Leseprobe / Inhaltsverzeichnis

QM-Vorlage nach DIN EN ISO / IEC 27001:2024 – Informationssicherheit

Inhalte

Handbuch gesamt mit Kapitel 1 bis 10

Prozessbeschreibungen / Verfahren (52)

6 1 0 Ermittlung Risiken Chancen
6 1 2 Informationssicherheitsrisikobeurteilung
6 1 3 Informationssicherheitsbehandlung
6 1 3 Risikomanagement IT
6 2 0 Informationssicherheitsziele
6 3 0 Planung Änderungen
7 2 0 Erforderliche Kompetenzen
7 2 0 Schulungen
7 2 0 Weiterbildung
7 4 0 Externe Kommunikation
7 4 0 Interne Kommunikation
7 5 3 Lenkung aufgezeichneter Informationen
7 5 3 Lenkung externer Informationen
7 5 3 Lenkung interner Informationen
8 3 0 Änderungen am System
8 3 0 Auswahl Anbieter
8 3 0 Benutzerzugang
8 3 0 Berechtigung
8 3 0 Beschaffung
8 3 0 Eigentum Kunden Anbieter
8 3 0 Entsorgung Datenträger
8 3 0 Entwicklungsänderungen
8 3 0 Entwicklungsbewertung
8 3 0 Entwicklungseingaben
8 3 0 Entwicklungsergebnisse
8 3 0 Entwicklungsplanung
8 3 0 Entwicklungsvalidierung
8 3 0 Entwicklungsverifizierung
8 3 0 Externe Wartungen
8 3 0 Genehmigung neuer Einrichtungen
8 3 0 Informationsübertragung
8 3 0 Informationen
8 3 0 Installation
8 3 0 Interne Wartung
8 3 0 Kennzeichnung und Rückverfolgbarkeit
8 3 0 Kennzeichnung von Informationen
8 3 0 Kommunikation Anbieter
8 3 0 Kontrolle Lieferungen
8 3 0 Lieferanten / Anbieteraudit
8 3 0 Notfallvorsorge Management
8 3 0 Registrierung / Deregistrierung
8 3 0 Sammlung Beweismaterial
8 3 0 Sicherheitsvorfall
8 3 0 Validierung Software
8 3 0 Wechselmedien
9 1 0 Leistung Anbieter
9 1 0 Leistungsanalyse
9 2 0 Internes Audit
10 1 0 Nichtkonformitäten Dienstleistung
10 1 0 Nichtkonformitäten Produkt
10 2 0 Planung Verbesserung

Arbeitsanweisungen (7)

Alle Dateien in MS-Office verfügbar wie MS-Word, MS-Excel und PowerPoint

4 4 0 Anweisung Prozesserstellung
8 3 0 Arbeiten in Sicherheitsbereichen
8 3 0 Entwicklungssteuerung
8 3 0 Kennzeichnung Informationen

Formblätter / Nachweisformen (64)

