Information Security Standards

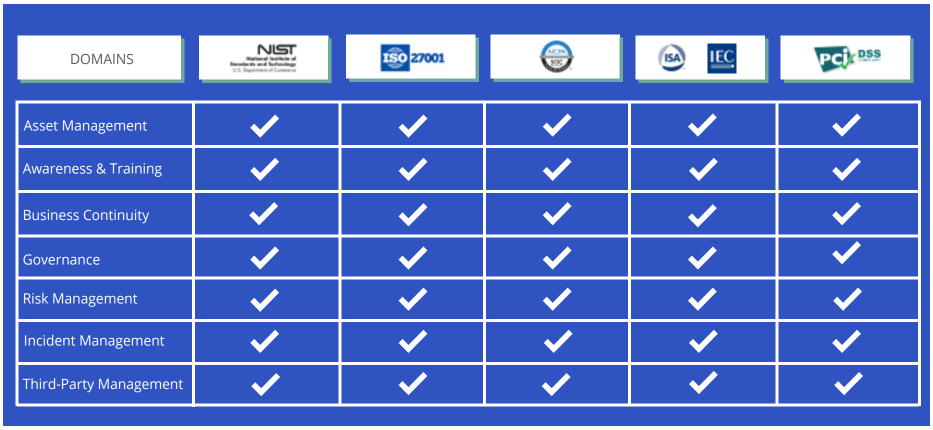
Differences, Benefits, Impacts, and Evolution

By **Antonella Commiato** – ISSA member, Los Angeles Chapter **and Michael Sturgill**

This article compares five common information security standards, discusses the benefits and challenges of adopting and maintaining a standard, and outlines factors for organizations to consider when deciding to adopt a standard.

Abstract

With a wealth of standards, frameworks, regulations, and guidelines available to the infosec community, each option can bring a variety of challenges and benefits to an organization. This article compares five common information security standards, discusses the benefits and challenges of adopting and maintaining a standard, and outlines factors for organizations to consider when deciding to adopt a standard.



DOMAINS	NIST	ISO 27001	AICPA SOC	ISA IEC	PCI DSS
Asset Management	✓	✓	✓	✓	✓
Awareness & Training	✓	✓	✓	✓	✓
Business Continuity	✓	✓	✓	✓	✓
Governance	✓	✓	✓	✓	✓
Risk Management	✓	✓	✓	✓	✓
Incident Management	✓	✓	✓	✓	✓
Third-Party Management	✓	✓	✓	✓	✓

Figure 1 – Domain coverage for infosec standards

Information security (infosec) standards bring structure to an organization's security initiatives and are essential in defining and maintaining the security functions, policies, and protocols necessary to protect and manage information.

There are a wealth of standards, frameworks, regulations, and guidelines available to the infosec community. While there is no denying the value that an established standard can bring to an organization, infosec professionals often find that many of the standards used today are pertinent to their business or industry and cover multiple domains. Furthermore, today's portfolio of standards often provides duplicate benefits, which may cause redundancy or confusion to stakeholders (figure 1).

Becoming familiar with available standards and understanding which are appropriate to adopt is vital for an organization, both to develop its security posture and maintain the security of its information, as well as support on-going assessment, monitoring, and improvements.

Which standards "stand-out"?

With so many different standards available, it is critical to the understand differences, recognize the benefits each standard provides, and identify the potential value it can bring to your organization.

Five of the most prominent, internationally-recognized organizations for establishing standards and guidelines for security controls are outlined below.

National Institute of Standards and Technology (NIST) Special Publication (SP) 800 Series of Standards – NIST 80-53A

NIST SP 800 provides solid support for frameworks such as the Cybersecurity Framework (CFS) and the Risk Management Framework. The standards in this series also provide best practices for information security domains. Within NIST, the Computer Security Resource Center provides cybersecurity and information security material to the US government, educational institutions, and civilian industries.[1] Compliance with NIST standards is mandatory for federal agencies, but they can also be a great source of information to all enterprises regardless of affiliation or size by tailoring the NIST SP 800 series to fit their requirements.

