RISIKOANALYSE-TEMPLATE

Version 1.0

EVANGELISCHE KIRCHE IN DEUTSCHLAND

MANAGEMENT SUMMARY

Ausgangslage

[Kurzfassung der Beschreibung der Ausgangslage sowie des organisatorischen/technischen Umfelds]

Zusammenfassung der Ergebnisse

A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen

- Zusammenfassung der Maßnahmen aus Kapitel 6

B. Risikovermeidung

- Zusammenfassung der Maßnahmen aus Kapitel 6

C. Risikoübernahme

- Zusammenfassung der Maßnahmen aus Kapitel 6

D. Risikotransfer

- Zusammenfassung der Maßnahmen aus Kapitel 6

1 ALLGEMEINES

Dieses Dokument beschreibt eine Möglichkeit zur Durchführung einer Risikoanalyse, wie im IT-Sicherheitskonzept gefordert wird (siehe Kapitel 8: Muster-IT-Sicherheitskonzept für mittlere und große Einrichtungen). In den folgenden Kapiteln wird eine Risikoanalyse nach dem BSI-Standard 100-3 durchgeführt.

2 EINLEITUNG

Ziel einer Risikoanalyse ist es, die vorhandenen Risiken durch eine Risikobehandlung auf ein verträgliches/akzeptables Maß (Restrisiko) zu reduzieren.

Ein Risiko ist ein mögliches Ereignis mit unerwünschter Wirkung und wird als Produkt von Eintrittswahrscheinlichkeit und Schadenshöhe betrachtet.

Im ersten Schritt werden **die relevanten Risiken** für das Zielobjekt herausgearbeitet. Dabei werden die in den IT-Grundschutz-Katalogen beschriebenen Gefährdungen, so genannte elementare G0 Gefährdungen (vgl. IT-Grundschutz – G0-Katalog), als Hilfsmittel verwendet. Bei den elementaren Gefährdungen wurde der Fokus darauf gelegt, **tatsächliche Gefahren** zu benennen. Gefährdungen, die überwiegend die fehlende oder unzureichende Umsetzung von Sicherheitsmaßnahmen thematisieren und somit auf indirekte Gefahren verweisen, werden somit bewusst vermieden.

Nicht alle potentiell möglichen Gefährdungen, welche im Gefährdungskatalog benannt sind, müssen untersucht werden, insbesondere wenn Gefährdungen durch eine besondere Technologie, ein spezielles Produkt oder einen besonderen Anwendungsfall bedingt sind oder in üblichen Einsatzszenarien nur unter sehr speziellen Voraussetzungen zu einem Schaden führen oder sehr gute Fachkenntnisse, Gelegenheiten und Mittel eines Angreifers voraussetzen.

Für die IT-Sicherheit **relevante Gefährdungen** sind solche, die zu einem **nennenswerten Schaden** führen können und die im vorliegenden Anwendungsfall und Einsatzumfeld realistisch sind.

Deshalb werden in einem zweiten Schritt alle Gefährdungen gestrichen, welche außerhalb des Zielobjektes existieren und nicht durch Sicherheitsmaßnahmen des Zielobjektes beeinflusst werden können. Beispiele dafür sind Gefährdungen wie Feuer und Wasser oder Einfluss durch Großereignisse im Umfeld.

Aus den verbleibenden Gefährdungen können sich Risiken ergeben. Deshalb werden abschließend die verbleibenden Gefährdungen mit den bisherigen bereits umgesetzten Maßnahmen auf eine ausreichende Risikominimierung hin untersucht und bewertet.

Die Prüfung erfolgt anhand des IT-Sicherheitskonzepts und folgender Prüfkriterien:

- **Mechanismenstärke**
  Wirken die in den Standard-Sicherheitsmaßnahmen empfohlenen Schutzmechanismen der jeweiligen Gefährdung ausreichend stark entgegen?
- **Zuverlässigkeit**
  Können die vorgesehenen Sicherheitsmechanismen nicht zu leicht umgangen werden?

- **Vollständigkeit**
  Bieten die Standard-Sicherheitsmaßnahmen Schutz gegen alle Aspekte der jeweiligen Gefährdung?

Immanent werden bei diesem Vorgehen die einzelnen Risiken mit ihrer Schadenshöhe und Eintrittswahrscheinlichkeit in einer Risikomatrix (vgl. Tabelle 19) gruppiert.

