Leveraging HITRUST CSF® Assessment Reports

A Guide for New Users

Topics

- **Background**
- **About HITRUST CSF Assurance Program Validated Reports**
  - Contents of the Report
  - Meaning of the Contents
  - Aligning the Report with an Organization's Current Approach
- **Additional Resources**

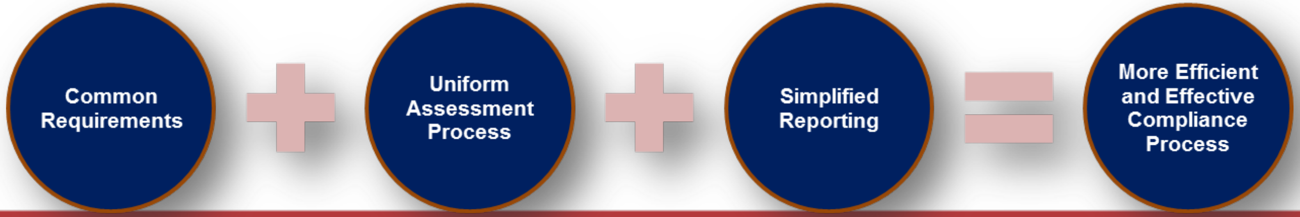
Third Party Assurance Challenges for *Covered Entities*

- Complex contracting process due to organization-specific security requirements
- Low rate, inaccurate and incomplete responses
- Inadequate due diligence of questionnaires
- Difficulty monitoring the status and effectiveness of corrective action plans
- Difficulty tracking down appropriate contacts at business associate
- Costly and time-intensive data collection, assessment and reporting processes
- Inability to proactively identify and track risk exposures at business associate
- Lack of visibility into downstream risks related to business associate (i.e., business associate's own business partners)
- Lack of consistent reporting to management on business associate risks

Third Party Assurance Challenges for *Business Associates*

- Complex contracting process due to unique security requirements
- Broad range and inconsistent expectations for responses to questionnaires—inability to effectively leverage responses across organizations
- Complex processes:
  - Maintaining broad range of reporting requirements
  - Tracking to varied expectations around corrective action plans
  - Tracking down appropriate contacts for customers
  - Expensive and time-intensive audits by customers
  - Difficult to consistently and effectively report to customers

- There are no scenarios where performing 15, 50 or 250 or more unique assessments makes sense for a business associate to communicate their information privacy and security posture (given the same breadth and depth of the assessments)
- Nor does it make sense to maintain and support organization-specific assessment methodologies and multiple assessments for each organization
- HITRUST has been working with organizations and business partners to identify a practical and implementable approach



Common Requirements + Uniform Assessment Process + Simplified Reporting = More Efficient and Effective Compliance Process

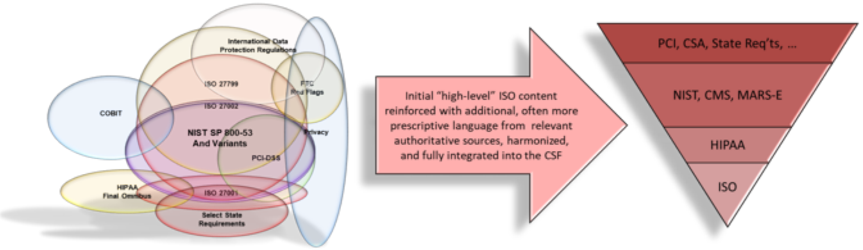
Third-Party Assurance Based on HITRUST CSF®

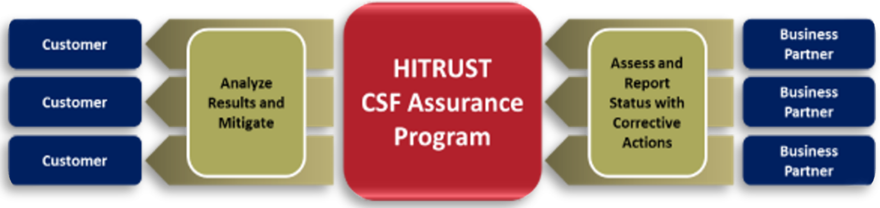
HITRUST CSF

- Developed in collaboration with privacy and security professionals
- Provides organizations a certifiable standard/framework with a comprehensive, flexible and consistent approach to regulatory compliance and risk management
- Helps organizations demonstrate a reasonable standard of due care and due diligence
- Due to continual updates and improvements it has become one of the most widely adopted frameworks
- https://hitrustalliance.net/hitrust-csf/

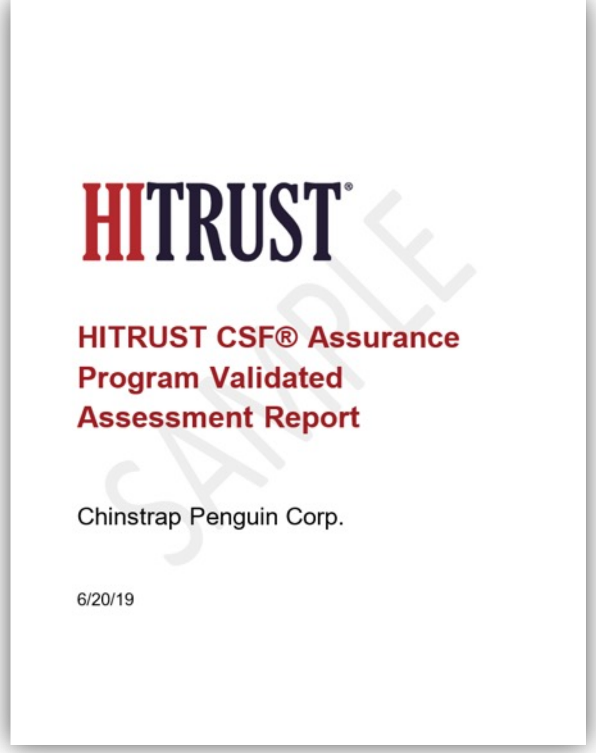
CSF Assurance Program

- Utilizes a common set of information security requirements with standardized assessment and reporting processes accepted and adopted by various organizations
- Through the program, organizations and their business associates can improve efficiencies and reduce the number and costs of security assessments
- The oversight and governance provided by HITRUST supports a process whereby organizations can trust that their third parties have essential security controls in place
- https://hitrustalliance.net/csf-assurance/


International Data Protection Regulations
ISO 27799
FTC Red Flags
COBIT
ISO 27002
NIST SP 800-53 And Variants
Privacy
PCI-DSS
HIPAA Final Omnibus
ISO 27001
Select State Requirements
Initial "high-level" ISO content reinforced with additional, often more prescriptive language from relevant authoritative sources, harmonized, and fully integrated into the CSF
PCI, CSA, State Req'ts, …
NIST, CMS, MARS-E
HIPAA
ISO


Customer
Customer
Customer
Analyze Results and Mitigate
HITRUST CSF Assurance Program
Assess and Report Status with Corrective Actions
Business Partner
Business Partner
Business Partner

The HITRUST CSF Assurance Program Validated Assessment Report



HITRUST

HITRUST CSF® Assurance Program Validated Assessment Report

Chinstrap Penguin Corp.

