Assessment of the NIST Cybersecurity Framework

Chinstrap Penguin Corp

August 20, 2023

HITRUST®

HITRUST

Contents

HITRUST

1. The NIST Cybersecurity Framework Scorecard

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.

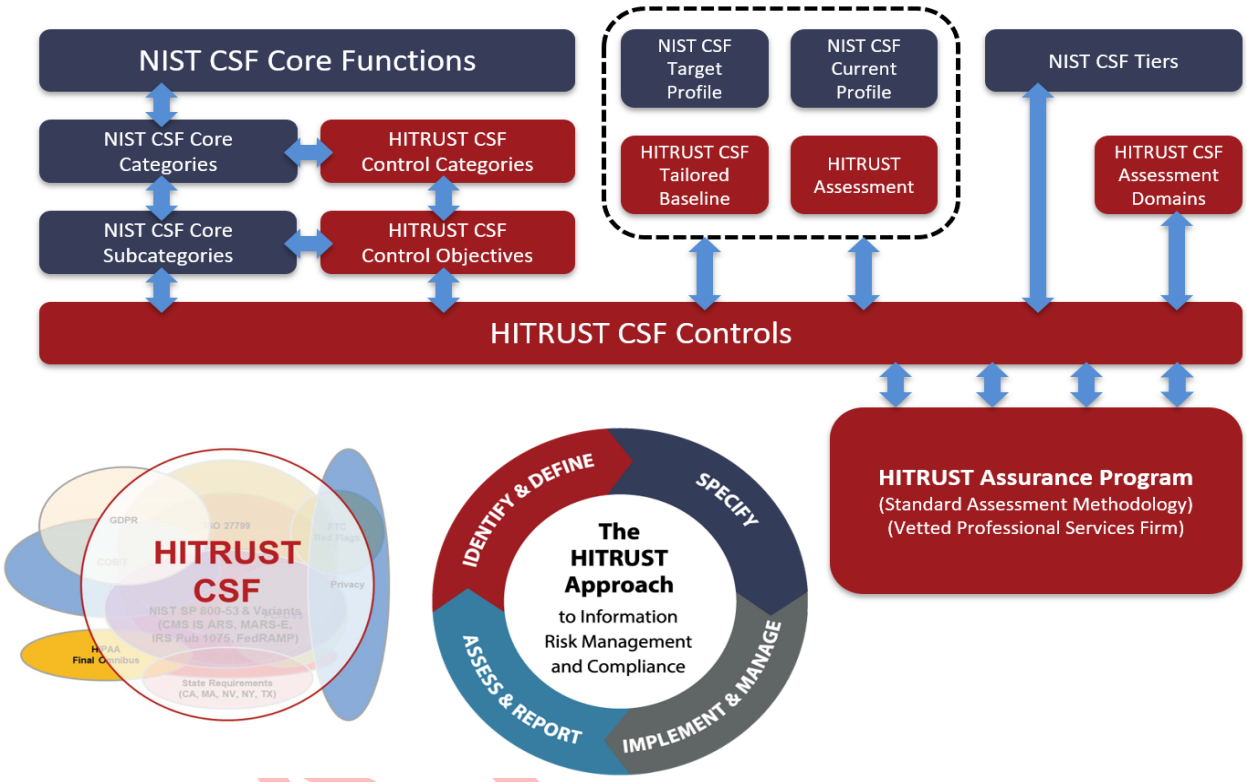

Figure 1. Implementing the NIST Cybersecurity Framework through the HITRUST CSF and CSF Assurance Program

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 an organization from the executive level to the implementation/operations level, from one organization to another, and from one industry to another.

NIST Cybersecurity Framework Core Functions provide an incident response and recovery-oriented view of an organization's cybersecurity needs; the NIST Cybersecurity Framework Core Categories provide topical groupings of cybersecurity activities related to each of the Core Functions; and the NIST Cybersecurity Framework Core Subcategories provide the specific outcomes intended for each Core Category.

HITRUST

2. Letter of NIST Cybersecurity Framework Certification

August 20, 2023

Chinstrap Penguin Corp
1234 Beach View Avenue
Las Vegas, NV 89103

Based on the results of a HITRUST® Risk-based, 2-year (r2) Validated Assessment performed by an Authorized External Assessor and documented in a HITRUST Risk-based, 2-year (r2) Validated Assessment Report ("Report"), the following platform and supporting infrastructure of the Organization ("Scope") are supported by an information protection program that is consistent with the objectives specified in the NIST Cybersecurity Framework v1.1:

Platforms:

- Customer Central (a.k.a. "Portal") residing at Pelican Data Center

Facilities:

- Pelican Data Center located in Salt Lake City, Utah, United States of America
- CP Headquarters and Manufacturing located in Las Vegas, Nevada, United States of America
- CP Framingham Manufacturing Facility located in Framingham, Massachusetts, United States of America

More specifically, HITRUST determined that:

- The HITRUST CSF controls specified by the Entity's organizational, system and regulatory risk factors provide a fair representation of its Target Profile, and
- The maturity of the Entity's implemented HITRUST CSF controls, as validated by an Authorized External Assessor and reflected in the HITRUST Scorecard for the NIST Cybersecurity Framework, provide a fair representation of its Current Profile, and
- The aggregated maturity scores for each of the Core Categories meet HITRUST's criteria for certification of the Scope addressed by the assessment.

