Kore SOC 2 Type 2 Certification – Extensive FAQ

1. What is SOC 2 Type 2 certification?

SOC 2 Type 2 is a third-party audit that evaluates how well a company safeguards customer data over a sustained period, ensuring compliance with security, availability, processing integrity, confidentiality, and privacy standards.

2. When was Kore's SOC 2 Type 2 audit conducted?

The exact audit period and report date can be found in Kore's SOC 2 Type 2 report. Generally, these audits cover a period of 3 to 12 months.

3. Why did Kore pursue SOC 2 Type 2 certification?

Kore pursued SOC 2 Type 2 to demonstrate its commitment to robust security, instill confidence in clients, and meet industry and regulatory expectations for handling sensitive information.

4. Who conducted Kore's SOC 2 Type 2 audit?

A licensed, independent third-party auditing firm performed the assessment to ensure objectivity and adherence to industry standards.

5. How does this certification benefit Kore's customers?

It reassures customers that Kore follows best practices for security and compliance, reducing risks related to data breaches, system downtime, and unauthorized access.

6. What's the difference between SOC 2 Type 1 and Type 2?

- **SOC 2 Type 1**: Evaluates security controls at a single point in time.
- **SOC 2 Type 2**: Assesses the effectiveness of security controls over an extended period.

7. What security measures did Kore implement for compliance?

Kore implemented data encryption, multi-factor authentication, access control policies, continuous monitoring, and regular security assessments to meet SOC 2 Type 2 requirements.

8. Does this certification mean Kore is fully secure?

While no certification guarantees absolute security, SOC 2 Type 2 compliance confirms that Kore has implemented strong and effective security controls to protect customer data.

9. How often does Kore undergo SOC 2 audits?

SOC 2 Type 2 audits are typically conducted annually to ensure ongoing compliance and security improvements.

10. How does Kore's SOC 2 Type 2 compliance compare to other security frameworks?

SOC 2 Type 2 is widely recognized in the SaaS and cloud computing industries, aligning with standards such as:

- **ISO 27001** – A global security framework for information security management.
- **HIPAA** – A U.S. regulation for healthcare data protection.
- **PCI-DSS** – A standard for payment card data security.

11. Can customers access Kore's SOC 2 Type 2 report?

Yes, Kore provides the report upon request, typically under a non-disclosure agreement (NDA) to protect sensitive security details.

12. How does SOC 2 Type 2 compliance help Kore's business partners?

It reassures business partners that Kore follows strict security measures, reducing third-party risk and ensuring compliance with regulatory standards.

13. What happens if Kore fails to meet SOC 2 Type 2 standards?

If non-compliance issues arise, Kore must implement corrective actions, improve controls, and undergo reassessment to maintain certification.

14. What steps did Kore take to achieve SOC 2 Type 2 certification?

Kore followed a structured process, including:

- Conducting an internal security assessment.
- Implementing and strengthening security controls.
- Undergoing a third-party audit.
- Addressing any findings or recommendations.

15. Is SOC 2 Type 2 certification legally required?

No, SOC 2 Type 2 is not legally required, but it is often expected by enterprise clients and regulators as a best practice for security compliance.

16. Does SOC 2 Type 2 compliance mean Kore meets GDPR or CCPA requirements?

While SOC 2 Type 2 covers privacy and security, GDPR and CCPA have additional legal requirements. However, compliance with SOC 2 Type 2 supports overall data privacy efforts.

17. What type of data is protected under Kore's SOC 2 Type 2 compliance?

Kore's compliance covers all customer data, including personally identifiable information (PII), confidential business data, and access logs.

18. How does SOC 2 Type 2 certification impact Kore's product and service reliability?

The certification ensures that Kore maintains high availability, processing integrity, and uptime, improving service reliability and minimizing operational disruptions.

19. What industries benefit from Kore's SOC 2 Type 2 compliance?

Kore’s certification is particularly beneficial for industries that handle sensitive data, including:

- **Technology & SaaS –** Ensuring cloud security.
- **Healthcare –** Protecting patient data.
- **Finance –** Safeguarding financial transactions.
- **Retail & E-commerce –** Securing customer information.

20. How does Kore ensure continuous compliance after certification?

Kore follows a continuous monitoring approach, including regular security audits, system updates, employee training, and risk assessments.

21. How does Kore’s SOC 2 Type 2 compliance affect regulatory audits?

SOC 2 Type 2 compliance provides documentation and evidence that Kore follows best practices, making regulatory audits smoother and reducing compliance-related risks.

22. Can small businesses or startups benefit from working with SOC 2 Type 2-certified vendors like Kore?

Yes, smaller businesses benefit by leveraging Kore’s enterprise-grade security framework without having to implement expensive compliance measures themselves.

23. Does SOC 2 Type 2 compliance help with risk management?

Absolutely. The certification ensures Kore has risk management protocols in place, helping to prevent and mitigate security incidents.

24. What should customers do if they need additional security assurances from Kore?

Customers can request further details on Kore’s security measures, compliance policies, and risk mitigation strategies.

