HITRUST

CMMC Level 1 Insights

Based upon a HITRUST Essentials, 1-year (e1) Validated Assessment

Chinstrap Penguin Corp.

As of August 18, 2025

SAMPLE FOR ILLUSTRATIVE USE ONLY

HITRUST

Contents

HITRUST

Transmittal Letter

August 18, 2025

Chinstrap Penguin Corp.
123 Main Street
Anytown, TX 12345

Through HITRUST's "Assess Once, Report Many" capability made possible through the HITRUST CSF, HITRUST has prepared this Cybersecurity Maturity Model Certification Level 1 ("CMMC Level 1") Insights Report at the request of Chinstrap Penguin Corp. ("the Organization"). This Insights Report contains detailed information regarding the coverage and maturity of controls supporting the Organization's compliance with HITRUST CSF requirements mapping to CMMC Level 1 for the scope outlined below, based on a HITRUST Essentials, 1-year (e1) assessment using v11.6.0 of the HITRUST CSF. The Organization can leverage this report to share information regarding their CMMC Level 1 compliance efforts with internal and external stakeholders.

The full e1 validated assessment report contains detailed information relating to the maturity of information protection controls as defined by the tailoring factors selected by management of the Organization. It includes detailed assessment results, a benchmark report comparing the Organization's results to industry results, and details on corrective action plans (if applicable). Such detailed information can best be leveraged by relying parties who are familiar with and understand the services provided by the Organization. Those interested in obtaining a copy of the full report should contact the Organization directly.

Scope

The e1 assessment that this Insights Report is based upon included the following platform, facilities, and supporting infrastructure of the Organization ("Scope"):

Platform:

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

Facilities:

- CP Framingham Manufacturing Facility (Office) located in Framingham, MA, United States of America
- CP Headquarters (Office) located in Salt Lake City, UT, United States of America
- Pelican Data Center (Data Center) located in Salt Lake City, UT, United States of America

HITRUST

The Organization's Responsibilities and Assertions

Management of the Organization is responsible for the implementation, operation, and monitoring of the control environment for the Scope. Through execution of this responsibility, and completion of a HITRUST Essentials, 1-year (e1) validated assessment, the Organization asserted that management of the Organization:

- Is responsible for the implementation of information protection controls.
- Disclosed all design and operating deficiencies in their information protection controls which they are aware, including those for which they believe the cost of corrective action may exceed the benefits.
- Is not aware of any events or transactions that have occurred or are pending that would have an effect on the Essentials, 1-year (e1) validated assessment that was performed and used as a basis by HITRUST for issuing that report.
- Is not aware of communications from regulatory agencies concerning noncompliance with or deficiencies regarding the information protection controls that are included within the scope of the Essentials, 1-year (e1) validated assessment.

Management of the Organization is also solely responsible for ensuring the Organization's compliance with any legal and/or regulatory requirements, including CMMC Level 1.

External Assessor Responsibilities

External Assessors are authorized by HITRUST based upon a thorough vetting process to demonstrate their ability to perform HITRUST CSF Assessments, and individual practitioners are required to maintain appropriate credentials based on their role in HITRUST assessments. In HITRUST validated assessments, the External Assessor is responsible for the following:

- Reviewing and gaining a detailed understanding of the information provided by the Organization.
- Performing sufficient procedures to validate the control maturity scores provided by the Organization.
- Meeting all HITRUST Assessment criteria described within the HITRUST Assessment Handbook.

HITRUST's Responsibilities

HITRUST is responsible for maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization completed the accompanying Essentials, 1-year (e1)

validated assessment. HITRUST is also responsible for producing the mappings from various authoritative sources, including CMMC Level 1, to the HITRUST CSF. Additional information about HITRUST's "Assess Once, Report Many" approach and on the HITRUST CSF Assurance Program used to support this compliance assessment can be found on the HITRUST website at https://hitrustalliance.net.

Limitations of Assurance

Parties relying on this report should understand the limitations of assurance specified in the Limitations of Assurance section of this report.

