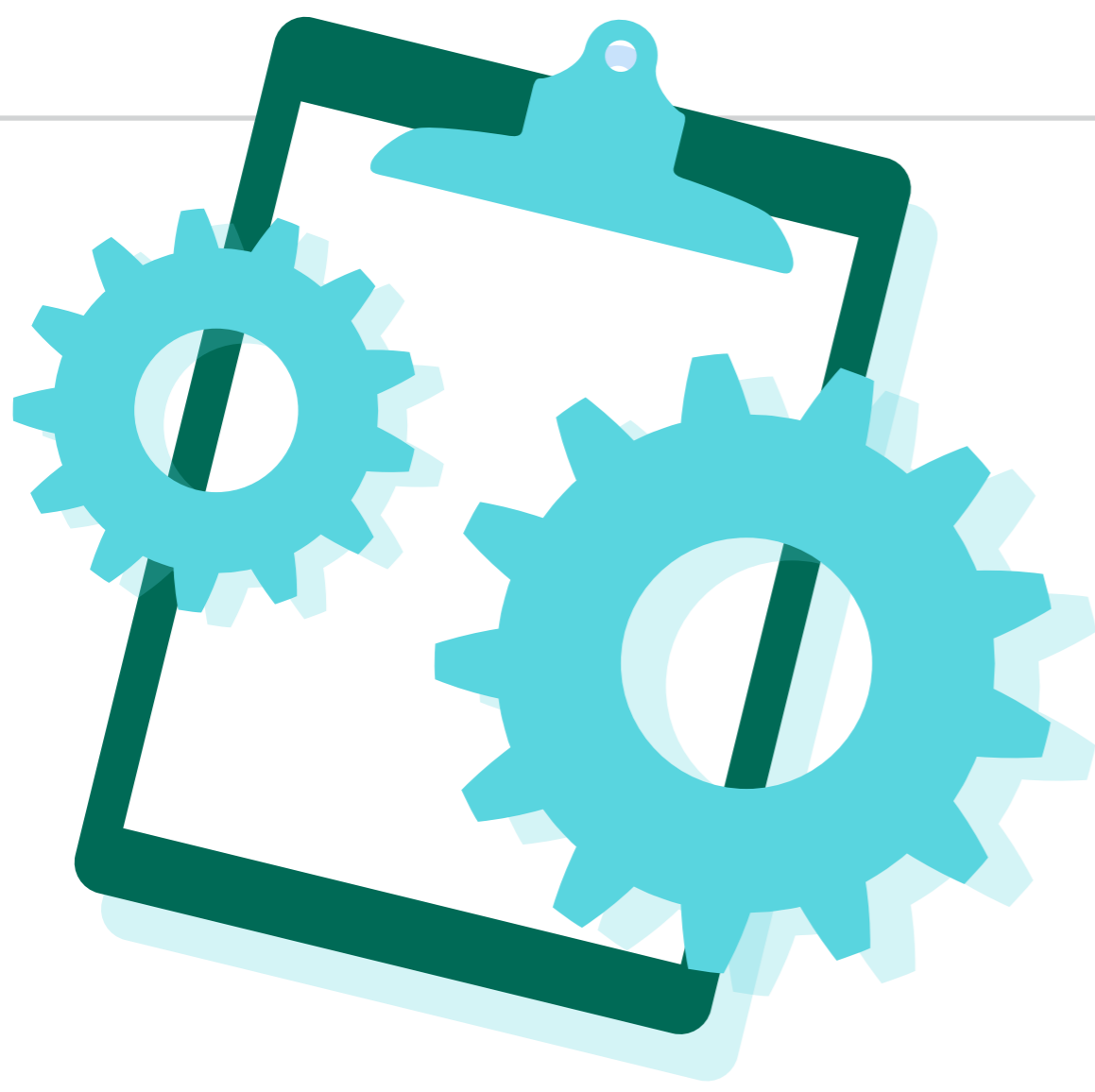




# SOC 2 COMPLIANCE CHECKLIST

SOC 2 compliance demonstrates to consumers that you take data protection seriously. It shows you're willing to go beyond basic compliance requirements to ensure their data is safe and secure in the face of ever-evolving security threats. It's important to note that SOC 2 audit reports can only be conducted by an independent CPA or CPA firm. **Here's how to obtain SOC 2 compliance:**


 Conduct a **self-assessment of your organization** to identify any security gaps you can address prior to the actual audit.