4 1 0 Kontext, Erfordernisse und Erwartungen
4 4 0 Grundriss Räumlichkeiten
4 4 0 Prozesse
5 2 0 Informationssicherheitsrichtlinie
5 2 0 Informationssicherheitsrichtlinie
5 2 0 Lieferantensicherheitsrichtlinie
5 3 0 Organisationsdiagramm
5 3 0 Verantwortungen und Befugnisse
6 1 0 Chancen und Risiken
6 1 2 / 6 1 3 Informationssicherheitsrisiko Beurteilung Behandlung
6 1 3 Statement of Applicability SoA
6 2 0 Informationssicherheitsziele
7 1 0 Werte
7 2 0 Benennung ISMS-Beauftragte
7 2 0 Kompetenzen
7 2 0 Schulungsplan
7 4 0 Liste Kommunikationswege
7 4 0 Protokoll Besprechung
7 5 1 Dokumentierte Informationen (diese Liste)
8 1 0 Planung und Steuerung
8 2 0 Behandlungsplan ISMS Risiken
8 3 0 Abnahmetest Software
8 3 0 Änderungssteuerung
8 3 0 Aktionsplan baulich organisatorisch
8 3 0 Ausgabe Mobilgeräte
8 3 0 Ausgabeliste Schlüssel
8 3 0 Berechtigungen
8 3 0 Entsorgungsprotokoll Wiederverwendung
8 3 0 Entwicklungsänderungen
8 3 0 Geheime Authentifizierungsinformationen
8 3 0 Information Arbeitsumgebung
8 3 0 Kontrolle Bereitstellungen
8 3 0 Transaktionen bei Anwendungsdiensten
8 3 0 Verwendung von Werten außerhalb des Unternehmens
8 3 0 Infrastruktur Netzwerkplan
8 3 0 Kapazitätssteuerung
8 3 0 Kennwortsystem
8 3 0 Kennzeichnung / Rückverfolgung
8 3 0 Konfiguration Medien
8 3 0 Liste Anbieter
8 3 0 Liste bindende Vorgaben
8 3 0 Liste der Berechtigungen
8 3 0 Maßnahmen Wartung
8 3 0 Notfallplan
8 3 0 Protokollierung Überwachung
8 3 0 Prüfplan
8 3 0 QSV-Qualitätssicherungsvereinbarung
8 3 0 Regelwerk Zugangskontrolle
8 3 0 Schweigepflicht externe Anbieter
8 3 0 Schweigepflicht Verantwortungsbelehrung
8 3 0 Sicherheitseinstufungen
8 3 0 Tätigkeiten Installation
8 3 0 Überwachung Änderungen
8 3 0 Unterschriftenliste
8 3 0 Zugangssteuerung
9 1 0 Informationssicherheitsbericht
9 1 0 Leistung Anbieter
9 1 0 Leistungsbewertung
9 1 0 Prüfplan
9 2 0 Auditbericht
9 2 0 Auditcheckliste 27001
9 2 0 Auditplan
9 2 0 Auditprogramm
9 3 0 Managementbewertung
10 1 0 Fehlerliste
10 1 0 Maßnahmenplan
10 1 0 4D Report
10 2 0 Liste Verbesserungen

Auf den kommenden Seiten finden Sie die Leseprobe.

Handbuch / Regelwerk zur Norm
DIN EN ISO/IEC 27001:2024

Inhaltsverzeichnis

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

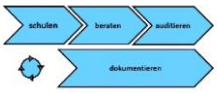
4 1 Die Organisation und ihren Kontext verstehen

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.

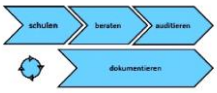
Arbeitsanweisung
AA 4 4 0 Anweisung Prozesserstellung
Nachweis(e)
FB 4 4 0 Prozesse

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 Informationssicherheitsziele. 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

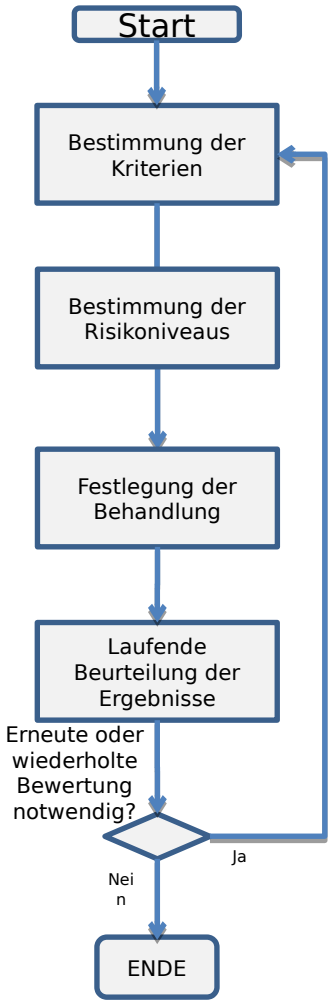
Aus unseren Themen zum Kontext (4.1) und Anforderungen (4.2) haben wir Risiken und Chancen bestimmt. Sie dienen dazu, die beabsichtigten Ergebnisse zu erzielen, unerwünschte Auswirkungen zu verhindern und zu verringern und eine fortlaufende Verbesserung zu erreichen.
Die Betrachtungen gewährleisten:

- Verringern und verhindern von unerwünschten 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

