HITRUST

NIST SP 800-171 Insights

Based upon a HITRUST Risk-based, 2-year (r2) Validated Assessment

Chinstrap Penguin Corporation

As of February 26, 2024

SAMPLE FOR ILLUSTRATIVE USE ONLY

HITRUST

Contents

© 2024 HITRUST Alliance
HITRUSTAlliance.net

HITRUST

1. Transmittal Letter

February 26, 2024

Chinstrap Penguin Corporation
123 Main Street
Anytown, TX 12345

Through HITRUST's "Assess Once, Report Many" capability made possible through the HITRUST CSF, HITRUST has prepared this NIST SP 800-171 Revision 3: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations ("NIST SP 800-171") Insights Report at the request of Chinstrap Penguin Corp. ("the Organization"). This Insights Report contains detailed information relating to the coverage and maturity of controls supporting the Organization's compliance with aspects of NIST SP 800-171 for the scope outlined below, based on control validation procedures executed during a HITRUST Risk-based, 2-year (r2) validated assessment using v11.4.0 of the HITRUST CSF. The Organization can leverage this report to share information regarding their NIST SP 800-171 compliance efforts with internal and external stakeholders.

The full r2 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 r2 assessment that this Insights Report is based upon included the following of the Organization ("Scope"):

Platform:

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

Facility:

- CP Framingham Manufacturing Facility (Other) located in Framingham, Massachusetts, United States of America
- CP Headquarters and Manufacturing (Office) located in Las Vegas, Nevada, United States of America
- Pelican Data Center (Data Center) managed by Pelican Hosting located in Salt Lake City, Utah, United States of America

© 2024 HITRUST Alliance
HITRUSTAlliance.net

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 Risk-based, 2-year (r2) Validated Assessment, the Organization asserted that management of the Organization:

- Is responsible for the implementation of information protection controls.
- Has made available to the HITRUST External Assessor all records and necessary documentation related to the information protection controls included within the scope of the Risk-based, 2-year (r2) Validated Assessment.
- 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 Risk-based, 2-year (r2) 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 Risk-based, 2-year (r2) Validated Assessment.

Section 3 of NIST SP 800-171 requires organizations to conduct a risk assessment, specifically to "assess the risk (including supply chain risk) of unauthorized disclosure resulting from the processing, storage, or transmission of CUI" and to "update risk assessments" at an organization-defined frequency. While numerous HITRUST CSF requirements dealing with the Organization's performance of risk analyses are evaluated during HITRUST CSF assessments, HITRUST CSF assessments are not risk assessments. Management of the Organization is responsible for performing and maintaining a risk analysis which adheres to 3.11.01 of NIST SP 800-171.

Management of the Organization is also solely responsible for ensuring the Organization's compliance with any legal and/or regulatory requirements, including NIST SP 800-171.

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:

© 2024 HITRUST Alliance
HITRUSTAlliance.net

- 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 the maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization and an Authorized HITRUST External Assessor completed this assessment.

HITRUST is also responsible for producing the mappings from various authoritative sources, including NIST SP 800-171, 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

© 2024 HITRUST Alliance
HITRUSTAlliance.net

HITRUST

2. NIST SP 800-171 Scorecard

The tables below provide insights on NIST SP 800-171 compliance for the environment assessed. Each NIST SP 800-171 requirement listed is assigned a compliance score for the policy, procedure, and implemented control maturity levels. The compliance scores are based on the assessment results of the HITRUST CSF requirement(s) as mapped to the NIST SP 800-171 requirement. The measured and managed control maturity levels are not included in this scorecard, as these control maturity levels were not assessed in the underlying HITRUST CSF assessment as a result of the Organization's assessment tailoring.

The Organization may have in place additional controls relevant to their NIST SP 800-171 compliance posture which were not evaluated in the underlying HITRUST assessment and therefore not reflected in this report.

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.

Scorecard Color Legend

SC	Somewhat Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the NIST SP 800-171 requirement averaged 11 - 32.99%.
MC	Mostly Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the NIST SP 800-171 requirement averaged 66 - 89.99%.
FC	Fully Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the NIST SP 800-171 requirement averaged 90 - 100%.
Does Not Apply	Does Not Apply: Based on information provided by the Organization (as outlined in the "Scope of the Assessment" and "Organizational characteristics impacting NIST SP 800-171" sections of this document), the NIST SP 800-171 requirement does not apply to the scoped aspects of the Organization.

