HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

BACHELORARBEIT

Frau
Anna Leist

Implementierung der ISO/IEC 27001:2022: Ein Leitfaden zur Umstellung von der ISO/IEC 27001:2013

Mittweida, 2024

Fakultät Angewandte Computer- und Biowissenschaften

BACHELORARBEIT

Implementierung der ISO/IEC 27001:2022: Ein Leitfaden zur Umstellung von der ISO/IEC 27001:2013

Autor:
Frau

Anna Leist

Studiengang:
Allgemeine und Digitale Forensik

Seminargruppe:
FO20w5-b

Erstprüfer:
Prof. Dr. rer. nat. Dirk Labudde

Zweitprüfer:
Ing. Martin Mallinger, MSc

Einreichung:
Vöcklamarkt, 15.04.2024

Verteidigung/Bewertung:
Mittweida, 2024

Bibliografische Beschreibung:

Leist Anna:
Implementierung der ISO/IEC 27001:2022: Ein Leitfaden zur Umstellung von der ISO/IEC 27001:2013 - 2024 – 29 Seiten – 3 Abbildungen – 0 Tabellen
Mittweida, Hochschule Mittweida, Fakultät Angewandte Computer- und Biowissenschaften, Bachelorarbeit, 2024

Referat:

In der vorliegenden Arbeit wird die ISO27001:2013 mit der ISO27001:2022 verglichen. Dabei wird darauf eingegangen wie man die Richtlinien anpassen muss um von einer ISO27001:2013 Zertifizierung zu einer gültigen ISO27001:2022 zu gelangen.

Inhalt

Abbildungsverzeichnis

Abkürzungsverzeichnis

ISO	International Organization for Standardization
IEC	International Electrotechnical Commission)
ISMS	Informationssicherheitsmanagementsystem
VIV	Vertraulichkeit, Integrität, Verfügbarkeit
CIA	Confidentiality, Integrity, Availability
IT	Information Technology
BSI	British Standards Institute
B2B	Business to Business
IKT	Informations- und Kommunikationstechnologie
BIA	Business-Impact-Analyse
RTO	Recovery Time Objective
PII	Persönlich Identifizierbare Informationen
SoA	Statement of Applicability

1 Einleitung

Organisationen müssen aufgrund der voranschreitenden Digitalisierung und der fortlaufenden Entwicklung von Informations- und Kommunikationstechnologie ihre Informationssicherheitsmaßnahmen fortlaufend verbessern und anpassen. Für viele Unternehmen wird in diesem Zusammenhang die Umstellung von ISO27001:2013 auf die neueste Fassung, ISO27001:2022, immer wichtiger. Bei der ISO27001 handelt es sich um eine weltweit anerkannte Norm, welche als Rahmenwerk für die Implementierung eines Informationssicherheitsmanagementsystems (ISMS) dient. Nachdem die überarbeitete Fassung am 25.Oktober 2022 veröffentlicht wurde, haben Firmen, welche nach der alten Norm zertifiziert worden sind, 36 Monate Zeit, ihre Richtlinien und Praktiken an die aktuellen Anforderungen anzupassen.

Trotz der Wichtigkeit dieses Themas für zahlreiche Unternehmen gibt es zur Implementation der ISO27001:2022 bisher kaum Literatur oder Anwendungsbeispiele.

1.1 Ziel der Arbeit

Im Rahmen dieser Forschungsarbeit wird daher der Frage nachgegangen, wie die Umstellung von der alten Fassung auf die aktuelle Version gelingt. Das Ziel dabei ist es, einen praktischen Leitfaden für eine Implementation der ISO27001 zu geben sowie einen Überblick über die größten Differenzen zwischen den beiden Versionen zu schaffen.

Anhand einer Fallstudie sowie Literaturarbeit wird die Implementierung erläutert. Diese Kombination aus Methodiken wurde gewählt, um gute Ergebnisse zu erzielen, obwohl das Thema bisher noch nicht weit erforscht wurde.

1.2 Inhalt der Arbeit

Diese Arbeit ist in 2 größere Teilabschnitte gegliedert. In der ersten Hälfte wird ein theoretischer Überblick über die Grundlagen eines Informationssicherheitssystems gegeben. Der zweite Teil befasst sich mit der Praxis einer Implementation der ISO27001:2022 bei einer bereits vorhandenen Zertifizierung nach der ISO27001:2013.

Im Theorieteil wird zu Beginn eine Einführung in das Informationssicherheitsmanagement gegeben. Hierbei wird zunächst Informationssicherheit definiert. Im Anschluss wird auf die Ziele eines Informationssicherheitsmanagementsystems eingegangen. Daraufhin folgt ein allgemeiner Überblick über die ISO27001 Norm , wobei auf die historische Entwicklung, auf Struktur und Inhalt sowie auf den Anwendungsbereich der ISO27001 eingegangen

wird. Im weiteren Verlauf wird eine Gegenüberstellung der beiden Versionen vorgenommen. Im Praxisteil wird kurz das Unternehmen vorgestellt, mit welchem die Implementation erarbeitet wurde. Daraufhin folgt eine Erklärung zur Methodik. Danach werden die Neuerungen und notwendigen Änderungen in den Richtlinien beschrieben.

2 Theoretischer Teil

Dieses Kapitel dient zur Einführung in das Informationssicherheitsmanagement. Es werden wichtige Begriffe definiert. Außerdem werden die Grundlagen zur ISO27001 Norm erläutert.

2.1 Einführung in Informationssicherheitsmanagement und ISO27001

2.1.1 Konzept des Informationssicherheitsmanagements

2.1.1.1 Definition von Informationssicherheit und dessen Bedeutung für Organisationen

Im Allgemeinen geht es bei der Informationssicherheit darum, die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen zu schützen. Die Vertraulichkeit (engl. Confidentiality) verlangt nach Nichtoffenlegung vertraulicher Informationen, sowie das Verhindern von unbefugtem Zugriff auf Daten. Die Integrität (engl. Integrity) stellt sicher, dass die Informationen vollständig und unverfälscht sind. Bei der Verfügbarkeit (engl. Availability) geht es darum, eine Redundanz zu schaffen und die Aufrufbarkeit von Daten jederzeit sicherzustellen. In der deutschen Sprache werden diese Schutzziele mit VIV abgekürzt, im englischen Sprachraum mit CIA. Des Weiteren können auch zusätzliche Schutzziele wie Autorisierung, Authentizität, Nicht-Abstreitbarkeit oder Kontrollierbarkeit inbegriffen sein.

