Handbuch / Regelwerk zur Norm

DIN EN ISO/IEC 27001:2024

Inhaltsverzeichnis

1 Anwendungsbereich....2
2 Normative Verweisungen....2
3 Begriffe (siehe Punkt 11)....2
4 Kontext der Organisation....2
4 1 Die Organisation und ihren Kontext verstehen....2
4 2 Verstehen der Bedürfnisse und Erwartungen interessierter Parteien....3
4 3 Festlegen des Anwendungsbereichs des ISMS....3
4 4 Managementsystem für Informationssicherheit....3
5 Führung....3
5 1 Führung und Engagement....3
5 2 Politik / Informationssicherheitsrichtlinie....4
5 3 Organisatorische Rollen, Verantwortlichkeiten und Befugnisse....4
6 Planung....4
6 1 Maßnahmen zum Umgang mit Risiken und Chancen....4
6 2 Informationssicherheitsziele und Planung zu deren Erreichung....5
6.3 Planung von Änderungen....6
7 Unterstützung....6
7 1 Ressourcen....6
7 2 Kompetenz....6
7 3 Bewusstsein....6
7 4 Kommunikation....6
7 5 Dokumentierte Information....7
7 5 1 Allgemeines....7
7 5 2 Erstellen und Aktualisieren....7
7 5 3 Lenkung dokumentierter Informationen....7
8 Betrieb....8
8 1 Operative Planung und Steuerung....8
8 2 Risikobewertung der Informationssicherheit....8
8 3 Umgang mit Informationssicherheitsrisiken....8
9 Bewertung der Leistung....9
9 1 Überwachung, Messung, Analyse und Bewertung....9
9 2 Internes Audit....9
9.2.1 Allgemeines....9
9.2.2 Internes Auditprogramm....10
9 3 Managementbewertung....10

9.3.1 Allgemeines....10
9.3.2 Eingaben der Managementbewertung....10
9.3.3 Ergebnisse der Managementbewertung....10
10 Verbesserung....10
10 1 Kontinuierliche Verbesserung....10
10.2 Nichtkonformität und Korrekturmaßnahmen....10
11.0 Begriffserklärung (Grundlage ISO 27000)....11

1 Anwendungsbereich

Unternehmensbezeichnung: QMKontakt.de
Straße: Zum Saibling 3
PLZ, Ort: D-88662 Überlingen

GF: xy
ISMS-Beauftragte(r): xy

Anzahl Mitarbeiter/-innen: 5

2 Normative Verweisungen

Im Rahmen unseres Informationsmanagementsystems beachten wir folgende normative Vorgaben (Beispiele):

- DIN EN ISO/IEC 27001:2024-01 Anforderungen Informationssicherheitsmanagementsysteme
- DIN EN ISO / IEC 27002:2024-01 Informationssicherheitsmaßnahmen
-

3 Begriffe (siehe Punkt 11)

4 Kontext der Organisation

4 1 Die Organisation und ihren Kontext verstehen

Unsere Rahmenbedingungen sind für die strategische Ausrichtung unseres Informationssicherheitsmanagementsystems relevant. Die Themen zur Erreichung der beabsichtigten Ergebnisse sind in externe und interne Zusammenhänge unterteilt. Die Themen werden laufend, formell aber jährlich geprüft und überwacht. Werden zwischen den Überwachungen neue Themen erkannt, werden diese umgehend umgesetzt.
Dabei berücksichtigen wir folgende Aspekte:

- soziale, kulturelle, politische, rechtliche, regulatorische, finanzielle, technologische, wirtschaftliche, natürliche und wettbewerbsspezifische Gegebenheiten internationaler, nationaler, regionaler oder lokaler Art,
- wesentliche Triebkräfte und Trends, welche unser Unternehmen beeinflussen,
- die Beziehungen zu interessierten Parteien sowie deren Wahrnehmungen und Werte.

Wir beachten die Anforderungen der ISO 31000 Abschnitt 5.4.1.

Nachweis(e)
FB 4 1 0 / 4 2 0 Kontext, Erfordernisse und Erwartungen

4 2 Verstehen der Bedürfnisse und Erwartungen interessierter Parteien

Wir haben die Erfordernisse und Erwartungen in einem Formblatt gelistet und kommunizieren diese im Unternehmen. Die Erfordernisse und Erwartungen werden laufend, formell aber jährlich geprüft und überwacht. Werden zwischen den Überwachungen neue Erfordernisse und Erwartungen erkannt, werden diese umgehend umgesetzt.

Nachweis(e)
FB 4 1 0 Kontext, Erfordernisse und Erwartungen

4 3 Festlegen des Anwendungsbereichs des ISMS

Geltungssbereich des ISMS:

- Entwicklung, Produktion und Vertrieb von Musterdokumentationen,
- Durchführung von Beratungsleistungen,
- Informationsmanagement für Kunden,
- Dokumentationsprüfungen und
- Dokumentationserstellung.

