AVERTIUM

SOC AUDIT REPORT SERVICES

ENSURE CUSTOMER CONFIDENCE, WIN MORE BUSINESS

Increasing cybersecurity threats pose a unique concern for those who outsource their business operations to companies that provide financial and technology-related third-party services. In turn, a service organization keeping or winning new business often requires proof of proper data management and protection.

A System and Organization Controls (SOC) report provides assurance to your customers and their auditors, investors and other stakeholders that the security and compliance controls you have in place are designed correctly and operating effectively to protect their systems or data you can access.

VALUE TO YOU: Avertium's qualified professionals carry the load to provide an independent third-party examination in partnership with an ecosystem of certified public accountants that makes SOC reporting easier so you can focus on your business and winning new customers.

		Readiness Assessment	Type 1 or Type 2
SOC 1	Tests internal control over financial reporting	✓	✓
SOC 2	Focuses on internal operational and IT controls	✓	✓
SOC 3	General use report to share and make freely available	✓	✓

> "I TRUST IMPLICITLY THE LEADERSHIP AND THE QUALITY OF RESOURCES THAT ARE BROUGHT TO THE TABLE. [THEY] ALWAYS ADVISE US IN THE DIRECTION OF A STRONG BALANCE BETWEEN HOW YOU MITIGATE RISK AND HOW YOU ALSO KEEP THE BUSINESS GOING."

- Avertium Customer

WHO NEEDS A SOC AUDIT REPORT?

SOC 1: Organizations that perform services with financial impact for clients such as payment processors, billing organizations, collections agencies and the CPAs that audit user entities' financial statements

SOC 2: Technology-based service organizations such as managed service providers, cloud service providers (Software as a Service, Infrastructure as a Service, etc.), and outsourced IT providers

SOC 3: SOC 2 service organizations who require both assurance about the controls relevant to the Trust Service Criteria and need reports that can be freely distributed

SOC2 + HITRUST

HITRUST
Authorized CSF Assessor

SOC 2 + HITRUST maps the HITRUST Common Security Framework (CSF) requirements to the AICPA's Trust Services Criteria. This allows your organization to report on controls that meet compliance for both standards and represent a secure environment with a unified report.

SOC 2 EXCEPTIONS REMEDIATION

For businesses who have SOC 2 exceptions, Avertium's highly certified experts remediate the findings found to have fallen outside expected results of an audit to set you on a path to success.

THE AVERTIUM ADVANTAGE

Attacking the chaos of the cybersecurity landscape takes context of your business, of your existing technology in cybersecurity, and of the threat landscape. Avertium's approach offers more flexibility, more control, and more resilience.

» KNOW THY SELF

Using proven frameworks like NIST CSF alongside our in-depth onboarding diagnostic, we get to know your business, your attack surface, your protocols, and your areas of greatest weakness + strength.

» KNOW THY ENEMY

Leveraging our cyber threat intelligence (CTI) alongside the MITRE ATT&CK framework, we then understand current and most likely future attack scenarios.

ABOUT AVERTIUM

Avertium is a cyber fusion and MXDR leader, delivering comprehensive security and compliance services to mid-market and enterprise customers. Our unique "Assess, Design, Protect" methodology addresses and improves security strategy, reduces attack surface risk, strengthens compliance, and provides continuous threat protection. Avertium maximizes customer security investments and enables customers to focus on growth, innovation, and business outcomes, while assuring that their security infrastructure is resilient and adaptive to evolving threats. That's why customers trust Avertium to deliver better security, improved compliance, and greater ROI.