Implementing the NIST Cybersecurity Framework with the HITRUST Approach
Presenters

Bryan Cline, Ph.D.
Chief Research Officer, HITRUST

Jason Taule
VP of Standards & CISO, HITRUST
Objectives

By the end of this presentation, you will have learned

• The value of the NIST Framework for Improving Critical Infrastructure Cybersecurity (“Cybersecurity Framework”) as well as its limitations

• A comprehensive security and privacy controls framework is needed to fully implement the NIST Cybersecurity Framework and achieve its desired outcomes

• The HITRUST CSF provides a more targeted, risk-based approach to specifying relevant controls than other frameworks like ISO 27001 and NIST SP 800-53

• The HITRUST approach, provided through a complete suite of products, services and tools, can
  – Provide an organization’s Current and Target Profiles,
  – Support estimates of its current Implementation Tiers, and
  – Help communicate this information to internal and external stakeholders in a repeatable, consistent and transparent way
Why would I want to integrate the NIST Cyber Framework into my existing info protection program?

- Aligns industry standards and best practices to the Framework Core in a particular implementation scenario
- Supports prioritization and measurement while factoring in business needs
- Cybersecurity activities and informative references, organized around particular outcomes
- Enables communication of cyber risk across an organization
- Describes how cybersecurity risk is managed by an organization and degree the risk management practices exhibit key characteristics
Does adopting the NIST Cyber Framework mean I don’t have to adopt another framework?
But if the NIST Cyber Framework helps ensure I address cyber comprehensively, can I use any framework?
So how exactly does the HITRUST CSF support my implementation of the NIST Cyber Framework?
Can I get my information protection program certified against the NIST Cyber Framework?

While it cannot endorse any commercial approach, NIST states in its Draft NIST Roadmap for Improving Critical Infrastructure Cybersecurity Version 1.1, December 5, 2017 that it “will continue working with those who manage confidence mechanisms programs to assist industry in further leveraging these resources[,] and private and public-sector entities that have a need for conformity demonstration, to help understand how these organizations can leverage existing programs.”
The NIST Cybersecurity Framework complements rather than replaces an organization’s existing risk management process and cybersecurity program by providing an overarching set of guidelines to provide a minimal level of consistency as well as depth, breadth and rigor of industry’s cybersecurity programs, as shown in Figure 1.

Figure 1. Implementing the NIST Cybersecurity Framework through the HITRUST CSF and CSF Assurance Program

The NIST Cybersecurity Framework Core is essentially a set of cybersecurity activities, desired outcomes, and applicable references that are common across government and industry. The Core presents industry standards, guidelines, and practices in a manner that allows for communication of cybersecurity activities and outcomes across the organization from the executive level to the implementation/operations level, from one organization to another, and from one industry to another.
Are there any best practices or lessons learned from implementing the NIST Cyber Framework you can share?
Attendee Q&A
Leveraging a Control-Based Framework to Simplify the Risk Analysis Process

This paper discusses HIPAA risk analysis, its purpose, and how a controls-based risk management framework can be leveraged to satisfy due diligence and due care obligations and comply with HIPAA.


Healthcare Sector Cybersecurity Framework Implementation Guide

Produced by the Joint Healthcare and Private Health (HPH) Cybersecurity WG under the auspices of the Critical Infrastructure Protection Advisory Council (CIPAC), this guide provides an explanation of how healthcare organizations can leverage a control framework-based approach to information security and privacy like the HITRUST CSF to implement the objectives outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity, or Cybersecurity Framework (CsF).

Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the Content Spotlight