HITRUST

HITRUST

CMMC Level 1 Scorecard

The tables below provide CMMC Level 1 findings for each requirement (e.g., AC.L1-B.1.I) in CMMC Level 1 for the environment assessed. Control observations associated with the CMMC Level 1 requirements, if present, are discussed in Appendix A.

These CMMC findings are based on the HITRUST assessment results of the mapped HITRUST CSF requirement(s). Where more than one HITRUST CSF requirement mapped to a CMMC requirement, a low-watermark approach is used to derive the CMMC finding. For example, a CMMC requirement with two mapped HITRUST CSF requirements—one with a control maturity of less than "Fully Compliant" in the HITRUST implemented control maturity and the other without—would result in a CMMC finding of “NOT MET”.

The Organization may have in place additional controls relevant to their CMMC compliance posture which were not evaluated in the underlying HITRUST assessment and therefore not reflected in this report.

The tables below also show the HITRUST assessment results for the HITRUST implemented control maturity level. To learn about the HITRUST control maturity evaluation and scoring approach, visit https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.

HITRUST Scorecard Color Legend

FC	Fully Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the CMMC Level 1 requirement averaged 90 - 100%.

CMMC Finding Legend

MET	The requirement was fully implemented by the Organization.
NOT MET	The requirement was not fully implemented by the Organization.
NOT APPLICABLE (N/A)	The requirement was deemed not relevant to the system or the system environment by the Organization.

The CMMC findings shown in this Insights Report have not been reviewed by a C3PAO or by the CMMC PMO and could be subject to change; they should therefore be viewed as preliminary.

HITRUST

AC - Access Control

Requirement Number	Requirement (per FAR clause 52.204-21)	Assessment Objectives (per NIST SP 171A)	CMMC Finding	HITRUST Implemented Scoring	Count of Observations
AC.L1-B.1.I	Authorized Access Control - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Determine if: [a] authorized users are identified; [b] processes acting on behalf of authorized users are identified; [c] devices (and other systems) authorized to connect to the system are identified; [d] system access is limited to authorized users; [e] system access is limited to processes acting on behalf of authorized users; and [f] system access is limited to authorized devices (including other systems).	MET	FC	0
AC.L1-B.1.II	Transaction & Function Control - Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	Determine if: [a] the types of transactions and functions that authorized users are permitted to execute are defined; and [b] system access is limited to the defined types of transactions and functions for authorized users	MET	FC	0
AC.L1-B.1.III	External Connections - Verify and control/limit connections to and use of external information systems.	Determine if: [a] connections to external systems are identified; [b] the use of external systems is identified; [c] connections to external systems are verified;	MET	FC	0

Requirement Number	Requirement (per FAR clause 52.204-21)	Assessment Objectives (per NIST SP 171A)	CMMC Finding	HITRUST Implemented Scoring	Count of Observations
		[d] the use of external systems is verified; [e] connections to external systems are controlled/limited; and [f] the use of external systems is controlled/limited.			
AC.L1-B.1.IV	Control Public Information - Control information posted or processed on publicly accessible information systems.	Determine if: [a] individuals authorized to post or process information on publicly accessible systems are identified; [b] procedures to ensure [FCI] is not posted or processed on publicly accessible systems are identified; [c] a review process is in place prior to posting of any content to publicly accessible systems; [d] content on publicly accessible systems is reviewed to ensure that it does not include [FCI]; and [e] mechanisms are in place to remove and address improper posting of [FCI].	MET	FC	0

HITRUST

IA - Identification and Authentication

Requirement Number	Requirement (per FAR clause 52.204-21)	Assessment Objectives (per NIST SP 171A)	CMMC Finding	HITRUST Implemented Scoring	Count of Observations
IA.L1-B.1.V	Identification - Identify information system users, processes acting on behalf of users, or devices.	Determine if: [a] system users are identified; [b] processes acting on behalf of users are identified; and [c] devices accessing the system are identified.	MET	FC	0
IA.L1-B.1.VI	Authentication - Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	Determine if: [a] the identity of each user is authenticated or verified as a prerequisite to system access; [b] the identity of each process acting on behalf of a user is authenticated or verified as a prerequisite to system access; and [c] the identity of each device accessing or connecting to the system is authenticated or verified as a prerequisite to system access.	MET	FC	0

