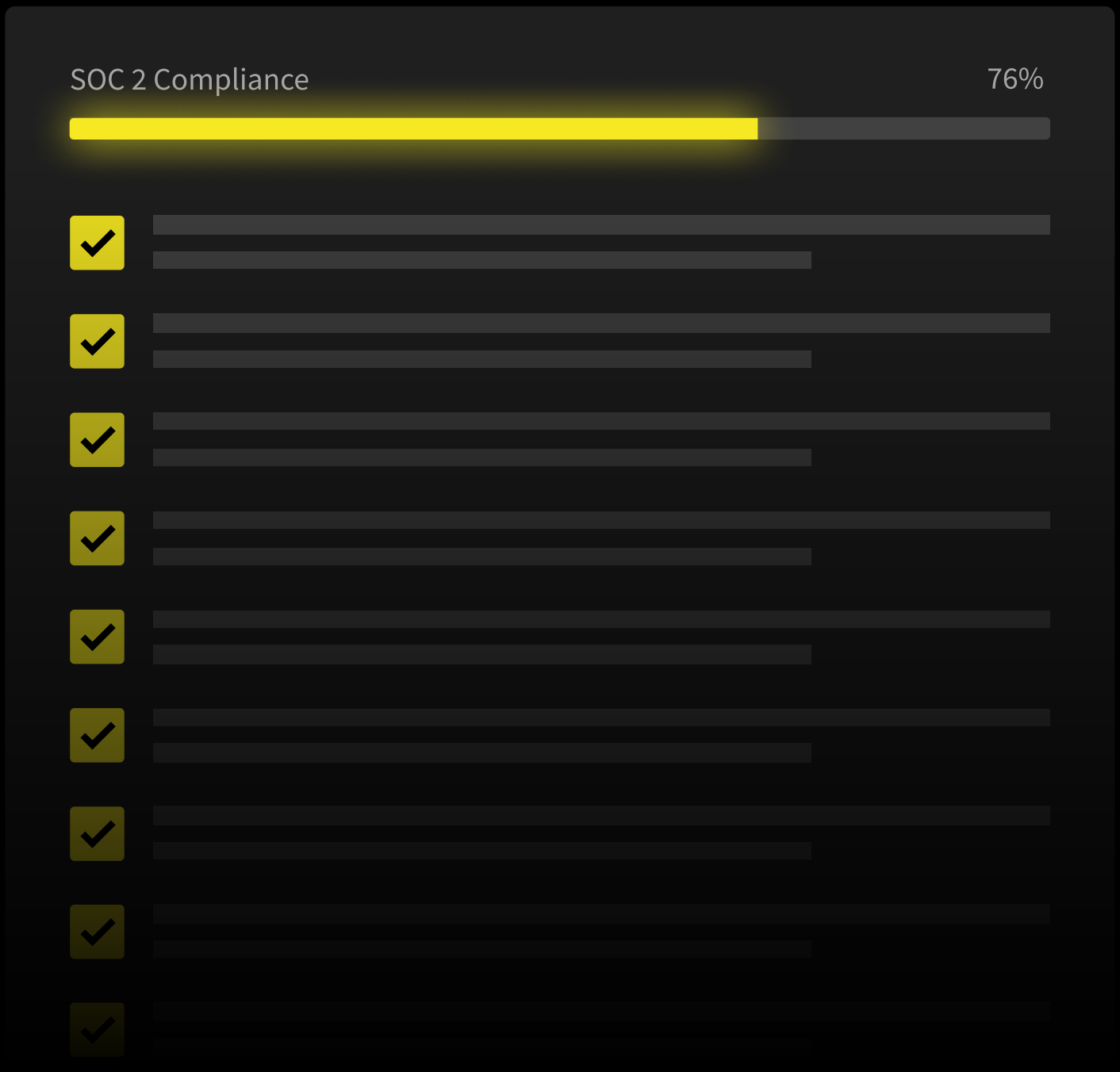
hicomply

The Ultimate SOC 2 Compliance Checklist

Build Trust and Protect Sensitive Data



Build Trust and Protect Sensitive Data

SOC 2 compliance isn't just a checkbox exercise: it's your proof that customer data is secure, your systems are resilient, and your business can be trusted. Whether you're working toward **SOC 2 Type 1** (a snapshot of compliance) or **Type 2** (continuous adherence over time), getting it right means fewer security gaps, streamlined audit readiness, and stronger customer confidence. Furthermore, Type 2 compliance requires permanent and ongoing security control evidence collection.

To make the process smoother and stress-free, this **comprehensive checklist**—enhanced with **Hicomply's compliance automation features**—will guide you through every step, ensuring you're always audit-ready.

Step 1

Define Your Compliance Scope

- [ ] **Know your "Why"** – Are you pursuing SOC 2 to win more deals? Meet regulatory requirements? Strengthen security? This is what is known as your "Scope".
- [ ] **Choose your Trust Services Criteria (TSC)** – Every SOC 2 audit includes **Security**, but do you need:
  - **Availability** (for uptime-sensitive services)
  - **Confidentiality** (for handling sensitive data)
  - **Processing Integrity** (for accurate data processing)
  - **Privacy** (for personal data protection)
- [ ] **Define your audit boundaries** – Which systems, tools, and teams fall under SOC 2?