© 2024 HITRUST Alliance
HITRUSTAlliance.net

HITRUST

3.1 - Access Control

3.1 - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
03.01.01 Account Management				
03.01.01.a	Account Management	FC	FC	FC
03.01.01.b	Account Management	FC	FC	FC
03.01.01.c.1	Account Management	FC	FC	FC
03.01.01.c.2	Account Management	FC	FC	FC
03.01.01.c.3	Account Management	FC	FC	FC
03.01.01.d.1	Account Management	FC	FC	FC
03.01.01.d.2	Account Management	FC	FC	FC
03.01.01.e	Account Management	FC	FC	FC
03.01.01.f.1	Account Management	FC	FC	FC
03.01.01.f.2	Account Management	FC	FC	FC
03.01.01.f.3	Account Management	FC	FC	FC
03.01.01.f.4	Account Management	FC	FC	FC
03.01.01.f.5	Account Management	MC	MC	MC
03.01.01.g.1	Account Management	FC	FC	FC
03.01.01.g.2	Account Management	FC	FC	FC
03.01.01.g.3	Account Management	FC	FC	FC
03.01.01.h	Account Management	FC	FC	FC
03.01.02 Access Enforcement				
03.01.02	Access Enforcement	FC	FC	FC
03.01.03 Information Flow Enforcement				
03.01.03	Information Flow Enforcement	FC	FC	FC
03.01.04 Separation of Duties				
03.01.04.a	Separation of Duties	FC	FC	FC
03.01.04.b	Separation of Duties	FC	FC	FC
03.01.05 Least Privilege				
03.01.05.a	Least Privilege	FC	FC	FC
03.01.05.b	Least Privilege	FC	FC	FC
03.01.05.c	Least Privilege	FC	FC	FC
03.01.05.d	Least Privilege	FC	FC	FC
03.01.06 Least Privilege – Privileged Accounts				
03.01.06.a	Least Privilege – Privileged Accounts	FC	FC	FC

HITRUST

3.1 - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
03.01.06.b	Least Privilege – Privileged Accounts	FC	FC	FC
03.01.07 Least Privilege – Privileged Functions				
03.01.07.a	Least Privilege – Privileged Functions	FC	FC	FC
03.01.07.b	Least Privilege – Privileged Functions	FC	FC	FC
03.01.07 Unsuccessful Logon Attempts				
03.01.08.a	Unsuccessful Logon Attempts	FC	FC	FC
03.01.08.b	Unsuccessful Logon Attempts	FC	FC	FC
03.01.09 System Use Notification				
03.01.09	System Use Notification	FC	FC	FC
03.01.10 Device Lock				
03.01.10.a	Device Lock	FC	FC	FC
03.01.10.b	Device Lock	FC	FC	FC
03.01.10.c	Device Lock	FC	FC	FC
03.01.11 Session Termination				
03.01.11	Session Termination	FC	FC	FC
03.01.12 Remote Access				
03.01.12.a	Remote Access	FC	FC	FC
03.01.12.b	Remote Access	FC	FC	FC
03.01.12.c	Remote Access	FC	FC	FC
03.01.12.d	Remote Access	FC	FC	FC
03.01.16 Wireless Access				
03.01.16.a	Wireless Access	FC	FC	FC
03.01.16.b	Wireless Access	FC	FC	FC
03.01.16.c	Wireless Access	FC	FC	FC
03.01.16.d	Wireless Access	FC	FC	FC
03.01.18 Access Control for Mobile Devices				
03.01.18.a	Access Control for Mobile Devices	FC	FC	FC
03.01.18.b	Access Control for Mobile Devices	FC	FC	FC
03.01.18.c	Access Control for Mobile Devices	FC	FC	FC
03.01.20 Use of External Systems				
03.01.20.a	Use of External Systems	FC	FC	FC
03.01.20.b	Use of External Systems	FC	FC	FC
03.01.20.c.1	Use of External Systems	FC	FC	FC

3.1 - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
03.01.20.c.2	Use of External Systems	FC	FC	FC
03.01.20.d	Use of External Systems	FC	FC	FC
03.01.22 Publicly Accessible Content				
03.01.22.a	Publicly Accessible Content	FC	FC	FC
03.01.22.b	Publicly Accessible Content	FC	FC	FC