This certification is valid for as long as the Entity's associated HITRUST Risk-based, 2-year (r2) Certification remains valid but shall not exceed a period of two years from the date of this letter.

A full copy of the HITRUST Risk-based, 2-year (r2) Validated Assessment Report has been issued to the organization listed above. The full Report contains detailed information relating to the effectiveness of information protection controls as defined by the scoping factors selected by

management. It also includes further details on the scope of the assessment, a representation letter from management, testing results, a benchmark report comparing the Organization's results to industry results, details on CAPs required for HITRUST Risk-based, 2-year (r2) Certification if applicable, and the completed questionnaire. Such detailed information can best be leveraged by individuals/organizations who are familiar with and understand the services provided by the organization listed above. If interested in obtaining a copy of the full Report, you will need to contact the Organization directly. If there are questions on interpreting the detailed contents found in the full report, please refer to the document *Leveraging HITRUST Assessment Reports: A Guide for New Users* and can contact HITRUST customer support at *support@hitrustalliance.net.*

Additional information on the HITRUST Assurance Program used to support HITRUST's certification of the NIST Cybersecurity Framework can be found on the HITRUST website: *https://hitrustalliance.net.*

HITRUST

3. NIST Target and Current Profiles

The HITRUST CSF and HITRUST Assurance Program directly support an organization's implementation of the NIST Cybersecurity Framework by specifying the controls required for its Target Profile and the assessment methodology used to provide reliable assurances about its Current Profile. Figure 2 below depicts the Organization's Target Profile viewed through the lens of the HITRUST CSF control implementation levels and industry segments. The Target Profile specifies an industry acceptable level of due care for the protection of sensitive information as determined by its organizational, system and regulatory risk factors.

Figure 2. Target Profile - HITRUST CSF Controls

The Organization's Current Profile, depicted in Figure 3 below, is determined by the HITRUST Risk-based, 2-year (r2) Validated Assessment used to support HITRUST Risk-based, 2-year (r2) Certification, which is based on a purposive sample of 75 security controls contained in the HITRUST CSF framework. The sample ensures the assessment provides relying parties reasonable assurances about an organization's implementation of the HIPAA Security Rule standards and implementation specifications; AICPA Trust Services Criteria for Security, Confidentiality and Availability; and NIST Cybersecurity Framework Core Subcategories at a reasonable cost to the assessed organization.