This section has been truncated for the sample report

HITRUST

Assessment Context

About the HITRUST e1 Assessment and Certification

HITRUST e1 assessments address the need for a continuously-relevant cybersecurity assessment focusing on foundational cybersecurity controls and mitigations for the most pressing cybersecurity threats. Organizations successfully achieving an e1 certification can reliably demonstrate they meet a bar of essential cybersecurity hygiene.

This assessment is designed for lower assurance scenarios (such as those needing greater assurances than achieved through information security questionnaires or readiness assessments but less so than those achieved through more robust, higher effort assessments). However, an e1 assessment can also serve as a starting point for enterprises that are in the early stages of implementing their information security controls.

To ensure foundational cybersecurity is in place, e1 assessments focuses on a pre-set selection of HITRUST CSF requirements curated by HITRUST. While not a compliance assessment, the subject matter does overlap with authoritative sources sharing similar goals (such as CISA Cyber Essentials, Health Industry Cybersecurity Practices for Small Healthcare Organizations, NIST SP 800-171's "Basic" requirements, and NIST IR 7621: Small Business Information Security Fundamentals).

HITRUST's analysis of cyber threat intelligence data from leading threat intelligence providers when curating the controls considered during e1 assessments, e1 is an evolving, threat-adaptive assessment. HITRUST continually evaluates this data in relation to the controls included in the e1 to ensure that the e1 continues to address the most critical cyber threats (such as ransomware, phishing, brute force, and abuse of valid accounts).

Assessment Approach

Management represented the Organization's security posture to an internal assessor to measure the control maturity of the HITRUST CSF requirements and corresponding evaluative elements included in this assessment for the scope of the assessment. Although guidance is available from HITRUST, the nature, timing, and extent of the procedures were designed entirely by the internal assessor.

Each requirement in the HITRUST CSF contains one or more evaluative elements. For example, requirement 0322.09u2Organizational.12, which reads "Media is encrypted when onsite unless physical security can be guaranteed, and always when offsite.", contains the following two evaluative elements: "1. The organization restricts the use of writable, removable media in organizational systems." and "2. The organization restricts the use of personally owned, removable media in organizational systems". The implementation and operation of all evaluative elements associated with applicable HITRUST CSF requirements included in the assessment was evaluated by the external assessor in reaching an implementation score.

HITRUST developed a scoring rubric that is used by internal or external assessors to determine implementation scoring in a consistent and repeatable way by evaluating both implementation strength and implementation coverage, described as follows:

- The HITRUST CSF requirement's implementation strength is evaluated using a 5-point scale (tier 0 through tier 4) by considering the requirement's implementation and operation across the assessment scope, which consists of all organizational and system elements, including the physical facilities and logical systems / platforms, within the defined scope of the assessment.

- The HITRUST CSF requirement's implementation coverage is evaluated using a 5-point scale (very low through very high) by considering the percentage of the requirement's evaluative elements implemented and operating within the scope of the assessment.

The implementation scoring model utilized on e1 assessments incorporates the following scale. The overall score for each HITRUST CSF requirement ranges from 0 to 100 points in quarter increments based directly on the requirement's implementation score.

Implementation Score	Description	Points Awarded
Not Compliant (NC)	Very few if any of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment. Rough numeric equivalent of 0% (point estimate) or 0% to 10% (interval estimate).	0
Somewhat Compliant (SC)	Some of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 25% (point estimate) or 11% to 32% (interval estimate).	25
Partially Compliant (PC)	About half of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 50% (point estimate) or 33% to 65% (interval estimate).	50
Mostly Compliant (MC)	Many but not all of the evaluative elements in HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 75% (point estimate) or 66% to 89% (interval estimate).	75
Fully Compliant (FC)	Most if not all of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 100% (point estimate) or 90% to 100% (interval estimate).	100

Scope of the Assessment

Company Background

Chinstrap Penguin Corp is a manufacturer, retailer and distributor of widgets for use in the care, feeding and housing of all Antarctic Chinstrap Penguins. Chinstrap Penguin Corp was established in 2005 and has grown to one of the largest widget producers in the world and now offers a number of specialized widgets to its customers and third-party distributors. In 2014 Chinstrap Penguin Corp entered the gadget market by acquiring Gadget Group and is now the third largest gadget manufacturer in the United States.