Geografischer Anwendungsbereich:
Siehe 1 Anwendungsbereich.

Nachweis(e)
FB 4 3 0 Grundriss Räumlichkeiten

4 4 Managementsystem für Informationssicherheit

Mit diesem Handbuch und den nachfolgenden Regelungen und Nachweisen haben wir nachgewiesen, dass wir ein ISMS eingeführt haben. Dieses System wird fortlaufend aufrechterhalten und verbessert.
Unsere Prozesse sind im Laufe dieses Regelwerks oder in gesonderten Prozessbeschreibungen beschrieben.
Die Prozessbeschreibungen beinhalten:

- die Prozesseingaben,
- das zu erwartende Prozessergebnis,
- Kriterien und Methoden zur Durchführung,
- die Art der Messung,
- Messmethoden,
- bedeutende Leistungsindikatoren, die für das Prozessergebnis von Bedeutung sind,
- Verantwortungen / Befugnisse im Rahmen des Prozessablaufes,
- Prozessrisiken und Chancen sowie abgeleitete Maßnahmen,
- die Form der Prozessüberwachung,
- letzte Änderungen,
- mögliche Prozessverbesserungen ,
- Dokumente und deren Aufbewahrung und
- die Prozessabfolge und deren Wechselwirkungen.

Dokumentierte Informationen, wie Aufzeichnungen und Vorgaben, stehen im Einklang mit der Notwendigkeit und unterstützen die Durchführung.

Arbeitsanweisung
AA 4 4 0 Anweisung Prozesserstellung
Nachweis(e)
FB 4 4 0 Prozesse

5 Führung

5 1 Führung und Verpflichtung

Wir zeigen Führung und Verpflichtung durch:

- Festlegung der Informationssicherheitsrichtlinie und der Informationssicherheitsziele unter Beachtung der strategischen Ausrichtung,
- die Integration der Anforderungen,
- Umsetzung in allen Geschäftsprozessen,
- Bereitstellung von notwendigen Ressourcen,
- Laufende Vermittlung des ISMS auf allen internen Ebenen,
- Gewährleistung der Zielerreichung,
- Unterstützung und Anleitung der Beteiligten,
- Fortlaufende Verbesserung und
- Unterstützung der Führungskräfte.

5 2 Politik / Informationssicherheitsrichtlinie

Unsere Informationssicherheitsrichtlinie ist für den Zweck und den Kontext unserer Organisation geeignet. Sie bildet den Rahmen zur Festlegung und Überprüfung der Informati-

onssicherheitsziele. Wir verpflichten uns zur Erfüllung der ermittelten Anforderungen und zur laufenden Verbesserung.
Unsere Informationssicherheitsrichtlinie ist im Formblatt 5.2.0 Informationssicherheitsrichtlinie festgelegt. Sie wurde allen Mitarbeitern/-innen vermittelt und wird angewendet. Die Informationssicherheitsrichtlinie wird den interessierten Parteien zur Verfügung gestellt.
Wir haben bei der Erstellung der Informationssicherheitsrichtlinie die ISO 27002 Abschnitt 5.1 Informationssicherheitsrichtlinien beachtet.

Nachweis(e)
FB 5 2 0 Informationssicherheitsrichtlinie

5 3 Organisatorische Rollen, Verantwortlichkeiten und Befugnisse

Die Verantwortlichkeiten und Befugnisse für relevante Rollen sind zugewiesen, intern kommuniziert und werden verstanden.
Wir haben Verantwortungen und Befugnisse zugewiesen für:

- die Sicherstellung, dass das ISMS die Normforderungen erfüllt,
- die Sicherstellung, dass die beabsichtigten Prozessergebnisse geliefert werden,
- eine Berichterstattung über die
  - Leistung,
  - Verbesserungsmöglichkeiten,
  - Änderungen und
  - Innovation des Informationssicherheitsmanagementsystems,
- die Förderung der Kundenorientierung,
- die Aufrechterhaltung der Integrität bei Änderungen des ISMS.

Nachweis(e)
FB 5 3 0 Organisationsdiagramm,
FB 5 3 0 Informationssicherheitsrichtlinien
FB 5 3 0 Lieferantensicherheitsrichtlinie
FB 5 3 0 Verantwortungen und Befugnisse

6 Planung

6 1 Maßnahmen zum Umgang mit Risiken und Chancen

6.1.1 Allgemeines

Aus unseren Themen zum Kontext (4.1) und Anforderungen (4.2) haben wir Risiken und Chancen bestimmt. Sie dienen dazu, die beabsichtigten Ergebnisse zu erzielen, unerwünschte Auswirkungen zu verhindern und zu verringern und eine fortlaufende Verbesserung zu erreichen.
Die Betrachtungen gewährleisten:

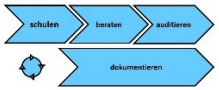
- Verringern und verhindern von ungewünschten Auswirkungen,
- Die Sicherstellung zur Erreichung der beabsichtigten Ergebnisse,
- Eine fortlaufende Verbesserung,
- die Planung zum Umgang mit Risiken, Chancen und der Integration von Prozessen sowie der
- Wirksamkeitsbeurteilung.