6.1.2 Informationsrisikobeurteilung

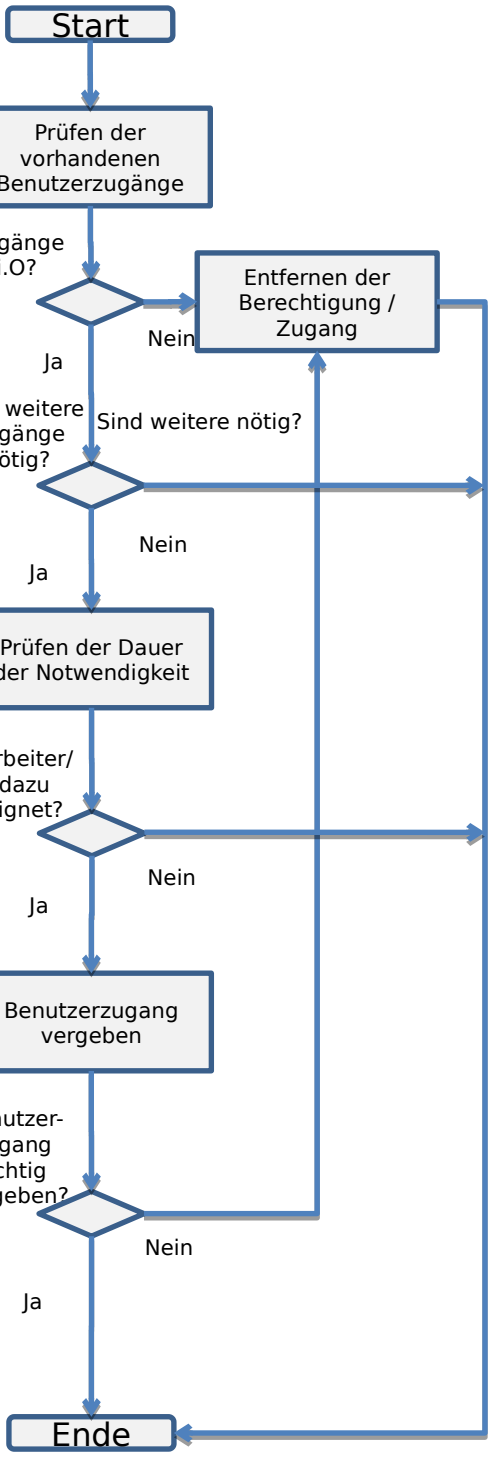
MW	VA	Ablauf / Tätigkeiten	Dokumente	Ablauf / Hilfsmittel
	ISMS-Beauftr.	Bestimmung der Kriterien	FB Informations-sicherheitsrisiko-beurteilung	Inklusive der Akzeptanzkriterien und der Beurteilungskriterien.
GF MA	ISMS-Beauftr.	Bestimmung der Risikoniveaus	FB Informations-sicherheitsrisiko-beurteilung	Vergleich der Risiken mit den Risikokriterien. Priorisierung der Risikobehandlung
MA	ISMS-Beauftr.	Festlegung der Behandlung	FB Informations-sicherheitsrisiko-beurteilung	Bewertung der Ergebnisse im Hinblick auf notwendige Änderungen.
Bereiche	ISMS-Beauftr.	Laufende Beurteilung der Ergebnisse	FB Informations-sicherheitsrisiko-beurteilung	Die betroffenen Bereiche (auch extern) werden in die Maßnahmen eingewiesen.
	ISMS-Beauftr.	Erneute oder wiederholte Bewertung notwendig? (Ja / Nein)	FB Informations-sicherheitsrisiko-beurteilung	Aufgrund einer Regelbeurteilung oder als Eintrittsfolge.



