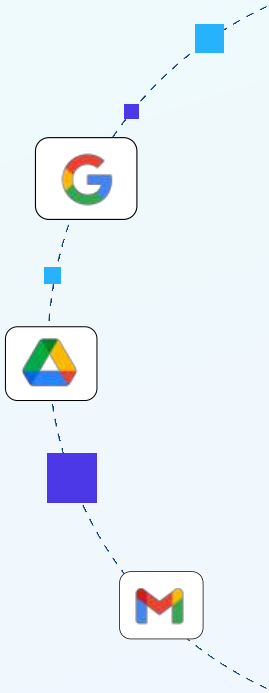
ENTERPRISE RESOURCES

DORA Compliance Checklist For Google Workspace



The Digital Operational Resilience Act (DORA) requires financial institutions to strengthen operational resilience across their technology ecosystem.
For organizations using Google Workspace, this extends beyond traditional infrastructure and includes collaboration, SaaS applications, browser activity, data sharing, and access governance.

This checklist helps IT, Security, and Compliance teams evaluate key operational controls that support DORA readiness.

1. ICT Risk Management & Governance

- [ ] Maintain a current inventory of Google Workspace users, groups, shared drives, and third-party applications.
- [ ] Review external file sharing across Drive and Shared Drives.
- [ ] Identify delegated Gmail access and privileged accounts.
- [ ] Review excessive permissions and dormant accounts.
- [ ] Locate sensitive data stored across Drive, Gmail, and Shared Drives.
- [ ] Establish regular access review procedures.

2. Incident Reporting & Response

- [ ] Define incident classification criteria for Google Workspace events.
- [ ] Configure alerts for suspicious sharing activity.
- [ ] Configure alerts for high-risk OAuth applications.
- [ ] Establish investigation procedures for browser activity and SaaS usage.
- [ ] Test incident escalation workflows.
- [ ] Document reporting responsibilities.

3. Operational Resilience Testing

- [ ] Test onboarding workflows.
- [ ] Test off-boarding workflows.
- [ ] Validate ownership transfer procedures.
- [ ] Verify application token revocation processes.
- [ ] Conduct incident response tabletop exercises.
- [ ] Review workflow audit logs.

4. ICT Third-Party Risk Management

- [ ] Maintain an inventory of OAuth-connected applications.
- [ ] Review application permission scopes.
- [ ] Identify high-risk applications.
- [ ] Review Shadow IT exposure.
- [ ] Audit browser extensions.
- [ ] Establish vendor review procedures.

5. Network & Information Systems Security

- [ ] Monitor uploads and downloads through Chrome.
- [ ] Review browser activity policies.
- [ ] Audit external data movement.
- [ ] Review DLP controls.
- [ ] Review access governance controls.
- [ ] Test multi-party approval procedures.

6. DORA Compliance Assessment

After completing this checklist, ask:

- [ ] Can we identify all third-party applications connected to Google Workspace?
- [ ] Can we investigate suspicious activity quickly?
- [ ] Can we demonstrate access governance controls?
- [ ] Can we locate sensitive information across the environment?
- [ ] Can we provide evidence during a regulatory review?
- [ ] Can we prove operational resilience through documented controls and testing?

Moving From Compliance To Continuous Oversight

Maintaining DORA compliance depends on being able to demonstrate how risks are identified, monitored, and addressed across your digital environment. Operational resilience requires ongoing visibility into users, data, applications, access controls, and operational workflows as your environment evolves.

For organizations using Google Workspace, maintaining that visibility can become challenging as SaaS applications, browser activity, external sharing, and collaboration patterns grow over time.

GAT Labs helps IT, Security, and Compliance teams strengthen operational resilience through auditing, automation, browser monitoring, access governance, and third-party application oversight. Together, these capabilities help organizations improve operational visibility, support compliance efforts, and maintain the evidence needed for regulatory reviews.
Use this checklist regularly to review your controls, identify gaps, and track progress as your DORA compliance program matures.

Learn How GAT Labs Supports DORA Compliance →