

## CYBER ASSURANCE

# Lista kontrolna przed audytem

Dziesięć kontroli, które oddzielają zespoły wchodzące na audyt z pewnością od tych, które improwizują.

<b>01</b>	<b>Kompletność inwentaryzacji zasobów</b>	[ ]
	Czy potrafisz wymienić każde aktywne urządzenie, aplikację i konto użytkownika w zakresie? Ocena regulacyjna zaczyna się tutaj.	
<b>02</b>	<b>Gotowość do zbierania dowodów</b>	[ ]
	Czy dowody techniczne zbierane są automatycznie, czy zależą od pracy ręcznej? Zbieranie ręczne kosztuje 3-8 tygodni; EviGen kosztuje godziny.	
<b>03</b>	<b>Mapowanie bazowych kontroli</b>	[ ]
	Czy wszystkie kontrole w zakresie są zmapowane do opublikowanego standardu: SWIFT CSCF, ISO 27001, DORA, NIS 2 lub LPM?	
<b>04</b>	<b>Otwarty rejestr luk</b>	[ ]
	Czy każda luka jest udokumentowana z właścicielem, harmonogramem naprawy i pisemnym uzasadnieniem biznesowym?	
<b>05</b>	<b>Kwantyfikacja ryzyka</b>	[ ]
	Czy potrafisz wyrazić ryzyko szacunkowe w ujęciu finansowym, w euro lub dolarach, a nie tylko jako czerwone, bursztynowe lub zielone?	
<b>06</b>	<b>Ekspozycja na strony trzecie</b>	[ ]
	Czy dostawcy są oceniani corocznie, a ich wkład w ryzyko ujęty w łącznej ekspozycji finansowej?	
<b>07</b>	<b>Ćwiczenie planu reagowania na incydenty</b>	[ ]
	Czy plan reagowania na incydenty był testowany w realistycznych warunkach obciążenia w ciągu ostatnich dwunastu miesięcy?	
<b>08</b>	<b>Raportowanie na poziomie zarządu</b>	[ ]
	Czy zarząd otrzymuje raport o ryzyku w wartościach pieniężnych, a nie w kolorach sygnalizacji?	
<b>09</b>	<b>Odniesienia regulacyjne</b>	[ ]
	Czy wszystkie obowiązkowe kontrole są powiązane z każdą obowiązującą regulacją, aby luki nie kryły się między standardami?	
<b>10</b>	<b>Kompletność ścieżki audytu</b>	[ ]
	Czy każde ustalenie z ostatniego cyklu audytu zostało formalnie zamknięte lub zaakceptowane jako ryzyko, z zachowaniem dowodów?	

## Punktacja

<b>9 - 10</b>	Gotowość do audytu
<b>6 - 8</b>	Drobne luki, do usunięcia w tygodniach przy skupionym wysiłku
<b>3 - 5</b>	Potrzebne znaczące przygotowanie, skontaktuj się z CCI teraz
<b>0 - 2</b>	Pilne, trzy miesiące mogą nie wystarczyć bez pomocy

Gotów przejść od listy kontrolnej do obliczonego obrazu ryzyka? Skontaktuj się z nami pod [contact@cambridgecyberinternational.com](mailto:contact@cambridgecyberinternational.com) lub odwiedź [cambridgecyberinternational.com/pl/contact/](https://cambridgecyberinternational.com/pl/contact/)