MW = Mitwirkung
VA = Verantwortung

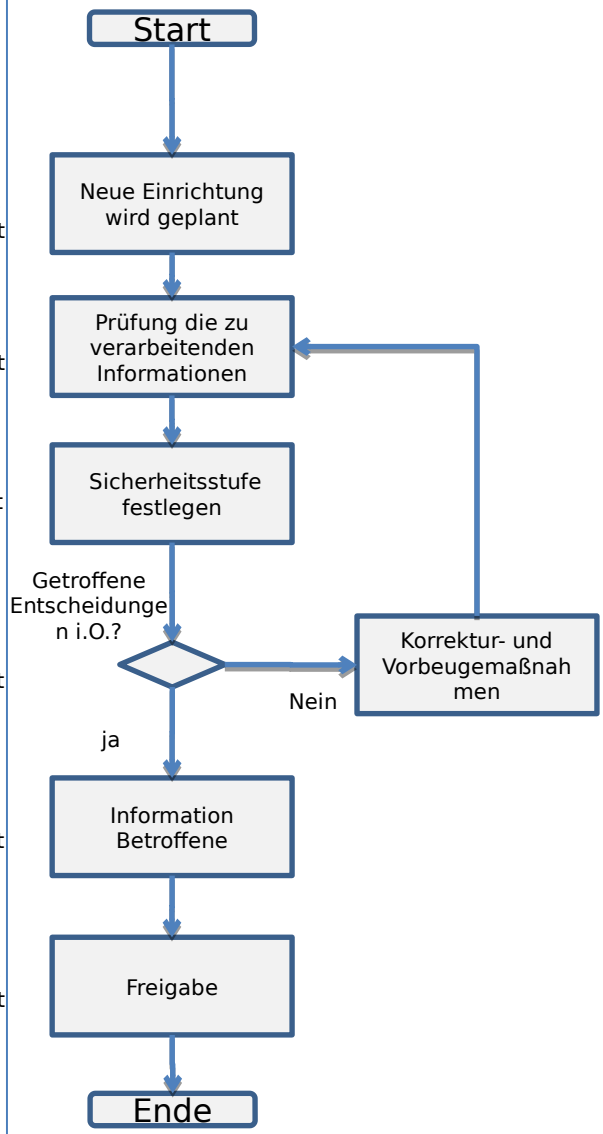
8.3.0 Benutzerzugang

MW	VA	Ablauf / Tätigkeiten	Dokumente	Ablauf Hilfsmittel
GF	ISMS-Beauftr.	Prüfen der vorhandenen Benutzerzugänge	Liste der Berechtigungen, Befugnismatrix	Die aktuellen Benutzerzugänge werden von der GF überprüft.
GF	ISMS-Beauftr.	Zugänge i.O? → Nein: Entfernen der Berechtigung / Zugang	Liste der Berechtigungen, Befugnismatrix	Sind die Benutzerzugänge nicht in Ordnung, werden diese abgeändert.
GF	ISMS-Beauftr.	Sind weitere Zugänge nötig? → Sind weitere nötig?	Liste der Berechtigungen, Befugnismatrix	Sollten neue Benutzerzugänge notwendig sein, werden diese auf die Dauer der Notwendigkeit geprüft.
GF	ISMS-Beauftr.	Prüfen der Dauer der Notwendigkeit	Liste der Berechtigungen, Befugnismatrix	Es wird laufend geprüft, ob die Benutzerzugänge noch berechtigt sind und aktuell.
GF	ISMS-Beauftr.	Mitarbeiter/-in dazu geeignet? → Nein	Liste der Berechtigungen, Befugnismatrix	Nach dem Ermitteln der Notwendigkeit der Dauer der Berechtigung wird geprüft, ob das Risiko der Vergabe der Berechtigung zu vertreten ist.
GF	ISMS-Beauftr.	Benutzerzugang vergeben	Liste der Berechtigungen, Befugnismatrix	Der Benutzerzugang wird vergeben und in die Liste der Berechtigungen eingetragen.
	ISMS-Beauftr.	Benutzerzugang richtig vergeben? → Nein	Liste der Berechtigungen, Befugnismatrix	Es werden die Aufgaben anhand der Benutzerzugänge ermittelt und überprüft, sollten die Mitarbeiter/-innen diese nicht erfüllen, wird der Zugang entfernt.



