

## **3.5 IT Security Coordinator (IT-Sicherheitskoordinator/in)**

### ***3.5.1 Kurzbeschreibung***

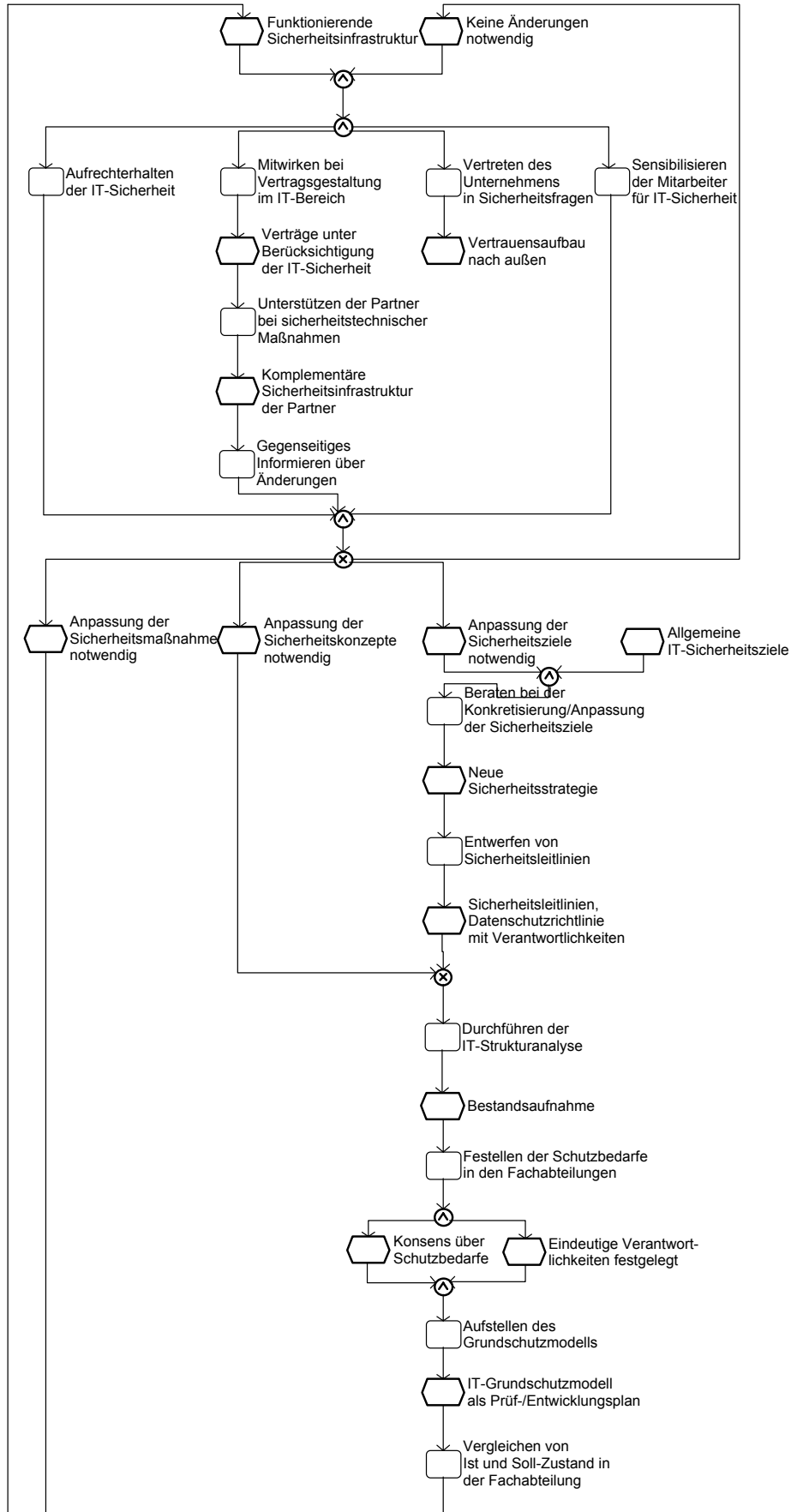
IT Security Coordinators konzipieren angemessene IT Sicherheitslösungen entsprechend geltender technischer Standards, Gesetze und Vorschriften, begleiten deren Umsetzung und passen sie laufend den aktuellen Gegebenheiten an.

