DGI® Deutsche Gesellschaft für Informationssicherheit AG

IT-Sicherheitskonzept gemäß ISO 27001

Kennzeichnung Vertraulichkeitskategorie

Inhaltsverzeichnis

1 Relevante Normen und Standards

Die Organisation berücksichtigt im Rahmen der Umsetzung des Informationssicherheitsmanagementsystems die ISO 270xx-Normenfamilie, explizit die ISO 27001, ISO 27002, ISO 27005 und die ISO 27031, die ISO 31000 sowie die ISO 223xx-Normenfamilie.

2 Abkürzungen

ISMS	Informationssicherheitsmanagementsystem

3 Begriffe

4 Das Informationssicherheitsmanagementsystem

Das systematische Management und die Steuerung der

- Verfahren, Prozesse, Anweisungen und Regelungen,
- Umsetzung der strategischen Ausrichtung in sämtlichen Teilprozessen und Wirkbereichen,
- Zielsetzungen,
- Zielerfüllungen,
- Ausbildung, Fort- und Weiterbildung, Unterweisung, Einweisung und Einarbeitung sämtlicher beteiligten Personen sowie
- Maßnahmen für die Umsetzung
    - der Einbindung des Kontexts der Organisation,
    - der Ausgestaltung und Festlegung der Führung,
    - der Planung und Steuerung des ISMS,
    - der Planung, Durchführung und Bewertung von Awareness-Schulungen,
    - der Überwachung, Messung, Analyse und Bewertung der Leistung und Qualität sowie
    - der Aufrechterhaltung und fortlaufenden Verbesserung,

um die Anforderungen an den Betrieb des ISMS zu erfüllen, stellen die fortlaufende Integration der aktuellen Anforderungen an die Informationssicherheit in die Aufbau- und Ablauforganisation des Informationssicherheitsmanagements sicher.

Die Steuerung, Pflege, Aktualisierung und Dokumentation sämtlicher Verfahren und Prozesse für die Umsetzung und den fortlaufenden Betrieb des ISMS liegt in der Verantwortung des Informationssicherheitsbeauftragten.

Um ein geeignetes, wirksames, normkonformes und effizientes ISMS aufzubauen sowie die Aufrechterhaltung und fortlaufende Verbesserung des ISMS sicherzustellen, werden

- sämtliche Anforderungen an die Verfahren, Prozesse, Anweisungen und Regelungen,
- an die Dokumentation,
- an die Vorhaltung, Bereitstellung und Verfügbarkeit der Ressourcen und Kompetenzen sowie
- die Abhängigkeiten und Wechselwirkungen des ordnungsgemäßen, sicheren und konformen Geschäftsbetriebs

kontinuierlich sowie anlassbezogen und bei signifikanten Änderungen auf Aktualität hin überprüft und bewertet.

Um die Prozesse für die Sicherstellung des geplanten und geforderten Betriebs des ISMS zu planen, umzusetzen, aufrechtzuerhalten und fortlaufend zu verbessern, werden folgende zentralen Wirkfaktoren

Wiederherstellung der geforderten und vereinbarten Informationssicherheit

- Initiierung, Integration und den Betrieb eines angemessenen Vorfallsmanagement
- Bestimmung der erforderlichen Funktionen, Verantwortlichkeiten und Befugnisse für die Verwirklichung des ISMS
- Überwachung, Messung, Analyse und Bewertung der geforderten und vereinbarten Informationssicherheit
- Initiierung, Integration und den Betrieb eines angemessenen Änderungsmanagements, um den aktuellen Anforderungen an die organisationsspezifisch geforderte und vereinbarte Informationssicherheit gerecht zu werden
- Durchführung von Schutzbedarfsfeststellungen sowie von Informationssicherheitsrisikobeurteilungen und -behandlungen
- Initiierung und Integration der Durchführung von Awareness-Schulungen

- Erstellung, Pflege, Aktualisierung und Lenkung der erforderlichen dokumentierten Informationen des ISMS
- Dokumentation der Prozesse des ISMS
- Dokumentation der Anweisungen und Regelungen für den Aufbau sowie die Aufrechterhaltung der geforderten und vereinbarten Informationssicherheit

4.1 Management und Steuerung des ISMS

Die Leistung und Qualität der Entwicklung sowie des Managements und der Steuerung des ISMS dient der obersten Leitung und den relevanten Stakeholdern als wichtige Bewertungsgrundlage für die Überwachung der Erfüllung der Zielsetzungen der Organisation und des ordnungsgemäßen, sicheren und konformen Geschäftsbetriebs sowie des Aufbaus und der Aufrechterhaltung der geforderten und vereinbarten Informationssicherheit.

und -Verbesserungen

- die fortlaufende
  - Bewertung der geforderten und vereinbarten Informationssicherheit
  - Identifizierung, Analyse und Bewertung der eingetretenen Informationssicherheitsvorfälle, Auswirkungen und Schäden
  - Identifizierung, Analyse und Bewertung der Schwachstellen sowie der Bedrohungs- und Risikolagen
  - Bewertung der Integration, Verwirklichung, Aufrechterhaltung und fortlaufenden Verbesserung des ISMS als Querschnittsfunktion der Organisation
- die Entwicklung der organisationsspezifischen Aufbau- und Ablauforganisation für den Betrieb des ISMS
- die Bereitstellung der geplanten und geforderten Ressourcen und Kompetenzen