6/20/19

Is based on …

- A common set of controls based on existing standards/regulations
- An established, industry-accepted baseline of security requirements
- Requirements prioritized by industry input and data breach analyses
- A standard set of assessment questionnaires, tools, and processes
- Specific risk factors that help tailor controls to the assessed organization
- An independent assessment by a HITRUST CSF Assessor

Provides organizations with …

- Standard report, compliance scorecard, and corrective action plan (CAP) formats for the industry
- Assurance there are minimal gaps in required controls for CSF certified entities
- Oversight and governance by HITRUST
- HITRUST validation of assessment results & remediation activity (CAPs)
- Reduced risk and compliance exposure
- Increased assurances around data protection for third parties

Our target audience

- Users of a **HITRUST CSF Assurance Program Validated Report** ("Report") with little or no familiarity with the HITRUST CSF and CSF Assurance Program, which includes:
  - Staff/management reviewing a third party's HITRUST Report to determine the level of risk incurred by providing access to the organization's information, and
  - Regulators reviewing an organization's HITRUST Report for statutory and regulatory compliance
- May also be used by an organization's workforce members who may be unfamiliar with the HITRUST CSF and CSF Assurance Program but need to understand what a HITRUST Report says about their own organization's information protection program

What we want to accomplish

Allow an organization's management or staff to understand and leverage a HITRUST Report to meet their specific requirements for third party assurance

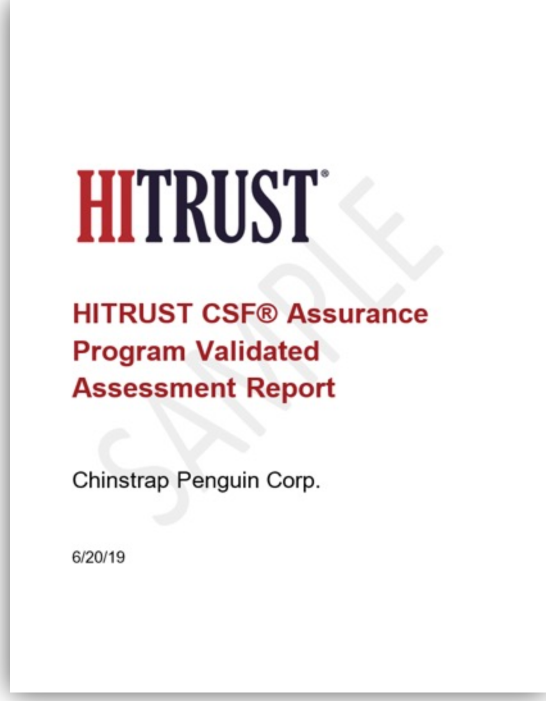
What we will cover

1. Contents of the Report
2. What the information means
3. How it describes an organization's security posture
4. How you can align it with your current approach
5. Where you can find more information

Section 1

WHAT THE REPORT CONTAINS

Cover



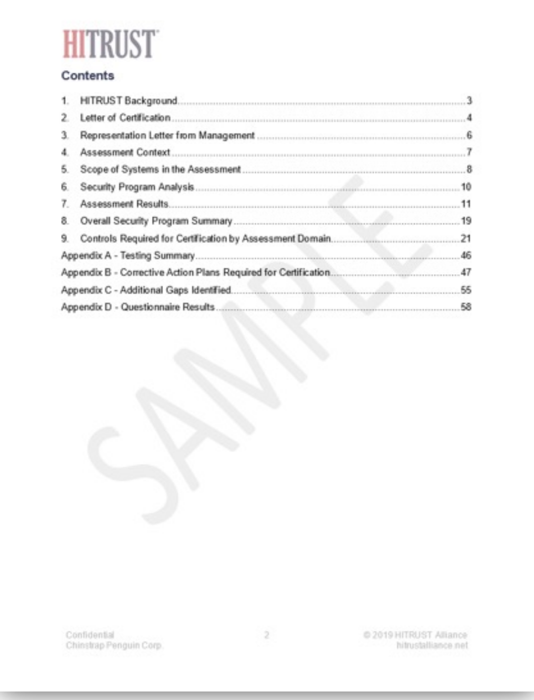
HITRUST®

HITRUST CSF® Assurance Program Validated Assessment Report

Chinstrap Penguin Corp.

6/20/19

Table of Contents

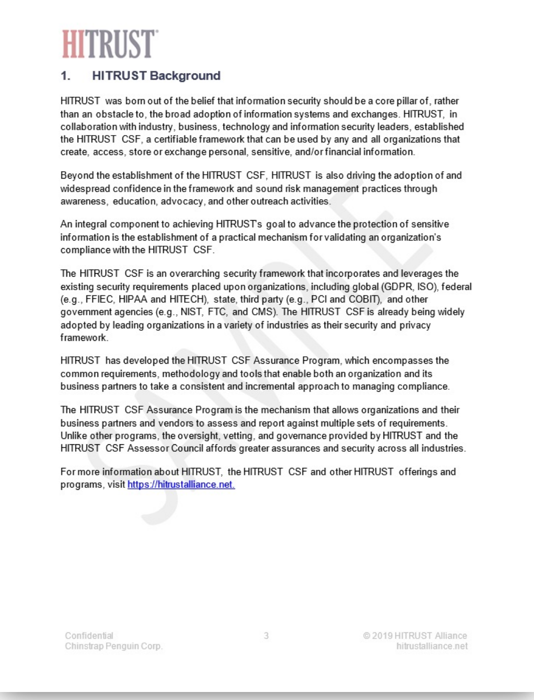


HITRUST

Contents

Confidential
Chinstrap Penguin Corp. 2 © 2019 HITRUST Alliance
hitrustalliance.net

1. HITRUST Background



HITRUST

1. HITRUST Background

HITRUST 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 global (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 security and privacy framework.

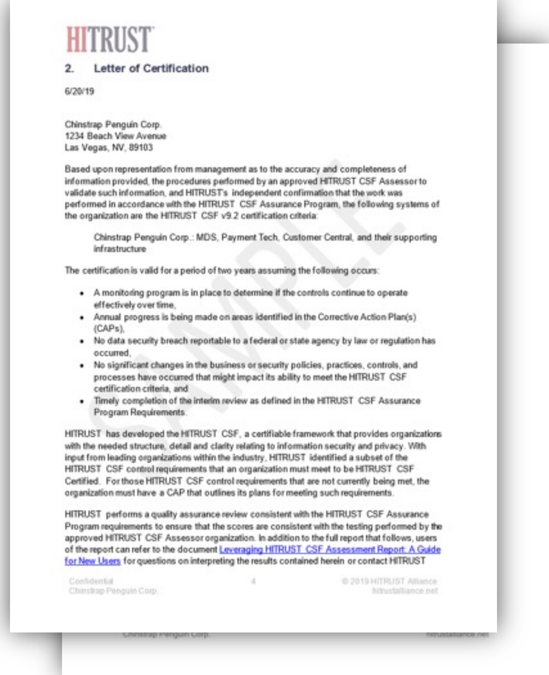
HITRUST has developed the HITRUST CSF Assurance Program, which encompasses the common requirements, methodology and tools that enable both an organization and its business partners to take a consistent and incremental approach to managing compliance.

The HITRUST CSF 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 CSF 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.

