Anlage 3

Risikomanagementmaßnahmen-Bereiche	
1.	Leitungsorgane
a.	Rollen und Verantwortlichkeiten der Leitungsorgane
2.	Sicherheitsrichtlinien
a.	Sicherheitsrichtlinien
b.	Funktionen, Aufgaben und Verantwortlichkeiten
3.	Risikomanagement
a.	Risikomanagementrichtlinie und -prozess
b.	Beurteilung der Effektivität von Risikomanagementmaßnahmen
c.	Überwachung der Einhaltung von Vorgaben
d.	Unabhängige Überprüfungen
4.	Verwaltung von Vermögenswerten
a.	Inventarisierung von Vermögenswerten
b.	Klassifikation von Vermögenswerten
c.	Handhabung von Vermögenswerten
d.	Umgang mit Wechseldatenträger
e.	Rücknahme oder Löschung von Vermögenswerten
5.	Personalwesen
a.	Sicherheit im Personalwesen
b.	Hintergrundüberprüfung
c.	Verfahren bei Beendigung oder Wechsel des Beschäftigungsverhältnisses
d.	Disziplinarmaßnahmen
6.	Grundlegende Cyberhygienemaßnahmen und Cybersicherheitsschulungen
a.	Bewusstseinsschaffung und Cyberhygiene
b.	Cybersicherheitsschulungen
7.	Sicherheit von Lieferketten
a.	Richtlinie zur Sicherheit von Lieferketten
b.	Lieferantenverzeichnis
8.	Zugangssteuerung
a.	Zugangssteuerungsrichtlinie
b.	Verwaltung von Zugriffsberechtigungen
c.	Privilegierte und administrative Zugänge
d.	Systeme und Anwendungen zur Systemadministration
e.	Identifikation
f.	Authentifikation
g.	Multi-Faktor-Authentifikation
9.	Sicherheit bei Beschaffung, Entwicklung, Betrieb und Wartung
a.	Konfigurationsmanagement
b.	Änderungsmanagement und Wartung
c.	Umgang mit Schwachstellen und deren Offenlegung
d.	Sicherheitstests
e.	Patchmanagement
f.	Sicherheit bei der Beschaffung von Dienstleistungen, Systemen und Produkten
g.	Sichere Softwareentwicklung
h.	Netzwerksegmentierung
i.	Netzwerksicherheit
j.	Schutz vor bösartiger und unautorisierter Software
10.	Kryptographie
a.	Kryptographierichtlinie
11.	Umgang mit Cybersicherheitsvorfällen
a.	Richtlinie zum Umgang mit Cybersicherheitsvorfällen
b.	Überwachung und Protokollierung
c.	Meldung von Ereignissen
d.	Erhebung und Klassifikation von Ereignissen
e.	Reaktion auf Cybersicherheitsvorfällen
f.	Erkenntnisse nach Cybersicherheitsvorfällen

12.	Betriebskontinuitäts- und Krisenmanagement
a.	Betriebskontinuitätsmanagement und Notfallwiederherstellungspläne
b.	Backup-, Redundanz- und Wiederherstellungsmanagement
c.	Krisenmanagement
13.	Umgebungsbezogene und physische Sicherheit
a.	Sicherheitsperimeter und physische Zutrittskontrollen
b.	Schutz vor umgebungsbezogenen Gefährdungen
c.	Versorgungseinrichtungen