MW = Mitwirkung
VA = Verantwortung

8.3.0 Genehmigung neuer Einrichtungen

MW	VA	Ablauf / Tätigkeiten	Dokumente	Ablauf Hilfsmittel
				
GF	ISMS-Beauftr.		Regelwerk	Übergabe der Firmeninfos, Leitlinie, Aufgabengebiet, Richtlinien, Verordnungen, Gesetze, etc.
GF	ISMS-Beauftr.		Sicherheitseinstufung	Die zukünftig zu verarbeitenden Informationen werden geprüft und einem Sicherheitsgrad zugeordnet.
GF	ISMS-Beauftr.		Sicherheitseinstufung, Liste Werte	Der Sicherheitsgrad für die gesamte Einrichtung wird festgelegt. Nur Mitarbeiter mit der passenden Einstufung dürfen hier mit Informationen und Daten umgehen.
	ISMS-Beauftr.		Sicherheitseinstufung, Liste Werte	
	ISMS-Beauftr.		Sicherheitseinstufung, Liste Werte	Die Informationen über die neue Einrichtung und die Sicherheitsstufe werden an alle Mitarbeiter weitergegeben. Mitarbeiter ohne die entsprechende Sicherheitsstufe dürfen nicht eingesetzt werden.
GF	ISMS-Beauftr.		Sicherheitseinstufung	Freigabe der Einrichtung durch die Leitung.

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.

6.1.0 Chancen und Risiken

Beispiele in Rot

Zusammenhang	Anforderung	Chance	Risiko	Maßnahme
ISMS	Aufrechterhaltung der Informationssicherheit	Angriffe von Externen abwehren	Datenverlust	Einführung ISMS im Unternehmen
	Datenverlust durch Raub	/	Andere können Daten zum Missbrauch nutzten	Erstellen von Richtlinien, um Datenverlust durch raub zu minimieren. Schützen der Verzeichnisse, Zutrittsregelungen
	Datenverlust durch Ausfall	/	Daten können verloren gehen oder nicht mehr nutzbar sein (Totalausfall)	laufende Wartung aller EDV-Einheiten und Überwachung der Funktion.
	Datenverlust durch Sabotage	/	Es kann zu einem kompletten Ausfall / Verlust von Daten kommen.	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.
Gesetzlich (extern)	Wir halten die Anforderungen der Berufsgenossenschaften ein.	keine	mangelnde Einhaltung.	Jährliche Begehung durch Arbeitsschutzbeauftragte(r)
	Wir beachten das Urheberschutzgesetz und das Bundesdatenschutzgesetz.	keine	Freigabeprüfungen bei dokumentierten Informationen	Qualitätsmanager/-in prüft Dokumente und Aufzeichnungen in Stichproben.
	Wir vertreiben unsere Produkte über das Internet (Fernabsatzgesetzt).	keine		Prüfung der Internetseiten bei Änderungen.
Technisch (extern)	Wir setzen Druck- und Verpackungsmaschinen ein.	Optimierte Leistung.	Veralterung der Maschinen und Hilfsmittel.	Jährliche Prüfung der Verwendbarkeit und neue Technologien.
	Wir betreiben ein Firmennetzwerk.	Daten können zentral verwaltet werden.	Daten können verloren gehen oder entwendet.	Mitarbeiter/-innen werden zur Verschwiegenheit verpflichtet.
	Wir beachten den Umweltschutz.	Verbesserung des Ansehens in der Gemeinde	keines	Keine Maßnahme
Wettbewerblich (extern)	Wir sind Anbieter von Musterdokumentationen (Printmedien).	Alleinstellungsmerkmal auf dem Markt.	Zunehmende Wettbewerber.	Laufende Marktüberwachung, neue innovative Produkte erstellen.