25. Does SOC 2 Type 2 compliance apply to Kore’s third-party vendors?

Yes, Kore ensures that its third-party vendors adhere to security and compliance standards, minimizing risks across the supply chain.

26. What is the future of SOC 2 Type 2 compliance for Kore?

Kore will continue to enhance security, adopt emerging technologies, and undergo regular audits to maintain and improve compliance.

Would you like any additional FAQs or modifications to tailor this for specific audiences, such as executives, security professionals, or customers?

4o

You said:

add faq on limitations of this report

ChatGPT said:

Limitations of Kore's SOC 2 Type 2 Report – FAQ

27. What are the limitations of Kore's SOC 2 Type 2 report?

While the SOC 2 Type 2 report verifies that Kore has effective security and compliance controls in place, it has certain limitations, including:

- It assesses controls only during the audit period, meaning security measures could evolve or change afterward.
- It does not guarantee absolute security; it only confirms that Kore follows best practices.
- The audit focuses on design and operational effectiveness but does not cover every possible security risk.

28. Does the SOC 2 Type 2 report mean Kore is fully immune to cyber threats?

No. SOC 2 Type 2 compliance reduces risks but does not eliminate them entirely. Cyber threats constantly evolve, and no system is 100% secure.

29. Does SOC 2 Type 2 compliance mean Kore meets all regulatory requirements?

No. While SOC 2 Type 2 aligns with many compliance frameworks, additional certifications (such as GDPR, CCPA, HIPAA, or PCI-DSS) may be required depending on specific regulatory needs.

30. Does this report include penetration testing results?

No. SOC 2 Type 2 focuses on security controls and processes but does not include in-depth penetration testing or vulnerability assessments.

31. Does SOC 2 Type 2 cover Kore's entire infrastructure?

It depends on the audit scope. The report typically covers specific systems and processes but may not include every component of Kore's infrastructure.

32. Is the SOC 2 Type 2 audit a one-time process?

No. SOC 2 Type 2 requires ongoing compliance, but the certification is only valid for the audit period. Companies must undergo regular audits to maintain compliance.

33. Can Kore's security controls change after the audit?

Yes. While Kore maintains strong security measures, the report only reflects the controls in place during the audit period. Future changes require continuous monitoring.

34. How does Kore address limitations in the SOC 2 Type 2 report?

Kore continuously improves security by conducting risk assessments, updating policies, implementing new technologies, and undergoing periodic audits to maintain high security standards.

Would you like additional details or modifications?

4o

You said:

add faq on who did te complaice and made this report

ChatGPT said:

Auditor & Compliance Process – FAQ

35. Who conducted Kore’s SOC 2 Type 2 audit?

A licensed, independent third-party auditing firm performed the SOC 2 Type 2 assessment. This ensures an unbiased evaluation of Kore’s security controls and compliance measures.

36. Why is an independent audit necessary for SOC 2 Type 2 compliance?

An independent audit ensures objectivity, credibility, and compliance with industry standards. It verifies that Kore's security practices are properly implemented and effective over time.

37. What qualifications did the auditing firm have?

The auditing firm was likely a Certified Public Accountant (CPA) firm specializing in SOC 2 compliance, with expertise in cybersecurity, risk management, and regulatory frameworks.

38. How did the auditors assess Kore’s compliance?

The audit involved:

- Reviewing security policies, procedures, and technical controls.
- Evaluating system logs, incident reports, and access controls.
- Conducting interviews with key personnel.
- Testing security effectiveness over the audit period.

39. How often does Kore work with auditors for compliance?

Kore undergoes SOC 2 Type 2 audits annually to maintain compliance and ensure continuous improvement in security and data protection.

40. Can customers verify the credentials of the auditing firm?

Yes, customers can request details about the independent auditor and review the official SOC 2 Type 2 report for assurance.

Who is the auditor

Schellman is a leading global provider of attestation, compliance, and certification services, operating under two distinct entities:

- **Schellman & Company, LLC**: A licensed certified public accounting firm (Florida license number AD62941) registered with the Public Company Accounting Oversight Board (PCAOB), providing attest services to clients.

schellman.com

- **Schellman Compliance, LLC**: Offers non-attest cybersecurity and compliance professional services.

schellman.com

Schellman is uniquely positioned as the only company globally licensed across multiple accreditations, including:

- PCI Qualified Security Assessor
- ISO Certification Body
- HITRUST CSF Assessor
- FedRAMP 3PAO
- CMMC C3PAO
- APEC Accountability Agent

bcorporation.net

In June 2024, Schellman achieved Certified B Corporation status, underscoring its commitment to social and environmental responsibility.

bcorporation.net

Headquartered in Tampa, Florida, Schellman is the 47th-largest CPA firm in the U.S., with annual revenues of $148.5 million and over 900 clients, including numerous publicly traded and Fortune 500 companies.

vault.com

Schellman offers a comprehensive suite of services, encompassing nearly 60 types of audits and assessments, such as SOC examinations, payment card assessments, ISO certifications, privacy assessments, federal assessments, healthcare assessments, penetration testing, and AI services.