



Virginia Information Technologies Agency

Health Information Trust Alliance (HITRUST) Common Security Framework (CSF): Proposed Work Plan and Schedule

Joseph W. Grubbs, Ph.D.
Staff Analyst

Presentation to the
Health IT Standards Advisory Committee
November 10, 2016



Background

- HITRUST Alliance (privately held company) formed in 2007 by leaders in the health care industry to establish a common framework for information security and compliance
- Developed the Common Security Framework (CSF) and CSF Assurance Program to support adoption, assessments, and compliance
- Partnered with U.S. Department of Health and Human Services beginning in 2014 to coordinate CyberRX, a series of no-cost, industry-wide simulation exercises for cyber preparedness and response



HITRUST Common Security Framework

- Developed to address security, privacy, and regulatory challenges faced by healthcare organizations
- Harmonizes and cross references existing standards and requirements: HIPAA, HITECH, NIST, ISO, PCI, FTC, COBIT and state laws
- Scales controls according to type, size, and complexity of an organization
- Provides prescriptive requirements to ensure clarity among adopters



HITRUST CSF Practical Action Plan

- Secure visible management support and commitment
- Partition organization into auditable business units
- Apply CSF to covered information regardless of form
- Apply CSF controls to all information systems
- Understand information security requirements
- Educate and train employees at all levels
- Provide adequate resources for information security management
- Implement performance measurement on information security management activities and controls



HITRUST CSF Control Categories

0. Information Security Management Program (1, 1)
 1. Access Control (7, 25)
 2. Human Resources Security (4, 9)
 3. Risk Management (1, 4)
 4. Security Policy (1, 2)
 5. Organization of Information Security (2, 11)
 6. Compliance (3, 10)
 7. Asset Management (2, 5)
 8. Physical and Environmental Security (2, 13)
 9. Communications and Operations Management (10, 32)
 10. Information Systems Acquisition, Development and Maintenance (6, 13)
 11. Information Security Incident Management (2, 5)
 12. Business Continuity Management (1, 5)
 13. Privacy Practices (3, 14)



HITRUST CSF Risk Factors

The HITRUST CSF defines a number of organizational, system, and regulatory risk factors that increase the inherent risk to an organization or system, necessitating a higher level of control:

- **Organizational Factors:** Defined based on the total inherent risk posed by the amount of sensitive information an organization holds and/or processes, or alternatively an annual number of records or the relative size of the organization based on a relevant estimator (e.g., number of beds, covered lives or transactions per year)
- **Regulatory Factors:** Defined based on the compliance requirements applicable to an organization and systems in its environment
- **System Factors:** Defined considering various system attributes that would increase the likelihood or impact of a vulnerability being exploited. These factors are to be assessed for each system or system grouping to determine the associated level of control



HITRUST CSF Document Reference

- HITRUST CSF Overview
https://hitrustalliance.net/documents/mycsf/mycsf_information/MyCSFRiskAndComplianceManagement.pdf
- HITRUST CSF Risk Assessment
https://hitrustalliance.net/documents/mycsf/mycsf_information/MyCSFRiskAssessment.pdf
- HITRUST CSF Policy Management
https://hitrustalliance.net/documents/mycsf/mycsf_information/MyCSFPolicyManagement.pdf
- HITRUST CSF Incident Management
https://hitrustalliance.net/documents/mycsf/mycsf_information/MyCSFIncidentManagement.pdf
- HITRUST CSF Corrective Action Plan Management
https://hitrustalliance.net/documents/mycsf/mycsf_information/MyCSFCAPManagement.pdf



HITRUST CSF Proposed Work Plan

Project Task	Description	Due Date / HITSAC Status Report
Task 1: Pre-Implementation Planning	Coordination among stakeholders to select target state agency; level-set on CSF implementation steps and develop a detailed implementation plan	01/31/2017 / 01/19/2017
Task 2: CSF Requirements & Specifications Analysis	Analysis of CSF requirements, controls, and related specifications; identification of performance measures to evaluate CSF implementation	03/31/2017 / 03/16/2017
Task 3: CSF Implementation & Risk Assessment	Implementation of CSF controls and risk assessment within the targeted state agency	05/30/2017 / 05/18/2017
Task 4: Performance Review & Measurement Analysis	Review and analysis of performance measurement data collected during CSF implementation	07/31/2017 / 07/20/2017
Task 5: CSF Action Plan & Recommendations	Document results from CSF implementation and performance review; develop an action plan and recommendations for enterprise adoption	09/30/2017 / 09/21/2017



Proposed HITSAC Action

- Direct HITSAC staff to work with Virginia Department of Health and other stakeholders to implement the proposed work plan and schedule



For More Information

Joseph W. Grubbs, Ph.D.

HITSAC Staff Analyst

Virginia Information Technologies Agency

Phone: (804) 467-7729

Email: Joseph.Grubbs@vita.virginia.gov