The Managed Provider Scorecard

Supplier Assurance Under NIS2 and the UK Cyber Security and Resilience Bill

Version 1.0.0

www.sakurasky.com

Not Legal Advice

The UK Cyber Security and Resilience Bill is before Parliament; duties described "as drafted" may change before and through secondary legislation. Obtain independent legal advice on how these regimes apply to your circumstances. Sources: DSIT Bill factsheets (updated 30 June 2026); Directive (EU) 2022/2555; Commission Implementing Regulation (EU) 2024/2690; bills.parliament.uk (HL Bill 32).

Sakura Sky operates managed services and answers this scorecard for its own customers. sakurasky.com/contact

Table of Contents

How to use this scorecard

Put the seven questions to every managed service provider, managed security service provider, or platform operator with access into your environment. Score each answer 0, 1 or 2. An answer earns points for artefacts, dates, and offers you can test, never for adjectives.

Scoring: 2 = artefact provided or committed with a date (document, page, pack, clause). 1 = credible description, no artefact yet, offered under NDA or with a date. 0 = adjectives, deflection, or "our legal team is looking at it" with no date.

Reading the total (max 14): 11–14: contract on the answers. 6–10: proceed with remediation milestones in the agreement. 0–5: assume the duties are unmet and price the risk accordingly.

The seven questions

1. Are you in scope, and can you show me the determination?

A provider that has not determined its own scope has not started on any duty that follows. UK (Bill, as drafted): ongoing management of IT systems with access into customer environments, wherever the provider is established; software-as-product out, managed cloud operation in, on-premises vs remote irrelevant. EU: MSPs and MSSPs named in NIS2 Annex I; medium and large captured, smaller entities in defined Article 2(2) cases. A substantive answer contains: a dated, counsel-reviewed determination naming which services fall where.

2. Who is your regulator, and what is your local anchor?

UK (as drafted): registration with the Information Commission within three months of commencement; overseas providers must also appoint a UK representative. EU: main establishment governs if the provider is EU-established; otherwise a designated representative; registration feeds the ENISA registry. A substantive answer contains: a named authority and a named anchor (establishment or representative), current or planned with a date.

3. If you are breached at 2am, what do I hear, and when?

Both regimes put the provider on an hours-denominated clock (see timeline overleaf), and both create customer notification duties on different triggers. If the provider's plan ends at its own regulator, you are an afterthought in it. A substantive answer contains: a rehearsed pipeline (detection, triage, named decision-maker, customer notification path), committed timings, and the date of the last exercise. These clocks are new for every provider, so a first exercise scheduled with a date also scores.

4. What protects the systems you use to reach into my environment?

The provider's management plane (privileged workstations, bastions, credential vaults, monitoring) is an attack surface you imported when you signed. For EU-serving MSPs/MSSPs, Implementing Regulation (EU) 2024/2690 already fixes the required technical measures; no transposition needed. A substantive answer contains: privileged access controls, session accountability, credential management, and management-plane monitoring, mapped to the published requirements.

5. Show me the evidence, not just the certificate

An annual certificate shows a control existed on audit day. Ask for it, then ask about the other 364 days. Hours-denominated reporting duties cannot be met with annually assembled evidence. A substantive answer contains: continuously generated control evidence, shareable under NDA, with a committed turnaround.

6. What about your subcontractors?

Your provider has providers. NIS2 Art. 21(2)(d) makes supply chain security a required measure; the UK Bill's reporting fields (as drafted) include incidents caused by another regulated entity; small subcontractors can still be designated critical suppliers. A substantive answer contains: a current, published sub-processor list with flow-down security obligations and a stated position on which subcontractors touch your environment, or an explicit, dated statement that none are used.

7. Will you put your answers in the contract?

Everything above is conversation until it is a clause. Notification timings, evidence access, sub-processor disclosure, and cooperation with your own regulatory reporting all belong in the agreement. A substantive answer contains: yes, with limits stated up front. Wariness about specific clauses, argued specifically, scores higher than an unexamined yes.

The reporting timelines, side by side

Stage	EU (NIS2, in force)	UK (CSR Bill, as drafted)
Trigger	Significant incident, per Implementing Regulation 2024/2690 criteria for MSPs/MSSPs	"Significant" threshold reserved to secondary legislation
+24 hours	Early warning to competent authority	Initial notification to regulator, NCSC sighted
+72 hours	Incident notification	Full report
Customer notification	Without undue delay, where appropriate, for significant incidents likely to adversely affect the service	After the full report: identify likely-affected customers, notify with reasons
+1 month	Final report	Not specified in factsheets

What to do if

Your provider notifies you of an incident. Start your own clock check immediately: if you are a regulated entity, your provider's incident can be your reportable event, on your regime's trigger, not theirs. Ask for their initial regulator notification content, their affected-scope statement for your services, and a commitment time for the full report. Log everything; your regulator may ask for the chain.

Your provider cannot show a determination. Treat every other answer as unverified. Set a remediation milestone in the contract or at renewal: determination with counsel within 90 days, shared under NDA. No determination at the milestone converts to a termination-assist or exit-planning conversation.

Your provider will not contract on its answers. Distinguish two refusals. Specific wariness (a timing that depends on your stack, a scope carve-out) argued at the table is a provider taking the clause seriously. Blanket refusal to commit to notification timings or evidence access from a soon-to-be-regulated provider means the questionnaire answers were marketing.

You suspect the incident before the provider tells you. Notify the provider in writing, timestamped. Both regimes' clocks run from the provider's awareness; your notice removes ambiguity about when that was. Then run the first playbook.

Watch-for patterns

Adjective answers. "Robust", "industry-leading", "bank-grade" in place of an artefact. Score 0. Certificate deflection. The certification is offered as the answer to questions 3–6. Certificates are necessary context, never the whole answer. Regulator vagueness. A provider in a regulated category that cannot name its authority or anchor has not started. The unexamined yes. Agreement to every clause without a stated limit means the MSA is not being read.