3.2 - Awareness and Training

3.2 - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
03.02.01 Literacy Training and Awareness				
03.02.01.a.01	Literacy Training and Awareness	FC	FC	FC
03.02.01.a.02	Literacy Training and Awareness	FC	FC	FC
03.02.01.a.03	Literacy Training and Awareness	FC	FC	FC
03.02.01.b	Literacy Training and Awareness	FC	FC	FC
03.02.02 Role-Based Training				
03.02.02.a.01	Role-Based Training	FC	FC	FC
03.02.02.a.02	Role-Based Training	FC	FC	FC
03.02.02.b	Role-Based Training	FC	FC	FC

This table has been truncated for this sample report

HITRUST

3. Assessment Context

About the HITRUST r2 Assessment and Certification

The HITRUST r2 assessment provides the highest level of information protection and compliance assurance. It is the most comprehensive and robust HITRUST certification, and can be optionally tailored to include coverage for additional authoritative sources such as HIPAA, the NIST Cybersecurity Framework, and GDPR.

The HITRUST r2 assessment is an evolving, threat-adaptive assessment with an accompanying certification. HITRUST r2 assessments leverage threat intelligence data and best practice controls to deliver an assessment that addresses relevant practices and active cyber threats. To do this, HITRUST continually evaluates cybersecurity controls to identify those relevant to mitigating known risks using cyber threat intelligence data from leading threat intelligence providers. Therefore, the HITRUST r2 includes controls that exclusively address emerging cyber threats actively being targeted today.

Assessment Approach

An *Authorized HITRUST External Assessor Organization* (the "External Assessor") performed validation procedures to measure the control maturity of the HITRUST CSF requirements and corresponding evaluative elements included in this assessment for the scope of the assessment. These validation procedures were designed by the External Assessor based upon the assessment's scope in observance of HITRUST's CSF Assurance Program Requirements and consisted of inquiry with key personnel, inspection of evidence (e.g. access lists, logs, configuration, sample items, policies, procedures, diagrams), on-site or virtual observations, (optionally) utilization of the work of others (as described elsewhere in this report), and (optionally) reperformance of controls.

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.

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

2025 HITRUST Alliance
HITRUSTAlliance.net

Implementation Score	Description	Points Awarded
Somewhat complaint (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

Risk Factors

The assessed entity completed the following tailoring questionnaire to derive this assessment's customized set of HITRUST CSF requirements based on organizational, technical, and regulatory risk factors.

Assessment Type	
HITRUST Risk-based, 2-year (r2) Security Assessment	
General Risk Factors	
Do you offer Infrastructure as a Service (IaaS)?	No
Organization Type	Service Provider (Information Technology, IT)
Organizational Risk Factors	
Number of Records that are currently held	Between 10 and 60 Million Records
Technical Risk Factors	

© 2025 HITRUST Alliance
HITRUSTAlliance.net

Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	Yes
Is any aspect of the scoped environment hosted on the cloud?	No - testing
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	Yes
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	No - testing
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - testing
Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)?	No - testing
Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?	Yes
Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - testing
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	Yes
Is the system(s) accessible from the Internet?	Yes
Number of interfaces to other systems	25 to 75
Number of transactions per day	6,750 to 85,000
Number of users of the system(s)	Fewer than 500
Is the system(s) publicly positioned?	No - testing
Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?	No - testing
Does the system(s) transmit or receive data with a third-party?	No - testing
Are hardware tokens used as an authentication method within the scoped environment?	No - testing
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - testing

© 2025 HITRUST Alliance
HITRUSTAlliance.net

Are wireless access points in place at any of the organization's in-scope facilities?	No - testing

Compliance Factors (Optional)
HICP 2023 Edition > For Large Orgs.
HICP 2023 Edition > For Medium Orgs.
HICP 2023 Edition > For Small Orgs.
Ontario Personal Health Information Protection Act > Health Data Institute
StateRAMP r5 > Impact level: Moderate
AI Risk Management > NIST AI RMF & ISO/IEC 23894
NIST SP 800-171 r3