Prozess(e)
PA 6 1 0 Chancen und Risiken
Nachweis(e)
FB 6 1 0 Chancen und Risiken

6.1.2 Risikobewertung der Informationssicherheit

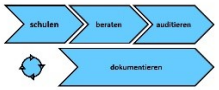
Wir haben einen Prozess zur Informationssicherheitsrisikobeurteilung festlegt und wenden diesen an.
Der Prozess gewährleistet:

- Die Festlegungen von Informationssicherheitsrisikokriterien inklusive
  - Akzeptanzkriterien und
  - Beurteilungskriterien,
- Erneute oder wiederholte Beurteilungen auf der Grundlage von Kriterien zu konsistenten, vergleichbaren und gültigen Ergebnissen führen,



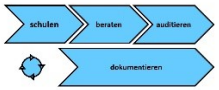
7.5.1 Dokumentierte Informationen

Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
Handbuch					
Handbuch gesamt mit Kapitel 1 bis 10	0		QM	QM	
Prozessbeschreibungen / Verfahren					
6 1 0 Ermittlung Risiken Chancen	0		QM	QM	
6 1 2 Informationssicherheitsrisikobeurteilung	0		QM	QM	
6 1 3 Informationssicherheitsbehandlung	0		QM	QM	
6 1 3 Risikomanagement IT	0		QM	QM	
6 2 0 Informationssicherheitsziele	0		QM	QM	
6 3 0 Planung Änderungen	0		QM	QM	
7 2 0 Erforderliche Kompetenzen	0		QM	QM	
7 2 0 Schulungen	0		QM	QM	
7 2 0 Weiterbildung	0		QM	QM	
7 4 0 Externe Kommunikation	0		QM	QM	
7 4 0 Interne Kommunikation	0		QM	QM	
7 5 3 Lenkung aufgezeichneter Informationen	0		QM	QM	
7 5 3 Lenkung externer Informationen	0		QM	QM	
7 5 3 Lenkung interner Informationen	0		QM	QM	
8 3 0 Änderungen am System	0		QM	QM	
8 3 0 Auswahl Anbieter	0		QM	QM	
8 3 0 Benutzerzugang	0		QM	QM	
8 3 0 Berechtigung	0		QM	QM	
8 3 0 Beschaffung	0		QM	QM	
8 3 0 Eigentum Kunden Anbieter	0		QM	QM	
8 3 0 Entsorgung Datenträger	0		QM	QM	
8 3 0 Entwicklungsänderungen	0		QM	QM	
8 3 0 Entwicklungsbewertung	0		QM	QM	
8 3 0 Entwicklungseingaben	0		QM	QM	
8 3 0 Entwicklungsergebnisse	0		QM	QM	



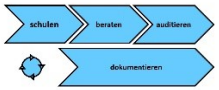
7.5.1 Dokumentierte Informationen

Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
8 3 0 Entwicklungsplanung	0		QM	QM	
8 3 0 Entwicklungsvalidierung	0		QM	QM	
8 3 0 Entwicklungsverifizierung	0		QM	QM	
8 3 0 Externe Wartungen	0		QM	QM	
8 3 0 Genehmigung neuer Einrichtungen	0		QM	QM	
8 3 0 Informationsübertragung	0		QM	QM	
8 3 0 Informationen	0		QM	QM	
8 3 0 Installation	0		QM	QM	
8 3 0 Interne Wartung	0		QM	QM	
8 3 0 Kennzeichnung und Rückverfolgbarkeit	0		QM	QM	
8 3 0 Kennzeichnung von Informationen	0		QM	QM	
8 3 0 Kommunikation Anbieter	0		QM	QM	
8 3 0 Kontrolle Lieferungen	0		QM	QM	
8 3 0 Lieferanten / Anbieteraudit	0		QM	QM	
8 3 0 Notfallvorsoge Management	0		QM	QM	
8 3 0 Registrierung / Deregistrierung	0		QM	QM	
8 3 0 Sammlung Beweismaterial	0		QM	QM	
8 3 0 Sicherheitsvorfall	0		QM	QM	
8 3 0 Validierung Software	0		QM	QM	
8 3 0 Wechselmedien	0		QM	QM	
9 1 0 Leistung Anbieter	0		QM	QM	
9 1 0 Leistungsanalyse	0		QM	QM	
9 2 0 Internes Audit	0		QM	QM	
10 1 0 Nichtkonformitäten Dienstleistung	0		QM	QM	
10 1 0 Nichtkonformitäten Produkt	0		QM	QM	
10 2 0 Planung Verbesserung	0		QM	QM	
Arbeitsanweisungen					
4 4 0 Anweisung Prozesserstellung	0		QM	QM	
8 3 0 Arbeiten in Sicherheitsbereichen	0		QM	QM	



