SAMPLE — PLEASE UPDATE ACCORDING TO YOUR RELEVANT BUSINESS INFORMATION

[COMPANY NAME] Has Achieved ISO/IEC 27001 Certification. Here's What That Means For You.

[COMPANY NAME] recently announced that we've achieved ISO/IEC 27001 certification. But what does that 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 sought out an independent assessment from an accredited auditing firm, BARR Certifications.

In this blog post, we'll explain what it means to achieve ISO/IEC 27001 certification and why we chose to undergo this rigorous compliance audit.

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.

HOW DOES THE CERTIFICATION PROCESS WORK?

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.

WHY DID WE PURSUE ISO/IEC 27001 CERTIFICATION?

Achieving certification against this internationally recognized standard marks a huge step forward in [COMPANY NAME]'s efforts to cement our commitment to data security and ensure that we're prepared to face the challenges of the ever-changing cybersecurity landscape.

"Achieving ISO 27001 certification is a major milestone 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 this certification inspires confidence and assures our customers and partners that we view data security as a top priority."

WHERE CAN I GO FOR MORE INFORMATION?

Our auditor digs deeper into the steps involved in pursuing and achieving ISO 27001 certification in a series of blog posts:

- Everything You Need to Know About ISO 27001 Certification: Part 1—The Internal Audit
- Everything You Need to Know About ISO 27001 Certification: Part 2—Stage 1 and Stage 2

Current and prospective customers interested in a copy of [COMPANY NAME]'s ISO/IEC 27001 certification report may contact [NAME] at [PHONE/EMAIL].