© 2025 HITRUST Alliance
HITRUSTAlliance.net

4. 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 Platforms

The following tables 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

SAMPLE

© 2023 HITRUST Alliance
HITRUSTAlliance.net

Customer Central (a.k.a. "Portal")	
Database Type(s)	Oracle
Operating System(s)	HP-UX
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
CP Framingham Manufacturing Facility	Other	No	(None)	Framingham	Massachusetts	United States of America
CP Headquarters and Manufacturing	Office	No	(None)	Las Vegas	Nevada	United States of America
Pelican Data Center	Data Center	Yes	Pelican Hosting	Salt Lake City	Utah	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 r2 assessment. HITRUST requires the inclusive method must be used on HITRUST r2 validated assessments. Under the Inclusive method, HITRUST CSF requirements performed by the

EXAMPLE

© 2023 HITRUST Alliance
HITRUSTAlliance.net

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.

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Seashore Offsite Data Storage	Seashore provides backup tape delivery and storage in a secure offsite facility. No customer, covered, otherwise confidential information is stored at Seashore's facilities, however.	Included
Pelican Hosting	Pelican Hosting provides a colocation facility where Chinstrap Penguin maintains a dedicated cage. Pelican Hosting personnel do not have logical access to any in-scope systems.	Included

EXAMPLE

© 2023 HITRUST Alliance
HITRUSTAlliance.net

5. Use of the Work of Others

An Authorized HITRUST External Assessor Organization (i.e., the external assessor) performed procedures to validate the Organization's asserted control maturity scores. These validation procedures were designed by the external assessor based upon the assessment's scope in observance of HITRUST's Assurance Program Requirements and consisted of inquiry with key personnel, inspection of system-generated evidence (e.g., access lists, logs, configurations, sample items), on-site or virtual observations, and (optionally) reperformance of controls.

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 procedures performed by the external assessor, 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 Organization (i.e., by internal assessors).

Assessment Utilized	Assessed Entity	Assessment Type	Report Date(s)	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Pelican Hosting HITRUST r2	Pelican Hosting	HITRUST r2	2/29/22	Inheritance	(All in-scope platforms)	(All in-scope facilities)	(All assessment domains)

© 2024 HITRUST Alliance
HITRUSTAlliance.net

HITRUST

6. 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 NIST SP 800-171 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 NIST SP 800-171 Compliance and is not a certification of NIST SP 800-171 Compliance.

- This Insights Report accompanies a HITRUST CSF r2 validated assessment. The accompanying r2 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:

    - HITRUST assessments are scoped based on a defined boundary inclusive of specified management systems, physical facilities, and IT platforms. Therefore, the HITRUST assessment may be scoped differently than an assessment focused exclusively to evaluating NIST SP 800-171 compliance across the entirety of the Organization. Parties relying on this report should therefore evaluate the Scope in relation to the Organization's NIST SP 800-171 obligations in consultation with the Organization.

    - 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 NIST SP 800-171 compliance and were not designed to specifically detect all instances of NIST SP 800-171 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 NIST SP 800-171 included in the Organization's HITRUST validated assessment and not in observance of any other criteria specific to NIST SP 800-171 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.

© 2024 HITRUST Alliance
HITRUSTAlliance.net

7. NIST SP 800-171 Overview

Controlled Unclassified Information (CUI) is information that is not classified but requires a level of protection from unauthorized access and release. Executive Order 13556 established the CUI Program to standardize practices for handling CUI across federal and nonfederal agencies and departments. Through CUI regulations, federal agencies using federal systems to process, store, or transmit CUI are required to comply with NIST standards and guidelines. When federal agencies share CUI with nonfederal organizations, their responsibility for protecting the information does not change.

NIST SP 800-171, titled "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations", contains the recommended security requirements for protecting the confidentiality of CUI when it is processed, stored, or transmitted by nonfederal organizations and systems. The security requirements in NIST SP 800-171 are derived from the controls in NIST SP 800-53 and are recommended to be incorporated into contracts and agreements between federal agencies and nonfederal organizations when CUI is involved.

The list below outlines the sections of NIST SP 800-171:

- **Section 1** sets out the purposes of NIST SP 800-171, explains the parties that NIST SP 800-171 applies to, and describes the organization of the publication.

- **Section 2** describes the assumptions and methodology used to develop the security requirements for protecting the confidentiality of CUI, the format of the requirements, and the tailoring criteria applied to the NIST guidelines to obtain the requirements.