How Hicomply Assists:

- [ ] Hicomply's ISMS Scoping Tool helps you plan your path to SOC 2 reporting by defining requirements and building an Information Security Management System (ISMS) tailored to your business.

15% completed

Step 2

Build Your Compliance Foundation

- [ ] **Establish internal champions** – Designate SOC 2 leads across IT, security, HR, and compliance.
- [ ] **Create policies that matter** – Define policies for security, access controls, data handling, and risk management.
- [ ] **Train your team** – Ensure every employee understands their security responsibilities; role-based security training is essential.
- [ ] **Implement background screening** – Vetting new hires before they handle sensitive data is crucial.

How Hicomply Assists:

- **Automated policy, procedure and record management** – Save hours with pre-written policies and procedures tailored to SOC 2. Automate updates, approvals, and distribution to ensure compliance without the headaches.
- **Dashboard with real-time monitoring** –Track risks, incidents, and compliance status in real-time. Tailored staff dashboards ensure everyone knows what they need to do to keep your organisation on track.

30% completed

Step 3

Conduct an Internal Audit (Gap Analysis or Readiness Assessment)

- [ ] **Identify security gaps before your auditor does** – Perform an internal audit to provide a gap analysis to uncover missing evidence and test controls.
- [ ] **Test your security measures** – Simulate security incidents, conduct penetration testing, and audit controls in real time.
- [ ] **Close compliance gaps** – Address weaknesses before the 3rd party external audit.

How Hicomply Assists:

- Hicomply's c**omprehensive risk management** tool allows you to manage risks seamlessly, fully integrated with your asset register, ensuring alignment with SOC 2 controls.
- Hicomply is unique in providing a full internal audit tools set that can be used to audit single, groups or or controls. Guidance on audit criteria is embedded into the platform.

45% completed

Step 4

Implement Strong Security Controls

- [ ] **Access controls** – Restrict system access to only those who need it—no exceptions.
- [ ] **Multi-Factor Authentication (MFA)** – Required for all critical systems.
- [ ] **Physical security** – Limit access to sensitive locations (server rooms, data centers).
- [ ] **Vendor management** – Assess third-party security risks regularly.
- [ ] **Audit logging & monitoring** – Track access and changes to critical systems in real-time.
- [ ] **Incident response plan** – Establish a clear process to detect, respond to, and recover from security incidents.

How Hicomply Assists:

- [ ] Hicomply integrates with leading business tools including HR, documents, helpdesk, project and task management, SaaS platforms, and identity providers: automating the tedious work of collecting evidence. From third-party risk checks to security controls, everything is tested and tracked continuously to keep your SOC 2 journey smooth and efficient.

60% completed

Step 5

Document Everything (The Audit-Proof Strategy)

- [ ] **Maintain records of system changes, access logs, and security reviews** – Auditors require comprehensive documentation.
- [ ] **Store evidence for Type 2 audits** – Ensure compliance records cover the full audit period.
- [ ] **Version-control your policies** – Keep policies up-to-date, reviewed annually, and easily accessible.

How Hicomply Assists:

- [ ] **Audit-ready documentation** – Generate detailed, organised reports for auditors at the click of a button. Hicomply keeps all your evidence stored and accessible, making the SOC 2 reporting process stress-free. Hicomply uniquely provides a published auditor ready control matrix or “statement of control applicability” at the push of a button.
- [ ] **Automated evidence collection** – Hicomply automates the collection and organisation of compliance evidence, ensuring you’re always prepared for audits.

75% completed

Step 6

Test, Review, and Stay Compliant

- [ ] **Perform regular risk assessments** – Identify new threats and update controls accordingly.
- [ ] **Simulate security incidents** – Run tabletop exercises to ensure your team is ready for real threats.
- [ ] **Review and update policies annually** – Compliance isn't a one-time task—make sure policies evolve with your business.
- [ ] **Automate compliance monitoring** – Use compliance automation tools to reduce manual work and maintain continuous audit readiness.

How Hicomply Assists:

- **Continuous compliance monitoring** – Hicomply automates real-time compliance tracking, alerting you to any control gaps before they become an issue.
- **Automated evidence collection** – Never scramble for evidence again—Hicomply gathers and stores compliance proof as you operate, keeping you always audit-ready.
- **Custom dashboards & alerts** – Stay on top of compliance requirements with personalised dashboards, automated workflows, and proactive alerts, ensuring you never miss an update.
- **Audit support & readiness reports** – Generate compliance reports instantly, keeping auditors happy and reducing back-and-forth requests.

100% completed

Pass Your SOC 2 Audit with Confidence

By following this checklist, you're not just getting SOC 2 compliant—you're building a security-first culture that customers and auditors will trust.

Need to automate your SOC 2 compliance process?

With Hicomply, you get an **all-in-one compliance automation platform** that streamlines SOC 2 from start to finish–helping you **secure sensitive data, demonstrate accountability, and strengthen your business.**

Say Hi to Faster, Smarter Compliance

Get a Demo