Confidential
Chinstrap Penguin Corp. 3 © 2019 HITRUST Alliance
hitrustalliance.net

2. Letter of Certification*



HITRUST

2. Letter of Certification

6/20/19

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

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an approved HITRUST CSF Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST CSF Assurance Program, the following systems of the organization are the HITRUST CSF v9.2 certification criteria:

> Chinstrap Penguin Corp.: MDS, Payment Tech, Customer Central, and their supporting infrastructure

The certification is valid for a period of two years assuming the following occurs:

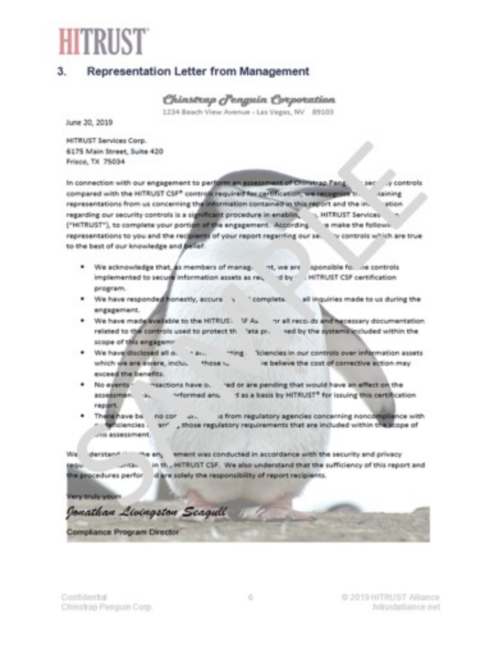
- A monitoring program is in place to determine if the controls continue to operate effectively over time,
- Annual progress is being made on areas identified in the Corrective Action Plan(s) (CAPs),
- No data security breach reportable to a federal or state agency by law or regulation has occurred,
- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST CSF certification criteria, and
- Timely completion of the interim review as defined in the HITRUST CSF Assurance Program Requirements.

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information security and privacy. With input from leading organizations within the industry, HITRUST identified a subset of the HITRUST CSF control requirements that an organization must meet to be HITRUST CSF Certified. For those HITRUST CSF control requirements that are not currently being met, the organization must have a CAP that outlines its plans for meeting such requirements.

HITRUST performs a quality assurance review consistent with the HITRUST CSF Assurance Program requirements to ensure that the scores are consistent with the testing performed by the approved HITRUST CSF Assessor organization. In addition to the full report that follows, users of the report can refer to the document Leveraging HITRUST CSF Assessment Report: A Guide for New Users for questions on interpreting the results contained herein or contact HITRUST

Confidential
Chinstrap Penguin Corp. 4 © 2019 HITRUST Alliance
hitrustalliance.net

3. Representation Letter



HITRUST

3. Representation Letter from Management

Chinstrap Penguin Corporation
1234 Beach View Avenue - Las Vegas, NV 89103

June 20, 2019

HITRUST Services Corp.
6175 Main Street, Suite 420
Frisco, TX 75034

In connection with our engagement to perform an assessment of Chinstrap Peng[illegible] sec[illegible]y controls compared with the HITRUST CSF® controls required for certification, we recognize t[illegible]aining representations from us concerning the information contained in this report and the in[illegible]ation regarding our security controls is a significant procedure in enablin[illegible], HITRUST Services [illegible] ("HITRUST"), to complete your portion of the engagement. According[illegible]e make the followi[illegible] representations to you and the recipients of your report regarding our se[illegible]y controls which are true to the best of our knowledge and belief:

- We acknowledge that, as members of manag[illegible]nt, we are [illegible]sponsible fo[illegible] the controls implemented to secure information assets as re[illegible]d by [illegible] HITRUST CSF certification program.
- We have responded honestly, accura[illegible] complete[illegible] all inquiries made to us during the engagement.
- We have made available to the HITRUS[illegible] As[illegible]r all reco[illegible]ds and necessary documentation related to the controls used to protect th[illegible] data pr[illegible]ed by the systems included within the scope of this engagem[illegible]
- We have disclosed all o[illegible] ar[illegible]ing [illegible]iciencies in our controls over information assets which we are aware, inclu[illegible] those [illegible] we believe the cost of corrective action may exceed the benefits.
- No events [illegible]nsactions have o[illegible]red or are pending that would have an effect on the assessmen[illegible]rformed and [illegible]d as a basis by HITRUST® for issuing this certification report.
- There have been no co[illegible]s from regulatory agencies concerning noncompliance with [illegible]deficiencies [illegible], those regulatory requirements that are included within the scope of [illegible]is assessment.

We [illegible]derstand [illegible] the en[illegible]ement was conducted in accordance with the security and privacy requ[illegible]ntai[illegible] in th[illegible] HITRUST CSF. We also understand that the sufficiency of this report and the procedures perfor[illegible]d are solely the responsibility of report recipients.

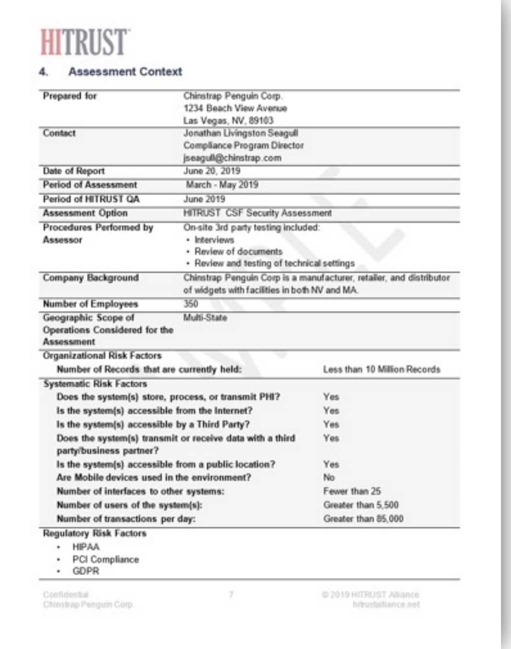
Very truly yours

Jonathan Livingston Seagull

Compliance Program Director

Confidential
Chinstrap Penguin Corp. 6 © 2019 HITRUST Alliance
hitrustalliance.net

4. Assessment Context



HITRUST

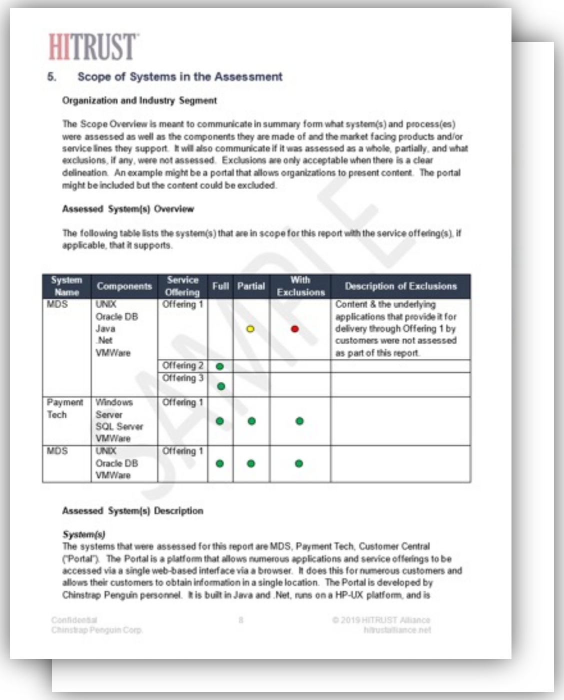
4. Assessment Context

Prepared for	Chinstrap Penguin Corp. 1234 Beach View Avenue Las Vegas, NV, 89103
Contact	Jonathan Livingston Seagull Compliance Program Director jseagull@chinstrap.com
Date of Report	June 20, 2019
Period of Assessment	March - May 2019
Period of HITRUST QA	June 2019
Assessment Option	HITRUST CSF Security Assessment
Procedures Performed by Assessor	On-site 3rd party testing included: • Interviews • Review of documents • Review and testing of technical settings
Company Background	Chinstrap Penguin Corp is a manufacturer, retailer, and distributor of widgets with facilities in both NV and MA.
Number of Employees	350
Geographic Scope of Operations Considered for the Assessment	Multi-State
Organizational Risk Factors	
Number of Records that are currently held:	Less than 10 Million Records
Systematic Risk Factors	
Does the system(s) store, process, or transmit PHI?	Yes
Is the system(s) accessible from the Internet?	Yes
Is the system(s) accessible by a Third Party?	Yes
Does the system(s) transmit or receive data with a third party/business partner?	Yes
Is the system(s) accessible from a public location?	Yes
Are Mobile devices used in the environment?	No
Number of interfaces to other systems:	Fewer than 25
Number of users of the system(s):	Greater than 5,500
Number of transactions per day:	Greater than 85,000
Regulatory Risk Factors • HIPAA • PCI Compliance • GDPR	