Informationen, sowohl in digitaler als auch in materieller Form, sind von enormem Wert für Unternehmen und es liegt somit im Interesse von Ebendiesen die Schutzziele zu verfolgen und Informationssicherheit zu gewährleisten. Dabei sind auch gesetzliche Anforderungen (Datenschutzgesetz, Telekommunikationsgesetz, …) zu beachten, welche im Zusammenhang mit Schutzzielen stehen. [Liedtke]

Die Bedeutung der Unterscheidung zwischen digitalen und materiellen Informationen liegt darin begründet, dass Informationssicherheit oft mit IT-Sicherheit verwechselt oder sogar gleichbedeutend mit ihr benutzt wird. Obwohl die IT-Sicherheit eine Komponente der Informationssicherheit ist, beinhaltet sie nur digitale Informationen, wohingegen sich die Informationssicherheit mit allen schützenswerten Daten beschäftigt. [ISO/IEC 27000:2018]

2.1.1.2 Ziele und Grundsätze des Informationssicherheitsmanagements

Der Zweck eines Informationssicherheitsmanagements (ISM) ist es, sämtliche Unternehmensdaten und Informationen zu schützen. Denn in der Zeit der Digitalisierung, der Künstlichen Intelligenz und der intelligenten Geräte sind Daten zunehmend der maßgebliche Faktor für die Wettbewerbsfähigkeit von Firmen. Immer mehr Geschäftsmodelle beruhen ebenfalls hauptsächlich auf dieser Basis. Neben den Schutzzielen aus der Informationssicherheit ist auch die Risikobewertung für das Informationssicherheitsmanagement relevant. Dies dient dazu, gewisse Sicherheitsmaßnahmen zu priorisieren. Des Weiteren muss das Informationssicherheitsmanagement kontinuierlich überwacht werden, um eine stetige Verbesserung zu erzielen. [ISMS]

2.1.2 Überblick über die ISO27001-Norm

2.1.2.1 Historische Entwicklung von ISO27001

Die Ursprünge der ISO 27000 bis ISO 27002-Standards lassen sich bis 1993 zurückverfolgen (Abbildung 1). Dort veröffentlichte ein britischer Berufsverband, das National Computing Centre (NCC), ein Dokument mit dem Titel „PD 0003 A Code of Practice for Information Security Management“. Daraufhin wurde dieses Dokument im Jahr 1995 vom Britischen Institut für Standardisierung (BSI) übernommen und als nationaler Standard unter dem Titel „BS 7799-1 IT-Security techniques-Code of practice for information security management“ eingeführt.

Die ISO übernahm diesen Standard mit anderen Standards wie der ISO 9001 und entwickelte im Oktober 2005 die ISO 27001. Seitdem können Unternehmen ihre Prozesse nach diesem internationalen Standard zertifizieren.

Die ISO 27001 legte den Grundstein für die ISO 27 K-Familie von Standards, die verschiedene Standards für die Informationssicherheit umfasst. Im Jahr 2009 erschien die ISO 27000, die eine Zusammenfassung, Einführung und Erläuterung der Terminologie lieferte.[Disterer] Im Jahr 2013 erschien eine erneuerte Version unter ISO27001:2013. Schlussendlich wurde am 25.Oktober 2022 die aktuellste Fassung unter ISO/IEC 27001:2022 veröffentlicht.

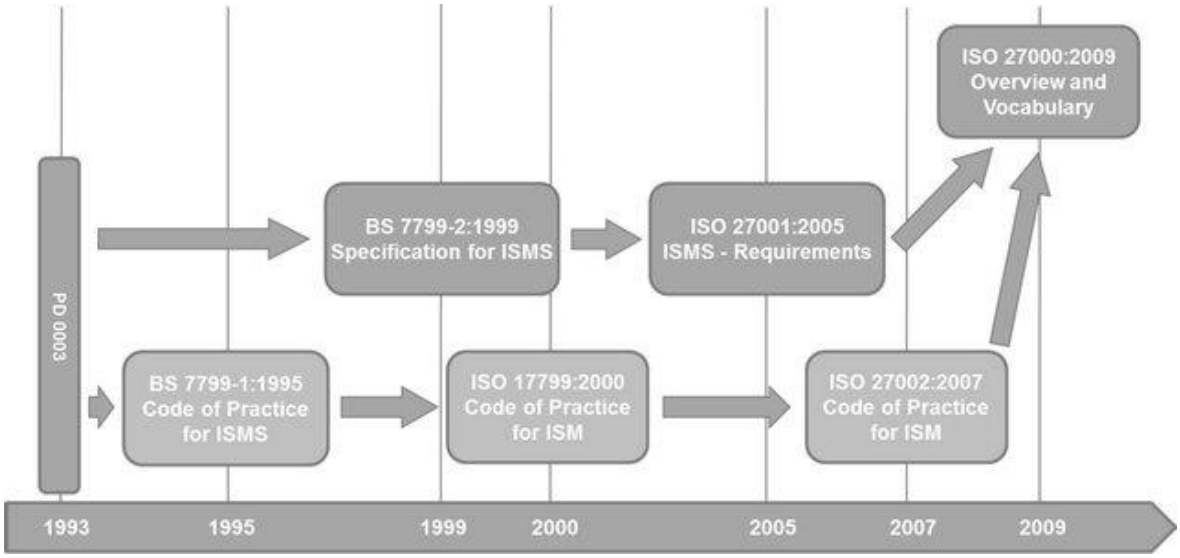

Abbildung 1 Historische Entwicklung der ISO27000 (entnommen aus: [Disterer])

2.1.2.2 Struktur und Inhalte der Norm

Die ISO27001 ist grundsätzlich in 10 Abschnitte gegliedert, wobei die Kapitel 4 bis 10 sowie der Anhang A relevant für die Zertifizierung sind.