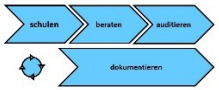
7.5.1 Dokumentierte Informationen

Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
8 3 0 Entwicklungssteuerung	0		QM	QM	
8 3 0 Kennzeichnung Informationen	0		QM	QM	
8 3 0 Kontrolle Bereitstellungen	0		QM	QM	
8 3 0 Transaktionen bei Anwendungsdiensten	0		QM	QM	
8 3 0 Verwendung von Werten außerhalb des Unternehmens	0		QM	QM	
Formblätter / Nachweisformen					
4 1 0 Kontext, Erfordernisse und Erwartungen	0		QM	QM	
4 4 0 Grundriss Räumlichkeiten	0		QM	QM	
4 4 0 Prozesse	0		QM	QM	
5 2 0 Informationssicherheitsrichtlinie	0		QM	QM	
5 2 0 Informationssicherheitsrichtlinie	0		QM	QM	
5 2 0 Lieferantensicherheitsrichtlinie	0		QM	QM	
5 3 0 Organisationsdiagramm	0		QM	QM	
5 3 0 Verantwortungen und Befugnisse	0		QM	QM	
6 1 0 Chancen und Risiken	0		QM	QM	
6 1 2 / 6 1 3 Informationssicherheitsrisiko Beurteilung Behandlung	0		QM	QM	
6 1 3 Relevante Risiken	0		QM	QM	
6 2 0 Informationssicherheitsziele	0		QM	QM	
7 1 0 Werte	0		QM	QM	
7 2 0 Benennung ISMS Beauftragte	0		QM	QM	
7 2 0 Kompetenzen	0		QM	QM	
7 2 0 Schulungsplan	0		QM	QM	
7 4 0 Liste Kommunikationswege	0		QM	QM	
7 4 0 Protokoll Besprechung	0		QM	QM	
7 5 1 Dokumentierte Informationen (diese Liste)	0		QM	QM	
8 1 0 Planung und Steuerung	0		QM	QM	
8 2 0 Behandlungsplan ISMS Risiken	0		QM	QM	
8 3 0 Abnahmetest Software	0		QM	QM	
8 3 0 Änderungssteuerung	0		QM	QM	



7.5.1 Dokumentierte Informationen

Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
8 3 0 Aktionsplan baulich organisatorisch	0		QM	QM	
8 3 0 Ausgabe Mobilgeräte	0		QM	QM	
8 3 0 Ausgabeliste Schlüssel	0		QM	QM	
8 3 0 Berechtigungen	0		QM	QM	
8 3 0 Entsorgungsprotokoll Wiederverwendung	0		QM	QM	
8 3 0 Entwicklungsänderungen	0		QM	QM	
8 3 0 Geheime Authentifizierungsinformationen	0		QM	QM	
8 3 0 Information Arbeitsumgebung	0		QM	QM	
8 3 0 Infrastruktur Netzwerkplan	0		QM	QM	
8 3 0 Kapazitätssteuerung	0		QM	QM	
8 3 0 Kennwortsystem	0		QM	QM	
8 3 0 Kennzeichnung / Rückverfolgung	0		QM	QM	
8 3 0 Konfiguration Medien	0		QM	QM	
8 3 0 Liste Anbieter	0		QM	QM	
8 3 0 Liste bindende Vorgaben	0		QM	QM	
8 3 0 Liste der Berechtigungen	0		QM	QM	
8 3 0 Maßnahmen Wartung	0		QM	QM	
8 3 0 Notfallplan	0		QM	QM	
8 3 0 Protokollierung Überwachung	0		QM	QM	
8 3 0 Prüfplan	0		QM	QM	
8 3 0 QSV Qualitätssicherungsvereinbarung	0		QM	QM	
8 3 0 Regelwerk Zugangskontrolle	0		QM	QM	
8 3 0 Schweigepflicht externe Anbieter	0		QM	QM	
8 3 0 Schweigepflicht Verantwortungsbelehrung	0		QM	QM	
8 3 0 Sicherheitseinstufungen	0		QM	QM	
8 3 0 Tätigkeiten Installation	0		QM	QM	
8 3 0 Überwachung Änderungen	0		QM	QM	
8 3 0 Unterschriftenliste	0		QM	QM	
8 3 0 Zugangssteuerung	0		QM	QM	
9 1 0 Informationssicherheitsbericht	0		QM	QM	



