SECURITY BASECAMP

SBC Alert: Summary of Notable Cybersecurity Frameworks and Standards

CYBERSECURITY FRAMEWORKS

Most regulatory guidance for companies follows and is informed by notable cybersecurity frameworks. The purpose of this alert is to summarize related information.

JANUARY 2021

Security Basecamp
(949) 330-0899

Table of Contents

NOTEABLE CYBESECURITY STANDARDS AND FRAMEWORKS

NIST Cybersecurity Framework

This voluntary Framework consists of standards, guidelines, and best practices to manage cybersecurity-related risk. The Cybersecurity Framework's prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

SSAE 18 / SOC Reports

Some organizations have heard of SAS 70, SSAE 16, and now SSAE 18, but, haven't seen the value, other than because one of their customers require it. Many companies will not even think about outsourcing functions to a Company who does not have a clean SOC 1 or SOC 2 Type II Report in place, especially since Vendor Management reviews are now required. SOC Reports are created under AICPA guidelines by trained auditors. SOC 2 Type II Reports require a summary of controls reasonably designed to protect confidential data and the testing of the control's effectiveness over an extended period. As of the latest SSAE 18 and SOC 2 updates, vendor management and review of any relevant compliance / audit reports (SOC 1, SOC 2, HITRUST, ISO 27001/2, PCI, etc.) has become a key component of monitoring for potential security and compliance risks when outsourcing functions that use a third-party's data.

ISO / IEC 27000

A set of standards and principles for creating an Information Security Management System (ISMS). It is similar to other ISO standards such as ISO 9000 but focused on those used to manage information security risks and controls within an organization. Bringing information security deliberately under overt management control is a central principle throughout the ISO/IEC 27000 standards.

PCI Security Standards Council

The PCI Security Standards Council is a global forum for the ongoing development, enhancement, storage, dissemination and implementation of security standards for account data protection. The Payment Card Industry Security Standards Council was originally formed by American Express, Discover Financial Services, JCB International, MasterCard and Visa Inc. on 7 September 2006, with the goal of managing the ongoing evolution of the Payment Card Industry Data Security Standard. Such standards are often related to protecting money movement transactions.

Center for Internet Security (CIS) — CIS Critical Security Controls (CIS First 5 / CIS Top 20)

The Center for Internet Security (CIS) is a non-profit entity focused on Information Security. According to CIS, its 20 'Controls' are a prioritized set of actions that protect your critical systems and data from the most pervasive cyber-attacks. The First 5 CIS Controls are often referred to as providing cybersecurity "hygiene," and studies show that implementation of the First 5 CIS Controls provides an effective defense against the most common cyber-attacks (~85% of attacks). The CIS Controls map to most major compliance frameworks such as the NIST Cybersecurity Framework, NIST 800–53, ISO 27000 series and regulations such as PCI DSS, HIPAA, NERC CIP (Critical Infrastructure Project), and Federal Information Security Management Act (FISMA).

ABOUT SECURITY BASECAMP

Security Basecamp is a consulting firm focused exclusively in the financial services industry. We partner with executives and managers to facilitate effective business planning and help you competitively leverage technology for profitable growth. Our mission is to help financial services firms solve their most challenging strategic business issues through critical thinking, rigorous project management, and/or the savvy use of practical technologies.

Collectively, our consultants have managed more than 100 strategy, operations, technology, compliance, and business development projects over the past 25 years. We bring a business-oriented approach to completing cybersecurity projects and the technical acumen to work effectively with your internal IT staff. We help you manage cybersecurity analysis, action planning, and execution that your busy management team doesn't have the time or resources to lead. We offer three primary cybersecurity services: 1) Risk Assessments, 2) a vCISO Service, and 3) Vendor Cybersecurity Due Diligence. To learn more, visit our website www.securitybasecamp.com or call (949) 330-0899.

AUTHOR INFORMATION

Paul Osterberg
Managing Director, Security Basecamp
(949) 330-0899
posterberg@securitybasecamp.com