Tabelle 1 Risikomatrix

Eintrittswahrscheinlichkeit	**Hoch**	Mittleres Risiko	Hohes Risiko	Hohes Risiko
	Mittel	Niedriges Risiko	Mittleres Risiko	Hohes Risiko
	Niedrig	Niedriges Risiko	Niedriges Risiko	Mittleres Risiko
		Niedrig	**Mittel**	**Hoch**
		Schadenshöhe		

In der hier beschriebenen Methodik nach BSI Standard 100-3 werden Eintrittswahrscheinlichkeiten nicht explizit, sondern lediglich implizit im Rahmen der Ermittlung und Bewertung von Gefährdungen betrachtet.

Risiken, die in der Risikomatrix im „roten Bereich“ liegen, können Auswirkungen haben, die nicht einfach tolerierbar sind. Entsprechend müssen Maßnahmen für die Risikobehandlung definiert werden, die

- die Wahrscheinlichkeit des Eintretens oder
- die Schadenshöhe bei einem Eintreten

verringern.

Liegt ein Risiko vor, können verschiedene Strategien bei der Auswahl der Maßnahmen zugrunde gelegt werden:

- **Risiko-Reduktion** durch weitere Sicherheitsmaßnahmen: Die verbleibende Gefährdung wird beseitigt, indem eine oder mehrere ergänzende Sicherheitsmaßnahmen erarbeitet und umgesetzt werden, die der Gefährdung hinreichend entgegenwirken und damit auch das daraus resultierende Risiko minimieren.

- **Risiko-Vermeidung** durch Umstrukturierung: Die verbleibende Gefährdung und damit auch das daraus resultierende Risiko wird durch Umstrukturierung beseitigt.
- **Risiko-Übernahme**: Die verbleibende Gefährdung und damit auch das daraus resultierende Risiko wird akzeptiert.
- **Risiko-Transfer**: Die verbleibende Gefährdung und damit auch das daraus resultierende Risiko wird durch eine Versicherung oder durch andere Vertragsgestaltung (Outsourcing) übertragen.

3 GEFÄHRDUNGSKATALOG G.0 – FESTLEGUNG DER RELEVANZ NACH DEM SICHERHEITSZIEL

Zielobjekt:

Zielobjekt XY

Sicherheitsziel:

Vertraulichkeit (C): Normal, Hoch, Sehr Hoch

Integrität (I): Normal, Hoch, Sehr Hoch

Verfügbarkeit (A): Normal, Hoch, Sehr Hoch

Vorgehensweise:

Reduktion der G.0 Gefährdungen hinsichtlich der Sicherheitsziele

- Fall 1: Sicherheitsziele unterschiedlich ausgeprägt
  - Reduzierung hinsichtlich der Sicherheitsziele
  - G.0 Gefährdungen mit normalen Schutzbedarf werden gemäß der Entscheidungen in der ergänzenden Sicherheitsanalyse nicht betrachtet
- Fall 2: Sicherheitsziele gleich ausgeprägt
  - Keine Reduktion, alle G.0 Gefährdungen sind relevant
  - Weiter mit Kapitel 4.
- Fall 3: Keine relevanten Bausteine vorhanden
  - Keine Reduktion, alle G.0 Gefährdungen sind relevant
  - Weiter mit Kapitel 4.

Tabelle 2: G.0 Gefährdungen

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel
G 0.1	Feuer	I, A
G 0.2	Ungünstige klimatische Bedingungen	I, A
G 0.3	Wasser	I, A
G 0.4	Verschmutzung, Staub, Korrosion	I, A
G 0.5	Naturkatastrophen	A
G 0.6	Katastrophen im Umfeld	A
G 0.7	Großereignisse im Umfeld	C, I, A
G 0.8	Ausfall oder Störung der Stromversorgung	I, A
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	I, A
G 0.10	Ausfall oder Störung von Versorgungsnetzen	A
G 0.11	Ausfall oder Störung von Dienstleistern	C, I, A
G 0.12	Elektromagnetische Störstrahlung	I, A
G 0.13	Abfangen kompromittierender Strahlung	C
G 0.14	Ausspähen von Informationen / Spionage	C
G 0.15	Abhören	C
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	C, A
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten	C, A
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A
G 0.19	Offenlegung schützenswerter Informationen	C
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	C, I, A
G 0.21	Manipulation von Hard- oder Software	C, I, A
G 0.22	Manipulation von Informationen	I
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I
G 0.24	Zerstörung von Geräten oder Datenträgern	A
G 0.25	Ausfall von Geräten oder Systemen	A

