Executive Summary

Table of Contents

Click here to download the Risk Management Handbook.

HITRUST®, since 2007, has been championing and delivering solutions to address the lack of a common understanding around the security and privacy controls needed to safeguard sensitive information and individual privacy. These solutions include:

1. An industry accepted information security and privacy control framework, the HITRUST CSF, that incorporates multiple regulatory requirements and best practice standards and frameworks;
2. A standard, open, and transparent assessment process to provide accurate, consistent, and repeatable assurances around the level of protection provided by an organization; and
3. An industry recognized certification of an organization's conformity to the protection requirements specified in the HITRUST CSF® through the HITRUST Assurance™ Program.

Together, the HITRUST CSF, HITRUST Assurance Program, and related products, services, tools, and methods make up the HITRUST Risk Management Framework, or RMF.

Loosely documented in various whitepapers, articles, blogs, and other resources over more than a decade, we now bring together a discussion of the major elements of the HITRUST RMF into a single document. We first identify basic risk concepts that provide a foundation for the HITRUST RMF, discuss the concept of an RMF based on a 4-step risk management process and use the National Institute of Standards and Technology (NIST) RMF for illustration, and then discuss the major elements of the HITRUST RMF based on the same 4-step process, which include but are not limited to:

- Control framework-based risk analysis
- A patent-pending approach to quasi-quantitative residual risk analysis
- The HITRUST CSF control overlay and control specification based on inherent risk
- Implementation through appropriate segmentation of the organization and its information systems
- A patent-pending model for evaluating the overall 'rely-ability' of an assurance method
- Control implementation maturity evaluation and scoring

Special topics related to the HITRUST RMF are presented in an appendix and range from a relatively narrow discussion around how controls function relevant to the threats they are meant to address to much broader topics such as third-party risk management and evaluating assurance requirements based on the inherent risk of a specific business relationship. In most instances, the reader is referred to external documents that provide a more robust treatment of the subject matter.

By presenting the HITRUST RMF in such a way, we hope to provide the context necessary for HITRUST Organizations and Assessors to best understand, implement, and leverage the products, tools, and services they use as part of a comprehensive and robust organizational information protection and risk management program.

Table of Contents