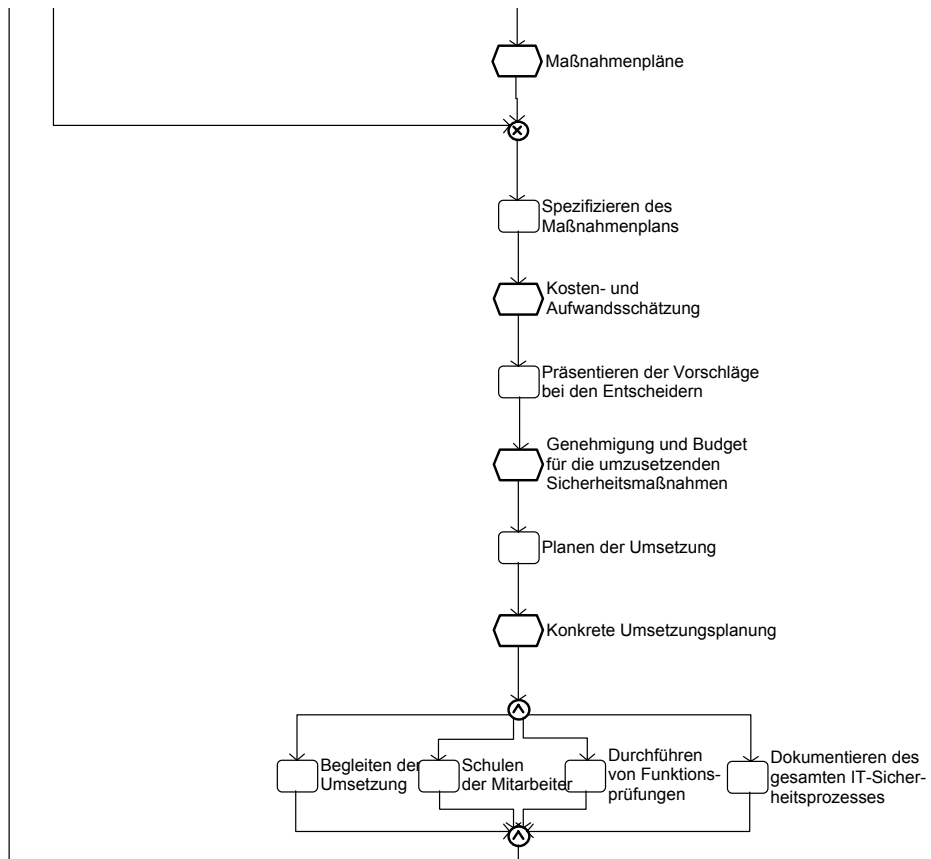
### ***3.5.2 Arbeitsgebiete und Aufgaben***

IT Security Coordinators beraten und unterstützen Unternehmensleitung, Partner und Kunden bezüglich IT-Sicherheit. Sie konzipieren angemessene Sicherheitslösungen entsprechend den geltenden technischen Standards, Gesetzen und anderen Vorschriften und betreuen ihre Realisierung. Sie erarbeiten mit den Fachkräften der verschiedenen Bereiche und Ebenen gemeinsam Lösungen (Organisation, Personal, Infrastruktur, Hard- und Softwaremanagement), beraten bei der Umsetzung und protokollieren die Realisierung.