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A
G 0.27	Ressourcenmangel	A
G 0.28	Software-Schwachstellen oder -Fehler	C, I, A
G 0.29	Verstoß gegen Gesetze oder Regelungen	C, I, A
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C, I, A
G 0.32	Missbrauch von Berechtigungen	C, I, A
G 0.33	Personalausfall	A
G 0.34	Anschlag	C, I, A
G 0.35	Nötigung, Erpressung oder Korruption	C, I, A
G 0.36	Identitätsdiebstahl	C, I, A
G 0.37	Abstreiten von Handlungen	C, I
G 0.38	Missbrauch personenbezogener Daten	C
G 0.39	Schadprogramme	C, I, A
G 0.40	Verhinderung von Diensten (Denial of Service)	A
G 0.41	Sabotage	A
G 0.42	Social Engineering	C, I
G 0.43	Einspielen von Nachrichten	C, I
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I, A
G 0.45	Datenverlust	A
G 0.46	Integritätsverlust schützenswerter Informationen	I

Tabelle 3: Reduzierung G.0 Gefährdungen hinsichtlich des Schutzziels

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel	Relevanz
G 0.1	Feuer	I, A	Ja/Nein
G 0.2	Ungünstige klimatische Bedingungen	I, A	Ja/Nein

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel	Relevanz
G 0.3	Wasser	I, A	Ja/Nein
G 0.4	Verschmutzung, Staub, Korrosion	I, A	Ja/Nein
G 0.5	Naturkatastrophen	A	Ja/Nein
G 0.6	Katastrophen im Umfeld	A	Ja/Nein
G 0.7	Großereignisse im Umfeld	C, I, A	Ja/Nein
G 0.8	Ausfall oder Störung der Stromversorgung	I, A	Ja/Nein
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	I, A	Ja/Nein
G 0.10	Ausfall oder Störung von Versorgungsnetzen	A	Ja/Nein
G 0.11	Ausfall oder Störung von Dienstleistern	C, I, A	Ja/Nein
G 0.12	Elektromagnetische Störstrahlung	I, A	Ja/Nein
G 0.13	Abfangen kompromittierender Strahlung	C	Ja/Nein
G 0.14	Ausspähen von Informationen / Spionage	C	Ja/Nein
G 0.15	Abhören	C	Ja/Nein
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	C, A	Ja/Nein
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten	C, A	Ja/Nein
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A	Ja/Nein
G 0.19	Offenlegung schützenswerter Informationen	C	Ja/Nein
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	C, I, A	Ja/Nein
G 0.21	Manipulation von Hard- oder Software	C, I, A	Ja/Nein
G 0.22	Manipulation von Informationen	I	Ja/Nein
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I	Ja/Nein
G 0.24	Zerstörung von Geräten oder Datenträgern	A	Ja/Nein
G 0.25	Ausfall von Geräten oder Systemen	A	Ja/Nein
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A	Ja/Nein
G 0.27	Ressourcenmangel	A	Ja/Nein
G 0.28	Software-Schwachstellen oder -Fehler	C, I, A	Ja/Nein

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel	Relevanz
G 0.29	Verstoß gegen Gesetze oder Regelungen	C, I, A	Ja/Nein
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C, I, A	Ja/Nein
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C, I, A	Ja/Nein
G 0.32	Missbrauch von Berechtigungen	C, I, A	Ja/Nein
G 0.33	Personalausfall	A	Ja/Nein
G 0.34	Anschlag	C, I, A	Ja/Nein
G 0.35	Nötigung, Erpressung oder Korruption	C, I, A	Ja/Nein
G 0.36	Identitätsdiebstahl	C, I, A	Ja/Nein
G 0.37	Abstreiten von Handlungen	C, I	Ja/Nein
G 0.38	Missbrauch personenbezogener Daten	C	Ja/Nein
G 0.39	Schadprogramme	C, I, A	Ja/Nein
G 0.40	Verhinderung von Diensten (Denial of Service)	A	Ja/Nein
G 0.41	Sabotage	A	Ja/Nein
G 0.42	Social Engineering	C, I	Ja/Nein
G 0.43	Einspielen von Nachrichten	C, I	Ja/Nein
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I, A	Ja/Nein
G 0.45	Datenverlust	A	Ja/Nein
G 0.46	Integritätsverlust schützenswerter Informationen	I	Ja/Nein

4 GEFÄHRDUNGSKATALOG G.0 – REDUKTION HINSICHTLICH DER SCHADENSAUSWIRKUNG AUF DAS ZIELOBJEKT

Vorgehensweise:

