

CYBER ASSURANCE

監査前チェックリスト

自信をもって監査に臨むチームと、その場しのぎのチームを分ける十の管理項目。

- | | |
|---|-----|
| 01 資産インベントリの網羅性 | [] |
| 対象範囲のすべての稼働デバイス、アプリケーション、ユーザーアカウントを列挙できますか。規制評価はここから始まります。 | |
| 02 証拠収集の準備 | [] |
| 技術的証拠は自動で収集されますか、それとも手作業に依存していますか。手作業の収集は3~8週間、EviGenなら数時間です。 | |
| 03 管理ベースラインへの対応付け | [] |
| 対象範囲のすべての管理項目が、公開された枠組み（SWIFT CSCF、ISO 27001、DORA、NIS 2、LPM）に対応付けられていますか。 | |
| 04 未解決ギャップ台帳 | [] |
| 各ギャップに責任者、是正の期限、書面による業務上の根拠が記録されていますか。 | |
| 05 リスクの定量化 | [] |
| 残存リスクを、赤・黄・緑だけでなく、金額（ユーロまたはドル）で表現できますか。 | |
| 06 第三者リスクのエクスポージャー | [] |
| 供給者は毎年評価され、そのリスク寄与が財務エクスポージャー総額に含まれていますか。 | |
| 07 インシデント対応計画の演習 | [] |
| インシデント対応計画は、過去十二か月以内に現実的な負荷条件下で試験されましたか。 | |
| 08 取締役会レベルの報告 | [] |
| 取締役会は、信号機の色ではなく金額でリスク報告を受け取っていますか。 | |
| 09 規制の相互参照 | [] |
| すべての必須管理項目が適用される各規制と相互参照され、ギャップが枠組みの間に隠れないようになっていますか。 | |
| 10 監査証拠の完全性 | [] |
| 前回の監査サイクルの各指摘は、証拠を保持したうえで正式に終結またはリスク受容されていますか。 | |

採点

- | | |
|------|---------------------------|
| 9-10 | 監査の準備が整っている |
| 6-8 | 軽微なギャップ。集中的な取り組みで数週間で対応可能 |
| 3-5 | 相当の準備が必要。今すぐCCIにご連絡を |
| 0-2 | 緊急。支援なしでは三か月でも足りない可能性 |

チェックリストから、計算されたリスク像へ移る準備はできましたか。ご連絡先：

contact@cambridgecyberinternational.com または cambridgecyberinternational.com/ja/contact/ へ