In-Scope Platform

The following table describes the platform that was included in the scope of this assessment.

Customer Central (a.k.a. "Portal")	
Description	The Portal is a platform that allows numerous applications and service offerings to be accessed by customers via a single web-based interface via a browser. It does this for numerous customers and allows their customers to obtain information in a single location. Chinstrap Penguin personnel access the Portal through a secure VPN to a bastion host. From the bastion host systems administrators connect via VDI to an administrative console for management of all in-scope applications and supporting infrastructure. The Portal is developed by Chinstrap Penguin personnel. It is built in Java and .Net. The solution leverages VMWare for scalability. The applications/service offerings that make up the Portal are Penguin Nest, Penguin Analytics, and South Pole Benefit Eligibility. • Penguin Nest is an application that delivers content and applications from customer systems via the Portal. The application collects and feeds critical metrics to Penguin Analytics. • Penguin Analytics is an application that delivers reporting and analytics capability to customers. It allows them to develop dashboards and reports and track KPIs with their information that is stored within the Portal. • South Pole Benefits Eligibility allows our customers to provide benefit eligibility information so that users of the system have a single place to go to get the eligibility information from multiple customers. Meta data from the application is fed to Penguin Analytics for further analysis by customers.
Application(s)	Penguin Nest, Penguin Analytics, South Pole Benefits Eligibility
Database Type(s)	Oracle
Operating System(s)	HP-UX

Customer Central (a.k.a. "Portal")	
Residing Facility	Pelican Data Center
Exclusion(s) from scope	Content and applications from customer systems that are delivered via the Portal are outside the scope of this assessment. This includes customers who choose to leverage the embedded credit card processing page, which is offered as an add-on service. The embedded credit processing page is provided and managed by a third-party service provider.

In-Scope Facilities

The following table presents the facilities that were included in the scope of this assessment.

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
Pelican Data Center	Data Center	Yes	-	Salt Lake City	UT	United States of America
CP Headquarters	Office	No	-	Salt Lake City	UT	United States of America
CP Framingham Manufacturing Facility	Office	No	-	Framingham	MA	United States of America

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this e1 assessment. Organizations undergoing e1 assessments have two options of how to address situations in which a HITRUST CSF requirement is fully or partially performed by a service provider (e.g., by a cloud service provider):

- The Inclusive method, whereby HITRUST CSF requirements performed by the service provider are included within the scope of the assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing by the external assessor, and

- The Exclusive (or Carve-out) method, whereby HITRUST CSF requirements performed by the service provider are excluded from the scope of the assessment and marked N/A with supporting commentary explaining that the HITRUST CSF requirement is fully performed by a party other than the assessed entity (for fully outsourced controls) or through commentary explaining the excluded partial performance of the HITRUST CSF requirement (for partially outsourced controls).

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Pelican Hosting	Pelican Hosting provides a colocation facility where Chinstrap maintains a dedicated cage. Pelican Hosting personnel do not have logical access to any in-scope systems.	Included

Use of the Work of Others

For certain portions of the assessment and as allowed by HITRUST's Assurance Program requirements, the external assessor may have utilized the work of other assessors, auditors, and/or inspectors in lieu of direct testing. All assessment Use of the Work of Others, including those where the external assessor utilized the work of others, were subject to HITRUST's quality assurance review procedures. The table below details assessments utilized by the external assessor.

