

## CYBER-ASSURANCE

# Voraudit-Checkliste

Zehn Kontrollen, die Teams, die souverän in ein Audit gehen, von denen unterscheiden, die improvisieren.

- 
- |           |   |     |
|-----------|---|-----|
| <b>01</b> | <b>Vollständigkeit des Asset-Inventars</b>  | [ ] |
|           | Können Sie jedes aktive Gerät, jede Anwendung und jedes Benutzerkonto im Geltungsbereich aufzählen?<br>Eine regulatorische Prüfung beginnt hier.                      |     |
| <b>02</b> | <b>Bereitschaft zur Beweiserhebung</b>  | [ ] |
|           | Wird technisches Beweismaterial automatisch gesammelt oder hängt es von manuellen Bemühungen ab?<br>Die manuelle Erfassung kostet 3–8 Wochen; EviGen braucht Stunden. |     |
| <b>03</b> | <b>Abbildung der Kontroll-Baseline</b>  | [ ] |
|           | Sind alle im Geltungsbereich befindlichen Kontrollen einem veröffentlichten Rahmenwerk zugeordnet —<br>SWIFT CSCF, ISO 27001, DORA, NIS 2 oder LPM?                   |     |
| <b>04</b> | <b>Offenes Lückenregister</b>   | [ ] |
|           | Ist jede Lücke mit einem Verantwortlichen, einem Behebungszeitplan und einer schriftlichen<br>Geschäftsbegründung dokumentiert?                                       |     |
| <b>05</b> | <b>Risikoberechnung</b>   | [ ] |
|           | Können Sie das Restrisiko in finanziellen Begriffen ausdrücken — Euro oder Dollar — und nicht nur als<br>Rot, Gelb oder Grün?   |     |
| <b>06</b> | <b>Drittpartei-Exposition</b>   | [ ] |
|           | Werden Lieferanten jährlich bewertet und ist ihr Risikobeitrag in Ihrer finanziellen Gesamtexposition<br>enthalten?   |     |
| <b>07</b> | <b>Übung des Vorfalldaktionsplans</b>   | [ ] |
|           | Wurde der IR-Plan in den letzten zwölf Monaten unter realistischen Lastbedingungen getestet?  |     |
| <b>08</b> | <b>Berichterstattung auf Vorstandsebene</b>   | [ ] |
|           | Erhält Ihr Vorstand einen Risikobericht in monetären Zahlen statt Ampelfarben?  |     |
| <b>09</b> | <b>Regulatorische Querverweise</b>  | [ ] |
|           | Sind alle Pflichtkontrollen mit jeder anwendbaren Vorschrift querverwiesen, damit sich Lücken nicht<br>zwischen den Rahmenwerken verstecken?                          |     |
| <b>10</b> | <b>Vollständigkeit des Prüfpfads</b>  | [ ] |
|           | Ist jeder Befund aus dem letzten Audit-Zyklus formell abgeschlossen oder als Risiko akzeptiert, mit<br>aufbewahrten Nachweisen?                                       |     |
- 

## Bewertung

- 9 – 10 Audit-bereit
- 6 – 8 Geringfügige Lücken — in wenigen Wochen mit gezieltem Aufwand behebbar
- 3 – 5 Erhebliche Vorbereitung erforderlich — jetzt CCI kontaktieren
- 0 – 2 Dringend — drei Monate reichen ohne Hilfe möglicherweise nicht

---

Bereit, von einer Checkliste zu einem berechneten Risikobild zu wechseln? Kontaktieren Sie uns unter [contact@cambridgecyberinternational.com](mailto:contact@cambridgecyberinternational.com) oder besuchen Sie [cambridgecyberinternational.com/de/contact/](https://cambridgecyberinternational.com/de/contact/)