Confidential
Chinstrap Penguin Corp. 7 © 2019 HITRUST Alliance
hitrustalliance.net

* Or Letter of Validation

5. Scope of the Assessment



HITRUST

5. Scope of Systems in the Assessment

Organization and Industry Segment

The Scope Overview is meant to communicate in summary form what system(s) and process(es) were assessed as well as the components they are made of and the market facing products and/or service lines they support. It will also communicate if it was assessed as a whole, partially, and what exclusions, if any, were not assessed. Exclusions are only acceptable when there is a clear delineation. An example might be a portal that allows organizations to present content. The portal might be included but the content could be excluded.

Assessed System(s) Overview

The following table lists the system(s) that are in scope for this report with the service offering(s), if applicable, that it supports.

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
MDS	UNIX Oracle DB Java .Net VMWare	Offering 1		🟡	🔴	Content & the underlying applications that provide it for delivery through Offering 1 by customers were not assessed as part of this report.
		Offering 2	🟢			
		Offering 3	🟢			
Payment Tech	Windows Server SQL Server VMWare	Offering 1	🟢	🟢	🟢	
MDS	UNIX Oracle DB VMWare	Offering 1	🟢	🟢	🟢	

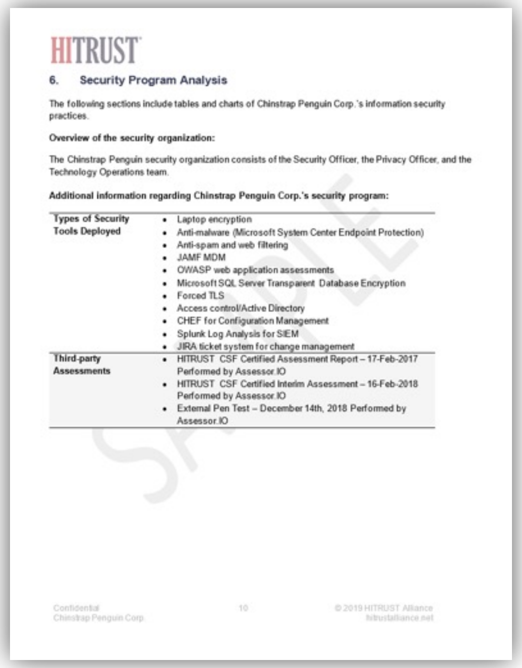
Assessed System(s) Description

System(s)

The systems that were assessed for this report are MDS, Payment Tech, Customer Central ("Portal"). The Portal is a platform that allows numerous applications and service offerings to be accessed 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. The Portal is developed by Chinstrap Penguin personnel. It is built in Java and .Net, runs on a HP-UX platform, and is

Confidential
Chinstrap Penguin Corp.
8
© 2019 HITRUST Alliance
hitrustalliance.net

6. Security Program Analysis



HITRUST

6. Security Program Analysis

The following sections include tables and charts of Chinstrap Penguin Corp.'s information security practices.

Overview of the security organization:

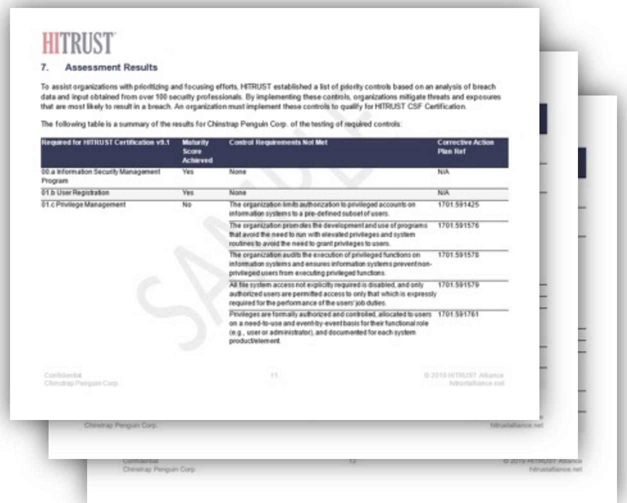
The Chinstrap Penguin security organization consists of the Security Officer, the Privacy Officer, and the Technology Operations team.

Additional information regarding Chinstrap Penguin Corp.'s security program:

Types of Security Tools Deployed	• Laptop encryption • Anti-malware (Microsoft System Center Endpoint Protection) • Anti-spam and web filtering • JAMF MDM • OWASP web application assessments • Microsoft SQL Server Transparent Database Encryption • Forced TLS • Access control/Active Directory • CHEF for Configuration Management • Splunk Log Analysis for SIEM • JIRA ticket system for change management
Third-party Assessments	• HITRUST CSF Certified Assessment Report – 17-Feb-2017 Performed by Assessor.IO • HITRUST CSF Certified Interim Assessment – 16-Feb-2018 Performed by Assessor.IO • External Pen Test – December 14th, 2018 Performed by Assessor.IO

Confidential
Chinstrap Penguin Corp.
10
© 2019 HITRUST Alliance
hitrustalliance.net

7. Assessment Results



HITRUST

7. Assessment Results

To assist organizations with prioritizing and focusing efforts, HITRUST established a list of priority controls based on an analysis of breach data and input obtained from over 100 security professionals. By implementing these controls, organizations mitigate threats and exposures that are most likely to result in a breach. An organization must implement these controls to qualify for HITRUST CSF Certification.

