

Continuous Compliance Checklist

Upgrading your compliance strategy is a complex undertaking, but this checklist helps teams cover every critical requirement.

01 Policy Management

- ☐ Ensure all policies are clear and accessible
- ☐ Set up automated reminders to ensure employees review and accept policy changes
- ☐ Schedule gap assessments to ensure policies reflect new and changing regulations
- ☐ Set up employee training on all necessary processes, like data handling

02 Data Management

- ☐ Make sure data is properly labeled and classified
- ☐ Set access controls and verify data is encrypted
- ☐ Make sure no sensitive data is stored unnecessarily
- ☐ Schedule regular data audits to confirm compliance

03 Vendor Management

- ☐ Set up security assessments to ensure vendors meet requirements
- ☐ Review contract clauses to ensure they include all necessary security frameworks
- ☐ Schedule regular tests or risk assessments to make sure vendors are compliant

04 Risk and Vulnerability Management

- ☐ Schedule assessments to help uncover potential risks
- ☐ Set up automations to identify vulnerabilities across all networks and applications
- ☐ Determine remediation priorities to ensure teams address the most vital risks first
- ☐ Document risks and vulnerabilities accordingly and define the mitigation or patch process

- ☐ Perform a risk analysis, including potential financial and operational impacts
- ☐ Schedule red team exercises to validate your processes and identify possible attack paths

05 Incident Management

- ☐ Set up continuous monitoring
- ☐ Review incident response procedures to ensure they're comprehensive and up to date
- ☐ Configure alerts to notify all necessary personnel
- ☐ Review incident remediation to ensure alerts were delivered as intended and teams followed proper protocol

06 HR Management

- ☐ Ensure onboarding and offboarding processes align with compliance requirements
- ☐ Set up necessary workflows and automations to support compliant onboarding and offboarding
- ☐ Schedule reviews to ensure employees have completed training on security, privacy, and regulatory policies
- ☐ Schedule reviews to ensure employee data access aligns with their role

07 Business Continuity Management

- ☐ Identify the processes and systems that have the most significant business impact (and should be restored first if you experience downtime)
- ☐ Review your disaster recovery plans to ensure they follow compliance and are up to date
- ☐ Schedule exercises and drills to identify potential challenges or process bottlenecks

Keep in mind that this is just an example and meant to serve as a template. Your checklist may look different depending on your frameworks, internal policies, and the industries you serve.