4 Regulatory Frameworks:

Retain and Grow Your Client Base

Erin Birckhead
Audit Senior Manager | SC&H Group

When it comes to data security and compliance, both domestically and internationally, companies must appropriately structure and properly equip their internal environments to mitigate risk and issues. In doing so, companies demonstrate that security is a top priority, which can help strengthen their relationships with current clients and elevate their ability to attract and recruit prospective clients. Below are four recognized frameworks that can help organizations accomplish this:

1. **International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001:** Focuses on how to manage information security and internal controls, and is also accepted internationally.
2. **National Institute of Standards and Technology (NIST) SP (Special Publication) 800-171:** Covers nonfederal information systems, specifically the protection of Controlled Unclassified Information (CUI).
3. **NIST SP 800-53:** Covers federal information systems and security controls.
4. **System and Organization Controls (SOC):** Assesses the suitability of the design of controls and the operating effectiveness at either a point in time or for a period of time, respectively.

Depending on the service or product a company is providing, they can benefit from implementing and maintaining one or more of these frameworks. When implemented, organizations can establish a secure and compliant internal control environment while also demonstrating to current and prospective clients that they take their information and data security seriously. In this article, we will define each framework, outline the associated benefits, and identify ideal users.

1: ISO/IEC 27001 Framework

What is it?

The ISO/IEC 27001 framework focuses on the processes and policies a company can implement, via a group of standards, to achieve optimal protection of critical and/or sensitive information.

ISO/IEC 27001 consists of two parts.

- **Part one** includes 11 clauses, which can be further divided into clauses 0 to 3, which serve as an introduction to the standard, while clauses 4 to 10 outline the standard's requirements to achieve compliance.
- **Part two**, also referred to as Annex A, consists of 14 domains, which are further divided into 114 controls (safeguards) that support the aforementioned clauses. Achieving compliance with these parts is optimal for companies to be eligible for certification.

A company can gain certification by invitation from an accredited certification body to complete an audit through the implementation of an Information Security Management System (ISMS). Certification means 100% compliance with the ISO/IEC 27001 standard, which remains in effect for three years. During that time period, certification is subject to annual surveillance visits and, after three years, a reassessment to be recertified.

How Can Companies Benefit?

The ISO/IEC 27001 certification process forces companies to take a step back and assess their internal controls over the security of their data, resulting in activities that pose several benefits including, but not limited to:

- The development of more robust controls;
- The creation of a stronger network of controls; and
- The demonstration of your organization providing optimal data security to both existing and prospective clients.

Furthermore, since the ISO/IEC framework is internationally accepted, it can be very appealing to companies that serve a wide range of multinational clients.

Who Are the Ideal Users?

ISO/IEC can be used by any company looking to ensure that client data is secure in their environment. Common industries that use this framework include, but are not limited to:

- Information Technology (IT)
- Finance
- Telecommunication

2: NIST SP 800-171 Framework

What is it?

NIST SP 800-171 recommends requirements to protect the confidentiality of CUI in nonfederal systems. CUI is defined as information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies. When contractors implement NIST SP 800-171, they provide the evidence of sufficient security to protect the information identified in their contract(s).

In total, there are 14 groups of recommended security requirements. These requirements are broken down into two sections; the first section is basic security requirements, while the second section is derived security requirements and further broken down into 110 controls.

To achieve compliance, contractors must first identify gaps based on the requirements, which can be complex and time-consuming. As such, contractors will often require the assistance of a cybersecurity consultant to implement NIST SP 800-171, which can be subject to the complexities of a company's environment and systems.

When all requirements have been met, the contractor is seen as being in compliance with NIST SP 800-171. Compliance is often required for government contracts.

How Can Companies Benefit?

Since NIST SP 800-171 is required for nonfederal system contractors that handle CUI to obtain government business, it ultimately benefits those with specialized products and services that the government would use. Those benefits can include:

- Establishing mature risk management practices
- Finding weaknesses in a contractor's cybersecurity processes
- Protecting assets and data

Compliance with NIST 800-171 can most certainly benefit government contracts that are current, but it could also serve as the main marketing point for a prospective contract. It should also be noted that NIST SP 800-171 is a globally recognized cybersecurity framework.

Who Are the Ideal Users?

The ideal users are any contractors that currently or has future plans to provide products and services from a nonfederal system to government entities, such as the Department of Defense (DoD) and the National Aeronautics and Space Administration (NASA).

3: NIST SP 800-53 Framework

What is it?