The following table is a summary of the results for Chinstrap Penguin Corp. of the testing of required controls:

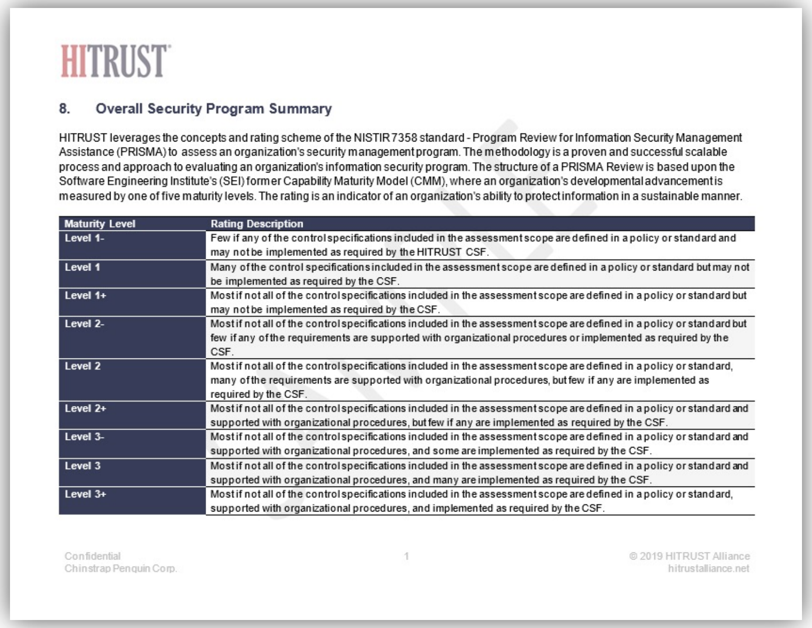
Required for HITRUST Certification v9.1	Maturity Score Achieved	Control Requirements Not Met	Corrective Action Plan Ref
00.a Information Security Management Program	Yes	None	N/A
01.b User Registration	Yes	None	N/A
01.c Privilege Management	No	The organization limits authorization to privileged accounts on information systems to a pre-defined subset of users.	1701.591425
		The organization promotes the development and use of programs that avoid the need to run with elevated privileges and system routines to avoid the need to grant privileges to users.	1701.591576
		The organization audits the execution of privileged functions on information systems and ensures information systems prevent non-privileged users from executing privileged functions.	1701.591578
		All file system access not explicitly required is disabled, and only authorized users are permitted access to only that which is expressly required for the performance of the users' job duties.	1701.591579
		Privileges are formally authorized and controlled, allocated to users on a need-to-use and event-by-event basis for their functional role (e.g., user or administrator), and documented for each system product/element.	1701.591761

Confidential
Chinstrap Penguin Corp.
11
© 2019 HITRUST Alliance
hitrustalliance.net

Chinstrap Penguin Corp.
hitrustalliance.net

Confidential
Chinstrap Penguin Corp.
12
© 2019 HITRUST Alliance
hitrustalliance.net

8. Overall Program Summary



HITRUST

8. Overall Security Program Summary

HITRUST leverages the concepts and rating scheme of the NISTIR 7358 standard - Program Review for Information Security Management Assistance (PRISMA) to assess an organization's security management program. The methodology is a proven and successful scalable process and approach to evaluating an organization's information security program. The structure of a PRISMA Review is based upon the Software Engineering Institute's (SEI) former Capability Maturity Model (CMM), where an organization's developmental advancement is measured by one of five maturity levels. The rating is an indicator of an organization's ability to protect information in a sustainable manner.

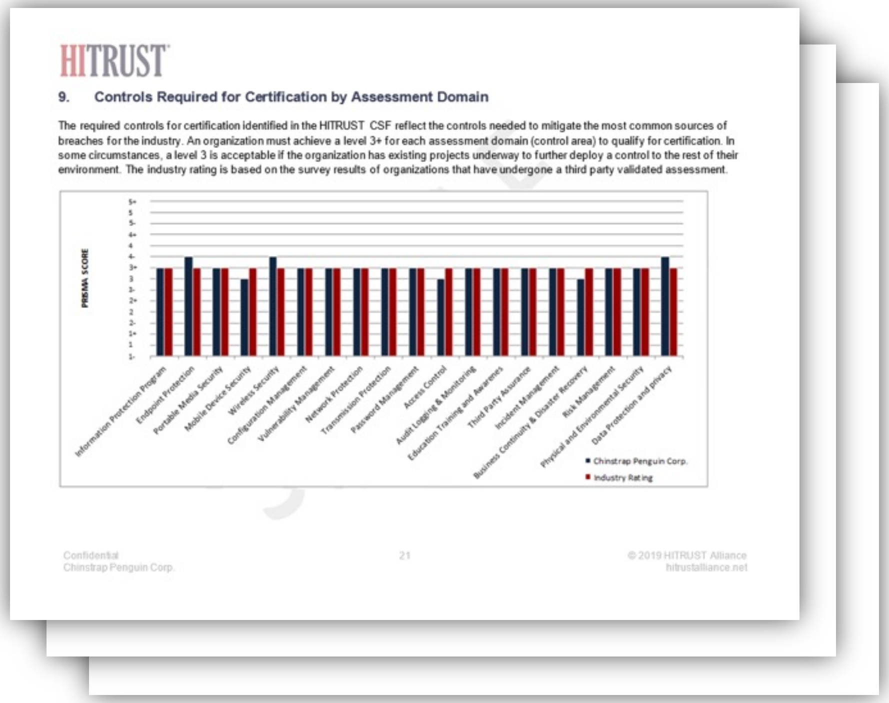
Maturity Level	Rating Description
Level 1-	Few if any of the control specifications included in the assessment scope are defined in a policy or standard and may not be implemented as required by the HITRUST CSF.
Level 1	Many of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.
Level 1+	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.
Level 2-	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard but few if any of the requirements are supported with organizational procedures or implemented as required by the CSF.
Level 2	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, many of the requirements are supported with organizational procedures, but few if any are implemented as required by the CSF.
Level 2+	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, but few if any are implemented as required by the CSF.
Level 3-	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and some are implemented as required by the CSF.
Level 3	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and many are implemented as required by the CSF.
Level 3+	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported with organizational procedures, and implemented as required by the CSF.

Confidential
Chinstrap Penguin Corp.

1

© 2019 HITRUST Alliance
hitrustalliance.net

9. Breakdown by Control Areas



HITRUST

9. Controls Required for Certification by Assessment Domain

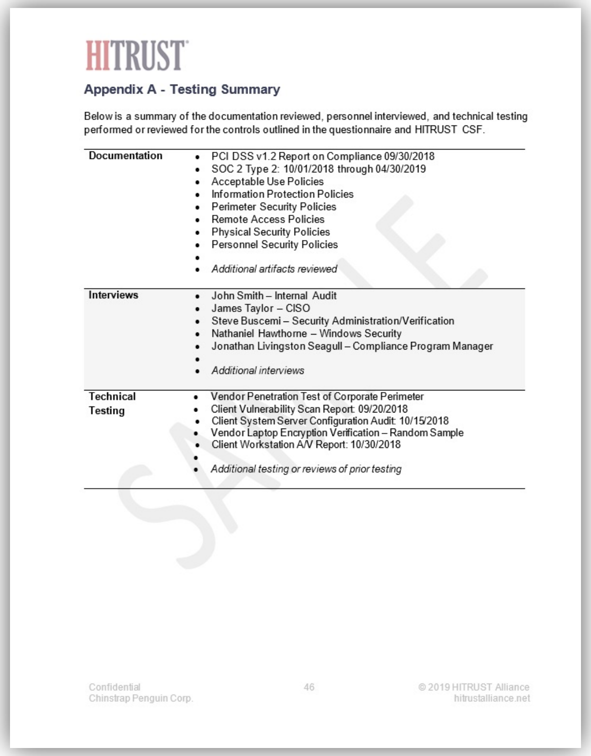
The required controls for certification identified in the HITRUST CSF reflect the controls needed to mitigate the most common sources of breaches for the industry. An organization must achieve a level 3+ for each assessment domain (control area) to qualify for certification. In some circumstances, a level 3 is acceptable if the organization has existing projects underway to further deploy a control to the rest of their environment. The industry rating is based on the survey results of organizations that have undergone a third party validated assessment.

Confidential
Chinstrap Penguin Corp.