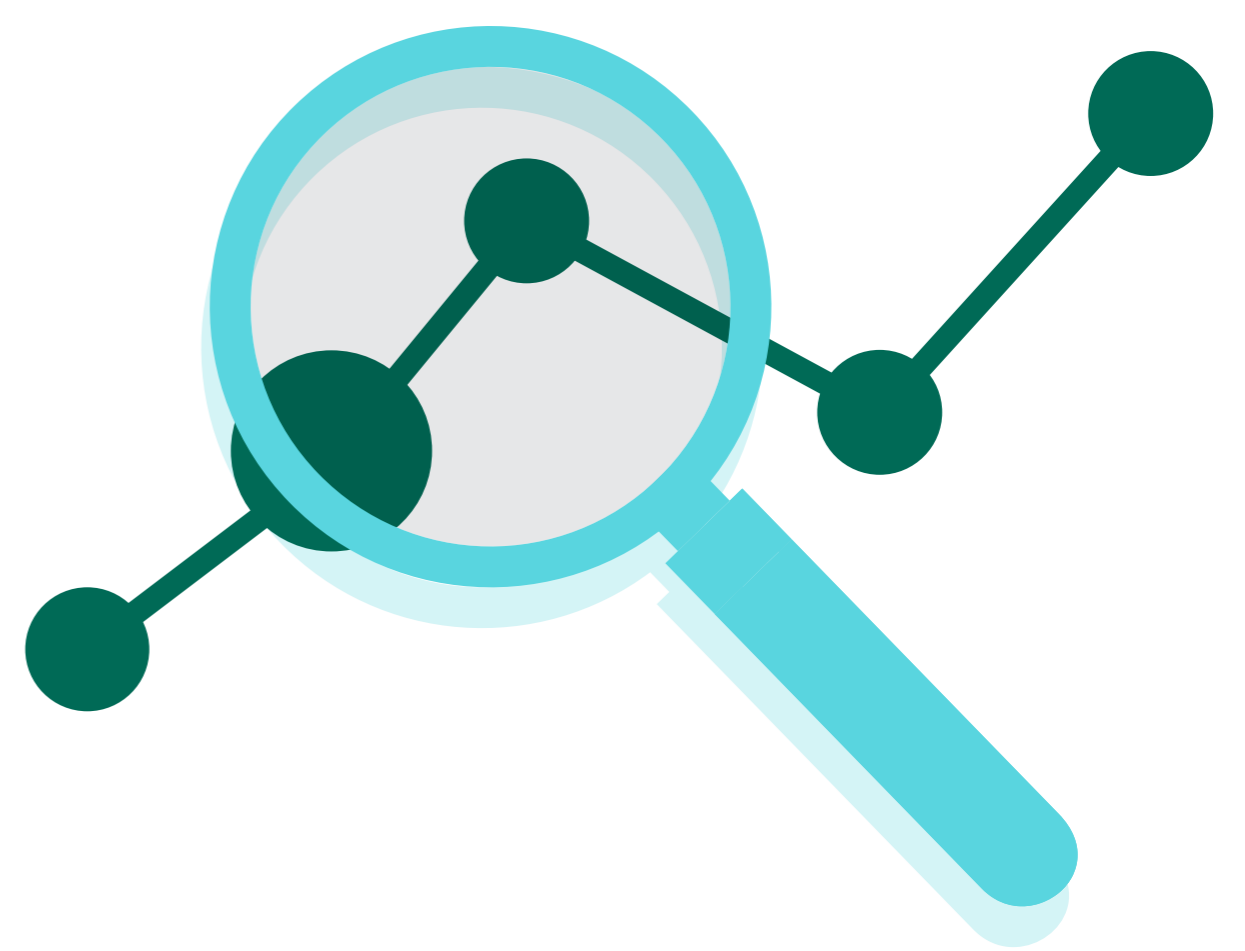
 Plan a **scope of work** so auditors know exactly which parts of the organization they need to assess.

 Select **type II audit report**. This type of SOC 2 audit will assess the organization's security posture over a period of time, usually between three and six months.



 Select any of the **5 SOC 2 trust principles** you want to test. These include security, availability, processing integrity, confidentiality, and privacy.

 Evaluate your **security controls, processes and procedures**. It will be important to provide this information to SOC 2 auditors.



 Consult a **cybersecurity expert** to ensure your security controls are able to meet the latest security challenges.

## FORTRA

At Fortra's Alert Logic, we provide unrivaled security for any environment. Learn how managed detection and response (MDR) solutions empower and expedite security compliance.

[alertlogic.com/managed-detection-and-response/compliance](https://alertlogic.com/managed-detection-and-response/compliance)