ICE
TRUSTED IT PARTNER

Why It's Important to Work with a SOC-2 Compliant Partner

ICE IS SOC2 CERTIFIED

ICE
TRUSTED IT PARTNER

Many of our clients today have different compliance requirements such as ISO, HIPAA, Hitrust, CLIA, GDPR, NIST, and others. All of these require that the IT service provider be SOC2 compliant, yet we've found that more than **less than 5% of MSPs have a SOC2 certified**, and we believe this really differentiates ICE. In fact, more and more organizations are asking that their managed service provider (MSP) undergo a SOC2 audit before engaging with them. This makes perfect sense to us—organizations want to know how secure an outside vendor really is.

The SOC2 certification is a coveted and hard-to-obtain information-security certification, and it demonstrates that an independent accounting and auditing firm has examined an organization's non-financial reporting control objectives and activities and has actually tested those controls over time to ensure that they are operating securely and effectively.

AICPA
SOC
™

What is SOC2?

Developed by the American Institute of CPAs **(AICPA)**, SOC stands for Service and Organization Control. It defines criteria for managing customer data based on five "trust service principles"—security, availability, processing integrity, confidentiality, and privacy.

Issued by outside auditors, SOC2 certification assesses the extent to which a vendor such as ICE Consulting complies with the ***five trust principles*** based on the systems and processes in place. Trust principles are broken down as follows:

1 SECURITY

Is the system protected against unauthorized access?

The security principle refers to the protection of system resources against unauthorized access. Access controls help prevent potential system abuse, theft or unauthorized removal of data, misuse of the software, and improper alteration or disclosure of information. IT security tools such as network and web application firewalls (WAFs), two-factor authentication, and intrusion detection are useful in preventing security breaches that can lead to unauthorized access of systems and data.

2 AVAILABILITY

Is the system available for operation and use as agreed?

The availability principle refers to the accessibility of the system, products, or services as stipulated by a contract or service level agreement (SLA). As such, the minimum acceptable performance level for system availability is set by both parties.
This principle does not address system functionality and usability but does involve security-related criteria that may affect availability. Monitoring network performance and availability, site failover, and security incident handling are critical in this context.

3 PROCESSING INTEGRITY

Is the system processing complete, valid, accurate, timely, and authorized?

The processing integrity principle addresses whether or not a system achieves its purpose —and delivers the right data at the right price at the right time. Accordingly, data processing must be complete, valid, accurate, timely, and authorized. However, processing integrity does not necessarily imply data integrity. If the data contains errors prior to being input into the system, detecting them is not usually the responsibility of the processing entity. Monitoring of data processing, coupled with quality assurance procedures, can help ensure processing integrity.

4 CONFIDENTIALITY

Is the information that's designated as confidential protected as agreed?

Data is considered confidential if its access and disclosure is restricted to a specified set of persons or organizations. Examples may include data intended only for company personnel, as well as business plans, intellectual property, internal price lists and other types of sensitive financial information. Encryption is an important control for protecting confidentiality during transmission. Network and application firewalls, together with rigorous access controls, can be used to safeguard information being processed or stored on computer systems.

5 PRIVACY

Is personal information collected, used, retained, disclosed, and destroyed in accordance with the entity's privacy notice?

The privacy principle addresses the system's collection, use, retention, disclosure, and disposal of personal information in conformity with an organization's privacy notice, as well as with criteria set forth in the AICPA's generally accepted privacy principles (GAPP). Personal identifiable information (PII) refers to details that can distinguish an individual (e.g., name, address, Social Security number). Some personal data related to health, race, sexuality, and religion is also considered sensitive and generally requires an extra level of protection. Controls must be put in place to protect all PII from unauthorized access.

WHAT DOES IT MEAN TO YOU OR FOR YOUR COMPANY?

Vendors who have the certification have been through rigorous audit processes to ensure information security. At ICE Consulting, we take this certification very seriously to ensure that we maintain the highest level of information security and that we always handle your sensitive data responsibly.

Key advantages of our SOC2 compliance include:

1. Peace of mind and trust:

Our clients can have peace of mind that their systems are always secure when working with us. As a SOC2 certified company, we make sure all of the above important principles—security, availability, process integrity, confidentiality, and privacy—are being practiced while managing our client's IT infrastructure.

2. Process-oriented business:

At ICE, we are a process-oriented company, and our SOC2 certification is a good example. It is a further demonstration of our trustworthiness as an outside vendor.

3. Ongoing audits:

Since ICE is now getting audited yearly with the SOC2 certification, we follow the above process to meet the required trust principles.