7.5.1 Dokumentierte Informationen

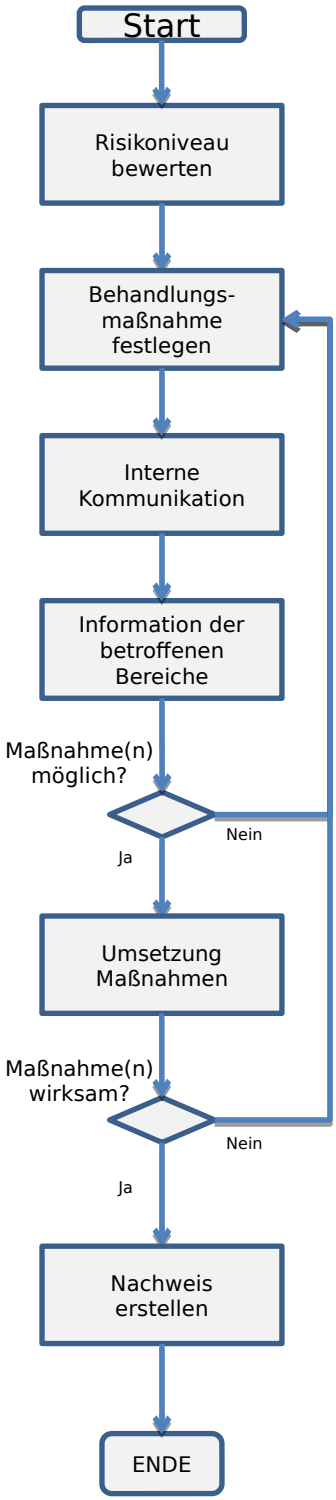
Dokumentenübersicht	Revision	vom	Ersteller/-in	Verteiler	Grund der letzten Änderung
9 1 0 Leistung Anbieter	0		QM	QM	
9 1 0 Leistungsbewertung	0		QM	QM	
9 1 0 Prüfplan	0		QM	QM	
9 2 0 Auditbericht	0		QM	QM	
9 2 0 Auditcheckliste 27001	0		QM	QM	
9 2 0 Auditplan	0		QM	QM	
9 2 0 Auditprogramm	0		QM	QM	
9 3 0 Managementbewertung	0		QM	QM	
10 1 0 Fehlerliste	0		QM	QM	
10 1 0 Maßnahmenplan	0		QM	QM	
10 1 0 4D Report	0		QM	QM	
10 2 0 Liste Verbesserungen	0		QM	QM	

Liste geprüft und freigegeben:

