Verzeichnis der Risikobehandlung durchgeführt von [Datum] bis [Datum]

Werte / Bedrohungen / Schwachstellen						[illegible]		
Nummer	**Name des Werts**	[illegible]	**Bedrohung**	[illegible]	[illegible]	[illegible]	**Wahrscheinlichkeit**	**Risiko**
	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		
	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		
	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		
	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		
	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		

Risikobehandlung		Werte nach Behandlung		
Auswahl der Optionen	Art der Umsetzung	Auswirkung	Wahrscheinlichkeit	**Risiko**
Übertragung der Risiken auf Dritte	A.15.1.1 Abhandlung von Sicherheitsaspekt			
Auswahl von Maßnahmen	A.12.1.1 Überwachung und Prüfung von			
Übertragung der Risiken auf Dritte	A.15.1.1 Abhandlung von Sicherheitsaspekt			
Auswahl von Maßnahmen	A.11.1.4 Schutz gegen externe und umwel			
Auswahl von Maßnahmen	A.11.2.1 Standortwahl und Schutz von Ge			

Risikobehandlungs-Optionen

1. Auswahl von Maßnahmen
2. Übertragung der Risiken auf Dritte
3. Risikovermeidung
4. Risikoakzeptanz

Maßnahmen entsprechend Anhang A der ISO/IEC 27001 Norm

A.5.1.1 Informationssicherheitspolitik
A.5.1.2 Überprüfung der Informationssicherheitspolitik
A.6.1.1 Rollen und Verantwortlichkeiten im Rahmen der Informationssicherheit
A.6.1.2 Pflichtentrennung
A.6.1.3 Kontakt mit Behörden
A.6.1.4 Kontakt mit besonderen Interessengruppen
A.6.1.5 Informationssicherheit im Projektmanagement
A.6.2.1 Richtlinie zu Mobilgeräten
A.6.2.2 Telearbeit
A.7.1.1 Überprüfung (Screening)
A.7.1.2 Arbeitsvertragsabschnitte
A.7.2.1 Verantwortlichkeiten der Leitung
A.7.2.2 Sensibilisierung, Ausbildung und Schulung für Informationssicherheit
A.7.2.3 Disziplinarverfahren
A.7.3.1 Beendigung oder Änderung der Verantwortlichkeiten bzgl. der Anstellung
A.8.1.1 Inventar der Werte
A.8.1.2 Eigentümerschaft der Werte
A.8.1.3 Zulässige Nutzung der Werte
A.8.1.4 Rückgabe von Werten
A.8.2.1 Klassifizierung von Informationen
A.8.2.2 Kennzeichnung von Informationen
A.8.2.3 Handhabung von Werten
A.8.3.1 Verwaltung von Wechsel-Datenträgern
A.8.3.2 Entsorgung von Datenträgern
A.8.3.3 Physische Übertragung von Datenträgern
A.9.1.1 Zugangssteuerungsrichtlinie
A.9.1.2 Zugang zu Netzwerken und Netzwerkdiensten
A.9.2.1 Benutzer-Registrierung und -Löschung
A.9.2.2 Bereitstellung von Benutzerzugängen
A.9.2.3 Verwaltung privilegierter Zugangsrechte
A.9.2.4 Verwaltung der geheimen Authentisierungsinformationen der Benutzer
A.9.2.5 Überprüfung der Benutzerzugangsrechte
A.9.2.6 Entziehung oder Anpassung der Zugangsrechte
A.9.2.7 Entfernung von Eigentum
A.9.3.1 Benutzung der geheimen Authentifizierungs-Informationen
A.9.4.1 Beschränkung des Informationszugangs
A.9.4.2 Sichere Anmeldeverfahren
A.9.4.3 System für Kennwort-Verwaltung
A.9.4.4 Nutzung privilegierter Dienstprogramme
A.9.4.5 Zugang zum Programm-Quellcode
A.10.1.1 Richtlinie zur Benutzung von Kryptografiemaßnahmen
A.10.1.2 Schlüsselverwaltung
A.11.1.1 Physischer Sicherheitsumkreis
A.11.1.2 Physische Zutrittskontrollen
A.11.1.3 Absicherung von Büros, Räumlichkeiten und Einrichtungen
A.11.1.4 Schutz gegen externe und umweltbedingte Bedrohungen
A.11.1.5 Arbeiten in sicheren Bereichen
A.11.1.6 Anlieferungs- und Ladebereiche

