

SAMPLE — PLEASE UPDATE ACCORDING TO YOUR APPLICABLE TRUST SERVICES CRITERIA AND COMPANY REPRESENTATIVE QUOTE

FOR IMMEDIATE RELEASE

[Month Day, Year]

[Company Media Contact]

[Company Name] Maintains Effective Security Controls According to Recent SOC 2 and SOC 3 Reports

[City, State] – [DATE] – Today, [Company Name] announced that the company has undergone a System and Organization Controls (SOC) 2 examination and a SOC 3 examination, each resulting in a CPA's report stating that management of [Company Name] maintained effective controls over the [insert applicable trust services criteria: security, availability, processing integrity, confidentiality, and privacy] of its [name of system] system. The engagements were performed by [BARR Advisory, P.A.](#)

A SOC 2 report is designed to meet the needs of existing or potential customers who need assurance about the effectiveness of controls used by the service organization to process customers' information. A SOC 3 report is similar in scope, but is shorter and allows for more general distribution.

"We are pleased that our SOC 2 and SOC 3 reports have shown we have the appropriate controls in place to mitigate risks related to [insert applicable trust services criteria: security, availability, processing integrity, confidentiality, and privacy], along with HIPAA Security Rule requirements," said [Insert name of company representative and title]. "[Insert explanation of why relevant principles are important to company business and client]."

The following principles and related criteria have been developed by the American Institute of CPAs (AICPA) for use by practitioners in the performance of trust services engagements:

- **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.*
- **HIPAA Security Rule Requirements:** *The system is compliant with the applicable HIPAA Security Rule requirements set forth in the U.S. Department of Health and Human Services' (HHS) Health Information Portability and Accountability Act.*

A SOC 2 report is an internal control report on the services provided by a service organization to its customers and provides valuable information that existing and potential customers of the service organization need to assess and address the risks associated with an outsourced service.

A SOC 3 report is a public-facing report for general use that communicates that an organization's controls are properly designed and implemented and operating effectively.

Current and prospective customers interested in a copy of our SOC 2 or SOC 3 reports may contact *[Insert contact name]*.

ABOUT *[Company Name]*

[Company Boilerplate]

[Company Logo]

ABOUT BARR Advisory

BARR Advisory is a cloud-based security and compliance solutions provider specializing in cybersecurity consulting and compliance for companies with high-value information in cloud environments like AWS, Microsoft Azure, and Google Cloud Platform. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements in highly regulated industries including technology, financial services, healthcare, and government.

BARR Advisory services include:

- Compliance Program Assistance
- SOC 1 Examinations
- SOC 2 and 3 Examinations
- SOC for Cybersecurity
- PCI DSS Assessment Services
- ISO 27001 and 27701 Assessments
- FedRAMP Security Assessments
- HIPAA/HITECH Services
- HITRUST Services
- Penetration Testing and Vulnerability Assessments
- Cybersecurity Consulting