Im Abschnitt 4 geht es um den Kontext der Organisation. In diesem Teil der Implementation muss das Unternehmen festlegen, für welchen Anwendungsbereich das Informationssicherheitsmanagementsystem gelten soll. Dabei soll die Organisation die externen und internen Themen in die Entscheidungsfindung mit einbeziehen sowie die Anforderungen und Erwartungen interessierter Parteien in Bezug auf Informationssicherheit.

Das nächste Kapitel setzt sich mit der Führung auseinander. Die Führung und Verpflichtung liegen bei der obersten Leitung. Des Weiteren muss die oberste Leitung eine angemessene Informationssicherheitspolitik festlegen, die die Informationssicherheitsziele beinhaltet. Außerdem muss sichergestellt werden, dass Rollen, Verantwortlichkeiten und Befugnisse zugewiesen und innerhalb der Organisation veröffentlicht werden.

Der sechste Abschnitt befasst sich mit der Planung. Es geht um Aktionen zur Risikobehandlung und ISMS-Risikobewertung sowie die Auswahl an Steuermaßnahmen.

Das Kapitel 7 beschäftigt sich mit der Unterstützung. Die Organisation muss die erforderlichen Ressourcen für die Umsetzung, Wartung und kontinuierliche Verbesserung des ISMS bereitstellen. Darüber hinaus müssen die Personen, welche für das Informationssicherheitsmanagementsystem verantwortlich sind, über ausreichende Kompetenzen verfügen. Das Unternehmen ist außerdem dafür verantwortlich, dass innerhalb der Organisation ein Bewusstsein für die Bedeutung und Einhaltung der Informationssicherheitsrichtlinien und -verfahren geschaffen wird. Außerdem müssen sicherheitsrelevante Informationen intern und extern kommuniziert werden.

Im nächsten Abschnitt steht der Betrieb im Vordergrund. Das Unternehmen plant und implementiert Sicherheitsmaßnahmen, welche Risiken behandeln, um dadurch Informationssicherheit zu erreichen. Außerdem wird im Kapitel 8 die betriebliche Steuerung geregelt.

Das neunte Kapitel behandelt die Bewertung der Leistung. Die Organisation muss bestimmen, was überwacht werden soll und wie diese Überwachung durchzuführen ist. Außerdem müssen regelmäßige interne Audits durchgeführt werden, um sicherzustellen, dass das Informationssicherheitsmanagementsystem sowohl den eigenen Anforderungen, als auch den Anforderungen der Norm entsprechen.

Im letzten Abschnitt wird geregelt, dass die Organisation das Informationssicherheitsmanagementsystem fortlaufend verbessern muss. Außerdem müssen bei Nichtkonformität Korrekturmaßnahmen ergriffen werden. Im Anschluss folgt der Anhang A. Dabei handelt es sich um eine Tabelle, in welcher Verweisungen auf Informationssicherheitsmaßnahmen enthalten sind. [ISO/IEC 27001:2022]

2.1.2.3 Anwendungsbereich und Vorteile der Zertifizierung nach ISO27001

Der Anwendungsbereich einer ISO27001 Zertifizierung umfasst den Bereich der Organisation, auf welchen das Informationssicherheitsmanagementsystem angewendet wird. Je nach den Anforderungen und Zielen des Unternehmens kann sich dieser Abschnitt unterscheiden. In der Regel beinhaltet der Anwendungsbereich sämtliche Bereiche der Organisation, in denen sensible Daten verarbeitet, gespeichert oder weitergegeben werden, sowie die dazugehörigen Prozesse, Technologien und Personen.

Eine gültige ISO27001 Zertifizierung bringt viele Vorteile mit sich, wie etwa eine Einsparung von Zeit und Geld durch eine frühzeitige Vorbereitung auf mögliche Probleme sowie eine fortlaufende Anpassung an sich wandelnde Gefahren durch interne Prüfungen und Risikomanagement. Außerdem trägt die ISO 27001 auch dazu bei, den Ruf der Organisation zu verbessern und Vertrauen in sie zu schaffen, indem sie durch eine unabhängige Überprüfung des ISMS Vertrauen in die Datensicherheit der Organisation schafft. Die ISO 27001 hilft Organisationen insgesamt dabei, die Sicherheit ihrer Informationen zu verbessern, Ausgaben zu reduzieren und das Vertrauen ihrer Interessengruppen zu erlangen. [ISMS-Online]

2.2 ISO27001:2013 im Vergleich zu ISO27001:2022

2.2.1 Hauptunterschiede und Änderungen zwischen den Versionen

2.2.1.1 Vergleichende Analyse der Struktur und Inhalte von ISO27001:2013 und ISO27001:2022

In der Einleitung wird in der alten Version eine kurze Einführung in das Informationssicherheitsmanagementsystem gegeben und der Anwendungsbereich definiert. Die Fassung aus 2022 beginnt ebenfalls mit einer Einführung, wobei das Augenmerk auf den neuen Herausforderungen in Bezug auf die Informationssicherheit liegt.

Im Kapitel 4 wird in der Version aus 2013 von der Organisation das Verständnis des Kontexts und die Berücksichtigung der Anforderungen und Erwartungen interessierter Parteien gefordert. Die ISO27001:2022 vertieft diese Anforderung und unterstreicht die Wichtigkeit einer fortlaufenden Kontrolle des organisatorischen Kontexts sowie der Bedrohungen von außen und innen.

Im Abschnitt über Führung und Verpflichtung fokussiert sich die ISO27001:2013 vor allem auf die Leitung des ISMS und auf die Ausarbeitung einer Informationssicherheitspolitik. In der überarbeiteten Fassung wird die Rolle der Führung auch für andere relevante Rollen betont.

Der Bereich der Planung beschäftigt sich mit Risikobeurteilung und der Auswahl von geeigneten Sicherheitsmaßnahmen. In der ISO27001:2022 wird im Gegensatz zu der alten Version speziell auf die Planung von Änderungen im Bereich des Informationssicherheitsmanagements eingegangen.

