DORA Compliance Playbook

Automating Incident Reporting and Operational Resilience (24-Hour & 72-Hour Mandates)

gartsolutions.com

info@gartsolutions.com

SOAR Playbook Template

24-Hour Initial Notification Playbook

Objective: To comply with DORA’s 24-hour notification mandate, the SOC team must immediately initiate the following steps upon the detection of a major incident.

gart.

gartsolutions.com

info@gartsolutions.com

1. Incident Detection & Classification:

- [ ] Verify incident classification using predefined DORA severity thresholds (e.g., Major, Critical).
- [ ] Automatically correlate logs from Security Information and Event Management (SIEM) to validate the incident.

2. Data Enrichment:

- [ ] Gather critical context from internal sources (e.g., Active Directory, HR systems, CMDB).
- [ ] Attach contextual details like asset ownership, user identity, system vulnerabilities, etc.

3. Impact Assessment:

- [ ] Determine the scope of the incident (e.g., systems, services, data impacted).
- [ ] Evaluate business-critical services that may be affected by the incident.
- [ ] Identify if the incident has cross-border implications (e.g., services across multiple EU jurisdictions).

gartsolutions.com

info@gartsolutions.com

4. Notification Drafting

- [ ] Populate the initial notification template with enriched data.
- [ ] Ensure the template follows the DORA regulatory technical standards (RTS/ITS) format.

5. Approval Process

- [ ] Verify all incident details and actions taken with the CISO or incident response lead.
- [ ] Get approval for submission from the authorized individual.

6. Notification Submission:

- [ ] Digitally sign the notification report.
- [ ] Securely transmit the report to the competent authority portal (or designated authority).
- [ ] Confirm receipt of the notification by the authority.
- [ ] Document the submission receipt and any immediate feedback from the authority.

SOAR Playbook Template

72-Hour Detailed Report Playbook

Objective: To comply with DORA’s 72-hour detailed incident reporting mandate, the SOC team must provide a comprehensive follow-up report detailing the incident, its impact, mitigation efforts, and next steps.

gart.

gartsolutions.com

info@gartsolutions.com

1. Incident Overview Update

- [ ] Provide an updated overview of the incident, including any developments or escalations since the initial notification.
- [ ] Confirm if the impact of the incident has evolved (e.g., more systems affected, recovery status).

2. Root Cause Analysis

- [ ] Document the root cause(s) of the incident, including technical failures or external factors.
- [ ] Verify with technical teams about corrective actions taken to mitigate the root cause.
- [ ] Ensure that all technical findings are corroborated with evidence (e.g., logs, alerts).

3. Mitigation Actions

- [ ] Describe all actions taken to mitigate the incident's impact (e.g., patching, isolation, system restoration).
- [ ] Include timelines for recovery and system restoration.
- [ ] Specify any back-up measures activated to restore services.

gartsolutions.com

info@gartsolutions.com

4. Impact Quantification

- [ ] Quantify the incident's business impact: downtime, data loss, revenue loss, customer impact, etc.
- [ ] Calculate the potential impact on EU residents, if applicable (e.g., data subjects for GDPR considerations).

5. Compliance & Legal Impact Assessment

- [ ] Confirm whether the incident triggered any legal obligations (e.g., GDPR breach reporting).
- [ ] Review compliance gaps or non-compliance caused by the incident.

6. Incident Recovery Status

- [ ] Document the current state of recovery for affected systems.
- [ ] Verify if normal operations have been restored or if they are still in progress.
- [ ] Identify any lingering issues or vulnerabilities that need resolution.

gartsolutions.com

info@gartsolutions.com

7. Future Prevention & Improvements

- [ ] Specify any changes to security processes or infrastructure to prevent similar incidents.
- [ ] Identify and implement any lessons learned from the incident (e.g., new tools, procedures, or training).

8. Prepare Detailed Report

- [ ] Populate the 72-hour report template with all the findings.
- [ ] Ensure the report follows DORA reporting standards for clarity, detail, and regulatory compliance.
- [ ] Include a summary of impact, response, and future mitigation strategies.

9. Approval Process

- [ ] Review and verify the contents of the report with legal, compliance, and management teams.
- [ ] Ensure all information aligns with internal guidelines and DORA requirements.

10. Submission (within 72 hours of initial notification)

- [ ] Digitally sign the detailed report.
- [ ] Securely transmit the report to the competent authority portal.
- [ ] Confirm submission acknowledgment and document any feedback.

gart.

gartsolutions.com

info@gartsolutions.com

Best Practices for Automation in SOAR Playbooks

gart.

gartsolutions.com

info@gartsolutions.com

Integration with SIEM:

- Ensure automated log collection and event detection from all security devices and applications.
- Automatically classify incidents based on severity and predefined criteria.

Data Enrichment Automation:

- Integrate with internal systems (e.g., HR, CMDB, AD) to automatically enrich incident data with context such as user identity, asset ownership, etc.

Playbook Automation:

- Use SOAR platform playbooks to automatically populate the 24-hour and 72-hour reports.
- Automate the notification submission process with secure, digitally signed messages.

Continuous Monitoring:

- Monitor the incident continuously, updating the playbook in real-time as more data comes in.

Incident Correlation & Classification:

- Automatically correlate and classify incidents using defined rules based on risk thresholds (impact, criticality).

Real-Time Tracking and Alerting:

- Implement automatic alerts to keep stakeholders informed of the incident's status and compliance deadlines.