21

© 2019 HITRUST Alliance
hitrustalliance.net

Appendix A – Testing Summary



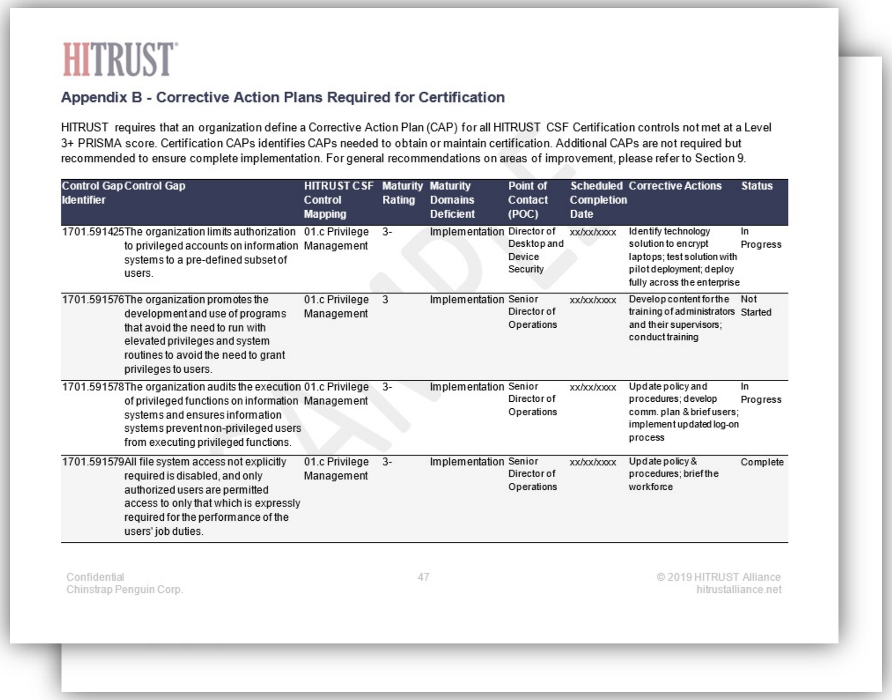
HITRUST

Appendix A - Testing Summary

Below is a summary of the documentation reviewed, personnel interviewed, and technical testing performed or reviewed for the controls outlined in the questionnaire and HITRUST CSF.

Documentation	• PCI DSS v1.2 Report on Compliance 09/30/2018 • SOC 2 Type 2: 10/01/2018 through 04/30/2019 • Acceptable Use Policies • Information Protection Policies • Perimeter Security Policies • Remote Access Policies • Physical Security Policies • Personnel Security Policies • • *Additional artifacts reviewed*
Interviews	• John Smith – Internal Audit • James Taylor – CISO • Steve Buscemi – Security Administration/Verification • Nathaniel Hawthorne – Windows Security • Jonathan Livingston Seagull – Compliance Program Manager • • *Additional interviews*
Technical Testing	• Vendor Penetration Test of Corporate Perimeter • Client Vulnerability Scan Report: 09/20/2018 • Client System Server Configuration Audit: 10/15/2018 • Vendor Laptop Encryption Verification – Random Sample • Client Workstation A/V Report: 10/30/2018 • • *Additional testing or reviews of prior testing*

Appendix B – Corrective Action Plan



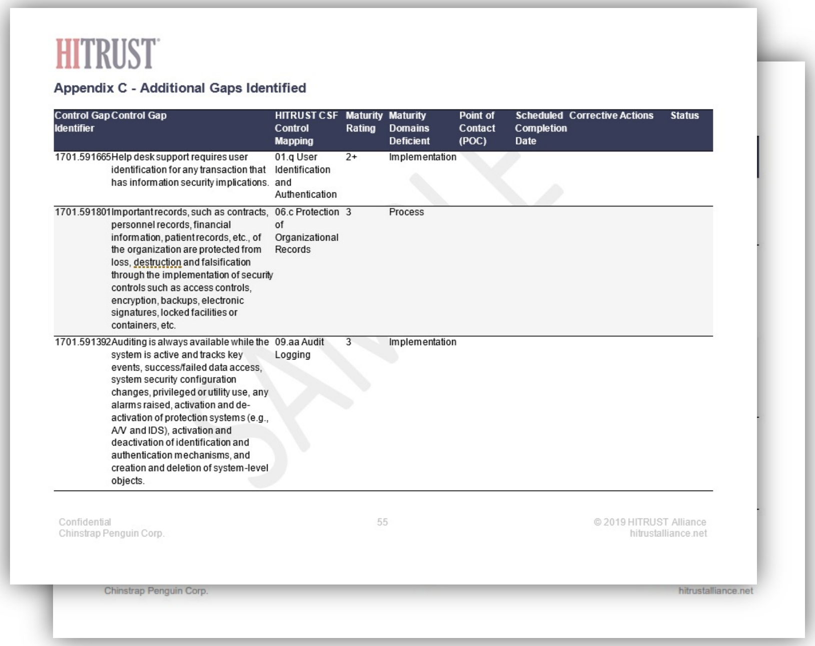
HITRUST

Appendix B - Corrective Action Plans Required for Certification

HITRUST requires that an organization define a Corrective Action Plan (CAP) for all HITRUST CSF Certification controls not met at a Level 3+ PRISMA score. Certification CAPs identifies CAPs needed to obtain or maintain certification. Additional CAPs are not required but recommended to ensure complete implementation. For general recommendations on areas of improvement, please refer to Section 9.

Control Gap Identifier	Control Gap	HITRUST CSF Control Mapping	Maturity Rating	Maturity Domains Deficient	Point of Contact (POC)	Scheduled Completion Date	Corrective Actions	Status
1701.591425	The organization limits authorization to privileged accounts on information systems to a pre-defined subset of users.	01.c Privilege Management	3-	Implementation	Director of Desktop and Device Security	xx/xx/xxxx	Identify technology solution to encrypt laptops; test solution with pilot deployment; deploy fully across the enterprise	In Progress
1701.591576	The organization promotes the development and use of programs that avoid the need to run with elevated privileges and system routines to avoid the need to grant privileges to users.	01.c Privilege Management	3	Implementation	Senior Director of Operations	xx/xx/xxxx	Develop content for the training of administrators and their supervisors; conduct training	Not Started
1701.591578	The organization audits the execution of privileged functions on information systems and ensures information systems prevent non-privileged users from executing privileged functions.	01.c Privilege Management	3-	Implementation	Senior Director of Operations	xx/xx/xxxx	Update policy and procedures; develop comm. plan & brief users; implement updated log-on process	In Progress
1701.591579	All file system access not explicitly required is disabled, and only authorized users are permitted access to only that which is expressly required for the performance of the users' job duties.	01.c Privilege Management	3-	Implementation	Senior Director of Operations	xx/xx/xxxx	Update policy & procedures; brief the workforce	Complete