6.1.0 Chancen und Risiken

Beispiele in Rot

Zusammenhang	Anforderung	Chance	Risiko	Maßnahme
	Wir beraten Kunden bei der praktischen Umsetzung von Normforderungen.	Kundenbindung über Jahre.	Große Projekte können nicht mehr bedient werden.	Vergrößerung der internen Kapazitäten.
Marktüblich (extern)	Unsere Kunden können unsere Produkte mittels Bestellung oder Angebot ordern. Bücher werden über Internetseiten, den Beuth-Verlag und den Fachhandel bestellt. Beratungen werden nach individuellen Kriterien schriftlich angeboten.	Schnelle Bestellungen sind möglich. Der Kunde kann verschiedene Bestellwege wählen. Der Tatsächliche Bedarf der Kunden wird erfasst und ggfs. angeboten.	Kein Risiko erkannt. der Kunde bleibt anonym. Anforderungen können falsch erfasst werden.	Keine Maßnahme. Ermittlung weiterer Bestellwege. Gegenprüfung von Angeboten und Anfragen.
Kulturell / Sozial (extern)	Wir beachten den Gender Mainstream. Wir erfassen religiöse und kulturelle Anforderungen. Wir sind Mitglied in gemeinnützigen Vereinen. Wir beachten die Anforderungen der gesellschaftlichen Verantwortung.	keine Chance erkannt. Kundengewinn durch Neutralität. Ansehen in der Gesellschaft verbessern. Ansehen in der Gesellschaft verbessern.	Verlust von Angeboten wegen Nichtbeachtung. Falsche Behandlung von religiösen Minderheiten. Die Vereine können zweckentfremdet arbeiten. Kein Risiko erkannt.	Prüfung der Bücher und Vorlagen. Keine Maßnahme Prüfen der Jahresberichte Keine Maßnahme
Wirtschaftlich (extern)	Wir erstellen Rechnungen auf Lieferungen oder erheben Vorkasse auf Rechnung. Wir liefern Produkte digital oder in Hardware.	Erhaltung der Liquidität. Schnelle Anlieferung. Schonung der Umwelt.	Kunden erkennen Rechnung nicht. Vorsätzlicher Betrug durch Kunden.	Bessere Kennzeichnung der Rechnungen, Digitaler Versand bei Abwicklung. Schlüssigkeitsprüfungen bei Bestellungen.
Produkte (intern)	Wir bieten Produkte zur Erreichung und Einhaltung von Normforderungen an. Die Produkte werden nach Aufkommen der Bestellungen produziert und in geringem Umfang bevorratet.	Dauerhafte Kundenbindung und Projektanfragen. Kosteneinsparung.	Inhaltliche Richtigkeit nicht vorhanden. Zu wenig Produkte am Lager.	Gegenprüfung von neuen Produkten. Berechnung der Regelbestellungen und Ableitung der individuellen Bestände.

6.1.0 Chancen und Risiken

Beispiele in Rot

Zusammenhang	Anforderung	Chance	Risiko	Maßnahme
	Wir beliefern digital über eine Schnittstelle im Internet.	Schnelle Zusendung.	Datenverlust oder –klau durch Anbieter.	Prüfung der Anbieter für Clouds.
Dienstleistungen (intern)	Wir beraten Kunden telefonisch und vor Ort.	Schnelle Hilfe für die Kunden.	Leistungen werden nicht entlohnt.	Grenzen der kostenlosen Beratung einführen.
	Wir führen Schulungen durch zu regulatorischen Anforderungen und Norminhalten.	Kundengewinnung bei guter Durchführung.	Kundenverlust bei schlechter Durchführung.	Prüfung der Schulungsunterlagen bei Erstellung und jährlich auf Aktualität.
	Wir auditieren Kunden und Partner entsprechend den Inhalten der DIN EN ISO 19011.	Kunde erhält objektive Ergebnisse.	Ergebnisse sind für Kunden nicht verständlich.	Unterlagen werden in transparenter und einfacher Sprache erstellt.
	Wir prüfen Dokumentationen auf die Einhaltung von Anforderungen.	Schnelle Umsetzung sowie Zeit- und Kostenersparnis für Kunden.	Falsche Kundenforderungen erfassen.	Schriftliche Bestätigung der Ergebnisse nach der Erfassung (Mail).
	Wir erstellen Dokumentationen nach Vorgaben die vertraglich festgelegt sind.			
Interessierte Parteien (intern)	Einhaltung von regulatorischen Anforderungen und Gesetzen.	Einhaltung der Gesetze und Vorgaben.	Keine ausreichende Erfassung.	Laufende Auswertung von Vorgaben im Internet und Newsletter.
	Erreichbarkeit und zeitnahe Umsetzung.	Dynamische Realisierung der Produktion und Dienstleistung.	Überlastung der internen Ressourcen.	Listen mit offenen Projekten und Angeboten führen.
	Belieferung binnen kurzer Zeit.	Hohe Begeisterung.	Kein Risiko erkannt.	Laufende Prüfung der 48 Stundenregel.
	Inhaltlich praktikable Produkte.	Hohe Begeisterung.	Kein Risiko erkannt.	Machbarkeitsprüfung der Vorlagen in Beratungsprojekten.

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