A well-known standard for infosec is NIST 800-53A "Assessing Security and Privacy Controls in Federal Information Systems and Organizations." According to the special publication outlining the standard, it "provides a set of procedures for conducting assessments of security controls and privacy controls employed within federal information systems and organizations. The assessment procedures, executed at various phases of the system development life cycle, are consistent with the security and privacy controls in NIST Special Publication 800-53, Revision 4."[2]

International Organization for Standards (ISO)

ISO 27000 Series of Standards – ISO 27001

The ISO/IEC 27000 family of standards is designed to help organizations secure their information assets and covers areas such as developing an information security management system (ISMS), implementing controls, managing risk, conducting audits, and more. Combining multiple ISO 27000 standards can be a valuable way to create and maintain a holistic, effective infosec program. These standards are especially useful to security managers looking to implement a framework that can be audited and compliance that can be verified through certification.

ISO 27001 is recommended to organizations interested in implementing infosec best practices regardless of their vertical or size. ISO 27001 prescribes management clauses and security controls from ISO 27002 that guide organizations in the implementation of an information security management system (ISMS) designed to safeguard the confidentiality, integrity, and availability of sensitive information. The management clauses provide a solid framework on the following components: leadership, planning, support, operation, performance evaluation, and improvement. The ISO 27002 "Code of Practice for Information Security Controls" outlines 114 safeguards for organizations to consider as part of the ISMS implementation in order to mitigate risk to meet the organizations' risk appetite such as encryption and access control. ISO 27001 also provides a solid base for compliance with regulatory requirements or laws such as the EU General Data Protection Regulation (GDPR) and the New York Department of Financial Services cybersecurity requirements, since it covers many controls that overlap with these regulations including breach notification, asset management, and vendor management for the protection of sensitive data.[3]

According to ISO, as of 2016, more than 33,000 organizations held an ISO 27001 certification. This number represents a 21 percent increase from 2015. The growth trend is projected to continue at a fast pace given that ISO 27001 provides a solid base for compliance with several significant regulations.[4]

American Institute of Certified Public Accountants (AICPA)

Statement of Standards for Attestation Engagement (SSAE) 18

The Auditing Standards Board (ASB) of the AICPA created the SSAE regulation to redefine and update how service com-

[1] "Computer Security Resource Center," NIST, accessed on June 18, 2018, https://csrc.nist.gov/.

[2] NIST, "Assessing Security and Privacy Controls in Federal Information Systems and Organizations," NIST (December 2014) – https://csrc.nist.gov/publications/detail/sp/800-53a/rev-4/final.

[3] Richard Menear, "How ISO 27001 Can Help Your Organisation Meet GDPR Requirements," SC Media UK, last modified on December 21, 2017 – https://www.scmagazineuk.com/how-iso-27001-can-help-your-organisation-meet-gdpr-requirements/article/712142/.

[4] IAPP, "IAAP and OneTrust Map ISO27001 to the GDPR," March 2018, https://iapp.org/news/a/iapp-and-onetrust-map-iso-27001-to-the-gdpr/.

panies report on compliance controls. SSAE 18 became effective in May 2017 and was preceded by SSAE 16 (effective in 2011), and SAS 70 (effective April 1992).[5]

Organizations achieve SSAE and infosec compliance through SOC 2 reporting. Organizations that are SOC 2 compliant demonstrate the ability to address criteria for managing customer data across five principles:

- Security
- Availability
- Processing integrity
- Confidentiality
- Privacy

As it pertains to information security, organizations are audited on controls related to the protection of assets including network and application firewalls, two-factor authentication, and intrusion detection.

PCI Security Standards Council
PCI Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) details the infosec standards for securing credit card data for merchants that process credit card information. This industry-specific security standard is managed by the PCI Security Standards Council, which was founded by five major credit payment brands.[6] PCI DSS focuses on six primary goals:

- Maintaining a security network
- Protecting cardholder information
- Protecting systems against hacking
- Restricting and controlling access to system information and operations
- Monitoring and testing networks
- Defining and maintaining a formal information security policy[7]

International Society of Automation (ISA)
ANSI/ISA-62443 Series of Standards

ISA is a leader and expert source for creating American National Standards Institute (ANSI) accredited standards that cover safety, efficiency, and profitability for the management of automation and control systems.[8] The ISA 62443 series of standards provide infosec best practices and controls for industrial automation control systems. These standards address requirements and controls that support the C-I-A triad throughout the entire life cycle of an automation control system. In addition to providing guidance and information sharing, the 62443 series provides the framework for product assessments and cybersecurity certificate programs.[9]

