem unsere Organisation verwirklichen und steuern, indem sie:

- Kriterien für die Verwirklichung und Steuerung im Risikomanagementprozess festlegt. Hierfür dient zum einen dieses Kapitel 10 im ISMS-Handbuch und zum anderen die operative Planung der regelmäßigen Durchführung der Risikomanagementprozesse im Jahresverlauf.
- Die Steuerung der Prozesse in Ubereinstimmung mit den Kriterien nachweislich durchführt.
- Dokumentierte Informationen zu den im Zusammenhang mit dem Risikomanagement der Organisation festgelegten Kriterien, Steuerung und Umsetzung sammelt.

Zum anderen müsssen Änderungen unserer Organisation, die sich aus dem Risikomanagement ergeben, geplant und überwacht werden. Dabei müssen auch die Folgen unbeabsichtigter Änderungen beurteilt werden. Falls notwendig, müssen Maßnahmen ergriffen werden, um jegliche negativen Auswirkungen zu vermindern.

Die Organisation muss sicherstellen, dass extern bereitgestellte Prozesse, Produkte oder Dienstleistungen, die für das Informationssicherheitsmanagementsystem relevant sind, kontrolliert werden.

11 Messung der Wirksamkeit des ISMS

11.1 Zweck

Die Messung der Wirksamkeit des ISMS von unserer Organisation erfordert einen systematischen Ansatz. Diese Richtlinie beschreibt die Methodik, zur Überwachung und Bewertung des ISMS, sowie die Art und Weise, wie die Ergebnisse analysieren werden sollen, um notwendige Maßnahmen zur Verbesserung zu identifizieren.

11.2 Überwachung und Messung

Die Organisation muss ein Überwachungs- und Messsystem einrichten, das aussagekräftige Erkenntnisse zur Wirksamkeit des ISMS liefert. Basis der Wirksamkeit sind die strategischen, taktischen und operativen Ziele der Informationssicherheit (siehe Kap. 2), die durch die oberste Leitung festgelegt wurden. Zur Überwachung und Messung der Zielergebnisse müssen folgende Aspekte, was überwacht und gemessen werden soll, definiert werden:

- die Methoden zur Überwachung, Messung, Analyse und Bewertung, um gültige Ergebnisse sicherzustellen. Die ausgewählten Methoden sollen zu vergleichbaren und reproduzierbaren Ergebnissen führen
- wann und durch wen die Überwachung und Messung durchzuführen ist
- wann und durch wen die Ergebnisse der Überwachung und Messung zu analysieren und zu bewerten sind

Die Dokumentation der Messungen und Ergebnisse erfolgt in[Es empfiehlt sich die Ziele aus Kap. 2 und die Ergebnisse Ihrer Ergebnismessung bzw. Zielerreichung in einer Dokumentation vorzunehmen. Bitte nennen Sie Ihr entsprechendes Kennzahlen-Management].

11.3 Interne und externe Audits

Dieses Kapitel beschreibt den Auditierungsprozess des Informationssicherheits-Managementsystems (ISMS) unserer Organisation.
Zusätzlich zu den externen Audits, die durch eine formal akkreditierte Zertifizierungsstelle durchgeführt werden muss, werden regelmäßige interne Audits durchgeführt, um die Einhaltung und Wirksamkeit des ISMS und dessen rechtliche und regulatorische Verpflichtungen zu überprüfen.

11.3.1 Ziele der Audits

Unsere Organisation erstellt ein Audit-Programm, das zur Erfüllung der folgenden Ziele dient:

- Sicherstellung, dass die Prozesse der Informationssicherheit mit den im ISMS definierten Prozessen und Verfahren übereinstimmen
- Überprüfung der effektiven, effizienten und wirtschaftlichen Durchführung von Aktivitäten im Bereich der Informationssicherheit zum Nutzen der Organisation
- Identifizierung von Bereichen, in denen die Anforderungen des zu folgenden Rahmenwerks eingehalten oder nicht eingehalten werden
- Identifizierung von Möglichkeiten zur kontinuierlichen Verbesserung über die bestehenden Kriterien hinaus
- Bestätigung, dass die Informationssicherheit effektiv verwaltet wird und die Risiken für das Unternehmen minimiert werden.

