

## CYBER ASSURANCE

# 감사 전 점검표

자신 있게 감사에 임하는 팀과 즉흥적으로 대응하는 팀을 가르는 열 가지 통제.

- |    |  |     |
|----|--|-----|
| 01 | <b>자산 인벤토리의 완전성</b><br>범위 내 모든 가동 장치, 애플리케이션, 사용자 계정을 열거할 수 있습니까? 규제 평가는 여기서 시작됩니다.            | [ ] |
| 02 | <b>증거 수집 준비도</b><br>기술 증거가 자동으로 수집되니까, 아니면 수작업에 의존합니까? 수작업 수집은 3-8주가 들고, EviGen은 몇 시간이면 됩니다.   | [ ] |
| 03 | <b>통제 기준선 매핑</b><br>범위 내 모든 통제가 공표된 프레임워크(SWIFT CSCF, ISO 27001, DORA, NIS 2, LPM)에 매핑되어 있습니까? | [ ] |
| 04 | <b>미해결 격차 대장</b><br>각 격차가 책임자, 시정 일정, 문서화된 사업적 근거와 함께 기록되어 있습니까?                               | [ ] |
| 05 | <b>위험의 정량화</b><br>잔여 위험을 빨강·노랑·초록뿐 아니라 금액(유로 또는 달러)으로 표현할 수 있습니까?                              | [ ] |
| 06 | <b>제3자 노출</b><br>공급업체를 매년 평가하며 그 위험 기여분이 총 재무 노출에 포함됩니까?                                       | [ ] |
| 07 | <b>사고 대응 계획 훈련</b><br>사고 대응 계획을 지난 12개월 내 현실적인 부하 조건에서 시험했습니까?                                 | [ ] |
| 08 | <b>이사회 수준 보고</b><br>이사회가 신호등 색이 아니라 금액으로 위험 보고를 받습니까?  | [ ] |
| 09 | <b>규제 교차 참조</b><br>모든 필수 통제가 적용 가능한 각 규제와 교차 참조되어, 격차가 프레임워크 사이에 숨지 않습니까?                      | [ ] |
| 10 | <b>감사 추적의 완전성</b><br>지난 감사 주기의 각 발견사항이 증거를 보존한 채 공식적으로 종결되거나 위험 수용되었습니까?                       | [ ] |

## 채점

- |        |                           |
|--------|---------------------------|
| 9 - 10 | 감사 준비 완료                  |
| 6 - 8  | 경미한 격차, 집중하면 수 주 내 해결 가능  |
| 3 - 5  | 상당한 준비 필요, 지금 CCI에 문의하십시오 |
| 0 - 2  | 긴급, 도움 없이는 3개월도 부족할 수 있음  |

점검표에서 계산된 위험 그림으로 넘어갈 준비가 되셨습니까? 문의:

[contact@cambridgecyberinternational.com](mailto:contact@cambridgecyberinternational.com) 또는 [cambridgecyberinternational.com/ko/contact/](https://cambridgecyberinternational.com/ko/contact/) 방문