Potential options available for using the work of others allowed by HITRUST's Assurance Program Requirements include the following and are reflected in the "Utilization Approach" column of the below table if leveraged in this assessment:

- Inheritance of results from or reliance on another HITRUST validated assessment,
- Reliance on a recent third-party assurance report, and/or
- Reliance on testing performed by the assessed entity (i.e., by internal assessors).

Work of other assessors was not relied upon in the HITRUST CSF assessment underlying this compliance insights report (i.e., no inheritance or third-party reliance was utilized).

Limitations of Assurance

Relying parties should consider the following in its evaluation of the findings in this report:

- This Insights Report provides transparency into the current state of CMMC Level 1 coverage and control maturity within the scoped environment for the Organization as described in the 'Coverage and Reportability' section above. This Insights Report supports the Organization in communicating the status of controls supporting CMMC Level 1 compliance and is not a certification of CMMC Level 1 compliance.

- This Insights Report accompanies a HITRUST CSF e1 Validated assessment. The accompanying e1 Validated assessment was scoped and performed in accordance with the HITRUST Assurance Program requirements designed to measure and report on control maturity for purposes of issuing HITRUST validated assessment reports. Consequently:

    - The nature, timing, and extent of the procedures performed by the HITRUST External Assessor Organization may differ from those performed in an assessment dedicated exclusively to evaluating CMMC Level 1 compliance and were not designed to specifically detect all instances of CMMC Level 1 non-compliance.

    - Compliance deficiencies noted in this report, if any, were identified through an evaluation of control maturity of the HITRUST CSF requirements mapping to CMMC Level 1 included in the Organization's HITRUST validated assessment and not in observance of any other criteria specific to CMMC Level 1 requirements.

- Mappings produced by HITRUST to authoritative sources are performed utilizing the NIST OLIR Program methodology outlined in NIST Interagency Report 8278 and subjected to HITRUST's internal quality review process.

- No assessment of controls or compliance status provides total assurance or 100% protection against possible control failures and instances of non-compliance. Because of their nature, controls may not prevent, or detect and correct, all errors or omissions relevant to compliance with regulatory statutes.

CMMC Overview

The Cybersecurity Maturity Model Certification (CMMC) Program was developed by the U.S. Department of Defense (DoD) as part of a broader effort to enhance cybersecurity across its supply chain. The CMMC Program verifies that contractors have implemented required security measures necessary to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

The CMMC model measures the implementation of cybersecurity requirements at 3 progressively advanced levels. The level that a contractor is required to achieve depends on the type and sensitivity of the FCI and/or CUI entrusted with the organization. Each level consists of a set of CMMC requirements as set forth in 32 CFR § 170.14 (c).

- Level 1: Focuses on the protection of FCI and consists of 15 basic cyber hygiene requirements aligned with Federal Acquisition Regulation (FAR) clause 52.204-21(b)(1)(i) – (b)(1)(xv). Level 1 requires an annual self-assessment and annual affirmation.

- Level 2: Focuses on the protection of CUI and consists of 110 requirements identical to the requirements in NIST SP 800-171 r2. Level 2 requires a C3PAO certification assessment every 3 years (or a self-assessment every 3 years for select programs) and annual affirmation.

- Level 3: Focuses on the protection of higher-priority or more sensitive CUI and consists of the 110 NIST SP 800-171 r2 requirements that make up Level 2 along with 24 additional requirements from NIST SP 800-172. Level 3 requires Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) certification assessment every three years and annual affirmation.

This Insights Report is limited to CMMC Level 1.

HITRUST

CMMC Level 1 Coverage and Reportability

A HITRUST validated assessment can provide evidence that specific HITRUST CSF control requirements mapping to CMMC Level 1 requirements have been implemented, how well they have been implemented, and the nature and volume of identified gaps in implementation. The HITRUST CSF, the inherent mappings to CMMC Level 1 as a supported authoritative source, and HITRUST's comprehensive assurance program are important tools for organizations with CMMC Level 1 compliance obligations.