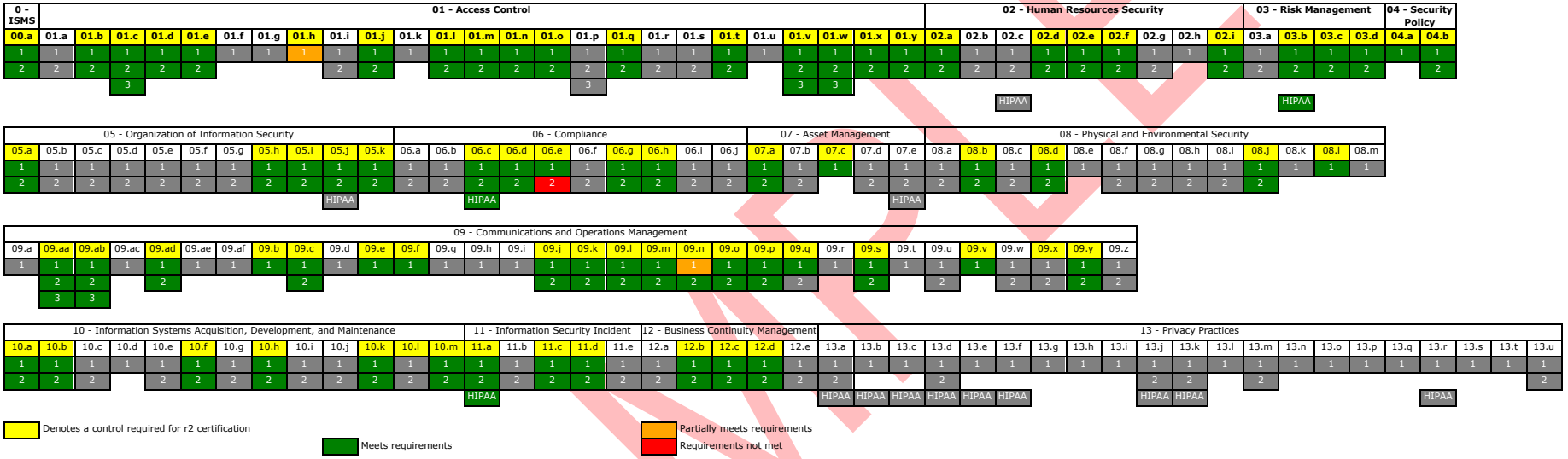

Figure 3. Current Profile - HITRUST CSF Controls (Purposive Sample)

Note more robust assurances, if needed, can be provided through a comprehensive assessment of all 135 HITRUST CSF security controls, as scoped by the Organization's risk factors.

4. HITRUST's NIST Cybersecurity Framework Scorecard

Although the Organization's Target and Current Profiles are expressed in terms of the HITRUST CSF controls, HITRUST certification of the Organization's NIST Cybersecurity Framework implementation is based on the NIST Cybersecurity Framework v1.1 Core and presented via HITRUST's NIST Cybersecurity Framework Scorecard. This Scorecard, presented in Figure 4 beginning on the next page, reflects the aggregated scores for the underlying HITRUST CSF controls as they are mapped by HITRUST to the NIST Cybersecurity Framework Core Subcategories. While HITRUST does its best to ensure the appropriate HITRUST CSF controls are mapped to each of the NIST Cybersecurity Framework v1.1 requirements, we make no representations around the suitability of the mappings as NIST might interpret them.

For more information on the HITRUST approach to assessment and certification, refer to the Risk Analysis Guide for HITRUST Organizations and Assessors, available from *https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf.*

More information about the controls framework-based approach to risk analysis and the HITRUST CSF as an industry overlay of the NIST SP 800-53 moderate-level baseline can be found in the document entitled Understanding HITRUST's Approach to Risk vs. Compliance-based Information Protection, available from *https://hitrustalliance.net/documents/csf_rmf_related/RiskVsComplianceWhitepaper.pdf.*

More information on how the HITRUST CSF is used to facilitate an organization's implementation of the NIST Cybersecurity Framework can be found in the Healthcare Sector Cybersecurity Framework Implementation Guide, available on the US CERT Cybersecurity Framework Website at *https://www.us-cert.gov/ccubedvp/cybersecurity-framework.* (Note the HITRUST CSF can be used to facilitate NIST Cybersecurity Framework implementation for any organization, regardless of industry.)

Scorecard Color Legend

Not applicable to the assessment
Requirements met (Avg. score of mapped HITRUST CSF requirements: 70-79.9)

HITRUST

Function	Status	Category	Status	Subcategory	Status
IDENTIFY(ID)		Identify: Asset Management (ID.AM)		**ID.AM-1:** Physical devices and systems within the organization are inventoried	
				ID.AM-2: Software platforms and applications within the organization are inventoried	
				ID.AM-3: Organizational communication and data flows are mapped	
				ID.AM-4: External information systems are catalogued	
				ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	
				ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	
		Identify: Business Environment (ID.BE)		**ID.BE-1:** The organization's role in the supply chain is identified and communicated	
				ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	
				ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	
				ID.BE-4: Dependencies and critical functions for delivery of critical services are established	
				ID.BE-5: Resilience requirements to support delivery of critical services are established	
		Identify: Governance (ID.GV)		**ID.GV-1:** Organizational information security policy is established	
				ID.GV-2: Information security roles & responsibilities are coordinated and aligned with internal roles and external partners	
				ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	
				ID.GV-4: Governance and risk management processes address cybersecurity risks	

Function	Status	Category	Status	Subcategory	Status
		Identify: Risk Assessment (ID.RA)		**ID.RA-1:** Asset vulnerabilities are identified and documented	
				ID.RA-2: Threat and vulnerability information is received from information sharing forums and sources	
				ID.RA-3: Threats, both internal and external, are identified and documented	
				ID.RA-4: Potential business impacts and likelihoods are identified	
				ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	
				ID.RA-6: Risk responses are identified and prioritized	
		Identify: Risk Management Strategy (ID.RM)		**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	
				ID.RM-2: Organizational risk tolerance is determined and clearly expressed	
				ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	
		Identify: Supply Chain Risk Management (ID.SC)		**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	
				ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	
				ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan	
				ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	
				ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	

