GRC+ SERVICE SHEET · NOVEMBER 2026

Incident Reporting Desk

One incident can start several reporting clocks at once: NIS2, DORA, the GDPR and, since September 2026, the Cyber Resilience Act. We decide with you what is reportable, draft every notification in the authority's own format and check or prepare each report before it goes out.

SERVICE
Managed service

What It Is

Incident notifications under NIS2, DORA, GDPR and, by market, the CRA, SEC, NYDFS and UK requirements: decided with you, drafted for you and, on the Covered plan, submitted where the authority allows, on time, from one hotline call to a monthly plan.

WHY IT MATTERS

Nobody is sure what to report, to whom or by when

- Your team is busy containing the incident
- Each law has its own threshold, authority, portal and form
- The first deadline can fall within hours
- A late or missing report is a breach in its own right

THE OUTCOME

Every report on time, and a record that holds up

- Your team stays on containment and recovery
- Notifications and final reports ready within the legal deadlines
- A decision record your board, auditors and supervisor can follow
- Regulator questions answered from one consistent file

What We Handle

Whether the incident is reportable	We assess it with you against the criteria of each regime that may apply, and record your decision and the reasons, also when the answer is no.
Where and to whom	The authority, CSIRT or supervisor for each regime and each country, and the portal or form it uses.
Every notification on time	Early warnings, initial notifications and breach notices drafted in the authority's format, approved by you, then submitted by you, or by us under your mandate where the authority allows it.
Follow-up and final reports	Intermediate, progress and final reports tracked against their own deadlines, with the facts kept consistent from one report to the next.
Customers and people affected	Notices to clients, service recipients and data subjects where a regime requires them, in plain words.
The evidence and the regulators' questions	A file with the timeline, decisions, reports sent and replies received, from which we answer the authorities' questions.

What You Get

The reporting decision record PDF	Per regime: the criteria applied, the facts, your decision and the reasons. It is what you show a supervisor who asks why you reported, or why you did not.
Every notification and report Authority forms and portal submissions	Early warnings, initial notifications, breach notices, intermediate and final reports, in each authority's format and as submitted.
The deadline log Shared log, kept live during the incident	Every clock that started, when it started, when it falls due and when the report went, so no deadline is missed.
The incident file Access-controlled folder	The timeline, decisions, reports sent and the authorities' questions and replies, kept as evidence.
Your reporting playbook, on the Ready and Covered plans Document and templates	A reporting procedure, a classification matrix per regime, templates per authority and regulator contacts, kept current every quarter and tested in a yearly reporting drill.

What Happens After You Accept the Proposal

1	**Start** Accept the proposal. You receive your client number for incident reports.	On signing
2	**Your reporting map** Which laws apply, to which authority you report in each country, and who in your organisation decides.	Within 2 working days
3	**Report the incident** Use the incident form with your client number. If your systems are down or not safe to use, call the Intake Line. A practitioner contacts you to start the reporting decision.	When something happens
4	**Close the file** Final reports sent, questions from authorities answered and what to change next time written down.	Afterwards

Regulations That Ask for It

NIS2	NIS2 early warnings, incident notifications and final reports, decided with you, drafted and filed on time.
SEC cyber rules (United States)	The materiality decision recorded and the Form 8-K Item 1.05 disclosure prepared within four business days.
DORA	Major ICT-related incident reports under DORA, from the 4-hour initial notification to the final report, on the standard forms.
GDPR	Personal data breach notices to the supervisory authority within 72 hours, and notices to the people affected.
NIS2 Implementing Regulation	Incident reports decided with you and drafted in each authority's format, so every reporting deadline is met.
DORA Incident Reporting ITS	
UK GDPR (United Kingdom)	UK GDPR breach reports to the regulator within 72 hours, and notices to the people affected.
NYDFS Part 500 (United States)	Notices to the Superintendent within 72 hours of an incident, and within 24 hours of an extortion payment.
CRA	CRA reports of actively exploited vulnerabilities and severe incidents, from the 24-hour early warning to the final report.
UK NIS (United Kingdom)	NIS incident notices to your competent authority within 72 hours, drafted and filed with you.
Digitalsikkerhetsloven (Norway)	
Cybersecurity Act (Singapore)	

Why GRC+

Every regime in one view	We track the EU, US and UK reporting requirements side by side, so one incident gets one assessment and one deadline log, not a separate exercise per law.
From decision to submission	We do not stop at advice. We draft each report in the authority's format, submit it for you where the authority allows, and handle the follow-up.
One set of facts	Every report is drafted from the same incident file, so what you tell one authority matches what you tell the next.
Ready before it happens	On the Ready and Covered plans your reporting map is set up before an incident, and the classification matrix, templates, contacts and portal access are in place and tested in a yearly reporting drill.
Alongside your lawyers and responders	We work with your legal counsel and your incident response firm. They advise and contain; we make sure every report goes out on time.
Records that hold up	Each decision is recorded with the criteria and facts behind it, so your board, auditors and supervisors can follow it later.

Questions Buyers Ask

Which incidents do we have to report, and to whom?

It depends on your sector, your market and what the incident affected. A significant incident goes to your CSIRT or competent authority under NIS2 and its national law; a major ICT-related incident goes to your financial supervisor under DORA; a personal data breach goes to the data protection authority under GDPR; and manufacturers report actively exploited vulnerabilities and severe incidents under the Cyber Resilience Act. One incident can fall under several of these at once. We assess each with you and record the decision.

When does the clock start?

Not always at the same moment. Under NIS2, GDPR and the CRA it runs from when you become aware. Under DORA the initial notification is due within 4 hours of classifying the incident as major, and at the latest 24 hours after you became aware. Under NYDFS Part 500 it runs from your determination that a cybersecurity incident occurred, and under the SEC requirements from your decision that it is material, which must be made without unreasonable delay. Our deadline log records each start time.

Do you replace our lawyers or our incident response firm?

No. We work alongside them. Your incident response firm contains and investigates the incident, your legal counsel advises on liability and legal privilege, and we make sure every report goes to the right authority, in the right form, on time. GRC+ does not give legal advice.

We report in the United States or the United Kingdom. Is that covered?

Yes. In the United States we cover Form 8-K Item 1.05 under the SEC cybersecurity disclosure requirements (within four business days of the materiality decision) and notices under NYDFS Part 500 (within 72 hours, and 24 hours for an extortion payment). In the United Kingdom we cover breach reports under UK GDPR and NIS incident notices under the UK NIS Regulations, both within 72 hours. We follow changes to the UK requirements as they are made.

Talk to Us

Tell us who you are and the regimes you report under. We will help clarify the scope and the information needed for a written proposal. You can share details of past incidents and documents after confidentiality arrangements are agreed.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/incident-reporting-desk