Datum: Funktion, Unterschrift

6.1.3 Informationssicherheitsbehandlung

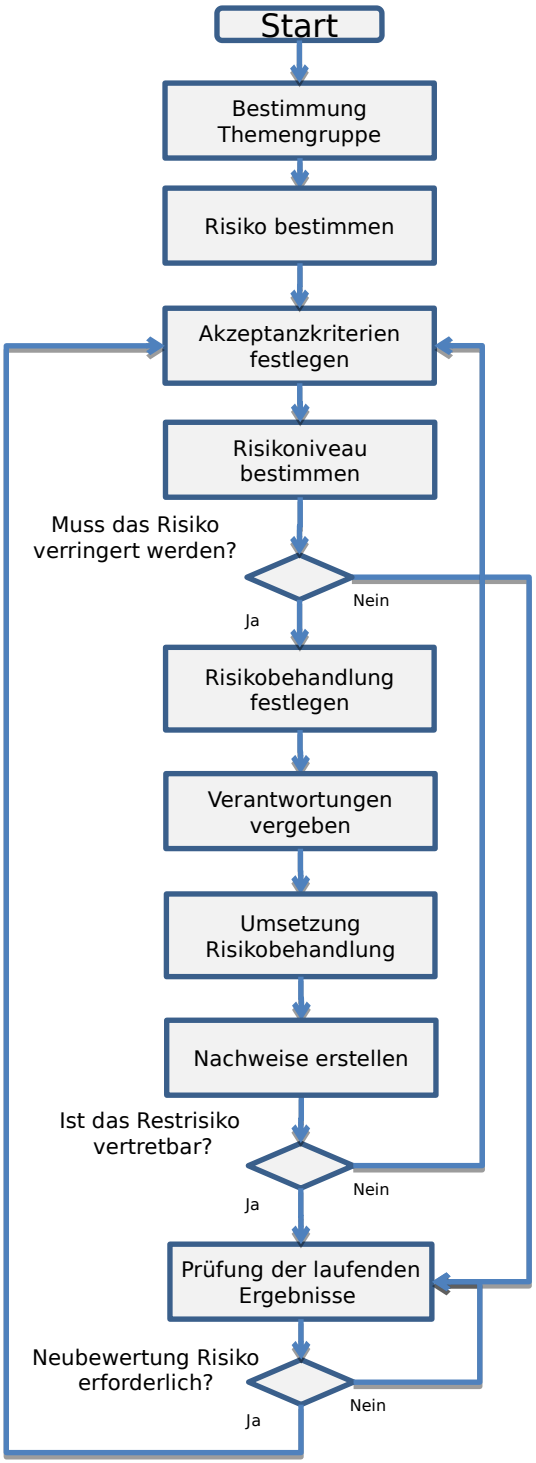
MW	VA	Ablauf / Tätigkeiten	Dokumente	Ablauf / Hilfsmittel
	ISMS-Beauftr.	Risikoniveau bewerten	FB Informationssicher-heitsrisiko Beurteilung Behandlung	Informationen aus der Excel-Datei wie Risiken bewertet wurden.
MA	ISMS-Beauftr.	Behandlungs-maßnahme festlegen	FB Informationssicher-heitsrisiko Beurteilung Behandlung	Ableiten von möglichen Risikobehandlungen
GL MA	ISMS-Beauftr.	Interne Kommunikation	FB Informationssicher-heitsrisiko Beurteilung Behandlung, Besprechungs-protokoll	Kommunikation mit den Betroffenen auf Leitungsebene. Besprechung von Optionen.
Bereiche	ISMS-Beauftr.	Information der betroffenen Bereiche	Mail, Notiz, Aushang	Information der betroffenen Bereiche auf allen Ebenen.
	ISMS-Beauftr.	Maßnahme(n) möglich?	Mail, Notiz, Aushang	Notiz der möglichen Maßnahmen und Beschluss der Vorgehensweise, Verteilung von Verantwortungen und Termine.
MA	ISMS-Beauftr.	Umsetzung Maßnahmen	Aktionsplan baulich , organisatorisch	Umsetzung der Maßnahmen gemäß Festlegung.
	ISMS-Beauftr.	Maßnahme(n) wirksam?	FB Informationssicher-heitsrisiko Beurteilung Behandlung	Die Maßnahme ist erfolgreich umgesetzt, wenn das Problem nicht oder nicht mehr auftritt oder wie beabsichtigt minimiert wurde. Es wird immer eine Wirksamkeits-prüfung durchgeführt.
MA	ISMS-Beauftr.	Nachweis erstellen	FB Informationssicher-heitsrisiko Beurteilung Behandlung	Abschließend: Informationen von betroffenen Bereichen und der GF über das Ergebnis. Die Ergebnisse gehen in die Managementbewertung ein.



MW = Mitwirkung
VA = Verantwortung

6.1.3 Risikomanagement IT

MW	VA	Ablauf / Tätigkeiten	Dokument	Ablauf / Hilfsmittel
	GF	Bestimmung Themengruppe	DIN ISO IEC 27001:2022	Entsprechend Anhang A
ISMS-Beauftr.	GF	Risiko bestimmen	FB Informationssicher-heitsrisiko Beurteilung Behandlung	Bestimmung des Risikos
ISMS-Beauftr.	GF	Akzeptanzkriterien festlegen	FB Informationssicher-heitsrisiko Beurteilung Behandlung	Kriterien für die Akzeptanz des Risikos festlegen
ISMS-Beauftr.	GF	Risikoniveau bestimmen		Bestimmung des Risikoniveaus durch Bewertung des Auftretens, der Bedeutung und der Wahrscheinlichkeit der Entdeckung.
ISMS-Beauftr.	GF	Muss das Risiko verringert werden?	FB Informationssicher-heitsrisiko Beurteilung Behandlung	Das Risiko muss verringert werden wenn die Akzeptanzkriterien nicht erreicht sind im aktuellen Status
ISMS-Beauftr.	GF	Risikobehandlung festlegen		Festlegung der Maßnahmen zur Beseitigung des Risikos.
ISMS-Beauftr.	GF	Verantwortungen vergeben	FB Informationssicher-heitsrisiko Beurteilung Behandlung	
ISMS-Beauftr.	GF	Umsetzung Risikobehandlung	Alle Dokumente	Handlungen zur Risikominimierung werden umgesetzt.
ISMS-Beauftr.	GF	Nachweise erstellen	Alle Dokumente	Führen der geeigneten Nachweise
ISMS-Beauftr.	GF	Ist das Restrisiko vertretbar?	FB Informationssicher-heitsrisiko Beurteilung Behandlung	Das Restrisiko ist vertretbar wenn die Akzeptanzkriterien eingehalten werden.
ISMS-Beauftr.	GF	Prüfung der laufenden Ergebnisse	Alle Dokumente	Laufende Auswertung von Ergebnissen und ständige Neubewertung aller erkannten Risiken
ISMS-Beauftr.	GF	Neubewertung Risiko erforderlich?		Bei abweichenden Ergebnissen oder Vorfällen