Function	Status	Category	Status	Subcategory	Status
PROTECT(PR)		Protect: Identity Management and Access Control (PR.AC)		**PR.AC-1:** Identities and credentials are managed for authorized devices and users	
				PR.AC-2: Physical access to assets is managed and protected	
				PR.AC-3: Remote access is managed	
				PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties	
				PR.AC-5: Network integrity is protected, incorporating network segregation where appropriate	
				PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	
				PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks)	
		Protect: Awareness and Training (PR.AT)		**PR.AT-1:** All users are informed and trained	
				PR.AT-2: Privileged users understand roles & responsibilities	
				PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities	
				PR.AT-4: Senior executives understand roles & responsibilities	
				PR.AT-5: Physical and information security personnel understand roles & responsibilities	
		Protect: Data Security (PR.DS)		**PR.DS-1:** Data-at-rest is protected	
				PR.DS-2: Data-in-transit is protected	
				PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	
				PR.DS-4: Adequate capacity to ensure availability is maintained	
				PR.DS-5: Protections against data leaks are implemented	
				PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	

Function	Status	Category	Status	Subcategory	Status
				PR.DS-7: The development and testing environment(s) are separate from the production environment	
				PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	
		Protect: Information Protection Processes and Procedures (PR.IP)		**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained	
				PR.IP-2: A System Development Life Cycle to manage systems is implemented	
				PR.IP-3: Configuration change control processes are in place	
				PR.IP-4: Backups of information are conducted, maintained, and tested periodically	
				PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	
				PR.IP-6: Data is destroyed according to policy	
				PR.IP-7: Protection processes are continuously improved	
				PR.IP-8: Effectiveness of protection technologies is shared with appropriate parties	
				PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	
				PR.IP-10: Response and recovery plans are tested	
				PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	
				PR.IP-12: A vulnerability management plan is developed and implemented	
		Protect: Maintenance (PR.MA)		**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	

Function	Status	Category	Status	Subcategory	Status
				PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	
		Protect: Protective Technology (PR.PT)		**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	
				PR.PT-2: Removable media is protected and its use restricted according to policy	
				PR.PT-3: Access to systems and assets is controlled, incorporating the principle of least functionality	
				PR.PT-4: Communications and control networks are protected	
				PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	
DETECT(DE)		**Detect: Anomalies and Events (DE.AE)**		**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	
				DE.AE-2: Detected events are analyzed to understand attack targets and methods	
				DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	
				DE.AE-4: Impact of events is determined	
				DE.AE-5: Incident alert thresholds are established	
		Detect: Security Continuous Monitoring (DE.CM)		**DE.CM-1:** The network is monitored to detect potential cybersecurity events	
				DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	
				DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	
				DE.CM-4: Malicious code is detected	
				DE.CM-5: Unauthorized mobile code is detected	

Function	Status	Category	Status	Subcategory	Status
				DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	
				DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	
				DE.CM-8: Vulnerability scans are performed	
		Detect: Detection Processes (DE.DP)		**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	
				DE.DP-2: Detection activities comply with all applicable requirements	
				DE.DP-3: Detection processes are tested	
				DE.DP-4: Event detection information is communicated to appropriate parties	
				DE.DP-5: Detection processes are continuously improved	
RESPOND(RS)		**Respond: Analysis (RS.AN)**		**RS.AN-1:** Notifications from detection systems are investigated	
				RS.AN-2: The impact of the incident is understood	
				RS.AN-3: Forensics are performed	
				RS.AN-4: Incidents are categorized consistent with response plans	
				RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	
		Respond: Communications (RS.CO)		**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	
				RS.CO-2: Events are reported consistent with established criteria	
				RS.CO-3: Information is shared consistent with response plans	
				RS.CO-4: Coordination with stakeholders occurs consistent with response plans	
				RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	

Function	Status	Category	Status	Subcategory	Status
		Respond: Improvements (RS.IM)		**RS.IM-1:** Response plans incorporate lessons learned	
				RS.IM-2: Response strategies are updated	
		Respond: Mitigation (RS.MI)		**RS.MI-1:** Incidents are contained	
				RS.MI-2: Incidents are mitigated	
				RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	
		Respond: Response Planning (RS.RP)		**RS.RP-1:** Response plan is executed during or after an event	
RECOVER(RC)		**Recover Communications (RC.CO)**		**RC.CO-1:** Public relations are managed	
				RC.CO-2: Reputation after an event is repaired	
				RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams	
		Recover: Improvements (RC.IM)		**RC.IM-1:** Recovery plans incorporate lessons learned	
				RC.IM-2: Recovery strategies are updated	
		Recover: Recovery Planning (RC.RP)		**RC.RP-1:** Recovery plan is executed during or after an event	

Figure 4. HITRUST Scorecard for the NIST Cybersecurity Framework