- die Zuordnung von Rollen, Verantwortlichkeiten und Befugnissen innerhalb des ISMS
- die Entwicklung von Kriterien für die Beurteilung eines abweichenden ordnungsgemäßen, sicheren und konformen Geschäftsbetriebs
- die Umsetzung der geforderten Erstellung, Pflege, Aktualisierung und Lenkung sowie der Verteilung und Aufbewahrung der dokumentierten Informationen des ISMS

5 Kontext der Organisation

Die Umsetzung der Maßnahmen für die Identifikation der Einflussfaktoren, um die Bestimmung und Festlegung des Kontexts der Organisation vornehmen zu können, werden kontinuierlich überwacht und bewertet sowie regelmäßig, anlassbezogen sowie bei signifikanten Änderungen aktualisiert, angepasst und verbessert.

5.1 Verstehen der Organisation und Ihres Kontextes

Im Rahmen der Bekanntmachung der strategischen Ausrichtung der Organisation sowie deren mitgeltenden Verfahren, Prozessen, Anweisungen und Regelungen hat die oberste Leitung die Zielsetzungen der Organisation in Bezug der geforderten und vereinbarten Informationssicherheit sowie einen Plan für die Erreichung der Ziele dokumentiert.

Abhängigkeiten, Wechselwirkungen, Einwirkungen und Zusammenhänge

- soziale, kulturelle, politische, rechtliche, behördliche, vertragliche, normative, finanzielle, technologische, wirtschaftliche und umweltbezogene Faktoren seien sie internationaler, nationaler, regionaler oder lokaler Art
- wesentliche Schlüsselfaktoren und Trends, welche die Zielsetzungen der Organisation beeinflussen
- die Beziehungen, Wahrnehmung, Werte, Bedürfnisse und Erwartungen interner und externer Stakeholder
- vertragliche Beziehungen und Verpflichtungen
- die Komplexität und Abhängigkeiten von internen und externen Faktoren
- die eigene Vision und Mission sowie die eigenen Werte
- die Leitungsorgane, die Organisationsstruktur, die Rollen und zu erfüllende Kontroll- und Rechenschaftspflichten

Die eruierten Informationen bezüglich der Bestimmung und Bestätigung der Optionen für die Informationssicherheitsrisikobehandlung sowie die Risikobehandlungspläne, die umzusetzenden Maßnahmen und die Bewertung der Umsetzung, Wirksamkeit und Einhaltung der Risikoakzeptanz werden anforderungsgerecht dokumentiert, kommuniziert, bereitgestellt und aufbewahrt.

9.2.2.1 Umsetzung der Maßnahmen aus der Informationssicherheitsrisikobehandlung

Das Management der Maßnahmenumsetzung, um die Anforderungen aus der Informationssicherheitsrisikobehandlung zu erfüllen, muss

- die Akzeptanz durch sämtliche Stakeholder berücksichtigen
- sämtlichen Stakeholder das Ausmaß des nach der Informationssicherheitsrisikobehandlung verbleibenden Restrisikos vermitteln
- in Übereinstimmung mit den festgelegten Organisationszielen und Risikokriterien stehen

- Maßgabe einer regelmäßigen Neubewertung der zurückgestellten Maßnahme
- es müssen Umfang und Inhalt der geforderten und vereinbarten dokumentierten Informationen für die Umsetzung der Einzelmaßnahme festgelegt und die anforderungsgerechten Nachweise erstellt, aufbewahrt und bereitgestellt sowie gegebenenfalls kommuniziert werden
- es muss eine kontinuierliche Überwachung, Messung, Analyse und Bewertung der Maßnahmenumsetzung implementiert werden
- die Aktualität, Eignung, Vollständigkeit, Wirksamkeit, Mechanismenstärke, Praktikabilität und Akzeptanz der Maßnahmen für die Gewährleistung der geplanten und vereinbarten Informationssicherheit muss regelmäßig bewertet werden

Als Maßnahmen für die Gewährleistung der geplanten und vereinbarten Informationssicherheit müssen insbesondere die Folgenden in Betracht gezogen werden

- Organisatorische Maßnahmen, wie
    - Erstellung von Dokumenten für die strategische, taktische und operative Steuerung
    - Festlegung von Verantwortlichkeiten und Befugnissen
    - Klassifizierung und Kennzeichnung von Informationen
    - Zugangs- und Zugriffssteuerung
    - Stakeholdermanagement
    - Lieferantenmanagement
    - Management von Informationssicherheitsvorfällen
    - Management des Zusammenwirkens mit dem Risikomanagement
    - Management des Zusammenwirkens mit dem Business Continuity Management
    - Datenschutzmanagement

    - infrastrukturelle Netzwerksicherheit
    - Support und Wartung
    - Löschung und Entsorgung von Daten und Datenträgern
- Technologische Maßnahmen, wie
    - Geräte- und Systemmanagement
    - Informationssicherheitsmaßnahmen für Entwicklungsumgebungen
    - Autorisierungs- und Authentifizierungsmechanismen
    - Schutz gegen Schadsoftware
    - Administration und Konfiguration
    - Backupmechanismen und -strategien
    - technische Netzwerksicherheit
    - Anwendung kryptographischer Verfahren