Des Weiteren lassen sich vereinzelt Änderungen bei Formulierungen feststellen. [ISO/IEC 27001:2022], [ISO/IEC 27001: 2013]

2.2.1.2 Vergleichende Analyse von Anhang A von ISO27001:2013 und ISO27001:2022

Die größten Veränderungen zwischen den beiden Versionen lassen sich im Anhang A finden. Anhang A der ISO 27001 ist ein Teil des Standards, der eine Reihe von speziellen Sicherheitsmaßnahmen auflistet, die von Organisationen verwendet werden, um die Einhaltung von ISO 27001 6.1.3 (Informationssicherheitsrisikobehandlung) und der damit verbundenen Anwendungserklärung zu belegen. Zuvor umfasste der Anhang 114 Maßnahmen, die in 14 Kategorien unterteilt waren. Diese behandelten eine Vielzahl von Themen. Mit der Veröffentlichung der ISO 27002: 2022 hat sich die Struktur grundsätzlich verändert. Die Anzahl der Maßnahmen wurde auf 93 Stück reduziert, wobei in diesen 11 gänzlich neue Punkte zu finden sind. Einige der alten Maßnahmen wurden zusammengefasst oder verändert.

Außerdem sind die Maßnahmen in der Fassung aus 2022 in 4 Gruppen eingeteilt: Organisatorische Maßnahmen (Abbildung 2), Personenbezogene Maßnahmen, Physische Maßnahmen, Technologische Maßnahmen. [ISO/IEC 27001:2022], [ISO/IEC 27001: 2013]

Anhang A
(normativ)

Verweisung auf Informationssicherheitsmaßnahmen

Die in Tabelle A.1 aufgeführten Informationssicherheitsmaßnahmen[N1] sind aus denjenigen, die in ISO/IEC 27002:2022 [1], Abschnitt 5 bis Abschnitt 8, genannt sind, direkt abgeleitet, daran ausgerichtet und müssen im Kontext mit 6.1.3 angewendet werden.

Tabelle A.1 — Informationssicherheitsmaßnahmen

5	Organisatorische Maßnahmen	
5.1	Informationssicherheitspolitik und -richtlinien	**Maßnahme** Informationssicherheitspolitik und themenspezifische Richtlinien müssen definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.
5.2	Informationssicherheitsrollen und -verantwortlichkeiten	**Maßnahme** Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.
5.3	Aufgabentrennung	**Maßnahme** Sich widersprechende Aufgaben und Verantwortungsbereiche müssen voneinander getrennt werden.
5.4	Verantwortlichkeiten der Leitung	**Maßnahme** Die Leitung muss vom gesamten Personal verlangen, dass es die Informationssicherheit im Einklang mit der eingeführten Informationssicherheitspolitik, und den themenspezifischen Richtlinien und Verfahren der Organisation umsetzt.
5.5	Kontakt mit Behörden	**Maßnahme** Die Organisation muss mit den zuständigen Behörden Kontakt aufnehmen und halten.

Abbildung 2 Ausschnitt aus Anhang A (entnommen aus: [ISO/IEC 27001:2022])

2.2.1.3 Neue Anforderungen und Schwerpunkte in der aktualisierten Version

Die Betonung des Datenschutzes ist einer der bedeutendsten Unterschiede zwischen den beiden Versionen. Die Version aus 2022 betont die Bedeutung des Schutzes von Daten und der Bewältigung von Datenschutzrisiken. Dies geschieht durch die Verpflichtung der Organisationen zur Einführung eines Datenschutz-Management-Systems, das den Datenschutzanforderungen entspricht.

Ein weiterer relevanter Unterschied besteht darin, wer für die Einhaltung der Datenschutzbestimmungen verantwortlich ist. Die neue Fassung verlangt die Einhaltung der Datenschutzgesetze und -vorschriften auf sämtliche Organisationsebenen. Dies umfasst die Verantwortung für die Einhaltung des Datenschutzes bei der Verarbeitung von persönlichen Daten sowie für die Nutzung externer Dienstleister.

Außerdem müssen Organisationen eine umfassende Risikoanalyse vornehmen, welche sich nicht nur auf technische Risiken, sondern auch auf geschäftliche und organisatori-

sche Risiken konzentriert. Dazu gehört unter anderem eine Überprüfung der Datenschutzrisiken, inklusive des Zugriffs auf personenbezogene Daten, der Datenübertragung- und Speicherung und der Nutzung externer Dienstleister.

Des Weiteren werden aktuelle Themen wie Cloud Computing, die Nutzung externer Geräte und die Sicherheit bei der Privatnutzung von Firmengeräten in den Vordergrund gestellt.

Ein weiterer Schwerpunkt liegt auf der konstanten Überarbeitung und Anpassung des Informationssicherheitsmanagementsystems. Dies beinhaltet eine regelmäßige Überprüfung, bei der sichergestellt wird, dass das System den aktuellen Bedrohungen gewachsen ist. [iso-27001]

2.2.2 Bewertung der Notwendigkeit und Relevanz einer Umstellung auf ISO27001:2022

Die Umstellung auf die ISO 27001:2022 ist für Organisationen sehr wichtig, weil sie zahlreiche Vorzüge mit sich bringt, die zur Stärkung der Informationssicherheit und zur Einhaltung internationaler Standards beitragen. Außerdem können Organisationen durch die Aktualisierung auf den neuesten internationalen Informationssicherheitsstandard sensible Daten vor einer Vielzahl von Cyberbedrohungen schützen.

Darüber hinaus dient die Implementierung der ISO27001:2022 dazu, Kunden, Partnern und anderen interessierten Parteien zu signalisieren, dass die Organisation sich zur Einhaltung von Informationssicherheitsstandards verpflichtet hat. Diese Standards werden in einem Zertifizierungsverfahren regelmäßig von einer externen Fachkraft geprüft und haben internationale Gültigkeit.

Die ISO 27001:2022 stellt außerdem einen Rahmen zur Verfügung, der die generellen Risikomanagementprozesse in einer Organisation verbessern kann. Organisationen können durch eine systematische Risikoerkennung, -bewertung und -behandlung nicht nur das Risiko von Datenverletzungen und anderen Vorfällen verringern, sondern auch die Effizienz und Effektivität ihrer Organisationen steigern.