Appendix C – Additional Gaps Identified



HITRUST

Appendix C - Additional Gaps Identified

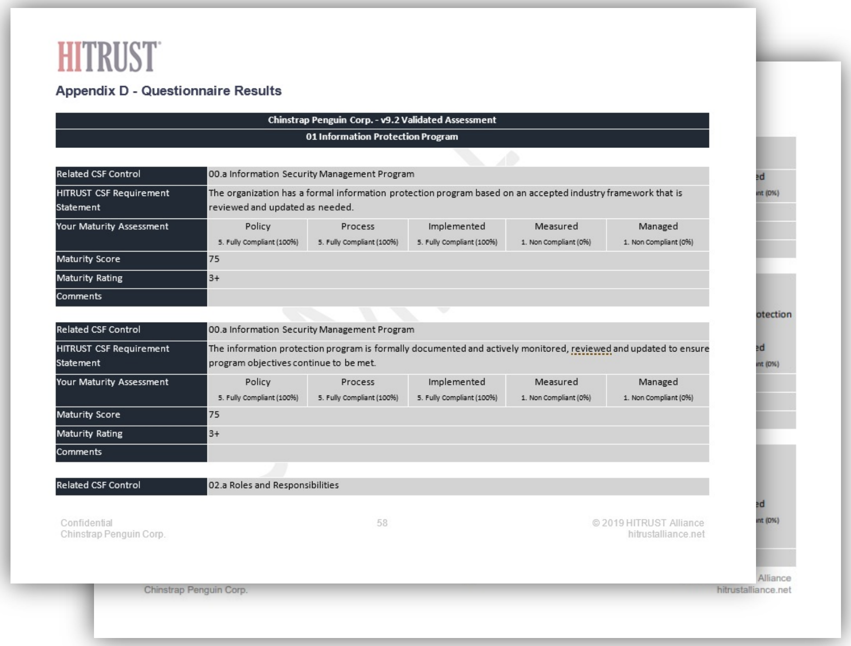
Control Gap Identifier	Control Gap	HITRUST CSF Control Mapping	Maturity Rating	Maturity Domains Deficient	Point of Contact (POC)	Scheduled Completion Date	Corrective Actions	Status
1701.591665	Help desk support requires user identification for any transaction that has information security implications.	01.q User Identification and Authentication	2+	Implementation				
1701.591801	Important records, such as contracts, personnel records, financial information, patient records, etc., of the organization are protected from loss, destruction and falsification through the implementation of security controls such as access controls, encryption, backups, electronic signatures, locked facilities or containers, etc.	06.c Protection of Organizational Records	3	Process				
1701.591392	Auditing is always available while the system is active and tracks key events, success/failed data access, system security configuration changes, privileged or utility use, any alarms raised, activation and de-activation of protection systems (e.g., A/V and IDS), activation and deactivation of identification and authentication mechanisms, and creation and deletion of system-level objects.	09.aa Audit Logging	3	Implementation				

Confidential
Chinstrap Penguin Corp.

55

© 2019 HITRUST Alliance
hitrustalliance.net

Appendix D – Questionnaire Results



HITRUST

Appendix D - Questionnaire Results

Chinstrap Penguin Corp. - v9.2 Validated Assessment

01 Information Protection Program

Related CSF Control	00.a Information Security Management Program				
HITRUST CSF Requirement Statement	The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.				
Your Maturity Assessment	Policy 5. Fully Compliant (100%)	Process 5. Fully Compliant (100%)	Implemented 5. Fully Compliant (100%)	Measured 1. Non Compliant (0%)	Managed 1. Non Compliant (0%)
Maturity Score	75				
Maturity Rating	3+				
Comments					

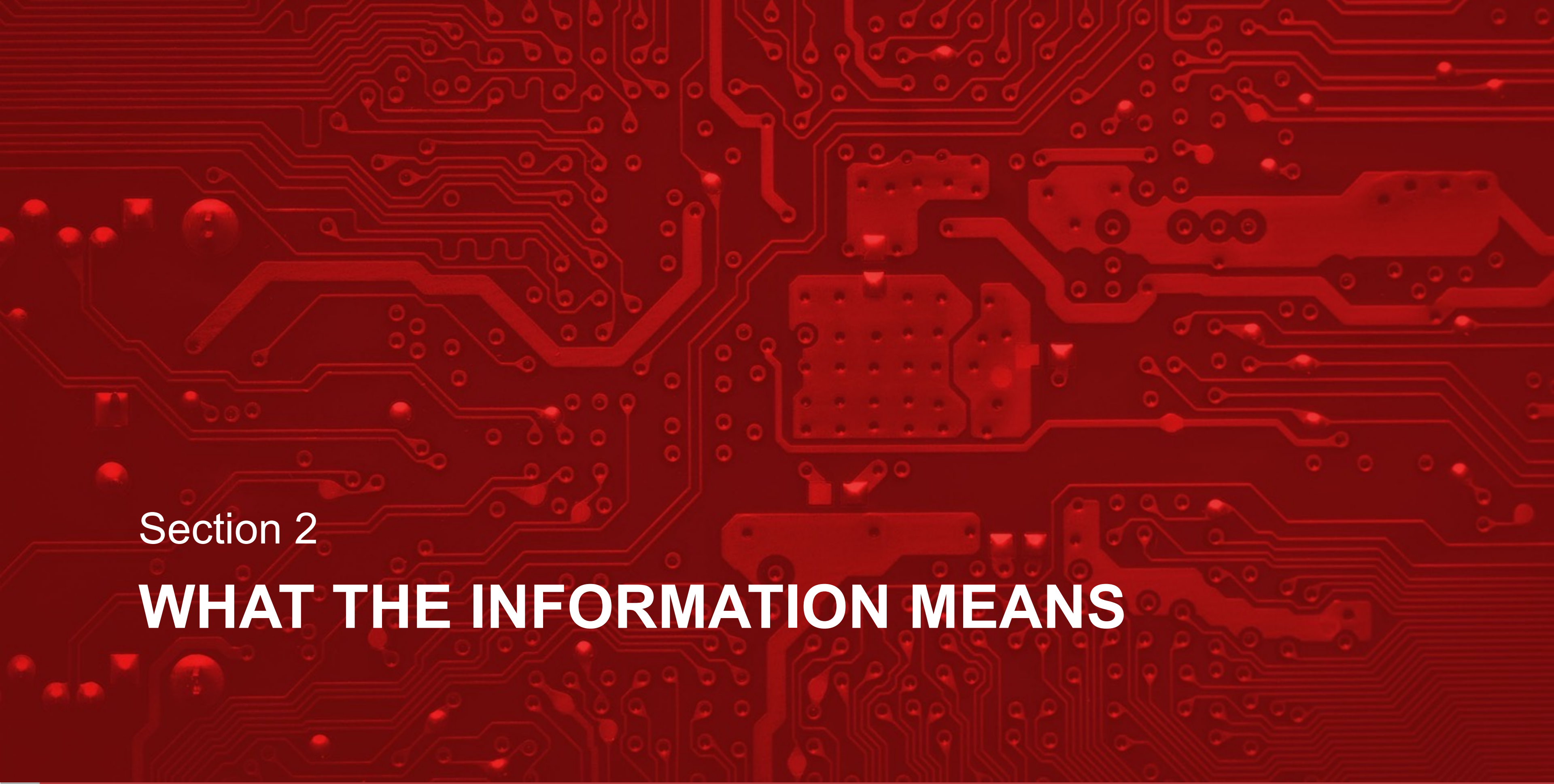
Related CSF Control	00.a Information Security Management Program				
HITRUST CSF Requirement Statement	The information protection program is formally documented and actively monitored, reviewed and updated to ensure program objectives continue to be met.				
Your Maturity Assessment	Policy 5. Fully Compliant (100%)	Process 5. Fully Compliant (100%)	Implemented 5. Fully Compliant (100%)	Measured 1. Non Compliant (0%)	Managed 1. Non Compliant (0%)
Maturity Score	75				
Maturity Rating	3+				
Comments					

Related CSF Control	02.a Roles and Responsibilities

Confidential
Chinstrap Penguin Corp.