MW = Mitwirkung
VA = Verantwortung

4.1.0 / 4.2.0 Kontext, Erfordernisse und Erwartungen

Beispiele in Rot

Externe Zusammenhänge:

- Gesetzlich;
  - Wir halten die Anforderungen der Berufsgenossenschaften ein,
  - Wir beachten das Bundesdatenschutzgesetz,
  - Wir beachten das Urheberschutzgesetz,
  - Wir vertreiben unsere Produkte über das Internet (Fernabsatzgesetz)
- Technisch;
  - Wir betreiben ein Firmennetzwerk,
  - Unserem Außendienst werden Smartphones, ein PDA und ein Laptop zur Verfügung gestellt,
  - Wir beachten den Umweltschutz,
- Wettbewerblich;
  - Wir sind Anbieter von Informationsdienstleistungen (Recherchen),
  - Wir beraten Kunden bei der Aquise von Neukunden,
  - Wir erstellen Analysen zu Branchen,
- Marktüblich;
  - Unsere Kunden können unsere Dienstleistung mittels Bestellung, Projektbeschreibung oder Angebot ordern,
  - Beratungen werden nach individuellen Kriterien schriftlich angeboten,
- Kulturell / Sozial
  - Wir beachten den Gender Mainstream,
  - Wir erfassen religiöse und kulturelle Anforderungen in den Aktionsländern,
  - Wir sind Mitglied in gemeinnützigen Vereinen,
  - Wir beachten die Anforderungen der gesellschaftlichen Verantwortung,
- Wirtschaftlich
  - Wir erstellen Rechnungen, Beratungsberichte, Analysen,
  - Wir liefern Produkte digital oder in Hardware,
  - Wir führen Arbeiten bei Kunden vor Ort durch,

Interne Zusammenhänge:

- Produkte;
  - Wir bieten Produkte zur Erreichung und Einhaltung von Normforderungen an,
  - Wir beliefern digital über eine Schnittstelle im Internet,
  - Wir bearbeiten Kundendaten nach vorheriger Absprache,
- Dienstleistungen;
  - Wir beraten Kunden telefonisch und vor Ort,
  - Wir führen Schulungen durch zu regulatorischen Anforderungen und Norminhalten,
  - Wir prüfen Kundendaten auf die Einhaltung von Anforderungen,
  - Wir erstellen Dokumentationen nach Vorgaben die vertraglich festgelegt sind,
  - Wir erstellen Analysen von Branchen,
- Interessierte Parteien;
  - Der Gesetzgeber und regelsetzende Dienststellen,
  - Kunden wie Personen, Unternehmen und öffentliche Einrichtungen,
  - Organisationen und NGO's,
  - Vertriebspartner.
- Erfordernisse und Erwartungen unserer Interessierten Parteien;
  - Einhaltung von regulatorischen Anforderungen und Gesetzen,
  - Erreichbarkeit und zeitnahe Umsetzung,
  - Belieferung binnen kurzer Zeit,
  - Inhaltlich praktikable Aussagen,
  - Auskünfte auf der Grundlage von wissenschaftlichen Kenntnissen,

Form der Überwachung und Überprüfung:

Während den laufenden Analysen, der Managementbewertung und in den internen Audits. Siehe Regelwerk ISMS.

Interessierte Parteien unseres Unternehmens

4.1.0 / 4.2.0 Kontext, Erfordernisse und Erwartungen

Beispiele in Rot

Partei	Erfordernisse / Erwartungen

Kunden	<u>Produkt:</u>
	- Datensicherheit,
	- Hohe Lieferbereitschaft,
	- Laufende Verbesserung,
	- Marktgerechte Preise,
	- Umgehende Reparaturen,
	- Betrieb Hotline,
	- Abgabe von dokumentierten Informationen wie:
	  ○ Gebrauchsanleitungen
	  ○ Verpackungshinweisen
	  ○ Allgemeine Geschäftsbedingungen,
	
	<u>Dienstleistung:</u>
	- Umgehende Erfüllung / Bereitstellung,
	- Laufende Verbesserung,
	- Aussagekräftige Informationen,
	- Transparente Leistungsangebote
	- Objektive Berichterstattung,
	- Kompetenz im Zielbereich,
	- Datensicherheit,
	- Freundliche und verständliches Auftreten,
	- Konfliktfähigkeit.