The Evolution of Infosec: The Standards' Role

Using an information security standard will create a strong foundation for managing an organization's information security program. Even more importantly, successfully complying with existing standards will provide an easier pathway to meet new regulatory requirements. Current standards play a role in the evolution of information security in three ways:

- **Evolution is often expected and built into the road map.** Many standards have mandatory review dates to ensure that the standard's content is still relevant to current technology and security trends. For example, ISO 27001 has a predefined life cycle of five years to ensure the document undergoes a complete review and update.
- **Expert collaboration and feedback polling drives change.** Members of the infosec community voluntarily collaborate on understanding security vulnerabilities and steps to mitigate them. For example, since 2010 the Open Web Application Security Project (OWASP) has published a top 10 report that identifies critical security risks to web applications based on a consensus of security experts.[1] The "OWASP Top 10" reports are always free to download and provide valuable information to help identify the details of each risk, from exploitation to prevention strategies.
- **Breaches shine the light on vulnerabilities and improvement opportunities.** Major infosec breaches bring to light vulnerabilities and force updates to infosec standards. The credit industry implemented PCI DSS to combat credit card fraud against older cards without chip technology. Laws are established to enforce infosec in the government and civilian sectors, and standards are created to provide compliance guidance.

[1] OWASP, "Open Web Application Security Project Top Ten Project," last modified June 3, 2018, https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project.

Should your organization adopt and follow a standard?

Standards bring practices recommended by experts, create common ground between and within organizations, and provide a sense of trust and confidence—especially when an organization certifies its compliance. In addition, there are a

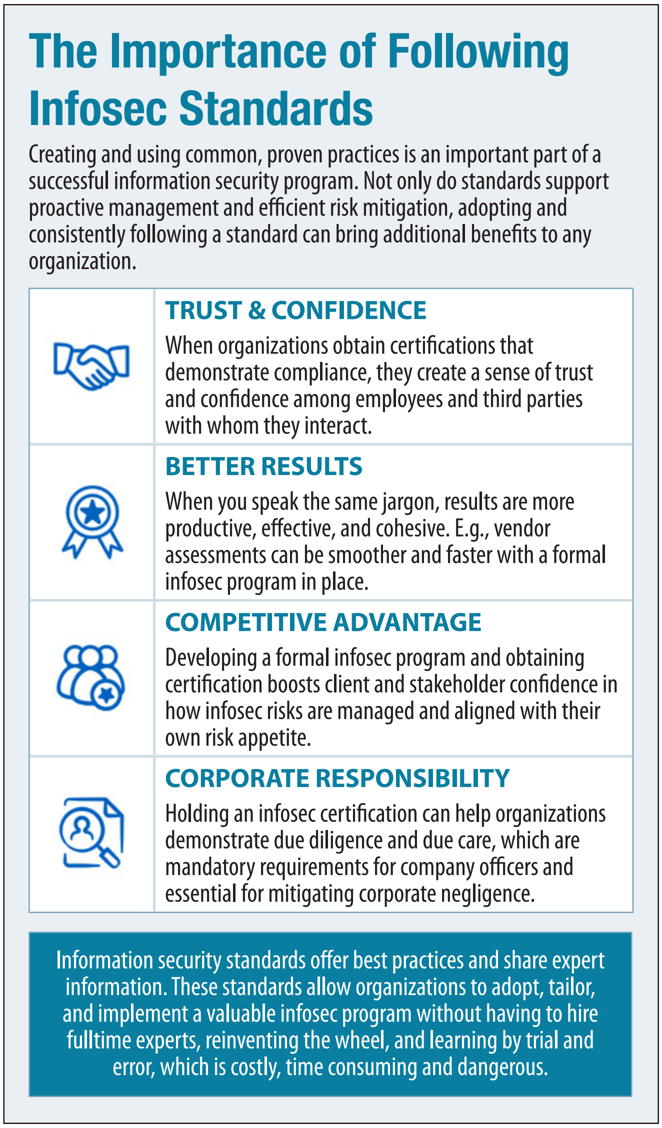
[5] Jaike Hornreich, "Understanding the New SSAE 18 – What You Need to Know," Skoda Minotti, April 2017, https://skodaminotti.com/blog/understanding-new-ssae-18-need-know/.