The following factors collectively determine the degree of CMMC Level 1 coverage and reportability in a HITRUST assessment:

- HITRUST's approach to incorporating CMMC Level 1 into the HITRUST CSF
- The Organization's assessment type selection, HITRUST CSF version selection, and assessment tailoring

Approach to incorporating CMMC Level 1 into the HITRUST CSF:

Each CMMC Level 1 requirement has Assessment Objectives that are equivalent to the NIST SP 800-171A r2 determination statements that correspond to the CMMC requirement. The results of a CMMC Level 1 self-assessment are based on whether each of the Assessment Objectives are implemented. Each requirement statement results in a finding of:

- MET when all applicable Assessment Objectives for the security requirement are satisfied based on evidence.
- NOT MET when one or more Assessment Objectives of the security requirement is not satisfied.
- NOT APPLICABLE when the Assessment Objectives do not apply at the time of the assessment.

The HIRUST CSF maps to CMMC Level 1 by mapping HITRUST requirement statements to the Assessment Objectives (NIST SP 800-171A r2 determination statements) for each CMMC Level 1 requirement.

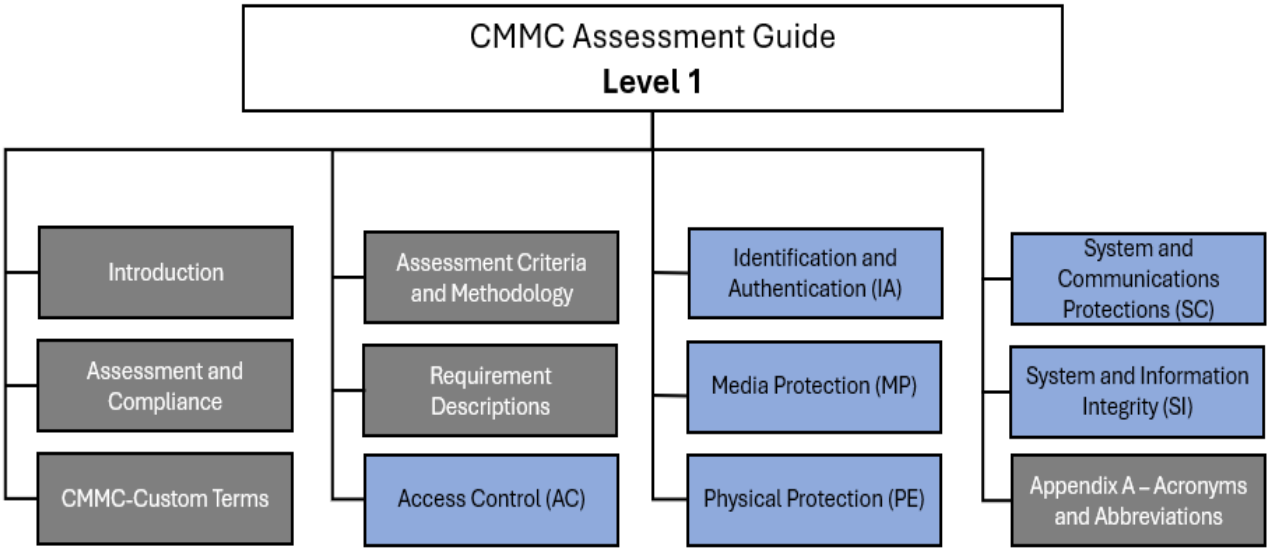
See below an example of a CMMC Level 1 Requirement and its Assessment Objectives.

CMMC Level 1 Requirement AC.L1-B.1.I	Assessment Objectives (NIST SP 800-171A r2 3.1.1)
Authorized Access Control - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	Determine if: [a] authorized users are identified; [b] processes acting on behalf of authorized users are identified; [c] devices (and other systems) authorized to connect to the system are identified; [d] system access is limited to authorized users; [e] system access is limited to processes acting on behalf of authorized users; and [f] system access is limited to authorized devices (including other systems).