11.3.2 ISMS-Auditverfahren

Für jedes spezifische Audit, das durchgeführt werden soll, wird ein separater, detaillierter Plan erstellt. Das generelle, sowie die spezifischen Auditprogramm wird vom Koordinator für Informationssicherheit gesteuert.

Ressourcen
Das Auditprogramm muss von einer qualifizierten, erfahrenen Person durchgeführt werden, die unabhängig ist und den Betrieb des ISMS zuvor nicht beeinflusst hat. [Beschreiben Sie hier die potenzielle Personengruppe, die in Ihrer Organisation als Auditor in Frage kommt (z.B. ein Auditor von DataGuard)]. Entsprechende Ressourcen für interne und externe Audits müssen durch die oberste Leitung bereitgestellt werden. Die Ausstattung mit Ressourcen für Audits muss regelmäßig im Rahmen des Management Reviews bewertet werden, um sicherzustellen, dass die Ausstattung angemessen ist, um die Ziele zu erfüllen.

Für die Vorbereitung und Durchführung der Audits sind weitere Personen - unter anderem der obersten Leitung und der Lenkungsgruppe für Informationssicherheit erforderlich. Diese müssen rechtzeitig vom Koordinator für Informationssicherheit über den Zeitplan des Audits und den Umfang informiert werden.

Audit-Kriterien
Das Auditprogramm basiert auf den Anforderungen des zu folgenden Rahmenwerks, bzw. auf den im Risikomanagement identifizierten anzuwendenden Maßnahmen.

Wenn Abweichungen vom Standard festgestellt werden, werden sie in eine der folgenden Kategorien eingeordnet:

- Beobachtung (observation): Eine Beobachtung, die auf Erfahrungen mit anderen ISMS-Implementierungen beruht und der geprüften Stelle nützliche Erkenntnisse liefern kann.
- Verbesserungsmöglichkeit (Opportunity for improvement): Bestimmte Aspekte, die im Allgemeinen den Anforderungen der Norm entsprechen, sollten verbessert werden.
- Geringfügige Nichtkonformität (minor non-conformity): Ein einzelner Fehler, der nicht auf ein vollständiges Versagen des Managementsystems hinweist.
- Wesentliche Nichtkonformität (major non-confomity): Ein bedeutendes Problem, das auf eine Störung in der Funktionsweise des Managementsystems hinweist.

Umfang und Methode
Der Auditor soll ein prozessbasiertes Audit durchführen, das sich auf die wesentlichen Aspekte, Risiken und Ziele konzentriert. Es sollen solche Auditverfahren eingesetzt werden, die Nachweise in ausreichender Quantität und Qualität sammeln, um die Konformität des Managementsystems der Organisation zu bestätigen. Durch den systematischen Einsatz von Auditverfahren soll das Auditrisiko verringert und die Objektivität der Auditschlussfolgerungen gestärkt werden.

Der Auditor hat bei der Erstellung seines Prüfplans eine Kombination von Verfahren zur Sammlung von Nachweisen zu verwenden. Die angewandten Auditmethoden sollen Befragungen, Beobachtungen von Aktivitäten, Überprüfung von Unterlagen und Aufzeichnungen, technische Tests und die Analyse von Stichproben umfassen. Dabei soll das Analyseverfahren durch die Untersuchung eines angemessenen Teils der Maßnahme Schlussfolgerungen über das Ganze zulassen. Es soll dem Prüfer ermöglichen, Merkmale einer Grundgesamtheit durch direkte Beobachtung eines Teils der gesamten Grundgesamtheit zu schätzen. Bei dieser Prüfung soll ein systematisches Stichprobenverfahren (oder Intervallstichprobenverfahren) angewendet werden.