Reduktion der G.0 Gefährdungen hinsichtlich der Schadenswirkung auf das Zielobjekt (Switche)

Tabelle 4: Reduzierte G.0 Gefährdung hinsichtlich der Schadensauswirkung auf das Zielobjekt

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel	Schaden möglich?
G 0.1	Feuer	I, A	Ja/Nein
G 0.2	Ungünstige klimatische Bedingungen	I, A	Ja/Nein
G 0.3	Wasser	I, A	Ja/Nein
G 0.4	Verschmutzung, Staub, Korrosion	I, A	Ja/Nein
G 0.5	Naturkatastrophen	A	Ja/Nein
G 0.6	Katastrophen im Umfeld	A	Ja/Nein
G 0.7	Großereignisse im Umfeld	C, I, A	Ja/Nein
G 0.8	Ausfall oder Störung der Stromversorgung	I, A	Ja/Nein
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	I, A	Ja/Nein
G 0.10	Ausfall oder Störung von Versorgungsnetzen	A	Ja/Nein
G 0.11	Ausfall oder Störung von Dienstleistern	C, I, A	Ja/Nein
G 0.12	Elektromagnetische Störstrahlung	I, A	Ja/Nein
G 0.13	Abfangen kompromittierender Strahlung	C	Ja/Nein
G 0.14	Ausspähen von Informationen / Spionage	C	Ja/Nein
G 0.15	Abhören	C	Ja/Nein
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	C, A	Ja/Nein
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten	C, A	Ja/Nein
G 0.18	Fehlplanung oder fehlende Anpassung	C, I, A	Ja/Nein
G 0.19	Offenlegung schützenswerter Informationen	C	Ja/Nein

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel	Schaden möglich?
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	C, I, A	Ja/Nein
G 0.21	Manipulation von Hard- oder Software	C, I, A	Ja/Nein
G 0.22	Manipulation von Informationen	I	Ja/Nein
G 0.23	Unbefugtes Eindringen in IT-Systeme	C, I	Ja/Nein
G 0.24	Zerstörung von Geräten oder Datenträgern	A	Ja/Nein
G 0.25	Ausfall von Geräten oder Systemen	A	Ja/Nein
G 0.26	Fehlfunktion von Geräten oder Systemen	C, I, A	Ja/Nein
G 0.27	Ressourcenmangel	A	Ja/Nein
G 0.28	Software-Schwachstellen oder -Fehler	C, I, A	Ja/Nein
G 0.29	Verstoß gegen Gesetze oder Regelungen	C, I, A	Ja/Nein
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	C, I, A	Ja/Nein
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	C, I, A	Ja/Nein
G 0.32	Missbrauch von Berechtigungen	C, I, A	Ja/Nein
G 0.33	Personalausfall	A	Ja/Nein
G 0.34	Anschlag	C, I, A	Ja/Nein
G 0.35	Nötigung, Erpressung oder Korruption	C, I, A	Ja/Nein
G 0.36	Identitätsdiebstahl	C, I, A	Ja/Nein
G 0.37	Abstreiten von Handlungen	C, I	Ja/Nein
G 0.38	Missbrauch personenbezogener Daten	C	Ja/Nein
G 0.39	Schadprogramme	C, I, A	Ja/Nein
G 0.40	Verhinderung von Diensten (Denial of Service)	A	Ja/Nein
G 0.41	Sabotage	A	Ja/Nein
G 0.42	Social Engineering	C, I	Ja/Nein
G 0.43	Einspielen von Nachrichten	C, I	Ja/Nein

Nr.	Bezeichnung der elementaren Gefährdung	Sicherheitsziel	Schaden möglich?
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	C, I, A	Ja/Nein
G 0.45	Datenverlust	A	Ja/Nein
G 0.46	Integritätsverlust schützenswerter Informationen	I	Ja/Nein

5 REDUKTION DURCH VORHANDENEN BAUSTEIN

Vorgehensweise:

Reduktion der G.0 Gefährdungen durch die in vorhandenen Bausteinen bereits umgesetzten Maßnahmen