The DoD has published the CMMC Assessment Guide - Level 1 that provides guidance for the preparation for and execution of a CMMC Level 1 self-assessment. The HITRUST CSF intentionally does not provide full coverage of the CMMC Level 1 Assessment Guide and intentionally does not contain mappings / cross-references to all text in the CMMC Level 1 Assessment Guide. Like many other authoritative sources, the CMMC Level 1 Assessment Guide contains several sections that are not directly actionable by organizations needing to achieve or evaluate compliance. The non-actionable sections are concentrated at the beginning (Introduction, Assessment and Compliance, CMMC-Custom Terms, Assessment Criteria and Methodology, and Requirement Descriptions) and ending (Appendix A: Acronyms and Abbreviations).

Like many other authoritative sources, the CMMC Level 1 Assessment Guide contains several sections that are not directly actionable by organizations needing to achieve or evaluate compliance. The non-actionable sections are concentrated at the beginning (Introduction, Assessment and Compliance, CMMC-Custom Terms, Assessment Criteria and Methodology, and Requirement Descriptions) and ending (Appendix A: Acronyms and Abbreviations).

The HITRUST CSF's coverage of the CMMC Assessment Guide - Level 1 at a high level, is as follows:



Assessment preferences and tailoring

HITRUST assessments are performed against a subset of HITRUST CSF's numerous requirements. The requirements included in the accompanying HITRUST assessment have been tailored based on the unique risks and compliance needs of the Organization.

Through tailoring, organizations can optionally add authoritative sources into their e1 assessments. When this occurs, the assessment is expanded to consider additional requirements mapping to the information security and/or privacy-related portions of the included authoritative sources. The resulting, tailored HITRUST e1 assessment then serves to directly evaluate the Organization's adherence to a subset of the HITRUST CSF and indirectly evaluate the assessed entity's compliance with the information security and/or privacy aspects of the included authoritative source(s).

The HITRUST CSF is constantly updated by HITRUST in response to changes in the cybersecurity threat landscape and updates to included authoritative sources. Organizations can utilize the most recent HITRUST CSF version in HITRUST e1 assessments. As HITRUST advances the framework, more and better reporting capabilities are unlocked. Not all versions allow for HITRUST insights reporting against CMMC Level 1; instead, only assessments utilizing version 11.6.0 and later can create CMMC Level 1 Insights Reports. The HITRUST assessment underlying this CMMC Level Insights Report utilized HITRUST CSF version v11.6.0.

HITRUST

CMMC Level

The CMMC model measures the implementation of cybersecurity requirements at 3 progressively advanced levels. Only CMMC Level 1 is available for addition into HITRUST e1 assessments using version v11.6.0.

CMMC Level(s) selected by the Organization	Level 1

Appendix A: CMMC Level 1-relevant Observations

During the Essentials, 1-year (e1) validated assessment, no deficiencies were noted during the evaluation of any HITRUST CSF requirements mapping to the considered CMMC Level 1 requirements.

HITRUST

Appendix B: Relevant HITRUST Assessment Results and Mappings

Below are the assessment results and control maturity evaluations for each assessed HITRUST CSF requirement mapped to the areas of CMMC Level 1 considered in the underlying HITRUST CSF assessment, organized by CMMC requirement.

This section also shows the HITRUST CSF requirements mapped by HITRUST to each considered CMMC requirement. Note that many more mappings exist between CMMC and the HITRUST CSF; this section lists only the mapping subset relevant to the underlying HITRUST assessment as determined through the factors described in the CMMC Level 1 Coverage and Reportability section of this document.

In addition to CMMC Level 1, the HITRUST CSF is mapped to dozens of additional authoritative sources, enabling a wide range of compliance coverage within HITRUST Assessments. Mappings produced by HITRUST are performed utilizing the NIST OLIR Program methodology outlined in NIST Interagency Report 8278. These mappings were created by HITRUST and have undergone HITRUST's internal quality review process consisting of at least five of review before being finalized: automated review, initial mapper review, peer review, management review, and quality assurance review. Questions about these mappings should be routed to HITRUST's Support team.

