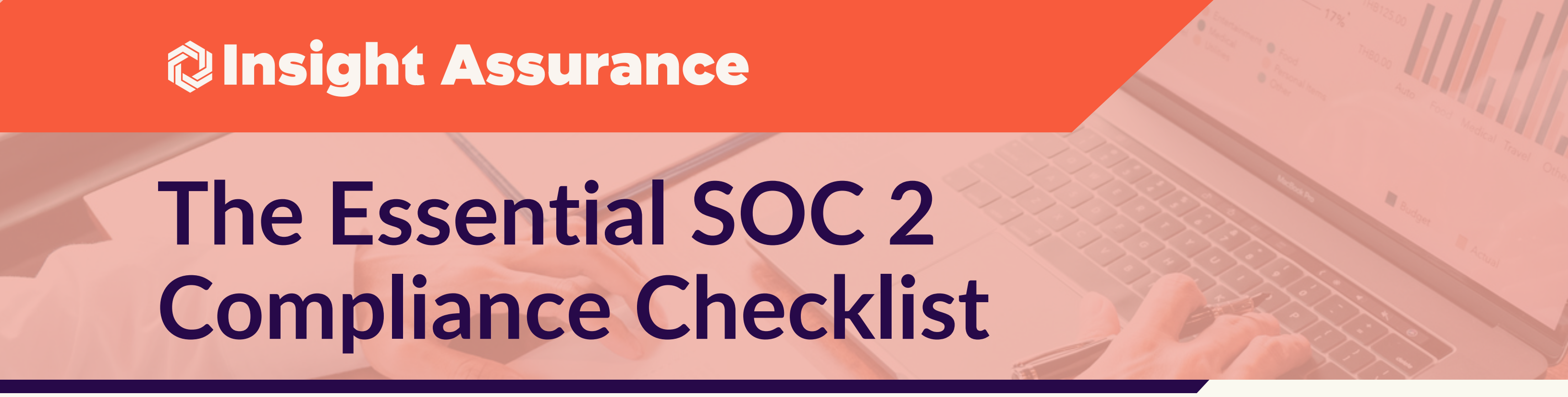
Insight Assurance



The Essential SOC 2 Compliance Checklist

With more companies using cloud services and working with outside vendors, SOC 2 compliance has become really important to show that a business is committed to protecting customer data and keeping it secure.

A good SOC 2 compliance checklist will list all the controls, policies, and procedures a company needs to have in place to meet the five SOC 2 trust services criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. This checklist will walk you through the key steps to get ready for a SOC 2 audit. For details on each area of the checklist, visit the corresponding blog post:

Policy and Procedure Documentation

- **Develop comprehensive security policies** (The policies should cover key areas like data management, access controls, and incident response)
- **Document procedures that enforce these policies** (Including steps for handling data, protocols for breach response, and guidelines for regular security assessments)

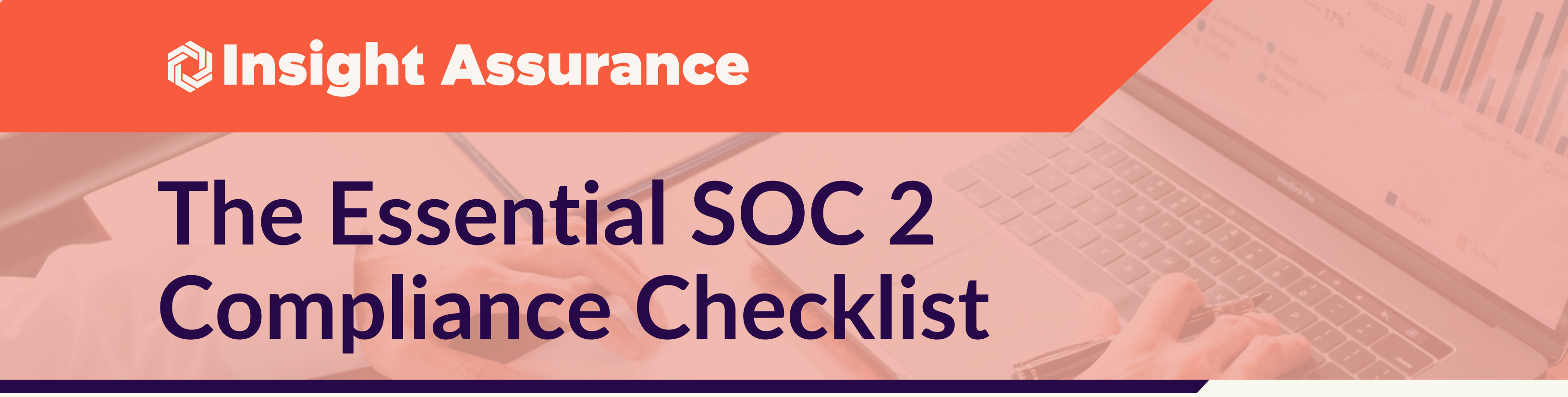
Implementing Security Controls

- **Access controls** (Including multi-factor authentication, secure passwords, and regularly reviewing who has access permissions)
- **Network security measures** (Including firewalls, intrusion detection systems, secure VPNs, etc.)
- **Encryption of data in transit and at rest** (Be sure to use strong encryption protocols like AES-256 to keep data secure)

Risk Management

- **Identifying and assessing risks** (Identify and prioritize the biggest risks to your IT systems and data practices)
- **Implementing a risk mitigation strategy** (Could involve using technology, changing internal processes, or continuous IT system monitoring)

Contact Us ☎ +1 877-607-7727 | ✉ sales@insightassurance.com



The Essential SOC 2 Compliance Checklist

Vendor Management

- **Assessing third-party vendors' compliance** (Their security policies, procedures, and controls should align with your standards)
- **Vendor risk management** (continuously monitor and assess the security of all your third-party providers with regular audits and updates to security requirements as needed)

Employee Training and Awareness

- **Regular training on security policies and procedures** (Keep employees informed about the latest security policies and procedures)
- **Phishing and security breach response training** (Train employees to recognize phishing attempts and how to respond to security breaches)

Incident Response Plan

- **Developing and documenting an incident response plan** (Should include steps to take during a security breach and damage mitigation procedures)
- **Regular testing of the incident response plan** (Frequent incident response drills ensure that employees know what to do)

Audit Preparation

- **Selecting a qualified auditor** (Should be an SOC 2 auditor who's familiar with your industry)
- **Gathering evidence and documentation for the audit** (Including but not limited to security policies, risk assessments, incident response plans, and compliance training records)

Ready to navigate the complexities of SOC 2 compliance with confidence? Contact the experts at Insight Assurance for personalized guidance or to connect with a qualified SOC 2 auditor. Let us help you secure your systems and meet compliance standards seamlessly.