- **Section 3** lists the security requirements for protecting the confidentiality of CUI in nonfederal systems and organizations. This security requirements are organized in the following security requirement families:
    - **3.1** Access Control
    - **3.2** Awareness and Training
    - **3.3** Audit and Accountability
    - **3.4** Configuration Management
    - **3.5** Identification and Authorization
    - **3.6** Incident Response
    - **3.7** Maintenance
    - **3.8** Media Protection
    - **3.9** Personnel Security
    - **3.10** Physical Protection
    - **3.11** Risk Assessment
    - **3.12** Security Assessment and Monitoring
    - **3.13** System and Communications Protection
    - **3.14** System and Information Integrity

EXAMPLE

© 2024 HITRUST Alliance
HITRUSTAlliance.net

- **3.15** Planning
- **3.16** System and Services Acquisition
- **3.17** Supply Chain Risk Management

- The remaining sections, **References, Appendix A: Acronyms, Appendix B: Glossary, Appendix C: Tailoring Criteria, Appendix D: Organization-Defined Parameters, and Appendix E: Change Log**, provide additional information to support the guidelines.

NIST SP 800-171A, titled "Assessing Security Requirements for Controlled Unclassified Information", is an additional publication which outlines the assessment procedures and methodology for assessing the security requirements defined in NIST SP 800-171.

The list below outlines the sections of NIST SP 800-171A:

- **Section 1** sets out the purposes of NIST SP 800-171A, explains the parties that NIST SP 800-171A applies to, and describes the organization of the publication.

- **Section 2** explains the structure and content of the procedures provided in Section 3.

- **Section 3** provides the assessment procedures for the security requirements defined in NIST SP 800-171. The assessment procedures are organized in the same 17 security requirement families used to organize the security requirements in NIST SP 800-171.

- The remaining sections, **References, Appendix A: Acronyms, Appendix B: Glossary, Appendix C: Security Requirement Assessments, Appendix D: Organization-Defined Parameters, and Appendix** E: Change Log provide additional information to support the guidelines.

EXAMPLE

© 2024 HITRUST Alliance
HITRUSTAlliance.net

8. NIST SP 800-171 Coverage and Reportability

A HITRUST validated assessment can provide evidence that specific HITRUST CSF control requirements mapping to the Section 3. The Security Requirements of NIST SP 800-171 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 NIST SP 800-171 as a supported authoritative source, and HITRUST's comprehensive assurance program are important tools for organizations with NIST SP 800-171 compliance obligations.

The following factors collectively determine the degree of NIST SP 800-171 coverage and reportability in a HITRUST assessment:

- HITRUST's approach to incorporating NIST SP 800-171 into the HITRUST CSF
- The Organization's assessment type selection, HITRUST CSF version selection, and assessment tailoring

Approach to incorporating NIST SP 800-171 into the HITRUST CSF

The HIRUST CSF maps to NIST SP 800-171 by mapping to the determination statements found in Section 3 of NIST SP 800-171A. For each NIST SP 800-171 security requirement, Section 3 of NIST SP 800-171A includes one or more determination statements which include instructions for assessing the security requirement beginning with "Determine if:". In addition to the determination statements, NIST SP 800-171A includes organizational-defined parameters (ODP) where necessary. See below an example of how the determination statements and ODPs in NIST 800-171A align with the security requirements in NIST SP 800-171.

