

## 1. Risikomanagement-Rahmenwerk

- Umfang und die Ziele des Risikomanagements sind geklärt.
- Policy für Risikomanagement ist entwickelt.
- Verantwortlichkeiten und Rollen sind definiert.

## 2. Identifikation von Risiken

- Interne und externe Risiken sind nach dem BSI Grundschutz-Kompendium identifiziert.
- Identifizierten Risiken sind dokumentiert.

## 3. Bewertung von Risiken

- Wahrscheinlichkeit und die potenziellen Auswirkungen jedes Risikos sind analysiert.
- Qualitative und quantitative Bewertungstechniken werden genutzt.
- Risiken basierend auf ihrer Bewertung sind priorisiert.

## 4. Bewältigungsstrategien

- Geeignete Maßnahmen zur Risikominderung, -vermeidung oder -akzeptanz sind identifiziert.
- Notfallpläne und Risikominderungsstrategien sind entwickelt.
- Kontrollen und Maßnahmen sind implementiert.
- Restrisiken nach Umsetzung der Maßnahmen sind eingeschätzt und Risk Ownern bekannt.

## 5. Kommunikation

- Alle Stakeholder sind über identifizierte Risiken und geplante Maßnahmen informiert.
- Kommunikation ist nachweisbar klar und verständlich.
- Regelmäßige Berichterstattung und Meetings zur Risikoüberwachung sind implementiert.

## 6. Dokumentation

- Alle Maßnahmen und deren Ergebnisse werden dokumentiert.
- Berichte und Analysen werden regelmäßig festgehalten.

## 7. Überwachung und Überprüfung

- System zur kontinuierlichen Überwachung von Risiken ist implementiert.
- Risikobewertungen und Maßnahmen werden regelmäßig überprüft und aktualisiert
- Regelmäßige Audits und Reviews werden durchgeführt.

## 8. Schulung und Sensibilisierung

- Mitarbeiter werden im Umgang mit Risiken und im Risikomanagementprozess geschult.
- Risikobewusste Unternehmenskultur wird gefördert.

## 9. Kontinuierliche Verbesserung (PDCA)

- Feedback und Lessons Learned zur Verbesserung des Risikomanagements werden genutzt.
- Prozesse und Strategien werden an neue Entwicklungen und Erkenntnisse angepasst.