Des Weiteren hilft die ISO 27001:2022 dabei, die Schutzziele der Informationssicherheit (Vertraulichkeit, Integrität und Verfügbarkeit von Daten) kontinuierlich zu verbessern, sodass alle schützenswerten Informationen jederzeit zugänglich, unverfälscht und vertraulich sind. [DataGuard]

3 Praktischer Teil - Umstellung auf ISO/IEC 27001:2022

In diesem Teil der Arbeit wird das Unternehmen, in welchem die Arbeit geschrieben wurde, vorgestellt. Außerdem wird beschrieben, welche Methodik angewandt wurde. Danach folgt eine ausgearbeitete Liste, welche die notwendigen Anpassungen enthält.

3.1 Vorstellung des Unternehmens

Die Firma Infotech EDV-Systeme GmbH wurde im Jahr 1993 gegründet und ist in Ried im Innkreis ansässig. Die Firma hat eine große Auswahl an verschiedenen Produkten sowie Dienstleistungen rund um den Bereich von Informations- und Kommunikationstechnologien. Zu den Kunden gehören sowohl große Unternehmen als auch Privatkunden. Die Dienstleistungen werden im B2B-Bereich österreichweit und international angeboten. Außerdem verkauft das Systemhaus auch im regionalen Umfeld Internetprodukte, Festnetztelefonie und interaktives IPTV-Fernsehen.

3.2 Methodik

Für die Methodik dieser Arbeit wurde eine sorgfältige Kombination aus Literaturrecherche und Zusammenarbeit mit den Mitarbeitern der Firma Infotech, welche Fachwissen im Bereich der Informationssicherheit haben, gewählt. Um den Übergang von der ISO27001:2013 zu der ISO27001:2022 erfolgreich zu implementieren, benötigt es eine gründliche Analyse der Unterschiede zwischen den beiden Dokumenten, insbesondere dem Anhang A.

3.3 Änderungen bezüglich Anhang A

Im Folgenden werden die einzelnen Kontrollpunkte aus Anhang A der ISO27001:2022 analysiert und mit dem Anhang A aus der ISO27001:2013 verglichen. Außerdem werden bei relevanten Änderungen Vorschläge gemacht, wie sich die alten Richtlinien und Praktiken an die neuen Gegebenheiten angepasst werden können. Maßnahmen bei denen sich ausschließlich die Formulierung geändert hat, werden nicht behandelt. Die Überschriften werden nach den einzelnen Maßnahmen aus der ISO27001:2022 benannt.

Eine Änderung die im kompletten Anhang A vorgenommen wurde ist das Ersetzen des Begriffs „Beschäftigte“ durch „Personal“ und das Ersetzen des Terms „relevante externe Parteien“ durch „interessierte Parteien“.

3.3.1 Organisatorische Maßnahmen

3.3.1.1 5.1 Informationssicherheitspolitik und Richtlinien

Die Maßnahme findet sich in der ISO27001:2013 unter A.5.1 und A.5.2 wieder. In der neuen Richtlinie wird die Informationssicherheitsrichtlinie mit dem Begriff Informationssicherheitspolitik umschrieben. Außerdem muss diese zusätzlich vom Personal und den interessierten Parteien zur Kenntnis genommen werden. Des Weiteren muss die Politik zukünftig sowohl in geplanten Abständen als auch bei wesentlichen Änderungen überprüft werden. Um diese Änderungen in den Richtlinien des Unternehmens zu übernehmen, sollte eine schriftliche Bestätigung der Informationssicherheitspolitik vom gesamten Personal sowie den interessierten Parteien gefordert werden. Darüber hinaus sollte das Revisionsintervall des Dokumentes zu „jährlich und bei wesentlichen Änderungen“ angepasst werden.

3.3.1.2 5.2 Informationssicherheitsrollen und -verantwortlichkeiten

Die Maßnahme findet sich in der ISO27001:2013 unter A.6.1.1 wieder. Ursprünglich war gefordert, dass Informationssicherheitsverantwortlichkeiten festgelegt und zugeordnet sein müssen. In der neuen Version wird zusätzlich die Zuweisung von Aufgaben entsprechend den Erfordernissen des Unternehmens verlangt. Damit das Unternehmen diese Maßnahme ausreichend erfüllt, muss es die Aufgaben klar definieren.

3.3.1.3 5.7 Informationen über die Bedrohungslage

Bei dieser Maßnahme handelt es sich um einen neuen Kontrollpunkt. Es wird gefordert, dass Bedrohungen für die Informationssicherheit erhoben sowie analysiert werden müssen. Umsetzen lässt sich dies beispielsweise durch anerkannte Newsletter, welche täglich oder wöchentlich Berichte über die aktuellen Sicherheitslücken berichten.

3.3.1.4 5.12 Klassifizierung von Informationen

Die Maßnahme findet sich in der ISO27001:2013 unter A.8.2.1 wieder. In der veralteten Norm wird gefordert, dass Informationen bezüglich ihres Wertes, gesetzlichen Anforderungen, ihrer Kritikalität und ihrer Empfindlichkeit gegenüber unbefugter Offenlegung oder Veränderung klassifiziert werden. In der neuen Fassung werden diese Punkte mit der Klassifizierung auf der Grundlage von Vertraulichkeit, Integrität und Verfügbarkeit zusammengefasst. Außerdem werden die gesetzlichen Anforderungen nicht mehr explizit erwähnt. An deren Stelle treten relevante Anforderungen von interessierten Parteien. Somit muss künftig bei der Klassifizierung von Daten darauf geachtet werden, dass nicht nur

gesetzliche Anforderungen erfüllt werden, sondern auch die Anforderungen von anderen interessierten Parteien, wie zum Beispiel Geschäftspartner. Dies sollte auch in der Klassifizierungsrichtlinie übernommen werden.

3.3.1.5 5.17 Authentisierungsinformationen

Die Maßnahme findet sich in der ISO27001:2013 unter A.9.2.4 wieder. Zusätzlich zu der Zuordnung und Verwaltung von Authentisierungsinformationen wird gefordert, dass das Personal mit dem angemessenen Umgang mit Authentisierungsinformationen bekannt gemacht wird. Diese Maßnahme sollte in der IT Nutzungsrichtlinie verankert und auch durchgeführt werden.

