ENCRYPTION CONSULTING

CASE STUDY

COMPLIANCE SERVICE

Bringing an online retailer up to SOC 2 with a full encryption audit

A global online retailer with over 10,000 employees needed SOC 2 compliance across all five trust service criteria. Our encryption audit exposed the gaps, from certificate failures to vendor risk, and mapped a clear path to compliance.

SECTOR	SIZE	ENGAGEMENT
Online retail	10,000+ employees	SOC 2 compliance audit

SOC 2
Compliance achieved

5
Trust service criteria met

Automated
Certificate lifecycle

A global online retailer, built on customer trust

Our client is an international online retail platform selling flagship products, electronics, and premium high-fashion apparel. Known for an uncompromising focus on customer experience, it serves millions of consumers across the United States and has become a primary choice for premium online shopping.

With more than 10,000 employees, the company is in constant demand, from fast delivery of premium brands to personal shopping experiences. As it expands its customer base and services, it handles a great deal of sensitive data, including personal and financial details, purchase history, login credentials, and biometric data, all of which it is committed to protecting.

For an online retailer trusted with biometric and financial data, SOC 2 isn't a checkbox. It's the proof that customer data is genuinely safe.

Compounding gaps, across the whole estate

A SOC 2 readiness audit found overlapping weaknesses across certificates, governance, vendors, and incident response.

1

Certificate failures

Recurring certificate expirations caused service outages and reputation damage, driving operational costs up 15% through emergency recovery and leaving data exposed.

2

Fragmented governance

Every system had its own encryption and access policies, with no central governance, making it nearly impossible to know who could reach sensitive data.

3

Non-compliant vendors

Payment and cloud vendors with access to PII failed SOC 2, using weak algorithms like DES, loose access controls, and slow patching.

4

No incident response

Without solid incident response plans or risk assessment, the firm couldn't reliably detect, contain, or respond to emerging threats.

5

None of the five trust criteria met

Together these gaps weakened monitoring and access control across the IT estate, leaving the company unable to satisfy any of SOC 2's five trust service criteria: security, availability, processing integrity, confidentiality, and privacy.

> The gaps weren't isolated: certificate failures, fragmented governance, non-compliant vendors, and absent incident response plans all compounded into a compliance posture that couldn't meet any of SOC 2's five trust service criteria.

ENGAGEMENT SUMMARY | ENCRYPTION CONSULTING · COMPLIANCE SERVICES

From audit to SOC 2 readiness

We audited the retailer against all five SOC 2 criteria, then delivered a customized report, strategy, and roadmap covering certificates, governance, vendors, and incident response.

Audit across five criteria

We assessed their environment against all five SOC 2 trust criteria: security, availability, processing integrity, confidentiality, and privacy.

Automated certificate lifecycle

We recommended CertSecure Manager to automate the full certificate lifecycle with real-time monitoring, alerts, and renewals, ending the outages.

Centralized governance and access

We replaced scattered, per-system policies with centralized governance and proper access controls, so access to sensitive data is known and controlled.

Gap analysis and roadmap

A detailed compliance gap analysis pinpointed where SOC 2 wasn't met, paired with a prioritized roadmap for the internal teams.

Vendor risk framework

We assessed every vendor's controls, RBAC, MFA, and incident response, and provided a structured framework with accountability and periodic audits.

Monitoring and incident response

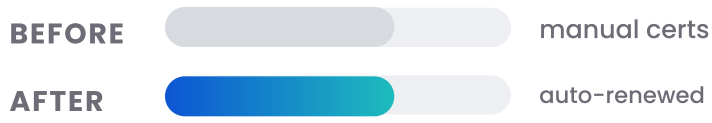
We recommended continuous monitoring and logging tools plus clear incident response workflows for threat detection, response, and mitigation.

Fewer outages, and full SOC 2 alignment

The roadmap closed the gaps and steadied operations, taking the retailer from scattered controls to SOC 2 compliance across all five criteria.

30%

Fewer service interruptions after automation



Always-on operations

Automated certificate monitoring and renewal keep the platform running smoothly, meeting SLAs and protecting customer trust.

Vendors aligned to SOC 2

A structured vendor risk framework brought third parties in line with SOC 2, shrinking risk across the supply chain.

Stronger, future-proof security

Scalable encryption, advanced access controls, and stronger algorithms harden the platform against evolving threats.

SOC 2 compliant

Meeting all five trust service criteria turned compliance into a foundation for growth and lasting customer trust.

IN SUMMARY

SOC 2 compliance, a foundation for growth

For an online retailer, SOC 2 is more than a milestone; it is the building block of customer trust and competitive advantage. Our audit and support services gave the client a clear, prioritized roadmap covering certificates, governance, vendors, and incident response. Automated certificate management cut service interruptions by 30%, centralized governance and stronger encryption hardened the platform, a structured framework brought vendors in line with SOC 2, and improved incident response keeps threats contained. The result is a SOC 2 compliant business with a more resilient, future-ready foundation, and the trust to keep growing.

GET STARTED

Get audit-ready for SOC 2.

Talk to our Compliance team →