A.11.2.1 Standortwahl und Schutz von Gerätschaften

A.11.2.2 Unterstützende Betriebsmittel

A.11.2.3 Sicherheit der Verkabelung

A.11.2.4 Wartung von Gerätschaften

A.11.2.5 Entfernung von Werten

A.11.2.6 Sicherheit der Gerätschaften und Werte außerhalb der Liegenschaft

A.11.2.7 Sichere Entsorgung oder Wiederverwertung von Gerätschaften

A.11.2.8 Unbeaufsichtigte Gerätschaften von Anwendern

A.11.2.9 Richtlinie zum aufgeräumten Arbeitsplatz und leeren Bildschirm

A.12.1.1 Dokumentierte Betriebsmaßnahmen

A.12.1.2 Änderungsverwaltung

A.12.1.3 Kapazitätsverwaltung

A.12.1.4 Trennung der Umgebungen für Entwicklung, Test und Betrieb

A.12.2.1 Maßnahmen gegen Schadsoftware

A.12.3.1 Backup von Informationen

A.12.4.1 Protokollierung von Ereignissen

A.12.4.2 Schutz protokollierter Informationen

A.12.4.3 Protokolle des Administrators und Benutzers

A.12.4.4 Uhren-Synchronisierung (Uhrsynchergleichschaltung)

A.12.5.1 Installierung von Software auf betrieblichen Systemen

A.12.6.1 Verwaltung technischer Schwachstellen

A.12.6.2 Beschränkungen für Software-Installation

A.12.7.1 Maßnahmen beim Audit von Informationssystemen

A.13.1.1 Netzwerkmaßnahmen

A.13.1.2 Sicherheit der Netzwerkdienste

A.13.1.3 Trennung von Netzwerken

A.13.2.1 Richtlinien und Verfahren zur Informationsübertragung

A.13.2.2 Vereinbarungen über Informationsübertragung

A.13.2.3 Elektronische Nachrichtenübermittlung

A.13.2.4 Vereinbarungen über Vertraulichkeit oder Geheimhaltung

A.14.1.1 Analyse und Spezifizierung der Informationssicherheitsanforderungen

A.14.1.2 Anwendungsdienste in öffentlichen Netzwerken absichern

A.14.1.3 Schutz von Transaktionen über Anwendungsdienste

A.14.2.1 Richtlinie zur Entwicklungssicherheit

A.14.2.2 Kontrollmaßnahmen bei Systemänderung

A.14.2.3 Technische Überprüfung von Anwendungen nach einem Wechsel der Betriebsplattform

A.14.2.4 Beschränkungen bei Änderungen von Software-Paketen

A.14.2.5 Grundsätze der Entwicklung sicherer Systeme

A.14.2.6 Sichere Entwicklungsumgebung

A.14.2.7 Ausgelagerte Entwicklung

A.14.2.8 Testen der Systemsicherheit

A.14.2.9 System-Abnahmetest

A.14.3.1 Schutz von Testdaten

A.15.1.1 Richtlinie zur Informationssicherheit in Lieferantenbeziehungen

A.15.1.2 Abhandlung von Sicherheitsaspekten in Lieferantenvereinbarungen

A.15.1.3 Lieferkette in der Informations- und Kommunikationstechnik

A.15.2.1 Überwachung und Prüfung von Lieferantenleistungen

A.15.2.2 Verwaltung von Änderungen in Lieferantenleistungen

A.16.1.1 Verantwortlichkeiten und Verfahren

A.16.1.2 Berichterstattung über Informationssicherheitsereignisse

A.16.1.3 Berichterstattung über Informationssicherheitsschwachstellen

A.16.1.4 Bewertung von und Entscheidung zu Informationssicherheits-ereignissen

A.16.1.5 Reaktion auf Informationssicherheitsvorfälle

A.16.1.6 Lernen aus Informationssicherheitsvorfällen

A.16.1.7 Beweissammlung

A.17.1.1 Planung der Informationssicherheits-Kontinuität

A.17.1.2 Umsetzung der Informationssicherheits-Kontinuität

A.17.1.3 Verifizierung, Prüfung und Bewertung der Informationssicherheits-Kontinuität

A.17.2.1 Verfügbarkeit von Datenverarbeitungseinrichtungen

A.18.1.1 Identifizierung der anzuwendenden gesetzlichen Vorgaben und vertraglichen Anforderungen

A.18.1.2 Geistige Eigentumsrechte

A.18.1.3 Schutz von Aufzeichnungen

A.18.1.4 Privatsphäre und Schutz persönlicher Informationen

A.18.1.5 Vorschriften zu kryptografischen Maßnahmen

A.18.2.1 Unabhängige Prüfung der Informationssicherheit

A.18.2.2 Einhaltung von Sicherheitsrichtlinien und -standards

A.18.2.3 Prüfung der technischen Einhaltung