

January 8, 2025 AuditOne LLP Q1 2025 Update:

Happy 2025! I can't believe it's been 25 years since the Y2K event. I was a network engineer back then. Expecting the worst but hoping for the best.

At AuditOne LLP, we officially became an ISO/IEC certification body as of January 1, 2025. We are currently working with two clients on ISO/IEC 27001:2022 projects. Our team has put in a lot of work to learn the various ISO standards to conform to the requirements of becoming a certification body. Even I took the ISO Lead Implementer and ISO Lead Auditor training courses. It has been a busy quarter.

AuditOne LLP Services:

- AICPA SOC 1, SOC 2, SOC 3 Attestation Reports
- ISO/IEC 27001:2022 Stage 1, Stage 2, and Surveillance Reviews
- HIPAA, CCPA, GDPR Privacy Audits

Security Questionnaires

Some of our clients receive dozens of security questionnaires on an annual basis. A SOC 2 report with a signed NDA, or a SOC 3 report can, and should replace many end customer security questionnaires. The following is a great example from our client Bitwarden of how they promote their SOC 2 and SOC 3 reports. <https://bitwarden.com/compliance/>

Section 5

Section 5 of a SOC 2 report is where clients normally respond to exceptions noted in the report. Section 5 can also be used to include any non-auditable information you would like to add to the SOC report. For example, you could add a penetration test summary, a risk assessment summary, your BCP, or your entire Information Security Program. Please keep this in mind during your next SOC audit.

Post Audit Tasks

At the conclusion of each audit, we provide a final version of the audit work program and best practice improvement suggestions. Please use this version of the work program for the next audit planning. Often the control numbering has been updated with this final version.

Ongoing Controls Review

No one wants exceptions in their audit report. Please review your SOC controls on an ongoing basis to ensure your processes are current and operating effectively. Please use these quarterly newsletters as a reminder to review your controls.

Please reach out if you have any questions.

Robert Kluba CISM CISSP ASOCC
Managing Director
Phone: 408.656.9300

Robert.Kluba@AuditOneLLP.com
<https://www.AuditOneLLP.com>