ecfirst Perfecting the Art of Active Cyber Defense

Quest for HITRUST Certification

A Cybersecurity Executive Brief

ISACA 2017 TOP-RATED SPEAKER

HITRUST Authorized CSF Assessor

Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP)
HITRUST (CCSFP), Member (FBI) InfraGard

Table of Contents

Executive Summary

Like the banks of a river, today's organization has a digital river flowing through it. This digital river is a river of Personally Identifiable Information (PII), Personal Data (PD), or other such sensitive and confidential information. This digital river flows through every business, every organization, across every industry, in every country. Unlike the great rivers of our planet Earth, this digital river flows through continents as a direct result of the Internet and the supply chain associated with every business – think cybersecurity supply chain.

And, like a river, the digital rivers has two banks, one that relates to compliance and regulatory mandates the business or organization must meet continually, and the other bank, cyber-attacks that are a constant threat. Failure, to address the dual requirements associated with compliance mandates and appropriate cyber defense, will result in a high disruptive risk to the business.

Any business, all business are vulnerable to disruptive cyber risk!

The key strategic challenge for senior executives is how does an organization effectively addresses the dual risks to the business – ensuring continual compliance with privacy and security mandates, and an appropriate capability to ensure assets are not compromised. That the cyber defense is credible.

There are several frameworks and standards that organizations can consider for their enterprise program, including the NIST CsF, ISO 27001, and others. And, any organization in today's interconnected web of businesses and business associates has to comply with a multitude of state, federal, and international regulatory mandates. Think HIPAA, or Texas HB.300, of the European Union's GDPR, among others.

This is where the HITRUST CSF emerges as a credible standard that every organization must examine closely to determine its application to mitigate business risks. HITRUST CSF supports a multitude of global standards and regulations, including HIPAA, HITECH, NIST CsF, PCI DSS, GDPR, 23 NYCRR 500, ISO 27001 and others.

Every business should pick a cybersecurity standard to establish the foundation for its compliance and cyber defense program. Identify a cybersecurity standard that is flexible, scalable, and comprehensive – that can be used to address a multitude of regulatory mandates – and provides the option to achieve certification. HITRUST CSF is a credible standard to "assess once, report many".

My final point is in the complex world of cybersecurity and compliance, two words are of strategic relevance. The standard you identify as the foundation for your program should be "credible," and "evidence" based. HITRUST CSF is an evidence-based standard. The HITRUST CSF delivers strategically on the relevance of these two important words - evidence and credible – and that is what establishes the foundation, the starting point for an active, cyber defense for any business, for every business.

HITRUST: Know the Facts

The HITRUST CSF is based on the ISO/IEC 27001:2005 and 27002:2005 control clauses. It includes additional domains for the information security risk management program and another devoted to privacy practices. The CSF is organized into 14 security control categories or domains, 49 control objectives, and 156 controls. The current version of HITRUST CSF is v9.2 and provides support for Singapore's PDPA, GDPR, HIPAA, HITECH, NIST CsF, and several U.S. state and other regulations.

A control consists of a control specification and supporting implementation requirements that may address policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, managerial, technical, operational, or physical nature. The CSF merges several ISO clauses in the area of development and support processes into a single control on change management.

The HITRUST Risk Management Framework is a custom framework built around a basic four-step risk management process model designed to meet the specific needs of the healthcare industry.

Step 1—Identify Risks and Define Protection Requirements

Step 2—Specify Controls

Step 3—Implement and Manage Controls

Step 4—Assess and Report

The objective of Step 4 is to assess the efficacy of implemented controls and the general management of information security against the organization's baseline. The end result of these assessment and reporting activities is a risk model that assesses internal controls and those of business associates based on the risk factors identified in Step 2.

Finally, the HITRUST approach is based on a control maturity model. This maturity model consists of five levels:

- Policy
- Procedure
- Implemented
- Measured
- Managed

HITRUST CSF Certification Requirements

HITRUST CSF v9.2 has 75 controls required for HITRUST CSF Certification. For example, the control category 0.0, Information Security Management Program, includes a requirement that an organization's Information Security Management Program (ISMP) shall be defined in terms of the characteristics of the business and established and managed using monitoring, maintenance and improvement.

Another example relates to Monitoring and Review of Third Party Services, defined in the control category for 09.0, Communications and Operations Management. This requires organizations to ensure the services, reports and records provided by the third party shall be regularly monitored and reviewed, and audits shall be carried out regularly to govern and maintain compliance with the service delivery agreements.

Figure 2 describes the 75 controls required for HITRUST CSF certification.

#	HITRUST CSF Certification Requirements	Description
0.0 - Information Security Management Program		
1.	Information Security Management Program (00.a)	An Information Security Management Program (ISMP) shall be defined in terms of the characteristics of the business and established and managed including monitoring, maintenance and improvement.
01.0 - Access Control		
2.	User Registration (01.b)	There shall be a formal documented and implemented user registration and deregistration procedure for granting and revoking access.
3.	Privilege Management (01.c)	The allocation and use of privileges to information systems and services shall be restricted and controlled. Special attention shall be given to the allocation of privileged access rights, which allow users to override system controls.
4.	User Password Management (01.d)	Passwords shall be controlled through a formal management process.
5.	Review of User Access Rights (01.e)	All access rights shall be regularly reviewed by management via a formal documented process.
6.	Clear Desk and Clear Screen Policy (01.h)	A clear desk policy for papers and removable storage media and a clear screen policy for information assets shall be adopted.