3.3.1.6 5.23 Informationssicherheit für die Nutzung von Cloud-Diensten

Bei dieser Maßnahme handelt es sich um einen neuen Kontrollpunkt. In dieser wird ein Verfahren für den Erwerb, die Nutzung, die Verwaltung und den Ausstieg aus Cloud-Diensten gefordert. Am besten lässt sich dies durch eine Checkliste für den sicheren Erwerb und den sicheren Ausstieg umsetzen. Außerdem sollten mit allen Cloud-Diensten Verträge abgeschlossen werden, welche mit den Anforderungen der Organisation kompatibel sind.

3.3.1.7 5.30 IKT-Bereitschaft für Business-Continuity

Bei dieser Maßnahme handelt es sich um einen neuen Kontrollpunkt. Hier liegt der Fokus auf der IKT-Bereitschaft. Diese muss auf der Grundlage von Business-Continuity-Zielen geplant, umgesetzt, aufrechterhalten und geprüft werden. Um diese Maßnahme im Unternehmen umsetzen zu können, muss eine Business-Impact-Analyse (BIA) durchgeführt werden, um feststellen zu können, welche Auswirkung Ausfälle auf das Unternehmen haben. Außerdem muss das Unternehmen einen RTO (Recovery Time Objective) festlegen. Im Anschluss daran müssen Prozesse entwickelt werden, um Business Continuity sicherzustellen.

3.3.2 Personenbezogene Maßnahmen

3.3.2.1 6.1 Sicherheitsüberprüfung

Die Maßnahme findet sich in der ISO27001:2013 unter A.7.1.1 wieder. Von der Norm wird verlangt, dass alle Angestellten einer Sicherheitsprüfung unterzogen werden müssen. Dabei müssen Gesetze, Vorschriften und ethnische Grundsätze berücksichtigt werden. In der ISO27001:2022 wird zusätzlich verlangt, dass die Organisation die Sicherheitsprüfung fortlaufend ausführt. Umsetzen könnte man diese Maßnahme durch eine Regelung, welche die Angestellten dazu verpflichtet, jegliche Verstöße gegen das Gesetz der Organisation zu melden.

3.3.2.2 6.4 Maßregelungsprozess

Die Maßnahme findet sich in der ISO27001:2013 unter A.7.2.3 wieder. Die Norm schreibt vor, dass es einen formal festgelegten Maßregelungsprozess geben muss, welcher dazu dient, Maßnahmen gegen Angestellte einzuleiten, die gegen die Informationssicherheitslinie verstoßen. In der neuen Fassung wird hinzugefügt, dass der Maßregelungsprozess nicht nur bekanntgegeben, sondern auch kommuniziert werden muss. Um dieser Maßnahme gerecht zu werden, benötigt es lediglich einen Prozess für die Maßregelung, welcher den Mitarbeitern mitgeteilt und angenommen wird.

3.3.3 Physische Maßnahmen

3.3.3.1 7.4 Physische Sicherheitsüberwachung

Bei dieser Maßnahme handelt es sich um einen neuen Kontrollpunkt. Die Norm legt fest, dass alle zum Informationssicherheitsmanagementsystem gehörenden Räume durchgehend vor dem Zugang von Unbefugten geschützt werden müssen. Damit diese Maßnahme ausreichend erfüllt ist, braucht es eine durchgehende Videoüberwachung sowie einen Bewegungsmelder in den betroffenen Bereichen.

3.3.3.2 7.5 Schutz vor physischen und umweltbedingten Bedrohungen

Die Maßnahme findet sich in der ISO27001:2013 unter A.11.1.4 wieder. In diesem Kontrollpunkt wird ein physischer Schutz vor Naturkatastrophen, Angriffen und Unfällen verlangt. In der ISO27001:2022 wird die Aussage erweitert und betrifft zusätzlich jegliche anderen absichtlichen oder unabsichtlichen physischen Bedrohungen.

3.3.3.3 7.10 Speichermedien

Die Maßnahme findet sich in der ISO27001:2013 unter A.8.3.1, A.8.3.2 und A.8.3.3 wieder. In der alten Norm wurden die Verwendung, die Entsorgung und der Transport von Datenträgern geregelt. Mit der neuen Version wird geregelt, dass Speichermedien während des gesamten Lebenszyklus, inklusive des Erwerbs, verwaltet werden müssen. Daher müssen die Richtlinien dementsprechend angepasst und die Beschaffung von IT-Equipment geregelt werden.

3.3.3.4 7.12 Sicherheit der Verkabelung

Die Maßnahme findet sich in der ISO27001:2013 unter A.11.2.3 wieder. Ursprünglich wurde festgelegt, dass Telekommunikationskabel sowie Stromkabel vor Unterbrechung, Störung und Beschädigung geschützt werden müssen. In der aktualisierten Norm wird des Weiteren angegeben, dass die Kabel auch vor Abhören geschützt werden müssen. Dementsprechend ist es notwendig, die Kabel soweit wie möglich zu schützen.

3.3.4 Technologische Maßnahmen

3.3.4.1 8.4 Zugriff auf den Quellcode

Die Maßnahme findet sich in der ISO27001:2013 unter A.9.4.5 wieder. In der Version aus 2013 wurde festgelegt, dass der Zugang zu dem Quellcode von Programmen eingeschränkt werden muss. In der Revision wurde genauer definiert, was mit Zugang gemeint ist. In diesem Sinn müssen der Lese- und Schreibzugriff, Softwarebibliotheken und Entwicklungswerkzeuge entsprechend überwacht werden.

3.3.4.2 8.9 Konfigurationsmanagement

Bei dieser Maßnahme handelt es sich um einen neuen Kontrollpunkt. Es wird verlangt, dass die Konfigurationen und Sicherheitskonfigurationen definiert, dokumentiert, durchgeführt, überwacht und überprüft. Ein Ansatz für die Einhaltung dieser Maßnahme könnte darin bestehen, eine eigene Konfigurationsrichtlinie zu erstellen, um alle relevanten Punkte abzudecken.

3.3.4.3 8.10 Löschung von Informationen

Bei dieser Maßnahme handelt es sich um einen neuen Kontrollpunkt. In diesem Punkt geht es darum, Informationen, welche nicht mehr benötigt werden, umgehend zu löschen. Diese Maßnahme könnte man in die Klassifizierungsrichtlinie mit einbeziehen. Dort sollte geregelt werden, wann Daten gelöscht werden müssen und wann man Daten nicht löschen darf.