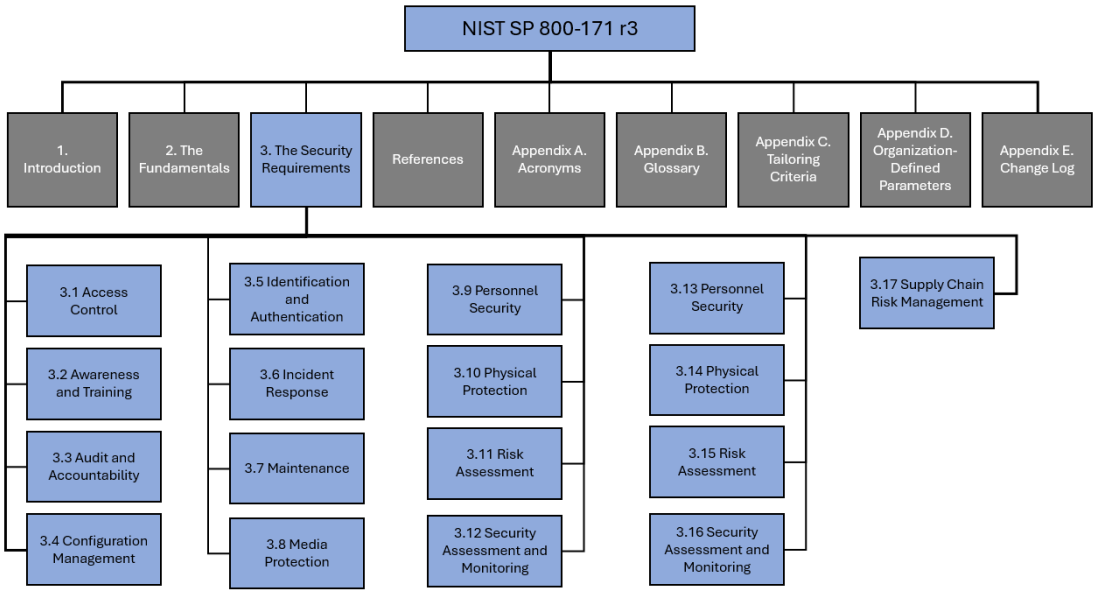
NIST 800-171: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations	NIST 800-171A: Assessing Security Requirements for Controlled Unclassified Information
03.01.06 Least Privilege - Privileged Accounts a. Restrict privileged accounts on the system to [Assignment: organization-defined personnel or roles]. b. Require that users (or roles) with privileged accounts use non-privileged accounts when accessing non-security functions or non-security information.	Determine if: A.03.01.06.ODP[01]: personnel or roles to which privileged accounts on the system are to be restricted are defined. A.03.01.06.a: privileged accounts on the system are restricted to <A.03.01.06.ODP[01]: personnel or roles> A.03.01.06.b: users (or roles) with privileged accounts are required to use non-privileged accounts when accessing non-security functions or non-security information.

© 2024 HITRUST Alliance
HITRUSTAlliance.net

By mapping to all determination statements in Section 3 of NIST 800-171A, the HITRUST CSF effectively maps to all security requirements in Section 3 of NIST 800-171.

The HITRUST CSF intentionally does not provide full coverage of NIST SP 800-171 and intentionally does not contain mappings / cross-references to all text in NIST SP 800-171. Like many other authoritative sources, NIST SP 800-171 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 (*Section 1. Introduction* and *2. The Fundamentals*) and ending (*References*, *Appendix A: Acronyms*, *Appendix B: Glossary*, *Appendix C: Tailoring Criteria*, *Appendix D: Organization-Defined Parameters*, and *Appendix E: Change Log*).

The HITRUST CSF's coverage of NIST SP 800-171 at a high level, is as follows:



Color	Meaning
Grey	Not mapped to the HITRUST CSF because not security related
Blue	Mapped to the HITRUST CSF

Impact of assessment preferences and tailoring on NIST 800-171 coverage and reportability

HITRUST assessments are performed against a subset of HITRUST CSF's numerous requirements. The requirements included in the accompanying HITRUST Risk-based, 2-year (r2) assessment have been tailored based on the unique risks and compliance needs of the Organization and on the HITRUST CSF version selected by the Organization (v11.4.0).

Through tailoring, organizations can optionally add authoritative sources into their r2 assessments. When this occurs, the assessment is expanded to consider additional

© 2024 HITRUST Alliance
HITRUSTAlliance.net

requirements mapping to the information security and/or privacy-related portions of the included authoritative sources. The resulting, tailored HITRUST r2 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 r2 assessments or can optionally utilize one of many prior HITRUST CSF versions. As HITRUST advances the framework, more and better reporting capabilities are unlocked. Not all versions allow for the HITRUST insights reporting against all portions of NIST SP 800-171; instead, only assessments utilizing version 11.4.0and later can create NIST SP 800-171 Insights Reports.

© 2024 HITRUST Alliance
HITRUSTAlliance.net

HITRUST

Appendix A: NIST SP 800-171-relevant Observations

During the HITRUST assessment accompanying this NIST SP 800-171 Insights Report, the policy, process, and/or implemented control maturity level on each of the following HITRUST CSF requirements scored less than "Fully Compliant". These conditions were identified as relevant to the Organization's NIST SP 800-171 compliance efforts, as each of these HITRUST CSF requirements map to one or more NIST SP 800-171 requirements. The relying party should evaluate these items (and the associated risk treatment) in consultation with the Organization.

