GRC+ SERVICE SHEET · NOVEMBER 2026

Incident Response Plan and Exercise

We write or update your incident response plan, with roles, decision points and the reporting deadlines of NIS2, DORA and the GDPR. Then we test it with your management team in a realistic tabletop exercise and improve it with what we learn.

SERVICE	USUALLY TAKES
Advisory service	**Weeks, usually, from kick-off to a tested plan**

What It Is

An incident response plan that meets NIS2 and DORA reporting deadlines, tested in a realistic tabletop exercise with your management.

Who It Is For

- A plan with roles, escalation and reporting deadlines
- A realistic tabletop exercise with management
- An exercise report and an improved plan

What Incident Handling Requires

Roles	Who leads, who decides and who stands in, named in the plan.
Decision points	When an event becomes an incident, and who decides to escalate, contain or notify.
Escalation	The route from first detection to management, with contacts that work out of hours.
Thresholds and deadlines	The reporting criteria and deadlines of each regime that applies to you, such as NIS2, DORA and the GDPR.
Communications	What you tell staff, customers, suppliers and authorities, and who approves it.
Evidence	Logs, decisions and timelines kept so you can explain each step to a supervisor.
Lessons learned	A review after each incident and exercise, and the plan updated with what it showed.

From Plan to Tested Plan

1 **Incident response plan**
We write or update the plan with you: roles, decision points, escalation and the reporting deadlines that apply to you.

2 **Scenario design**
We design a realistic scenario around your business, with the decisions your management team will have to take.

3 **Tabletop exercise**
Your management team and the heads of IT, security, legal and communications work through the scenario with us.

4 **Report and improved plan**
An exercise report on what worked and what did not, and the plan updated with what we learned.

Regulations That Ask for It

NIS2	**Incident response and reporting** Classification requirements, reporting templates and a tested playbook for the 24-hour, 72-hour and one-month steps.
DORA	**Incident response and reporting** Classification requirements, reporting templates and a tested playbook, so a major incident reaches your supervisor on time.
DORA Incident Classification RTS	An incident response plan that meets NIS2 and DORA reporting deadlines, tested in a realistic tabletop exercise with your management.
DORA Incident Reporting RTS	
Part-IS	
CER	
HIPAA (United States)	
ISO 22301	
UK NIS (United Kingdom)	
SEC cyber rules (United States)	
Safeguards Rule (United States)	
OSFI B-13 (Canada)	

Questions Buyers Ask

Which reporting deadlines does the plan cover?

The plan covers the deadlines that apply to you, such as NIS2 early warnings and notifications, DORA incident reports and GDPR breach notifications.

Who takes part in the exercise?

Usually the management team and the heads of IT, security, legal and communications. We design the scenario around your business.

Do you write the plan or do we?

We write it with you. The plan has to be yours, so we keep it short and make sure the owners know it.

Talk to Us

Thirty minutes with a principal consultant on what applies to you and what to do first.
Book a 30-Minute Call · sales@grc.plus · grc.plus/service/incident-response-plan-and-exercise