- Fall 1: Relevante Bausteine vorhanden
    - Verwendung der Kreuzreferenztabelle des entsprechenden Bausteins
    - Reduktion aufgrund vorhandener Gegenmaßnahmen
        - Mechanismenstärke (Durchschnitt über alle Maßnahmen, welche die entsprechende G.0 Gefährdung adressieren)
        - Zuverlässigkeit (Durchschnitt über alle Maßnahmen, welche die entsprechende G.0 Gefährdung adressieren)
        - Vollständigkeit (Durchschnitt über alle Maßnahmen, welche die entsprechende G.0 Gefährdung adressieren)
    - Qualität des Maßnahmenbündels ausreichend?
        - Fall 1: Ja, G.0 Gefährdung wird gestrichen
        - Fall 2: Nein, G.0 Gefährdung wird nicht gestrichen
            - Risikoanalyse der G.0 Gefährdung im Kapitel 7.
- Fall 2: Keine relevanten Bausteine vorhanden
    - Verwendung der Kreuzreferenztabelle entfällt bei nicht vorhandenem Baustein
    - nutzerdefinierten Baustein erstellen oder
    - Risikoanalyse der übrigen G.0 Gefährdungen im Kapitel 7.

5.1 Kreuzreferenztabellen der zugehörigen Bausteine

Tabelle 5: Kreuzreferenztabelle des Bausteins "XY"

B XY	**Siegel-stufe**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**	**Spezielle Gefahrdung des Bausteins**
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			
Maßnahme des Bausteins	A, B, C, Z, W																			

Maßnahme des Bausteins	A, B, C, Z, W																		

5.2 Reduktion aufgrund vorhandener Gegenmaßnahmen

Tabelle 6: Bewertung der Reduktion der Gefährdungen aufgrund vorhandener BSI-IT-Grundschutzmaßnahmen aus einem angewendeten Baustein

Nr.	Bezeichnung der elementaren Gefährdung	Maßnahmen-Nr. im Baustein	Qualität des Maßnahmenbündels			Wirksame Gegenmaßnahme vorhanden?
			Mechanismenstärke	Zuverlässigkeit	Vollständigkeit	
G 0.1	Feuer	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.2	Ungünstige klimatische Bedingungen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.3	Wasser	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.4	Verschmutzung, Staub, Korrosion	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.5	Naturkatastrophen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.6	Katastrophen im Umfeld	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.7	Großereignisse im Umfeld	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.8	Ausfall oder Störung der Stromversorgung	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.9	Ausfall oder Störung von Kommunikationsnetzen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.10	Ausfall oder Störung von Versorgungsnetzen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.11	Ausfall oder Störung von Dienstleistern	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.12	Elektromagnetische Störstrahlung	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.13	Abfangen kompromittierender Strahlung	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein

Nr.	Bezeichnung der elementaren Gefährdung	Maßnahmen-Nr. im Baustein	Qualität des Maßnahmenbündels			Wirksame Gegenmaßnahme vorhanden?
			Mechanismenstärke	Zuverlässigkeit	Vollständigkeit	
G 0.14	Ausspähen von Informationen / Spionage	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.15	Abhören	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.16	Diebstahl von Geräten, Datenträgern oder Dokumenten	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.17	Verlust von Geräten, Datenträgern oder Dokumenten	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.18	Fehlplanung oder fehlende Anpassung	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.19	Offenlegung schützenswerter Informationen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.20	Informationen oder Produkte aus unzuverlässiger Quelle	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.21	Manipulation von Hard- oder Software	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.22	Manipulation von Informationen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.23	Unbefugtes Eindringen in IT-Systeme	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.24	Zerstörung von Geräten oder Datenträgern	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.25	Ausfall von Geräten oder Systemen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.26	Fehlfunktion von Geräten oder Systemen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.27	Ressourcenmangel	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein

Nr.	Bezeichnung der elementaren Gefährdung	Maßnahmen-Nr. im Baustein	Qualität des Maßnahmenbündels			Wirksame Gegenmaßnahme vorhanden?
			Mechanismenstärke	Zuverlässigkeit	Vollständigkeit	
G 0.28	Software-Schwachstellen oder -Fehler	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.29	Verstoß gegen Gesetze oder Regelungen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.30	Unberechtigte Nutzung oder Administration von Geräten und Systemen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.31	Fehlerhafte Nutzung oder Administration von Geräten und Systemen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.32	Missbrauch von Berechtigungen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.33	Personalausfall	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.34	Anschlag	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.35	Nötigung, Erpressung oder Korruption	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.36	Identitätsdiebstahl	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.37	Abstreiten von Handlungen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.38	Missbrauch personenbezogener Daten	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.39	Schadprogramme	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.40	Verhinderung von Diensten (Denial of Service)	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.41	Sabotage	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein

Nr.	Bezeichnung der elementaren Gefährdung	Maßnahmen-Nr. im Baustein	Qualität des Maßnahmenbündels			Wirksame Gegenmaßnahme vorhanden?
			Mechanismenstärke	Zuverlässigkeit	Vollständigkeit	
G 0.42	Social Engineering	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.43	Einspielen von Nachrichten	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.44	Unbefugtes Eindringen in Räumlichkeiten	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.45	Datenverlust	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein
G 0.46	Integritätsverlust schützenswerter Informationen	[Maßnahmen-Nr.]	Ja/Nein	Ja/Nein	Ja/Nein	Ja/Nein

6 IDENTIFIKATION WEITERER GEFÄHRDUNGEN AUSSERHALB VOM G.0 GEFÄHRDUNGSKATALOG

Vorgehensweise:

Identifikation weiterer Gefährdungen durch:

- Brainstorming,
- Quellenrecherche und
- Expertenrunden
-

7 RISIKOANALYSE GEFÄHRDUNGSKATALOG ELEMENTARE GEFÄHRDUNGEN

Vorgehensweise:

- Geeignete Maßnahmen pro verbleibende Gefährdung auflisten
- Risiken pro verbleibende Gefährdung ableiten
- Bewertung des Risikos anhand der Qualität des Maßnahmen-Bündels pro verbleibende Gefährdung
- Hinweis für zusätzliche Maßnahmen: Z Maßnahmen, Maßnahmen mit „Umsetzung entbehrlich“, „nicht umgesetzt“ und abgeleitet Maßnahmen in Risikobehandlung aufnehmen (A,B,C,D)

G 0.1 Feuer

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.2 Ungünstige klimatische Bedingungen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.3 Wasser

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.4 Verschmutzung, Staub, Korrosion

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.5 Naturkatastrophen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.6 Katastrophen im Umfeld

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.7 Großereignisse im Umfeld

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.8 Ausfall oder Störung der Stromversorgung

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

-

G 0.9 Ausfall oder Störung von Kommunikationsnetzen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]

Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.10 Ausfall oder Störung von Versorgungsnetzen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.11 Ausfall oder Störung von Dienstleistern

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.12 Elektromagnetische Störstrahlung

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.13 Abfangen kompromittierender Strahlung

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.14 Ausspähen von Informationen/Spionage

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.15 Abhören

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.18 Fehlplanung

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.19 Offenlegung schützenswerter Informationen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.21 Manipulation von Hard- oder Software

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.22 Manipulation von Informationen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.23 Unbefugtes Eindringen in IT-Systeme

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.24 Zerstörung von Geräten oder Datenträgern

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.25 Ausfall von Geräten oder Systeme

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.26 Fehlfunktion von Geräten oder Systemen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.27 Ressourcenmangel

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.28 Software-Schwachstellen oder –Fehler

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.29 Verstoß gegen Gesetze oder Regelungen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.32 Missbrauch von Berechtigungen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.33 Personalausfall

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.34 Anschlag

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.35 Nötigung, Erpressung oder Korruption

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.36 Identitätsdiebstahl

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.37 Abstreiten von Handlungen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.38 Missbrauch personenbezogener Daten

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.39 Schadprogramme

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.40 Verhinderung von Diensten (Denial of Service)

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.41 Sabotage

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.42 Social Engineering

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.43 Einspielen von Nachrichten

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.44 Unbefugtes Eindringen in Räumlichkeiten

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.45 Datenverlust

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]

Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

G 0.46 Integritätsverlust schützenswerter Informationen

Vorhandene Maß-nahmen	[Beschreibung]
Risiko	[Beschreibung]
Bewertung	[Beschreibung einfärben in „Rot“, „Gelb“ oder „Grün“]
Risikobehandlung	**A. Risiko-Reduktion durch weitere Sicherheitsmaßnahmen** **B. Risikovermeidung** **C. Risikoübernahme** **D. Risikotransfer**

KONTAKT

Evangelische Kirche in Deutschland

Koordinierungsstelle-IT@ekd.de

Herrenhäuser Straße 12

30419 Hannover

Telefon: +49 511 2796 0

Telefax: +49 511 2796 700

HiSolutions AG

info@hisolutions.com

www.hisolutions.com

Bouchéstraße 12

12435 Berlin

Telefon: +49 30 533 289 0

Telefax: + 49 30 533 289 900

Theodor-Heuss-Ring 23

50668 Köln

Telefon: +49 221 771 09-550