3.6 - Incident Handling

Reference	Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Management's stated corrective actions (unvalidated)
03.06.04.b	**BUID: 1314.02e2Organizational.5 / CVID: 0339.0** . The organization conducts an internal annual review of the effectiveness of its security and privacy education and training program and updates the program to reflect risks identified in the organization's risk assessment.	Procedure	No corrective action plans were communicated to HITRUST for this condition.

Appendix A has been truncated for this sample report

EXAMPLE

© 2024 HITRUST Alliance
HITRUSTAlliance.net

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 NIST SP 800-171 considered in the underlying HITRUST CSF assessment, organized by NIST SP 800-171 section.

This section also shows the HITRUST CSF requirements mapped by HITRUST to each considered NIST SP 800-171 requirement. Note that many more mappings exist between NIST SP 800-171 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 NIST SP 800-171 Coverage and Reportability section of this document.

In addition to NIST 800-171 r3, 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.

The Organization believes certain of its products and/or services can assist its customers in meeting specific HITRUST requirement statements. The section below contains links to the HITRUST Products and Services Directory (PSD) where the Organization's customers can learn more.

3.1 - Access Control

HITRUST CSF Requirement	Policy Score	Procedure Score	Implemented Score
3.01.01 Account Management			
03.01.01.a. Define the types of system accounts allowed and prohibited.			
BUID: 1139.01b2System.10 / CVID: 0023.0. The organization ensures account types are identified (individual, shared/group, system, application, guest/anonymous, emergency, and	Fully Compliant	Mostly Compliant	Somewhat Compliant

SAMPLE

© 2024 HITRUST Alliance
HITRUSTAlliance.net

HITRUST CSF Requirement	Policy Score	Procedure Score	Implemented Score
temporary) and conditions for group and role membership are established. If used, shared/group account credentials are modified when users are removed from the group.			

03.01.01.b. Create, enable, modify, disable, and remove system accounts in accordance with policy, procedures, prerequisites, and criteria.			
BUID: 1139.01b2System.10 / CVID: 0023.0. The organization ensures account types are identified (individual, shared/group, system, application, guest/anonymous, emergency, and temporary) and conditions for group and role membership are established. If used, shared/group account credentials are modified when users are removed from the group.	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 11220.01b2System.9 / CVID: 0025.0. User registration and de-registration formally addresses establishing, activating, modifying, reviewing, disabling, and removing accounts. Further, at a minimum, the organization addresses how access requests to information systems are submitted, how access to the information systems is granted, how requests to access sensitive information are submitted, how access to covered and/or confidential information is granted, how authorization and/or supervisory approvals are verified, and how a workforce members level of access to covered and/or confidential information is verified.	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 1107.01b1System.2 / CVID: 0019.0. Default and unnecessary accounts are removed, disabled, or otherwise secured.	Fully Compliant	Mostly Compliant	Somewhat Compliant
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).	Fully Compliant	Mostly Compliant	Somewhat Compliant

EXAMPLE

© 2024 HITRUST Alliance
HITRUSTAlliance.net

HITRUST CSF Requirement	Policy Score	Procedure Score	Implemented Score
03.01.01.c. Specify: 1. Authorized users of the system, 2. Group and role membership, and 3. Access authorizations (i.e., privileges) for each account.			
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).	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 1139.01b2System.10 / CVID: 0023.0. The organization ensures account types are identified (individual, shared/group, system, application, guest/anonymous, emergency, and temporary) and conditions for group and role membership are established. If used, shared/group account credentials are modified when users are removed from the group.	Fully Compliant	Mostly Compliant	Somewhat Compliant

Appendix B has been truncated for this sample report

EXAMPLE

© 2024 HITRUST Alliance
HITRUSTAlliance.net

HITRUST

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 a harmonized information protection framework that incorporates and leverages the existing security requirements placed upon organizations, including international (e.g., GDPR, ISO), federal (e.g., FFIEC, HIPAA), state / province (e.g., PHIPA, CCPA), third party (e.g., PCI, COBIT), and other government agencies (e.g., NIST, FTC, 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.

EXAMPLE

© 2024 HITRUST Alliance
HITRUSTAlliance.net