3.3.4.4 8.11 Datenmaskierung

Bei dieser Maßnahme handelt es sich um einen neuen Kontrollpunkt. Die Maßnahme soll dafür sorgen, dass Datenmaskierung geregelt und ordnungsgemäß abläuft. Eine Möglichkeit, wie diese Maßnahme umzusetzen ist, wäre Anonymisierung und Pseudonymisierung aller Persönlich Identifizierbaren Informationen (PII).

3.3.4.5 8.12 Verhinderung von Datenlecks

Bei dieser Maßnahme handelt es sich um einen neuen Kontrollpunkt. Dieser Punkt legt fest, dass auf allen Geräten, Netzwerken und Systemen, welche sensible Daten verarbeiten, Maßnahmen gesetzt werden müssen um Datenlecks zu verhindern. Mögliche Maßnahmen die Organisationen ergreifen könnten wären Monitoring von Datenübertragung, Autorisierung, Kopieren und Einfügen einschränken, Screenshots verhindern sowie weitere generelle Sicherheitsmaßnahmen

3.3.4.6 8.15 Protokollierung

Die Maßnahme findet sich in der ISO27001:2013 unter A.12.4.1, A.12.4.2 und A.12.4.3 wieder. In dieser Version aus 2013 wurde festgelegt, dass Protokolle aller relevanten Ereignisse erstellt, gespeichert und geschützt werden müssen. Zusätzlich verlangt die ISO27001:2022 auch eine Analyse der Protokolle.

3.3.4.7 8.16 Überwachung von Aktivitäten

Bei dieser Maßnahme handelt es sich um einen neuen Kontrollpunkt. Ziel dieser Maßnahme ist es, abnormales Verhalten in Netzwerken, Systemen und Anwendungen festzustellen und entsprechend zu reagieren. Neben der Meldung von verdächtigen Vorfällen sollten folgende Prozesse implementiert werden: Audits, Suche nach Schwachstellen im System und Monitoring.

3.3.4.8 8.23 Webfilterung

Bei dieser Maßnahme handelt es sich um einen neuen Kontrollpunkt. Um die Gefahr von bösartigen Inhalten zu minimieren, muss der Zugang zu externen Webseiten verwaltet werden. Um dieser Maßnahme gerechtzuwerden, sollten Organisationen Regeln festlegen, auf welche Webseiten zugegriffen werden darf und auf welche nicht. Im Anschluss muss dieses Regelwerk auch technisch umgesetzt werden.

3.3.4.9 8.28 Sichere Codierung

Bei dieser Maßnahme handelt es sich um einen neuen Kontrollpunkt. Sie regelt den Umgang für eine sicherere Softwareentwicklung. Unternehmen können beispielsweise einen Leitfaden erstellen, in dem die Grundsätze für sichere Codierung festgehalten sind. Außerdem sollten sich alle Beteiligten dazu verpflichten, nach dem Stand der Technik zu arbeiten.

3.4 Erstellung einer SoA

Ein wichtiger Punkt bei einer gelungenen ISO Zertifizierung ist ein Statement of Applicability (SoA). Bei der SoA handelt es sich um ein Dokument, in welchem alle in Anhang A beschriebenen Maßnahmen aufgeführt sind. Eine SoA ist für eine gültige Zertifizierung notwendig. Des Weiteren muss in der SoA ein Grund für die Miteinbeziehung, beziehungsweise ein Grund für die Auslassung von Maßnahmen angegeben werden. Außerdem müssen Referenzen angeführt werden (siehe Abbildung 3).

Control	Titel	Maßnahme	Anwendbar	Umgesetzt	Referenz
A.5	**Organisatorische Maßnahmen**				
A.5.1	Informationssicherheitspolitik und -richtlinie	Informationssicherheitspolitik und themenspezifische Richtlinien müssen definiert, von der Geschäftsleitung genehmigt, veröffentlicht, dem zuständigen Personal und den interessierten Parteien mitgeteilt und von diesen zur Kenntnis genommen sowie in geplanten Abständen und bei wesentlichen Änderungen überprüft werden.	ja	ja	Informationssicherheitsleitlinie, Management Review
A.5.2	Informationssicherheitsrollen und -verantwortlichkeiten	Die Aufgaben und Zuständigkeiten im Bereich der Informationssicherheit müssen entsprechend den Erfordernissen des Unternehmens definiert und zugewiesen werden.	ja	ja	Rollen und handelnde Personen
A.5.3	Aufgabentrennung	Sich widersprechende Aufgaben und Verantwortungsbereiche müssen voneinander getrennt werden.	ja	ja	Informationssicherheitsleitlinie, Klassifizierungsrichtlinie
A.5.4	Verantwortlichkeiten der Leitung	Die Leitung muss vom gesamten Personal verlangen, dass es die Informationssicherheit im Einklang mit der eingeführten Informationssicherheitspolitik, und den themenspezifischen Richtlinien und Verfahren der Organisation umsetzt.	ja	ja	IT-Nutzungsrichtlinie, Informationssicherheitsleitlinie
A.5.5	Kontakt mit Behörden	Die Organisation muss mit den zuständigen Behörden Kontakt aufnehmen und halten.	ja	ja	Kontakt mit RTR, Kontakt mit DSB
A.5.6	Kontakt mit speziellen Interessensgruppen	Die Organisation muss mit speziellen Interessensgruppen oder sonstigen sicherheitsorientierten Expertenforen und Fachverbänden Kontakt aufnehmen und halten.	ja	ja	CERT Mailinglisten, Kontakt mit CERT, ISPA AG Datenschutz, ISPA AG Recht
A.5.7	Informationen über die Bedrohungslage	Informationen über Bedrohungen der Informationssicherheit müssen erhoben und analysiert werden, um Erkenntnisse über Bedrohungen zu gewinnen.	ja	ja	CERT Mailinglisten, BSI Mailingliste, CISA Mailingliste, Risikomanagement
A.5.8	Informationssicherheit im Projektmanagement	Die Informationssicherheit muss in das Projektmanagement integriert werden.	ja	ja	Rollen und handelnde Personen
A.5.9	Inventar der Informationen und anderen damit verbundenen Werte	Ein Inventar der Informationen und anderen damit verbundenen Werte, einschließlich der Eigentümer, muss erstellt und gepflegt werden.	ja	ja	Informationssicherheitsleitlinie, Klassifizierungsrichtlinie

Abbildung 3 Beispiel einer SoA (entnommen aus internen Richtlinien von Infotech)

4 Diskussion und Schlussfolgerung

In diesem Kapitel sollen die Ergebnisse und Erkenntnisse der theoretischen Implementation kurz und prägnant dargestellt werden. Außerdem sollen allgemeine Unterschiede zwischen den beiden ISO27001 Versionen bewertet werden. Zum Schluss wird noch ein Ausblick auf zukünftige Entwicklungen gegeben.