Technische Tests, einschließlich der Prüfung der Wirksamkeit eines Prozesses oder einer Kontrolle sollen nicht vom Auditor persönlich, sondern vom Personal der geprüften Stelle durchgeführt werden.

Zeitplan
Interne Audits sollen mindestens einmal im Jahr durchgeführt werden. Nachdem ein initiales umfassendes Audit erfolgt ist, das alle Aspekte des Managementsystems abdeckt, werden anschließend jährlich die Audits in Teilgebieten durchgeführt, sodass alle zwei Jahre jeder grundlegende Aspekt des ISMS mindestens einmal überprüft wird.

Der detaillierte Prüfungsplan soll vom Koordinator für Informationssicherheit (ISB) gemeinsam mit dem internen Auditor erstellt werden und kann auf Anfrage angefordert werden. Das interne Auditprogramm umfasst mindestens Folgendes:

- Audit-Bezeichnung
- Geplante Termine für jedes Audit
- Umfang der einzelnen Prüfungsaktivitäten
- Zugewiesener Prüfer
- Audit-Status (z.B. Geplant, In Arbeit, Abgeschlossen)

Das Auditprogramm muss regelmäßig überprüft und aktualisiert werden, wenn die Audits voranschreiten oder abgeschlossen wurden. Im Rahmen des Management Reviews wird die oberste Leitung die Leistung der Audits bewerten.

Bericht der Ergebnisse
Zu jedem Audit muss vom Auditor ein formal dokumentierter Auditbericht erstellt und an die auditierte Stelle übermittelt werden, damit diese Kommentare abgeben und die Schlussfolgerungen und Feststellungen diskutieren kann.

Für alle festgestellten Nichtkonformitäten müssen angemessene kurz- und langfristige Korrekturmaßnahmen vereinbart werden, einschließlich der angestrebten Fertigstellungstermine. Der vollständige und abgestimmte Bericht muss anschließend der obersten Leitung zur Verfügung gestellt werden. Alle Mitarbeiter, die für die Behandlung und Behebung von Audit-Nichtkonformitäten verantwortlich sind, sollen eine Kopie der Audit-Nichtkonformitätsberichte erhalten.

Aktivitäten nach dem Audit
Die Lenkungsgruppe für Informationssicherheit muss die Beseitigung aller Nichtkonformitäten überwachen und verfolgen, um sicherzustellen, dass die Korrekturmaßnahmen innerhalb der vereinbarten Fristen angemessen umgesetzt werden.

Bei schwerwiegenden Nichtkonformitäten werden in Übereinstimmung mit dem Aktionsplan Folgeprüfungen durch den Auditor durchgeführt, um sicherzustellen, dass alle Abhilfemaßnahmen angegangen und umgesetzt wurden.

11.4 Managementbewertungsprozess

Die Managementbewertung ist ein formelles, dokumentiertes Treffen zwischen dem Informationssicherheitsbeauftragten (ISO) und dem Top-Management. Sie stellt sicher, dass das Informationssicherheitsmanagementsystem (ISMS) wirksam, auf die organisatorischen Ziele ausgerichtet und konform mit den gesetzlichen Anforderungen bleibt.

Zweck

Die Bewertung dient der Überprüfung der ISMS-Leistung, der Analyse wesentlicher Ereignisse und der Wirksamkeit von Sicherheitsmaßnahmen, um das Top-Management zu informieren und notwendige Anpassungen vorzunehmen.