[6] PCI Security Standards Council, "About Us," accessed on June, 18, 2018, https://www.pcisecuritystandards.org/about_us/.

[7] Margaret Rouse, "PCI DSS (Payment Card Industry Data Security Standard)," TechTarget, May 2009 – https://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard.

[8] International Society of Automation, "ISA Standards," ISA, accessed on June 18, 2018 – https://www.isa.org/standards-and-publications/isa-standards/.

[9] ISA, "ISA/IEC 62443 Cybersecurity Certificate Programs," ISA – https://www.isa.org/training-and-certifications/isa-certification/isa99iec-62443/isa99iec-62443-cybersecurity-certificate-programs/.



The Importance of Following Infosec Standards

Creating and using common, proven practices is an important part of a successful information security program. Not only do standards support proactive management and efficient risk mitigation, adopting and consistently following a standard can bring additional benefits to any organization.

TRUST & CONFIDENCE
When organizations obtain certifications that demonstrate compliance, they create a sense of trust and confidence among employees and third parties with whom they interact.

BETTER RESULTS
When you speak the same jargon, results are more productive, effective, and cohesive. E.g., vendor assessments can be smoother and faster with a formal infosec program in place.

COMPETITIVE ADVANTAGE
Developing a formal infosec program and obtaining certification boosts client and stakeholder confidence in how infosec risks are managed and aligned with their own risk appetite.

CORPORATE RESPONSIBILITY
Holding an infosec certification can help organizations demonstrate due diligence and due care, which are mandatory requirements for company officers and essential for mitigating corporate negligence.

Information security standards offer best practices and share expert information. These standards allow organizations to adopt, tailor, and implement a valuable infosec program without having to hire fulltime experts, reinventing the wheel, and learning by trial and error, which is costly, time consuming and dangerous.

Figure 2 – The importance of following infosec standards

variety of benefits and challenges to consider when deciding to follow a standard (figure 2).

Benefits of speaking the same infosec language

When stakeholders and team members speak the same infosec language, the results are often more productive, effective, and cohesive. For example, companies performing vendor assessments to vet the information security posture of suppliers benefit from vendors that hold an infosec certification like ISO 27001 or are compliant with a mainstream infosec framework. Because their policies and practices are already well documented, evaluating vendors with an established program is often smoother and faster compared to assessing a company that does not have a formal infosec program in place.

Organizations that create standards and security professionals know the importance of establishing common ground between security standards and using hybrid control maps to show how standards are comparable with each other. For example, AICPA offers Trust Service Criteria mappings to show how their security controls are similar to the NIST CSF and ISO 27001 frameworks.[10]

We can also look to the federal government to see an illustration of adopting infosec standards to improve communication and increase efficiency. Along with other benefits, in 2014 the US Department of Defense (DoD) decided to adopt NIST to be more compatible with civilian companies.[11]

Competitive advantages

Adopting infosec standards makes good business sense for private organizations. Compliance with or certification of an infosec standard provides customers and stakeholders with confidence in how a company is managing information security-related risks in accordance with the organization's risk appetite. Compliance and certification offer an advantage over competitors that haven't adopted an infosec standard. In some instances, compliance is expected or required by potential clients, such as financial institutions, banks, and insurance companies.[12]

Demonstrating corporate responsibility

Compliance with infosec standards also demonstrates corporate responsibility. Company officers are ultimately responsible for information security at their organizations and can be held liable for negligence and be fined significant penalties in case of a breach. Due diligence and due care are mandatory processes that must be identifiable to mitigate corporate negligence. Demonstrating due diligence and due care by holding an infosec standard certification can help mitigate these circumstances by demonstrating commitment through these efforts. In addition, insurance companies might offer cybersecurity at a lower premium to certified organizations.

Challenges of implementing and maintaining standards

While there are real, valuable benefits to implementing one or more standards, organizations should be aware of potential challenges related to implementation and maintenance.