IT Security Coordinators analysieren Netzwerk- und arbeitsplatzspezifische Risiken und Schwachstellen, erstellen organisatorische und technische Sicherheitskonzepte gemeinsam mit den zuständigen Fachkräften und erarbeiten Richtlinien und Vorschriften zur Informationssicherheit. Sie realisieren IT-Sicherheitsmaßnahmen und entwickeln unter Berücksichtigung neuer Produkte sowie der wirtschaftlichen Gegebenheiten risikomindernde Maßnahmen und innovative Sicherheitsverfahren und führen sie ein. Sie schulen und sensibilisieren Nutzer.

### 3.5.3 Referenzprozess





### **3.5.4 Prozesskompass**

1. Aufrechterhalten der IT-Sicherheit
2. Mitwirken bei Vertragsgestaltung im IT-Bereich
3. Vertreten des Unternehmens in Sicherheitsfragen
4. Sensibilisieren der Mitarbeiter für IT-Sicherheit
5. Unterstützen der Partner bei sicherheitstechnischen Maßnahmen
6. Gegenseitiges Informieren über Änderungen
7. Beraten bei der Konkretisierung der Sicherheitsziele
8. Entwerfen von Sicherheitsleitlinien
9. Durchführen der IT-Strukturanalyse
10. Festellen der Schutzbedarfe in den Fachabteilungen
11. Aufstellen des Grundschutzmodells
12. Vergleichen von Ist und Soll-Zustand in der Fachabteilung
13. Spezifizieren des Maßnahmenplans
14. Präsentieren der Vorschläge bei den Entscheidern
15. Planen der Umsetzung
16. Begleiten der Umsetzung
17. Schulen der Mitarbeiter
18. Durchführen von Funktionsprüfungen
19. Dokumentieren des gesamten IT- Sicherheitsprozesses

### **3.5.5 Profilprägende Kompetenzfelder**

Die Beherrschung der profiltypischen Arbeitsprozesse setzt Kompetenzen unterschiedlicher Reichweite in den nachstehend aufgeführten beruflichen Kompetenzfeldern voraus. Den Kompetenzfeldern sind Wissen und Fähigkeiten sowie typische Methoden und Werkzeuge unterschiedlicher Breite und Tiefe zugeordnet.

Grundlegend zu beherrschende, gemeinsame Kompetenzfelder:

- Unternehmensziele und Kundeninteressen,
- Problemanalyse, -lösung,
- Kommunikation, Präsentation,
- Konflikterkennung, -lösung,
- Fremdsprachliche Kommunikation (englisch),
- Projektorganisation, -kooperation,
- Zeitmanagement, Aufgabenplanung und -priorisierung,
- Wirtschaftliches Handeln,
- Selbstlernen, Lernorganisation,
- Innovationspotenziale,
- Datenschutz, -sicherheit,
- Dokumentation, -standards,
- Qualitätssicherung.

Fundiert zu beherrschende, gruppenspezifische Kompetenzfelder:

- System-Analyse, -modellierung, -entwicklung, -integration,
- Entwicklungsstandards (Leistungsfähigkeit, Sicherheit, Verfügbarkeit, Innovation),
- Engineering-Prozesse,
- Analysemethoden, -strategien, -muster,
- Designmethoden,
- Qualitätsstandards,
- Vernetztes Denken,
- Wirtschaftlichkeitsanalysen,
- Marktüberblick,
- Nutzerorientierte Problemanalyse, -lösung,
- Projektplanung und -management,
- Moderation.

Routiniert zu beherrschende, profilspezifische Kompetenzfelder:

- Informationstechnologie: Netzwerke, Protokolle, Betriebssysteme, Anwendungen,
- System- und Netzmodellierung,
- Sicherheitsanforderungen und -lösungen,
- Sicherheitsüberwachung, Schutzstrategien und -methoden,
- Rechtliche Grundlagen, Datenschutz,
- Verschlüsselung,
- Wirtschaftlichkeitsanalysen,
- Projektspezifikation, -überwachung,
- Risikomanagement.

### **3.5.6 Qualifikationserfordernisse**

Im Regelfall wird ein hinreichendes Qualifikationsniveau auf der Basis einschlägiger Berufsausbildung oder Berufserfahrung vorausgesetzt.