Chapter 5
Pragmatic Risk-Based Approach to Cybersecurity: Establishing a Risk-Enhanced Unified Set of Security Controls

Stephen G. Fridakis
https://orcid.org/0009-0005-7436-7213
Oracle Health, USA

ABSTRACT

Sometimes security and technology professionals confuse their state of compliance with their security posture. While an organization can meet the requirements to any regulatory standard (HIPAA, SOC, etc.), doing so should not be construed as meeting the requirements to defend a potential cyberattack, provide data protection during business processing, or maintain a highly secure development environment. In this chapter, the authors discuss how security and compliance can co-exist. They associate each one of these with controls that are either derived from formal frameworks or meet custom operational or other requirements of an organization. They explore how each control needs to be implemented with a risk perspective in mind, and finally, they suggest methods on how to manage such a control catalog.

WHY COMPLIANT DOES NOT MEAN SECURE

Compliance guidelines are provided as a generalized method to define common minimum standards for a specific area of concern such as payment industry, healthcare, financial information and so on. Given the high degree of interpretation that each guideline is subject to, any blind strict adherence will not result in any material improvements in security or operations. There are many factors that can still cause a security failure despite an organization's adherence to the standard. Lack of skilled staff, human error, availability of information to support breach detection, dysfunctional organizational structures are all contributors to bad security despite meeting the compliance standards.

DOI: 10.4018/978-1-6684-9018-1.ch005

Establishing a framework is a very complicated undertaking. As Table 1 suggests, most frameworks are updated in regular intervals, yet keeping up with the pace and implementation of certain updates can be challenging.

Table 1. Popular frameworks and their latest version/release date

Framework	Current Version	Release Date
NIST	1.1	April 2018
ISO 27001/27002	35.030 -35.030	October 2022 - March 2022
CIS	8	May 2021
SOC2	Oct 2022	Oct 2022
PCI-DSS	4	Mar 2022
COBIT	2019	2018
HiTrust	11	Jan 2023
Cloud Control Matrix (CSA)	4	Jan 2021
CMMC	2	Nov 2021
HIPAA	2023	Jan 2023

In their 2018 (GAO, 2018) report titled "Critical Infrastructure Protection: Additional Actions are Essential for Assessing Cybersecurity Framework Adoption", the US Government Accountability Office (GAO) stated that while there may be regular updates of a certain framework such as NIST, their timely adoption may be hindered by conflicting and overlapping standards or tools that have not kept up with the updates. Despite that, using a framework is useful, not to say essential. One can argue that the tools, other frameworks and lack of necessary knowledge challenge strict adherence to what is specified. HIPAA establishes the minimum security controls for administrative, physical and technical safeguards. The standard itself provides no guidance regarding the implementation of specific methods (the "how"). Instead it uses open ended suggestions to implement what is "reasonable" or what is "a best practice" reducing security posture to mere concepts.

Another such example relevant to medical - life sciences applications that include hardware and sensors is ISO27034 (IEC, 2022). This standard devotes significant space in application security controls which it defines as "data structure containing a precise enumeration and description of a security activity and its associated verification measurement to be performed at a specific point in an application's lifecycle." Furthermore it defines the targeted Level of Trust as "name or label of a set of Application Security Controls deemed necessary by the application owner to lower the risk associated with a specific application to an acceptable (or tolerable) level, following an application security risk analysis." Implementing such a standard is quite overwhelming, and any organization's ability to associate the standard with its own operations and perform a risk analysis based on it is quite challenging.

There is more vagueness and ambiguity that suggest the need for close review and customization with other controls as well. NIST 800-53 control AU-11 addresses the matter of log retention in the following terms (NIST, 2022): "Retain audit records to provide support for after-the-fact investigations of incidents and to meet regulatory and organizational information retention requirements. Organizations retain audit records until it is determined that the records are no longer needed for administrative,