Umfang

Wesentliche Schwerpunkte der Managementbewertung sind:

1. **Überprüfung früherer Maßnahmen:**
    a. Aktualisierungen zu Maßnahmen aus früheren Bewertungen, einschließlich der Nachverfolgung der Umsetzung oder der Nennung von Verzögerungen.
2. **Änderungen im Kontext:**
    a. Bewertung von Änderungen in externen und internen Faktoren, die das ISMS betreffen (Kontext der Organisation).
3. **Erwartungen der Interessengruppen:**
    a. Überprüfung von Änderungen in den Bedürfnissen und Erwartungen der Interessierten Parteien, um die fortlaufende Relevanz des ISMS sicherzustellen.
4. **Leistungsrückmeldung:**
    a. Analyse der Entwicklungen von Nichtkonformitäten, Korrekturmaßnahmen, Auditergebnissen und der Erreichung von Sicherheitszielen.

5. **Risikobewertung:**
    a. Überprüfung der Risikobewertungen und der Behandlungspläne, um sicherzustellen, dass Risiken entsprechend der Risikobereitschaft der Organisation gesteuert werden.
6. **Rückmeldungen von Interessierten Parteien:**
    a. Bewertung von Rückmeldungen von Interessierten Parteien, wie Mitarbeitern, Kunden und Lieferanten.
7. **Kontinuierliche Verbesserung:**
    a. Identifizierung von Möglichkeiten zur Verbesserung des ISMS durch Prozessoptimierung, Technologieanpassungen oder Schulungen.

Dokumentation und Berichterstattung

Die Ergebnisse und Entscheidungen werden in einem formellen Bericht dokumentiert, der als Nachweis für das Engagement der Organisation zur Verbesserung ihres ISMS dient.

Häufigkeit

Die Bewertungen werden mindestens einmal jährlich oder bei Bedarf häufiger durchgeführt.

12. Kontinuierliche Verbesserung

12.1 Zweck

Informationssicherheit ist kein Zustand, der einmal erreicht wird und dann fortbesteht, sondern ein Prozess, der fortlaufend und kontinuierlich angepasst werden muss. Geänderte Verfahren und Prozesse in der Organisation, der Wandel in den gesetzlichen Rahmenbedingungen, neue Technik, aber auch bislang unbekannte Schwachstellen und daraus erwachsende Gefährdungen stellen immer wieder neue Anforderungen, sodass die nachhaltige Angemessenheit und Wirksamkeit des ISMS nicht automatisch gewährleistet sind.

12.2 PDCA - Kontinuierliche Verbesserung

Um eine kontinuierliche Verbesserung der Informationssicherheit in unserer Organisation zu erreichen, setzt die Organisation die PDCA-Methode ein: Planen, Durchführen, Prüfen, Verbessern. Demnach müssen die geplanten (plan) und umgesetzten (do) Aktivitäten im Managementsystem nach dem Plan-Do-Check-Act-Kreislauf ständig auf ihre Wirksamkeit hin geprüft (check) und gegebenenfalls angepasst (act) werden.

Am Ende des PDCA-Zyklus steht der Anfang. Durch die Wiederholung des Zyklus wird eine weitere Schärfung und Verbesserung der Prozesse gewährleistet.

Der Informationssicherheitsprozess unserer Organisation soll ebenfalls dem PDCA-Zyklus unterliegen, der sich in folgende Phasen gliedert:

- Plan – Planung von Sicherheitsmaßnahmen
- Do – Umsetzung der Maßnahmen
- Check – Erfolgskontrolle, Überwachung der Zielerreichung
- Act – Beseitigung von Defiziten, Verbesserung.

Insbesondere die Erfolgskontrolle und die kontinuierliche Verbesserung gehören zu den wichtigsten Managementprinzipien im Sicherheitsprozess. Daher muss eine regelmäßige Überprüfung der Wirksamkeit der organisatorischen und technischen Schutzmaßnahmen auf Dauer sichergestellt werden.

Der kontinuierliche Verbesserungsprozess muss aus der ISMS-Dokumentation der Organisation ersichtlich sein, um den Sicherheitsprozess und getroffene Entscheidungen nachvollziehbar zu gestalten und Missverständnisse zu vermeiden.

