IMPACT
RISK ADVISOR

30/60/90-Day SOC 2 Roadmap

Impact Risk Advisors | For Small SaaS Startups

www.impactriskadvisor.com

Day 1–30: Get Oriented & Lay the Foundation

- Identify if you process/store customer data
- List in-scope systems (MS 365, Google Workspace, Slack, Notion, VPN)
- List vendors (antivirus, cloud platforms, backup tools)
- Draft your Information Security Policy
- Begin building a Vendor Tracker
- Write your Access Control Policy (including MFA)
- Enforce MFA on all systems
- Deploy antivirus / EDR on laptops
- Begin using a password manager
- Send out basic security awareness training (free or DIY)
- Ensure Acceptable Use policy is acknowledged (can be part of Employee Handbook)

Day 31–60: Operationalize Key Controls

- Complete documentation: Incident Response, Risk Management, DR/BCP, Employee Handbook
- Start tracking: Monthly log reviews, Risk Register, Change Logs (GitHub, Notion, etc.)
- Conduct a mini DR test (e.g., restore from backup)
- Simulate an incident and document response steps
- Review vendors' SOC 2 or security documentation and store it

Day 61–90: Prep for Readiness

- Finalize and version all policies
- Ensure evidence exists for all key controls
- Document your offboarding process
- Conduct an internal readiness check using SOC 2 criteria
- Schedule a readiness review with an advisor or auditor
- Prepare a SOC 2 FAQ or talking points for your sales team

For more support, visit Impact Risk Advisors