- **Time:** Implementing and maintaining information security standards is not a one-time project. Rather, it is a process that requires dedicated, qualified personnel, support from senior leadership, and continuous monitoring and improvement. A successful effort will require buy-in from the entire organization.
- **Cost:** Standards can be expensive to implement and just as costly to maintain. In the case of ISO 27001, for example, in addition to the time and effort necessary to meet the

[10] AICPA, "Mappings Relevant to the SOC Suite of Services," AICPA, accessed on June 18, 2018, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/mappingsrelevanttothesocsuiteofservices.html.

[11] Joey Cheng, "DOD Switches to NIST Security Standards," Defense Systems, April 2014 – HTTPS://DEFENSESYSTEMS.COM/ARTICLES/2014/04/03/DOD-ADOPTS-NIST-SECURITY-STANDARDS.ASPX.

[12] Certification Europe, "ISO 27001:2013 – Information Security Management Systems," https://www.certificationeurope.com/certification/iso-27001-information-security/.

standard requirements, organizations must budget for annual audit fees, which can be substantial.

- **Buy-in:** Senior leadership buy-in and program ownership at the C-level are critical elements for an organization to deploy an information security program effectively. The information security team must share metrics, report the effectiveness of the program, and demonstrate its value and strategic alignment with the organization's business objectives to maintain senior leadership support.
- **Change management:** In general, everyone appreciates the value of securing information until it requires a change. Security teams implementing standards are challenged to strike a delicate balance between security and convenience.
- **Continuous improvement:** Standards have life cycles. When a standard is updated, it is the responsibility of all compliant organizations to be aware of the updates and implement them by specified dates, or as soon as possible if a time line is not mandated. In some cases, a standard might become obsolete, and a new standard must be researched and presented to senior leadership for approval for implementation.

Deciding which standard is right for your organization

With many varying standards and guidelines available, choosing the right fit and best value for your organization can be a time-consuming task. Whether you require a standard specific to your industry or need a customized solution, start by educating yourself and understanding all the options. Research established standards, frameworks, and best practices so you can tailor components to meet your company's requirements and overall business strategy. Key considerations include:

- **Hybrid approach:** Some organizations may need to select specific components from a variety of standards and frameworks and tailor them to meet their specific needs because of gaps of standard coverage for organizations involved within multiple industries or compliance requirements
- **Alignment with business strategy:** Examine the requirements and determine which standards are compatible with current business operations
- **Leverage in-house expertise:** When regulatory or client requirements don't impact the decision, organizations may choose to select a standard based on the experience of in-house subject matter experts
- **Client requirements:** To do business within a particular market, a company might need to hold a certification or show compliance with a standard to be eligible or competitive
- **Regulatory compliance or compulsory requirements:** Some organizations, depending on the industry or government regulations and laws, will not have a choice and must implement standards and frameworks to demonstrate compliance
- **Implementation and maintenance costs:** The cost of deployment, maintenance, and continuously improving compliance with a standard can be a significant factor in selection and budgeting
- **Build your knowledge:** Join organizations such as ISSA to continue learning and share knowledge and experiences with the infosec community
- **Supporting technology:** Identify and adopt tools and platforms that automate your processes and communications, and support the efficient development, maintenance, and improvement of your information security program
- **Organizational awareness:** Provide regular updates and training to build a culture of information security among all team members and ensure all stakeholders are informed so they make take leadership roles and establish themselves as a cohesive part of the solution

Conclusion

Information security standards have proven to be valuable resources for sharing information best practices as established by industry experts. Specific infosec guidance is available for government agencies and civilian organizations and varies depending on factors such as industry, laws, and regulatory compliance requirements. When selecting a standard, organizations should consider the importance of certification as a way to demonstrate infosec compliance and perform a cost-benefit analysis to determine if certification is the right path. The process of selecting the appropriate infosec standard can be intimidating, but with careful research, any organization can choose the right standard to achieve its goals.

About the Authors

Antonella Commiato, Chief Technology Officer/Chief Information Security Officer EXTEND Resources, has 23 years of IT leadership experience across a broad range of disciplines that include marketing, social expression, transportation, and logistics. With her technological expertise and guidance companies are able to support their complex business initiatives, grow their businesses, and implement efficient internal operations. She may be reached at acommiato@extendresources.com.

Michael Sturgill, CISM, CEH, and SEC+, Information Security Manager EXTEND Resources, has more than 15 years of experience in information systems, program management, security, and technical solutions for the US government and civilian sector. He may be reached at msturgill@extendresources.com.