13. Umgang mit Nichtkonformitäten

13.1 Zweck

Der Zweck dieses Kapitels besteht darin, die notwendigen Maßnahmen zu beschreiben, die im Falle der Feststellung einer

Nichtkonformität innerhalb des Informationssicherheitsmanagementsystems (ISMS) zu ergreifen sind.
Eine Nichtkonformität definieren wir als ein Vorkommen, in dem das ISMS die gesetzlichen, regulativen oder vertraglichen Anforderungen an die Informationssicherheit nicht erfüllt.

13.2 Identifizierung von Nichtkonformitäten

Nichtkonformitäten können aus verschiedenen Quellen, in unterschiedlichen Formen und aus verschiedenen Gründen auftreten. Unsere Organisation muss in regelmäßigen Abständen explizite Maßnahmen zur Identifikation von Nichtkonformitäten im ISMS-Kalender planen. Diese sind:

- Sicherheitsüberprüfungen
- interne und externe Audits
- Management Reviews

Zudem liegt es in der Verantwortung des Koordinators für Informationssicherheit, Mitarbeiter, IT-Benutzer, Kunden, Lieferanten und weitere interessierte Parteien des ISMS zu ermutigen, Nichtkonformitäten aufzudecken und über die bekannten Kanäle für die Meldung von Sicherheitsereignissen zur Kenntnis zu bringen.

13.3 Verfahren zur Behandlung von Nichtkonformitäten

Wenn sofortige Maßnahmen zur Behebung der Nichtkonformität erforderlich sind, müssen diese umgehend durch die Lenkungsgruppe für Informationssicherheit initiiert werden. Dies bedeutet, das Problem zu beheben, seine Verschlimmerung zu verhindern oder seine Auswirkungen zu minimieren, bis weitere Maßnahmen ergriffen werden können.

Die Zuweisung geeigneter Ressourcen sollte auf der aktuell möglichen Bewertung der Schwere der Nichtkonformität beruhen. Alle ergriffenen Maßnahmen müssen im Ereignisprotokoll dokumentiert werden. Für weitere Schritte ist es wichtig, detaillierte Informationen über die Art der Nichtkonformität über das Protokoll bereitzustellen.

Ursachenermittlung
Um die zugrunde liegende Ursache der Nichtkonformität zu ermitteln, muss die Nichtkonformität analysiert werden. Hierzu sollen ggf. weitere Parteien konsultiert werden, um die Ereignisse und Mechanismen zu verstehen, die zu der Nichtkonformität geführt haben. Die Ergebnisse der Ursachenermittlung müssen im Ereignisprotokoll dokumentiert werden.

Bewertung möglicher Auswirkungen

Sobald die Ursache bekannt ist, sollte eine umfassende Überprüfung durchgeführt werden, um festzustellen, ob ähnliche Nichtkonformitäten innerhalb des ISMS bereits bestehen und ob die Möglichkeit besteht, dass sie in Zukunft auftreten. Die Ergebnisse dieser Überprüfung müssen im Ereignisprotokoll dokumentiert werden.

Durchführung von Abhilfemaßnahmen

Sobald die Ursache und die tatsächliche oder potenzielle Auswirkung der Nichtkonformität ermittelt wurden, müssen geeignete Korrekturmaßnahmen festgelegt werden, um sowohl die aktuelle Situation als auch die potenziellen künftigen Auswirkungen zu beheben. Der erwartete Nutzen aus den Korrekturmaßnahmen sollte die erforderlichen Ressourcen ausreichend rechtfertigen. Das Ereignisprotokoll soll die Einzelheiten der Korrekturmaßnahmen enthalten, einschließlich dem Umsetzungsplan und den zugewiesenen Ressourcen.