AC - Access Control

CMMC Level 1 Requirement:	AC.L1-B.1.I . Authorized Access Control - Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	*CMMC Finding: MET*
Assessment Objectives: Determine if: [a] authorized users are identified; [b] processes acting on behalf of authorized users are identified; [c] devices (and other systems) authorized to connect to the system are identified; [d] system access is limited to authorized users; [e] system access is limited to processes acting on behalf of authorized users; and [f] system access is limited to authorized devices (including other systems).		
Mapped HITRUST CSF Requirement Statement	BUID: 1143.01c1System.123 / CVID: 0035.0. The allocation of privileges for all systems and system components is controlled through a formal authorization process. The organization ensures access privileges associated with each system product (e.g., operating system, database management system and each application) and the users associated with each system product which need to be allocated are identified. Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (e.g., the minimum requirement for their functional role–user or administrator, only when needed).	
Implemented Control Maturity Score Per HITRUST Validated Assessment	Fully Compliant (100%)	

Mapped HITRUST CSF Requirement Statement	BUID: 0820.01k1System.3 / CVID: 0933.0. The organization uniquely identifies and authenticates network devices that require authentication mechanisms before establishing a connection. Network devices that require authentication mechanisms use shared information (e.g., MAC or IP address) to control remote network access and access control lists to control remote network access.
Implemented Control Maturity Score Per HITRUST Validated Assessment	Fully Compliant (100%)

Mapped HITRUST CSF Requirement Statement	BUID: 11110.01q2System.10 / CVID: 0205.0. Non-organizational users, or processes acting on behalf of non-organizational users, determined to need access to information residing on the organization's information systems, are uniquely identified and authenticated.
Implemented Control Maturity Score Per HITRUST Validated Assessment	Fully Compliant (100%)

CMMC Level 1 Requirement:	AC.L1-B.1.II . Transaction & Function Control - Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	*CMMC Finding: MET*
Assessment Objectives: Determine if: [a] the types of transactions and functions that authorized users are permitted to execute are defined; and [b] system access is limited to the defined types of transactions and functions for authorized users		
Mapped HITRUST CSF Requirement Statement	BUID: 1143.01c1System.123 / CVID: 0035.0. The allocation of privileges for all systems and system components is controlled through a formal authorization process. The organization ensures access privileges associated with each system product (e.g., operating system, database management system and each application) and the users associated with each system product which need to be allocated are identified. Privileges are allocated to users on a need-to-use basis and on an event-by-event basis in line with the access control policy (e.g., the minimum requirement for their functional role–user or administrator, only when needed).	
Implemented Control Maturity Score Per HITRUST Validated Assessment	Fully Compliant (100%)	

This section has been truncated for the sample report

Appendix C: HITRUST Background

HITRUST Alliance, Inc. was born out of the belief that information security should be a core pillar of, rather than an obstacle to, the broad adoption of information systems and exchanges. HITRUST®, in collaboration with industry, business, technology and information security leaders, established the HITRUST CSF, a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal, sensitive, and/or financial information.

Beyond the establishment of the HITRUST CSF®, HITRUST is also driving the adoption of and widespread confidence in the framework and sound risk management practices through awareness, education, advocacy, and other outreach activities.

An integral component to achieving HITRUST's goal to advance the protection of sensitive information is the establishment of a practical mechanism for validating an organization's compliance with the HITRUST CSF.

The HITRUST CSF is an overarching security framework that incorporates and leverages the existing security requirements placed upon organizations, including international (GDPR, ISO), federal (e.g., FFIEC, HIPAA and HITECH), state, third party (e.g., PCI and COBIT), and other government agencies (e.g., NIST, FTC, and CMS). The HITRUST CSF is already being widely adopted by leading organizations in a variety of industries as their information protection framework.

HITRUST has developed the HITRUST Assurance Program, which encompasses the common requirements, methodology and tools that enable both an organization and its business partners to take a consistent and incremental approach to managing compliance.

The HITRUST Assurance Program is the mechanism that allows organizations and their business partners and vendors to assess and report against multiple sets of requirements. Unlike other programs, the oversight, vetting, and governance provided by HITRUST and the HITRUST Assessor Council affords greater assurances and security across all industries.

For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit https://hitrustalliance.net.