Überprüfungsverfahren

Es gibt eine Reihe von bewährten Verfahren (z.B. Abarbeitung von Checklisten, Penetrationstests usw.), mit denen die Effizienz und Effektivität der Vorkehrungen für Informationssicherheit geprüft werden können. Grundsätzlich gilt, dass umfassende Prüfungen in regelmäßigen Intervallen (jährlich bis maximal drei Jahre) durchgeführt werden sollten. Aber auch fallweise Prüfungen sind zweckmäßig, beispielsweise bei der Änderung von Geschäftsprozessen und insbesondere nach Sicherheitsvorfällen. Die Ergebnisse aller Überprüfungen müssen dokumentiert und der Leitung mitgeteilt werden. Die Überprüfungen des IS-Prozesses sollten sich dabei an folgenden Leitfragen orientieren:

- Welche Ziele der Informationssicherheit sind aktuell vordringlich?
- Wer ist verantwortlich für die Überwachung des Informationssicherheitsprozesses?
- Wie häufig sind die Verfahren zu überprüfen?

Im Folgenden werden zwei Varianten von Überprüfungsverfahren vorgestellt.

Überprüfung mithilfe von Kennzahlen

Kennzahlen können als Indikator für die Güte des gesamten Sicherheitsprozesses oder einzelner Teilprozesse und -aspekte dienen. Sie sind ein bewährtes Instrument in der Kommunikation mit der Leitung einer Institution über Erfolge, aber auch Probleme der Informationssicherheit. Mit Kennzahlen können sowohl technische als auch organisatorische Aspekte der Informationssicherheit erfasst werden. Für eine umfassende Bewertung der Informationssicherheit ist oftmals eine Vielzahl an Kennzahlen nötig. Damit der Aufwand in einem angemessenen Verhältnis zum Ergebnis steht, ist es wichtig, dass die Ziele der Kennzahlen klar formuliert und der erforderliche Aufwand für die Erhebung der Messwerte gut abgeschätzt werden.

Beispiel aus dem Baustein *ISMS.1 Sicherheitsmanagement*:

Anforderung: Die Leitungsebene SOLLTE regelmäßig über den Stand der Informationssicherheit informiert werden.

Kennzahl: Anzahl der Leitungsmeetings mit Sicherheitsreport / Anzahl aller Leitungsmeetings

Überprüfung auf Basis eines Reifegradmodells

Einen sehr umfassenden Blick auf die Qualität des Informationssicherheitsprozesses kann mit Hilfe eines Reifegradmodells erreicht werden. Hierzu muss das ISMS über Jahre hinweg analysiert und bewertet werden. Der Maßstab für die „Reife“ des gesamten ISMS oder aber auch Teilen hiervon ist der Grad der Strukturierung und der systematischen Steuerung des Prozesses.

Folgende Tabelle zeigt ein Beispiel für die Definition von Reifegraden.

Reifegrad	Kennzeichen
0	Es existiert kein Prozess, es gibt auch keine Planungen hierzu.
1	Es gibt Planungen zur Etablierung eines Prozesses, jedoch keine Umsetzungen.
2	Teile des Prozesses sind umgesetzt, es fehlt jedoch an systematischer Dokumentation.
3	Der Prozess ist vollständig umgesetzt und dokumentiert.
4	Der Prozesse wird darüber hinaus auch regelmäßig auf Effektivität überprüft.
5	Zusätzlich sind Maßnahmen zur kontinuierlichen Verbesserung vorhanden.

Ziel der Anwendung eines Reifegradmodells ist es, die Qualität aller Teilbereiche des ISMS zu erhöhen. Durch regelmäßige Analysen kann überprüft werden, welche Prozesse noch unzureichend gesteuert sind.

Beispiel für die graphische Darstellung (Spinnennetzdiagramm):

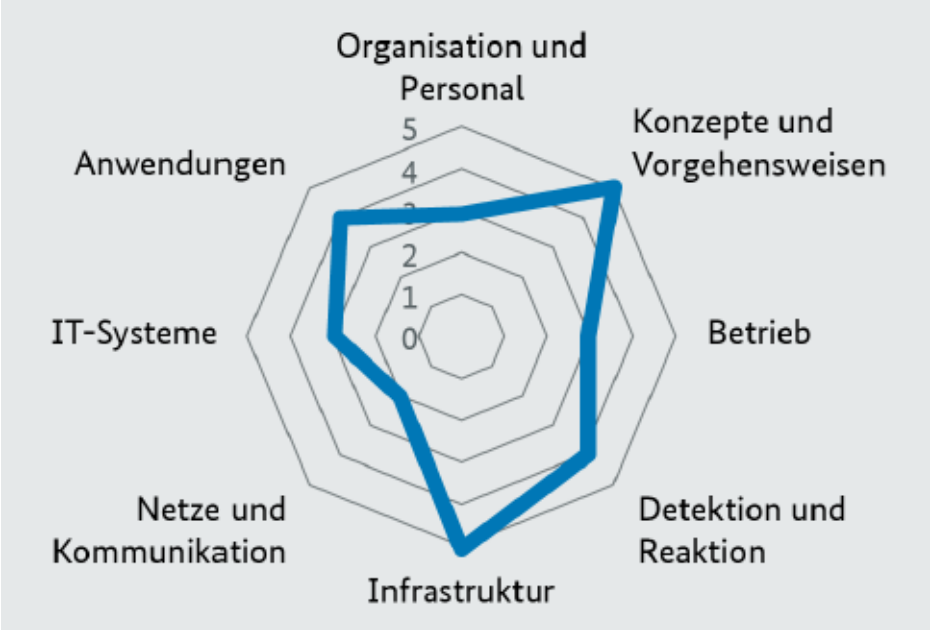

Abbildung 1: Reifegrad von Themenfeldern der Informationssicherheit der Abrechnungsabteilung

Aufgabenstellung:

Beantworten Sie folgenden Fragen:

- **Nennen** Sie mindestens drei **Verfahren**, mit denen die Effizienz und Effektivität von Vorkehrungen für die Informationssicherheit geprüft werden können!

  Überprüfung auf Basis eines Reifegradmodells

  Überprüfung mithilfe von Kennzahlen

  Penetrationstests

- In welchen **zeitlichen Abständen** sollten **Überprüfungen** der Informationssicherheit stattfinden?

  Jährlich bis max. 3 Jahre

- **Beschreiben** Sie, wieso die Überprüfung von **Kennzahlen ein bewährtes Instrument** zur Kommunikation mit der Leitungsebene ist!

  Erfolge und Probleme können leicht kommuniziert werden

  Technische und organisatorische Aspekte werden erfasst

- **Nennen** Sie mögliche **Gefahren**, die bei der Überprüfung mithilfe von Kennzahlen auftreten können!

  Zu viel Aufwand hinein gesteckt wird

- **Beschreiben** Sie anhand der Abbildung 1 die Qualität der Informationssicherheit von **drei gewählten** Themenfeldern!
  - Nutzen Sie zur Beschreibung die Tabelle der Reifegrade!

  Die Netze und Kommunikation ist noch sehr schlecht geschützt, da Umsetungen nur in der Planung sind

  Die Infrastruktur ist sehr gut schützt und wird ständig überprüft und verbessert

  Die Anwendungen sind sehr gut geschützt und werden ständig überprüft, jedoch nicht verbessert