SAMPLE — PLEASE UPDATE ACCORDING TO YOUR RELEVANT ENGAGEMENT INFORMATION

Here's What [COMPANY NAME]'s ISO/IEC 27001 Certification and SOC 2 Report Mean For You

[COMPANY NAME] recently announced that we've achieved ISO/IEC 27001 certification and completed a SOC 2 [Type 1/Type 2] report. But what do these accomplishments mean for us as an organization—and for you as our customer?

At [COMPANY NAME], keeping customer and stakeholder data secure is our top priority. To demonstrate that our systems and controls have been designed appropriately to achieve that goal, we pursued two highly-regarded independent assessments of our cybersecurity posture.

In this blog post, we'll explain what ISO/IEC 27001 certifications and SOC 2 reports are, and why we chose to undergo these rigorous compliance audits.

WHAT IS ISO/IEC 27001?

Considered the gold standard in information security, ISO/IEC 27001 is an internationally accepted compliance standard that mandates numerous controls for the establishment, operation, monitoring, maintenance, and continual improvement of an Information Security Management System (ISMS).

The certification attests that an organization has deep-rooted methodologies for business, people, and IT processes, along with an established framework to help identify, manage, and reduce risks surrounding information security.

In simpler terms, achieving ISO/IEC 27001 certification demonstrates that an organization adheres to industry standards for designing, maintaining, and continuously improving their security posture.

Pursuing ISO/IEC 27001 certification is a multi-step process that begins with an internal audit assessing whether an organization's ISMS has been developed, implemented, and maintained in accordance with the organization's own standards, as well as those defined by ISO and the International Electrotechnical Commission (IEC).

Following the internal audit, organizations pursuing ISO/IEC 27001 certification are ready to begin the two-stage remediation and certification process, commonly known as the "certification audit."

During Stage 1, an accredited third-party auditor tests the *design* of the organization's ISMS, including reviewing documentation, identifying potential nonconformities, and evaluating the organization's plan to remediate any issues. Organizations that successfully complete Stage 1 then move on to Stage 2, where the auditor tests the *effectiveness* of the ISMS, including ensuring areas of concern have been remediated.

At the conclusion of both stages, the auditor reviews the results of their assessments and makes a final decision on certification.

WHAT IS A SOC 2 REPORT?

Obtaining a System and Organization Controls (SOC) 2 report is another way for a service organization to attest to the security of its digital environment.

Unlike ISO/IEC 27001, completing a SOC 2 examination through an accredited third-party auditor does not result in any certification. Instead, the resulting CPA's report functions as a tool to help an organization communicate whether the internal controls they've put in place governing the security of customers', partners', and stakeholders' data are properly designed, implemented, and maintained.

In simpler terms, a SOC 2 report provides an avenue for current and potential stakeholders to assess risk by giving them a closer look at the policies and procedures put in place to ensure the organization's services are provided safely and reliably.

All SOC 2 examinations are performed by accredited CPA firms under the standards defined by SSAE 18. An auditor tests the effectiveness of the internal controls outlined by the organization, then maps those controls to one or a combination of Trust Services Criteria established by the American Institute of Certified Public Accountants (AICPA).

In our case, [that criterion includes/those criteria include]:

- **Security**: The system is protected against unauthorized access (both physical and logical).
- **Availability**: The system is available for operation and use as committed or agreed.
- **Processing Integrity:** System processing is complete, valid, accurate, timely, and authorized to meet the entity's objectives.
- **Confidentiality**: Information designated as confidential is protected as committed or agreed.
- **Privacy:** Personal information is collected, used, retained, disclosed, and disposed of to meet the entity's objectives.

The scope of a SOC 2 report can also vary with regard to the time period covered.

[INCLUDE ONLY IF APPLICABLE] SOC 2 Type 1 reports examine an organization's controls at a single point in time and include a list of the controls tested.

[INCLUDE ONLY IF APPLICABLE] SOC 2 Type 2 reports examine controls over a period of time, usually between three and 12 months, and include both a list of the controls tested as well as the auditor's test results. The reporting period for [COMPANY NAME]'s latest SOC 2 report spanned from [DATE] to [DATE].

WHY DID WE PURSUE ISO 27001 AND SOC 2 COMPLIANCE?

Achieving certification against the internationally recognized ISO 27001 standard marks a huge step forward in [COMPANY NAME]'s efforts to ensure that we're prepared to face the challenges of the ever-changing cybersecurity landscape. In addition, completing a SOC 2 [Type 1/Type 2] examination helps cement our ongoing commitment to data security.

“Achieving ISO 27001 certification and completing a SOC 2 examination is a huge accomplishment for [COMPANY NAME] that shows our unwavering commitment to securing and protecting the data of our valued customers,” said [COMPANY REPRESENTATIVE NAME AND TITLE]. “We hope these attestations inspire confidence and assure our customers and partners that we view data security as a top priority.”

WHERE CAN I GO FOR MORE INFORMATION?

Current and prospective customers interested in a copy of [COMPANY NAME]’s SOC 2 [Type 1/Type 2] report and/or our ISO/IEC 27001 certification report may contact [NAME] at [PHONE/EMAIL].