Überprüfung der Wirksamkeit von Abhilfemaßnahmen

Innerhalb eines angemessenen Zeitraums, der je nach Art der Nichtkonformität und der ergriffenen Korrekturmaßnahmen variiert, muss die Wirksamkeit der Korrekturmaßnahmen bewertet werden, um festzustellen, ob das Problem und die damit verbundenen Auswirkungen erfolgreich behoben wurden.

Wird der erwartete Nutzen nicht erreicht, sollen die Gründe dafür im regulären Management-Review behandelt werden. Im Falle einer erfolgreichen Lösung werden das Datum der Überprüfung und die Ergebnisse dokumentiert, und der Status der Nichtkonformität aktualisiert.

Änderung des ISMS, falls erforderlich

Wenn festgestellt wird, dass die Nichtkonformität auf einen Fehler im ISMS, einschließlich der relevanten Richtlinien, Verfahren und Formulare, zurückzuführen ist, kann es erforderlich sein, das ISMS zu überarbeiten. Alle Änderungen müssen dann nach den festgelegten ISMS-Lenkungsverfahren erfolgen.

14. Norm-Referenzen

14.1 Normreferenzen zu ISO27001:2022

Kapitel in diesem Dokument	Normkapitel (ISO27001:2022)
1. Einleitung: ISMS Struktur & Prozesse	4.4; 5.2; 6.3
2. Ziele der Informationssicherheit:	6.2
3. Beschreibung des Kontext der Organisation	4.1
4. Interessierte Parteien und deren Anforderungen an die Informationssicherheit	4.2; A 5.31
5. Anwendungsbereich des ISMS	4.3
6. Rollen und Verantwortlichkeiten im ISMS: Führung & Verpflichtung, Verantwortlichkeiten, Kompetenzen, Ressourcen	5.1; 5.3; 7.1; 7.2; 7.3; A 5.2; A 5.3; A 5.4
7. Kommunikation: Empfänger, Methoden, Themen, Planung	7.4
8. Dokumentenlenkung	7.5; A 5.33
9. Inventar der Informationswerte (Assets)	A 5.9
10. Risikomanagement	6.1; 6.2; 8.1; 8.2; 8.3
11. Messung der Wirksamkeit des ISMS: Überwachung, Interne/Externe Audit, Mgmt. Review	9.1; 9.2; 9.3; A5.35; A 5.36
12. Kontinuierliche Verbesserung	10.1
13. Umgang mit Nichtkonformitäten	10.2

14.2 Referenzen zu TISAX-ISA 6.0

Kapitel in diesem Dokument	Kapitel (TISAX-ISA 6.0)
1. Einleitung: ISMS Struktur & Prozesse	1.1.1; 1.2.1
2. Ziele der Informationssicherheit:	1.1.1
3. Beschreibung des Kontext der Organisation	1.1.1
4. Interessierte Parteien und deren Anforderungen an die Informationssicherheit	1.1.1; 1.3.3; 7.1.1
5. Anwendungsbereich des ISMS	1.2.1
6. Rollen und Verantwortlichkeiten im ISMS: Führung & Verpflichtung, Verantwortlichkeiten, Kompetenzen, Ressourcen	1.2.1; 1.2.2; 1.6.2; 1.6.3; 2.1.1; 2.1.3
7. Kommunikation: Empfänger, Methoden, Themen, Planung	1.1.1
8. Dokumentenlenkung	1.1.1
9. Inventar der Informationswerte (Assets)	1.2.4; 1.3.1; 3.1.3; 5.2.4
10. Risikomanagement	1.1.1; 1.4.1; 1.2.2; 1.4.1; 5.2.1
11. Messung der Wirksamkeit des ISMS: Überwachung, Interne/Externe Audit, Mgmt. Review	1.5.1; 5.2.6; 1.5.2
12. Kontinuierliche Verbesserung	1.5.1; 1.6.2
13. Umgang mit Nichtkonformitäten	1.5.1; 1.5.2