CYBER ASSURANCE

Контрольный список перед аудитом

Десять проверок, которые отличают команды, входящие в аудит уверенно, от тех, кто импровизирует.

01 Полнота инвентаризации активов [ ]
Можете ли вы перечислить каждое активное устройство, приложение и учётную запись в периметре? Регуляторная оценка начинается здесь.

02 Готовность к сбору доказательств [ ]
Технические доказательства собираются автоматически или зависят от ручного труда? Ручной сбор стоит 3–8 недель; EviGen — часы.

03 Сопоставление с базой контролей [ ]
Все контроли в периметре сопоставлены с опубликованным стандартом: SWIFT CSCF, ISO 27001, DORA, NIS 2 или LPM?

04 Открытый реестр пробелов [ ]
Каждый пробел задокументирован с владельцем, сроком устранения и письменным бизнес-обоснованием?

05 Количественная оценка риска [ ]
Можете ли вы выразить остаточный риск в финансовых единицах, в евро или долларах, а не только как красный, жёлтый или зелёный?

06 Подверженность риску от третьих сторон [ ]
Поставщики оцениваются ежегодно и их вклад в риск включён в вашу совокупную финансовую подверженность?

07 Учения по плану реагирования на инциденты [ ]
Тестировался ли план реагирования на инциденты при реалистичной нагрузке за последние двенадцать месяцев?

08 Отчётность на уровне совета директоров [ ]
Получает ли совет директоров отчёт о риске в денежных величинах, а не в цветах светофора?

09 Регуляторные перекрёстные ссылки [ ]
Все обязательные контроли сопоставлены с каждым применимым регламентом, чтобы пробелы не прятались между стандартами?

10 Полнота аудиторского следа [ ]
Каждое наблюдение прошлого цикла аудита формально закрыто или принято как риск, с сохранением доказательств?

Оценка

9 – 10	Готовы к аудиту
6 – 8	Незначительные пробелы, устранимы за недели при сфокусированных усилиях
3 – 5	Нужна серьёзная подготовка, свяжитесь с CCI сейчас
0 – 2	Срочно, трёх месяцев может не хватить без помощи

Готовы перейти от контрольного списка к расчётной картине риска? Свяжитесь с нами:
contact@cambridgecyberinternational.com или посетите cambridgecyberinternational.com/ru/contact/