4.1 Zusammenfassung der wichtigsten Erkenntnisse aus dem Praxisteil

Der im Praxisteil durchgeführte Vergleich hat deutlich gemacht, dass die Unterschiede zwischen der ISO27001:2013 und der ISO27001:2022 oftmals im Detail liegen, da häufig lediglich kleine Änderungen vorgenommen wurden. Außerdem können Organisationen die Möglichkeit der Umstellung auf die ISO27001:2022 nutzen, um ihre Informationssicherheit in vielen verschiedenen Bereichen zu stärken. Darunter auch in Gebieten, welche zuvor noch keine Relevanz für ihre Informationssicherheit hatten.

Darüber hinaus wird deutlich, dass die Hauptaufgabe in Unternehmen, welche eine bereits bestehende ISO27001:2013 Zertifizierung haben und die ISO27001:2022 anstreben, darin bestehen wird, Kleinigkeiten in den Richtlinien zu verändern und den technologischen Aspekt des Informationssicherheitsmanagementsystems auszubauen.

4.2 Bewertung der allgemeinen Unterschiede zwischen ISO/IEC 27001:2013 und ISO/IEC 27001:2022

In den Unterschieden lässt sich erkennen, dass sich Informationssicherheitsmanagementsysteme stetig entwickeln müssen, um den Sicherheitsanforderungen zu entsprechen. Die Bedrohungen verändern sich und dementsprechend müssen auch Normen angepasst werden. Diese Veränderungen spiegeln sich im Anhang A in den neuen Kontrollpunkten wieder. Außerdem wird in der ISO27001:2022 der Fokus verstärkt auf das Thema Datenschutz gelegt. Darüber hinaus wird verstärkt auf die Risikoanalyse eingegangen.

4.3 Ausblick auf zukünftige Entwicklungen

Ausblicke auf kommende Entwicklungen im Bereich der Informationssicherheit deuten darauf hin, dass es zukünftig immer mehr Bedrohungen und Risiken für Informationssicherheitssysteme geben wird. Die Technik entwickelt sich schnell und es werden immer häufiger gezielte Angriffe auf Unternehmen geführt. Daher müssen sich Organisationen bemühen ihre Informationssicherheitsmanagementsysteme stetig zu verbessern und an

die aktuellen Gegebenheiten anzupassen. Es ist außerdem davon auszugehen, dass in den kommenden Jahren die ISO27001 erneut angepasst und weiterentwickelt werden muss.

5 Fazit

Diese Arbeit hat sich mit dem Thema „Implementierung der ISO/IEC 27001:2022: Ein Leitfaden zur Umstellung von der ISO/IEC 27001:2013“ auseinandergesetzt. Dabei wurden die Unterschiede zwischen den Normen verdeutlicht und die notwendigen Änderungen im Informationssicherheitsmanagementsystem, um nach der ISO27001:2022 erfolgreich zertifiziert zu werden, wurden entwickelt.

Es hat sich herausgestellt, dass die Anpassungen die vorgenommen werden müssen in der Theorie leicht darzustellen sind. In der Praxis kann es aber bei einigen Maßnahmen zu Herausforderungen und Problemen kommen.

Zusammenfassend kann diese Arbeit als Grundlage für die Umstellung von der ISO27001:2013 auf die ISO27001:2022 verstanden werden. Details und angepasste Umsetzung müssen von den Organisationen selbst übernommen werden.

5.1 Schlussbemerkung

Die Aktualität des Themas sowie die begrenzte Verfügbarkeit von Forschungsquellen sind die Hauptursache für die geringe Seitenanzahl dieser Arbeit. Außerdem gibt es kaum kostengünstige Fachliteratur in diesem Bereich. Außerdem fehlen Abbildungen fast zur Gänze, da es sich bei der Umstellung auf die ISO27001:2022 hauptsächlich um eine Dokumentenanalyse handelt. Diese Arbeit sollte trotz ihrer Einschränkungen wesentlich für die Literatur in diesem Themengebiet sein. Sie bietet eine Orientierung für Unternehmen, die eine Umstellung planen.

Literatur

[DataGuard] https://www.dataguard.de/wissen/iso-27001/2022-version-uebergangsleitfaden/, verfügbar am 19.03.2024, 08:12

[Disterer] Disterer, Georg: ISO/IEC 27000, 27001 and 27002 for Information Security Management, Journal of Information Security, Vol. 4 No.2, 2013

[ISMS] https://www.forum-verlag.com/blog-di/informationssicherheitsmanagementsystem-isms, verfügbar am 13.03.2024, 15:34

[ISMS-Online] https://de.isms.online/iso-27001/, verfügbar am 14.03.2024, 09:12

[ISO/IEC 27000:2018] ÖVE/ÖNORM EN ISO/IEC 27000:2020 Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Überblick und Terminologie (ISO/IEC 27000:2018)

[ISO/IEC 27001: 2013] ISO/IEC 27001: 2013, Information technology - Security techniques - Information security management systems – Requirements

[ISO/IEC 27001:2022] ISO/IEC 27001:2022, Information security, cybersecurity and privacy protection – Information security management systems - Requirements

[iso-27001] https://www.iso-27001.at/welche-anderungen-ergeben-sich-in-der-iso-270012013-zur-iso-270012022/, verfügbar am 14.03.2024, 11:35

[Liedtke] Liedtke, Thomas: Informationssicherheit, Heidelberg, Springer Gabler Berlin, 2022

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Vöcklamarkt, den 15.4.2024

Anna Leist