NIST SP 800-53 recommends requirements and controls for federal information security and privacy policies to protect an organization's confidential data. By implementing NIST SP 800-53, organizations can strengthen their internal infrastructure.

NIST SP 800-53 includes 20 groups of recommended security and privacy requirements and is further broken down into over 1,000 controls. These controls are mandatory, at a minimum, for all federal information systems. It's not uncommon for the assistance of a security and privacy specialist to implement NIST SP 800-53 due to the extensive amount of controls involved.

Based on the organization's security objective (confidentiality, integrity, or availability), they will determine which standards will need to be applied to obtain their compliance goal. NIST SP 800-53 is known as a common starting point for securing data.

When all requirements have been met, the contractor is seen as being in compliance with NIST SP 800-53.

How Can Companies Benefit?

Maintaining compliance is seen as a great negotiation tool for both current and prospective organizations looking to have contracted work with government agencies, as it shows a high level of commitment to a company's cybersecurity environment. Like NIST SP 800-171, NIST SP 800-53 is also a globally recognized framework, which allows for a larger client base.

Who Are the Ideal Users?

The ideal users are any organizations that currently or have future plans to provide products and services from a federal information system or agency to government entities, such as the DoD.

4: SOC 2 Framework

What is it?

The SOC 2 framework is structured to provide a report on controls related to the American Institute of Certified Public Accountants (AICPA) trust services categories of security, availability, processing integrity, confidentiality, and/or privacy. A SOC 2, at a minimum, contains controls over security, referred to as the common criteria, with the option to include the additional four trust services categories. Further, the SOC 2 scope is specific to the security of client data.

The SOC 2 framework contains 200 points of focus and can be further delineated to 64 individual criteria/requirements. To comply with SOC 2 framework, a company must develop a set of controls (no set number) that address the applicable points of focus and criteria. Once a company implements controls that map to the SOC 2 criteria, they then undergo an audit that validates those controls are designed appropriately for Type I and Type II; validating that they are operating effectively.

Unlike the other frameworks discussed, a SOC 2 report must be issued by a Certified Public Accountant (CPA). Additionally, there are two types of SOC 2 reports:

1. SOC 2 Type I Report: As of a point in time
2. SOC 2 Type II Report: Over a period of time

SOC 2 compliance is completely voluntary but is widely recognized in the United States. A SOC 2 report is typically completed at least annually.

How Can Companies Benefit?

For U.S.-based companies, implementing the SOC 2 framework demonstrates to current and prospective clients that their data is appropriately protected—and that the company is committed to the protection of their client data. Internally, it allows companies to evaluate their risk and security position.

Who Are the Ideal Users?

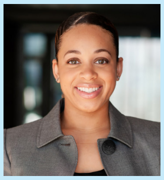
The ideal users are U.S.-based companies that wish to provide comfort to current and future clients that their data is secure, and that the control environment is being continuously monitored.

Next Steps for Framework Implementation

There are several options to explore when it comes to the security of a company's and/or their clients' data. The ideal framework for a company will depend on two key indicators: the company's client base and restrictions based on regulations. Companies must continually assess the optimal framework that suits their objectives now, and in the future, taking into consideration their intended audience.

Implementing the proper framework(s) will help to ensure a company is providing products and services of the highest caliber. There is no lack of data security options, and with the increasing concern around confidential data, more companies will need to implement one or more of these frameworks. To get started, those charged with monitoring data security and regulatory compliance should reach out to a certified audit firm or audit specialist with expert experience implementing these frameworks. 🔒

ABOUT THE AUTHOR



Erin Birckhead *is a Senior Manager with SC&H Group's Audit practice and a Certified Information Systems Auditor (CISA) with more than 10 years of experience in System and Organization Controls (SOC) audits, financial audits, employee benefit plan audits, and internal audits. As an integral part of the team, Erin provides strategic guidance and expert execution to make sure clients have robust control environments while ensuring compliance with AICPA standards across a multitude of industries.*

ABOUT SC&H GROUP

SC&H Group *is a nationally recognized management consulting, audit, and tax firm serving clients across the globe, from rapidly growing startups to world-renowned Fortune 500 companies. As a diversified consultancy and professional services firm with expertise in 11 practices, our offerings span enterprise technology, risk management, and cybersecurity to investment banking, wealth management, and accounting. With more than 340 employees, we help individuals and organizations prepare, innovate, and evolve their business and financial needs in this complex and highly competitive landscape. Learn more at* ***schgroup.com****.*

SC&H GROUP