Eigentümer	- Rechtliche Sicherheit, - Wirtschaftliches Handeln, - Innovation, - Transparente Berichterstattung, - Entwicklung der Organisation
Personal	- Sichere Arbeitsplätze, - Transparente Kommunikation, - Laufende Kompetenzerweiterung, - Zeitnahe Informationsabgabe, - Zusammenarbeit.
Externe Anbieter (Lieferanten)	- Fairer Umgang, - Dokumentierte Informationen im notwendigen Rahmen, - Einbindung bei Entwicklungen / Zulassungen.
Partner	- Offene Kommunikation, - Informationen über grundlegende Korrekturen und Fehler, - Einbindung in Entwicklungen.
Gesellschaft	- Beteiligung, - Offenheit, - Transparenz, - Datensicherheit, - Vermeidung von Belastungen der Umwelt.
Gesetzgeber	- Einhaltung regulatorischer Vorgaben und Gesetze, - Berichterstattung bei Nichtkonformitäten.

Qualitätsziele 20xx	Soll	Maßnahmen zur Erreichung	Verantwortlich	IST am:
ISMS-Ziele				
Ziel: Aufrechterhaltung der Informationssicherheit	100% Bereitschaft	Einführung ISMS im Unternehmen	ISMS-Beauftr.	
Ziel: Datenverlust durch Raub	Kein Verlust	Erstellen von Richtlinien um Datenverlust durch raub zu minimieren. Schützen der Verzeichnisse, Zutrittsregelungen	ISMS-Beauftr.	
Ziel: Datenverlust durch Ausfall	Kein Verlust	Zu c) laufende Wartung aller EDV-Einheiten und Überwachung der Funktion.	ISMS-Beauftr.	
Ziel: Datenverlust durch Sabotage	Kein Verlust	Zu d) Es wird ein redundantes System aufgebaut um Daten in jedem Fall beibehalten zu können. Es werden Regelungen auf allen Ebenen getroffen zum Umgang und Zugang zu Daten.	ISMS-Beauftr.	
Kundenzufriedenheit				
Ziel: Besuch der wichtigen Kunden	1x per anno	Besuchsplan erstellen.	Vertrieb	
Führung				
Ziel: Einführung DIN EN ISO 9001 (Zertifizierung)	100%	Aufbau Handbuch Zertifizierer ver-	QM	

Qualitätsziele 20xx	Soll	Maßnahmen zur Erreichung	Verantwortlich	IST am:
		traglich binden.		
Mitarbeiter/-innenzufriedenheit **Ziel: Kündigungen wegen Unzufriedenheit**	0	Formlose Personalgespräche Halb-jährlich. Liste erstellen.	GF	
Mitarbeiter/-innen **Ziel: Maschinenausfall wegen mangelnder Wartung**	0	Wartungsplan an jeder Maschine aushängen und überwachen.	Prod. Leitung	
Qualität Produkt **Ziel: Beanstandungen wegen Genauigkeit**	0	Prüfplan erstellen und überwa-chen.	QM, Ltg. Entwick-lung, Ltg. Produkti-on	
Bereitstellung von Mitteln **Ziel: Planung eines Neubaus**	100%	Planungsbüro beauftragen und überwachen.	GF	
Verbesserung der Prozesse **Ziel: Beschreibung der Prozesse im Rahmen des Qualitäts-managementsystems**	Schulungskonzept Wartung	Schulungskonzept erstellen, prü-fen und freigeben.	Ltg. Entwicklung, Vertrieb	

Qualitätsziele 20xx	Soll	Maßnahmen zur Erreichung	Verantwortlich	IST am:
Anbieter von Lieferungen und Leistungen **Ziel: Bewertung der Anbieter**	1x komplett	Ermittlung der wichtigsten Anbieter	Einkauf	
Akquisition, Vertriebsziele **Ziel: Aufbau neuer Stammkunden**	> 1	Messebesuch in Saarbrücken	Vertrieb	
Vorkehrungen zum Schutz der Gesundheit und der Sicherheit am Arbeitsplatz **Ziel: Durchführung der Erst- und Folgeunterweisungen im Rahmen des Arbeitsschutzes.**	1x per anno	Externen Arbeitsschützer beauftragen	GF	
Umsetzung von Maßnahmen aus vorliegenden Bewertungen **Ziel: nicht belegbar**				
Ausschluss von Haftungsrisiken, Risikominimierung **Ziel: Ausführliche Einarbeitung von Auszubildenden und neuen Mitarbeiter/-innen**	100%	Ausbilder beauftragen und Bericht anfordern	GF, Ausbilder	

Qualitätsziele 20xx	Soll	Maßnahmen zur Erreichung	Verantwortlich	IST am:
Regulatorische Anforderungen **Ziel: Prüfung auf Neuerungen durch die Entwicklung**	2x per anno	Überwachung Internetseiten und Informationen der benannten Stelle	Qualitätsmanager/-in	
Technische Dokumentationen **Ziel: Prüfung der Produktakte auf Aktualität**	2x per anno	Prüfung halbjährlich und bei Anlässen wie Rückmeldungen, Fehler und vielem mehr.	Ltg. Entwicklung	

Freigegeben am: xx.xx.xxxx

Unterschrift GF, Datum