VACO Reference Material

NAVIGATING THE IT SECURITY LANDSCAPE

A GUIDE TO STANDARDS AND COMPLIANCE

Researched and Collated By:
VACO Middle East Est.
Abu Dhabi, United Arab Emirates
info@vaco.ae
+971 56 947 9733
Visit us at www.vaco.ae

Guideline on various IT security Standard - decoded

ISO 27000 SERIES

The ISO 27000 Series was developed by the International Organization for Standardization. It is a flexible information security framework that can be applied to all types and sizes of organizations. The two primary standards -- ISO 27001 and 27002 -- establish the requirements and procedures for creating an information security management system (ISMS). Having an ISMS is an important audit and compliance activity. ISO 27000 consists of an overview and vocabulary and defines ISMS program requirements. ISO 27002 specifies the code of practice for developing ISMS controls. Compliance with ISO 27000 Series standards is established through audit and certification processes, typically provided by third-party organizations approved by ISO and other accredited agencies.

The ISO 27000 Series has 60 standards covering a broad spectrum of information security issues, for example:

ISO 27018	Addresses cloud computing
ISO 27031	Provides guidance on IT disaster recovery programs and related activities
ISO 27037	Addresses the collection and protection of digital evidence
ISO 27040	Addresses storage security
ISO 27799	Defines information security in healthcare, which is useful for companies that require HIPAA compliance

There are many IT security frameworks and standards for organizations to choose from.

NIST SP 800-53

NIST has developed an extensive library of IT standards, many of which focus on information security. First published in 1990, the NIST SP 800 Series addresses virtually every aspect of information security, with an increasing focus on cloud security.

NIST SP 800-53 is the information security benchmark for U.S. government agencies and is widely used in the private sector. SP 800-53 has helped spur the development of information security frameworks, including the NIST Cybersecurity Framework (CSF).

NIST SP 800-171

NIST SP 800-171 has gained popularity due to requirements set by the U.S. Department of Defense regarding contractor compliance with security frameworks. Government contractors are a frequent target for cyber attacks due to their proximity to federal information systems. Government manufacturers and subcontractors must have an IT security framework to bid on federal and state business opportunities.

Controls included in the NIST SP 800-171 framework are directly related to NIST SP 800-53 but are less detailed and more generalized. It's possible to build a crosswalk between the two standards if an organization must show compliance with NIST SP 800-53, using NIST SP 800-171 as the base. This creates flexibility for smaller organizations -- they can show compliance as they grow using the additional controls included in NIST SP 800-53.

NIST CSF

The NIST Framework for Improving Critical Infrastructure Cybersecurity, or NIST CSF, was developed under Executive Order 13636, released in February 2013. It was developed to address U.S. critical infrastructure, including energy production, water supplies, food supplies, communications, healthcare delivery and transportation. These industries must maintain a high level of preparedness, as they have all been targeted by nation-state actors due to their importance.

Unlike other NIST frameworks, NIST CSF focuses on risk analysis and risk management. Security controls in the framework are based on the five phases of risk management: identify, protect, detect, respond and recover. Like all IT security programs, these phases require the support of senior management. NIST CSF can be used by both public and private sectors.

NIST SP 1800 SERIES

The NIST SP 1800 Series is a set of guides that complement the NIST SP 800 Series of standards and frameworks. The SP 1800 Series of publications offers information on how to implement and apply standards-based cybersecurity technologies in real-world applications.

The SP 1800 Series publications provide the following:

- Examples of specific situations and capabilities;
- Experience-based, how-to approaches using multiple products to achieve the desired result;
- Modular guidance on implementation of capabilities for organizations of all sizes; and
- Specifications of required components and installation, configuration and integration information so organizations can easily replicate the process themselves.

COBIT

COBIT was developed in the mid-1990s by ISACA, an independent organization of IT governance professionals. ISACA offers the well-known Certified Information Systems Auditor and Certified Information Security Manager certifications.

COBIT originally focused on reducing IT risks. COBIT 5, released in 2012, included new technology and business trends to help organizations balance IT and business goals. The current version is COBIT 2019. It's the most used framework to achieve Sarbanes-Oxley compliance. Numerous publications and professional certifications address COBIT requirements.

CIS CONTROLS

The Center for Internet Security (CIS) Critical Security Controls, Version 8 -- formerly the SANS Top 20 -- lists technical security and operational controls that can be applied to any environment. It does not address risk analysis or risk management like NIST CSF; rather, it is solely focused on reducing risk and increasing resilience for technical infrastructures.

Cont.

Controls include the following:

- Inventory and Control of Enterprise Assets
- Data Protection
- Audit Log Management
- Malware Defenses
- Penetration Testing

CIS Controls link with existing risk management frameworks to help remediate identified risks. They're useful resources for IT departments lacking technical information security experience.

HITRUST COMMON SECURITY FRAMEWORK

The HITRUST Common Security Framework includes risk analysis and risk management frameworks, along with operational requirements. The framework has 14 different control categories and can be applied to almost any organization, including healthcare.

HITRUST is a massive undertaking for any organization due to the heavy weight given to documentation and processes. As a result, many organizations end up scoping smaller areas of focus for HITRUST. The costs of obtaining and maintaining HITRUST certification adds to the level of effort required to adopt this framework. The certification is audited by a third party, which adds a level of validity.

GDPR

GDPR is a framework of security requirements that global organizations must implement to protect the security and privacy of EU citizens' personal information. GDPR requirements include controls for restricting unauthorized access to stored data and access control measures, such as least privilege, role-based access and multifactor authentication.

COSO

COSO is a joint initiative of five professional organizations. Its 2013 framework covers internal controls, and its 2017 framework covers risk management.

Cont.

The COSO internal control framework identified five interrelated components:

- Control Environment
- Risk Assessment
- Control Activities
- Information and Communication
- Monitoring

Need More?

VACO Has You Covered

VACO Middle East is a leading consulting firm that provides innovative and customized solutions to help businesses thrive in the dynamic global market. We specialize in a range of services, including strategic planning, human resource development, accreditations, and marketing strategy development, tailored to meet the unique needs of start-ups and established companies alike. With our expertise and collaborative approach, we can help you take your business to the next level and achieve your goals. Reach out to our team today and find out how you can grow your business.

VACO Middle East Est.

Abu Dhabi, United Arab Emirates

Visit us at www.vaco.ae

info@vaco.ae

+971 56 947 9733