58

© 2019 HITRUST Alliance
hitrustalliance.net



Section 2

WHAT THE INFORMATION MEANS

Cover Page

HITRUST

HITRUST CSF® Assurance Program Validated Assessment Report

Chinstrap Penguin Corp.

6/20/19

- Cover page provides:
  - The name of the entity that is the subject of the assessment report
  - The date of the report, which tells you how long the report is valid, i.e., date of the report + 2 years

1. HITRUST Background

HITRUST

1. HITRUST Background

- Provides a brief overview of HITRUST and the information protection framework, the CSF, upon which the report is based
- For more information, you can refer to the following resources:
  - www.hitrustalliance.net
  - https://hitrustalliance.net/documents/csf_rmf_related/CSFComparisonWhitpaper.pdf

2. Letter of Certification*

HITRUST

2. Letter of Certification

- Letters from HITRUST stating the assessed entity meets all the requirements for HITRUST CSF certification. Two versions will be provided.

  Certification Letter with scope:
  - Provides organization's name and date of certification (consistent with the cover page)
  - Specifies the certification is good for 2 years if certain conditions are met
  - https://hitrustalliance.net/content/uploads/CSFAssuranceProgramRequirements-2.pdf

  Stand-alone certification letter:
  - Excludes the assessed entity's scope information
  - Intended to allow entities the flexibility to provide the correct level of detail they wish to share around the environment

**If certification requirements are not met, then a letter stating the assessment has been validated by HITRUST is included instead of the Letter of Certification*

3. Representation Letter

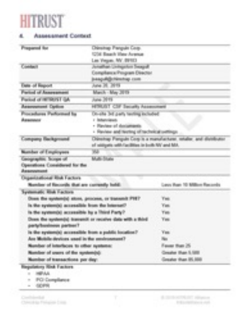
HITRUST

3. Representation Letter from Management

Chinstrap Penguin Corporation

- Letter from the organization that was the subject of the validated assessment
- It basically provides attestation from the organization that they:
  - Are responsible for the controls,
  - Have responded to the assessor in good faith and that nothing has been misrepresented, and
  - They foresee nothing that might adversely impact the assessment results
- Any misrepresentation by the entity could cause HITRUST to invalidate the report

4. Assessment Context



HITRUST

4. Assessment Context

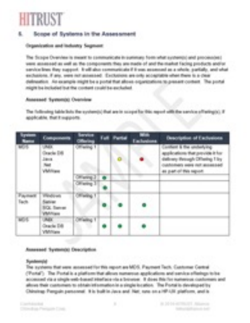
Prepared for	Chinstrap Penguin Corp. 1234 Beach View Avenue Las Vegas, NV 89103
Contact	Jonathan Livingston Seagull Compliance/Program Director jseagull@chinstrap.com
Date of Report	June 28, 2019
Period of Assessment	March - May 2019
Period of HITRUST QA	June 2019
Assessment Option	HITRUST CSF Security Assessment
Procedures Performed by Assessor	On-site 3rd party testing included: • Interviews • Review of documents • Review and testing of technical settings
Company Background	Chinstrap Penguin Corp is a manufacturer, retailer, and distributor of widgets with facilities in both NV and MA.
Number of Employees	350
Geographic Scope of Operations Considered for the Assessment	Multi-State
Organizational Risk Factors	
Number of Records that are currently held:	Less than 10 Million Records
Systematic Risk Factors	
Does the system(s) store, process, or transmit PHI?	Yes
Is the system(s) accessible from the Internet?	Yes
Is the system(s) accessible by a Third Party?	Yes
Does the system(s) transmit or receive data with a third party/business partner?	Yes
Is the system(s) accessible from a public location?	Yes
Are Mobile devices used in the environment?	No
Number of interfaces to other systems:	Fewer than 25
Number of users of the system(s):	Greater than 5,000
Number of transactions per day:	Greater than 85,000

Regulatory Risk Factors
- HIPAA
- PCI Compliance
- GDPR

Confidential
Chinstrap Penguin Corp.
7
© 2019 HITRUST Alliance
[illegible]

- Provides additional information about the organization, e.g.:
  - Entity name and address
  - Background information
  - Point of contact for the assessment
- It also provides information about the assessment, including:
  - Assessment type (e.g., 3rd party / validated)
  - Specific risk factors used to tailor the CSF controls to the entity
  - For more information on scoping & tailoring: https://hitrustalliance.net/content/uploads/CSFAssessmentMethodology-1.pdf

5. Scope of Systems in the Assessment



HITRUST

5. Scope of Systems in the Assessment

Organization and Industry Segment

The Scope Overview is meant to communicate in summary form what system(s) and process(es) were assessed as well as the components they are made of and the market facing products and/or service lines they support. It will also communicate if it was assessed as a whole, partially, and what exclusions, if any, were not assessed. Exclusions are only acceptable when there is a clear delineation. An example might be a portal that allows organizations to present content. The portal might be included but the content could be excluded.

Assessed System(s) Overview

The following table lists the system(s) that are in scope for this report with the service offering(s), if applicable, that it supports.

System Name	Components	Service Offering	Full	Partial	With Exclusions	Description of Exclusions
MDS	UNIX Oracle DB Java .Net VMWare	Offering 1		○	●	Content & the underlying applications that provide it for delivery through Offering 1 by customers were not assessed as part of this report.
		Offering 2	●			
		Offering 3	●			
Payment Tech	Windows Server SQL Server VMWare	Offering 1	●	●	●	
MDS	UNIX Oracle DB VMWare	Offering 1	●	●	●	

Assessed System(s) Description

System(s)
The systems that were assessed for this report are MDS, Payment Tech, Customer Central ("Portal"). The Portal is a platform that allows numerous applications and service offerings to be accessed 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. The Portal is developed by Chinstrap Penguin personnel. It is built in Java and .Net, runs on a HP-UX platform, and is

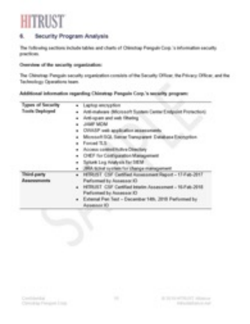
Confidential
Chinstrap Penguin Corp.
8
© 2019 HITRUST Alliance
[illegible]

- An overview of the assessed entity and the industry segment within which it operates
- The services / products provided by the entity
- Primary systems placed in scope of the assessment with description of the platforms, their functions and the PII (Personally Identifiable Information) involved
- Any services within scope of the report that are outsourced to a third party
- Additional information about the scope of the report, such as business units and/or processes included as well as those not included

Risk Factors

- Risk factors support (1) the "flexibility of approach" allowed under the HIPAA Security Rule and (2) NIST's concept of tailoring a specified set of controls, referred to as a control baseline, to meet an entity's needs
  - http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/combined/hipaa-simplification-201303.pdf
  - http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- HITRUST uses three (3) types of risk factors to help provide a tailored "fit"
  - Organizational factors (e.g. type, size, locations)
    - Includes Geographical (e.g., Multi-State)
  - System factors (e.g., connection to the internet, use of mobile devices)
  - Regulatory factors (e.g., PCI / CMS / State requirements)

6. Security Program Analysis



HITRUST

6. Security Program Analysis

The following sections include tables and charts of Chinstrap Penguin Corp.'s information security practices.

Overview of the security organization:

The Chinstrap Penguin security organization consists of the Security Officer, the Privacy Officer, and the Technology Operations team.

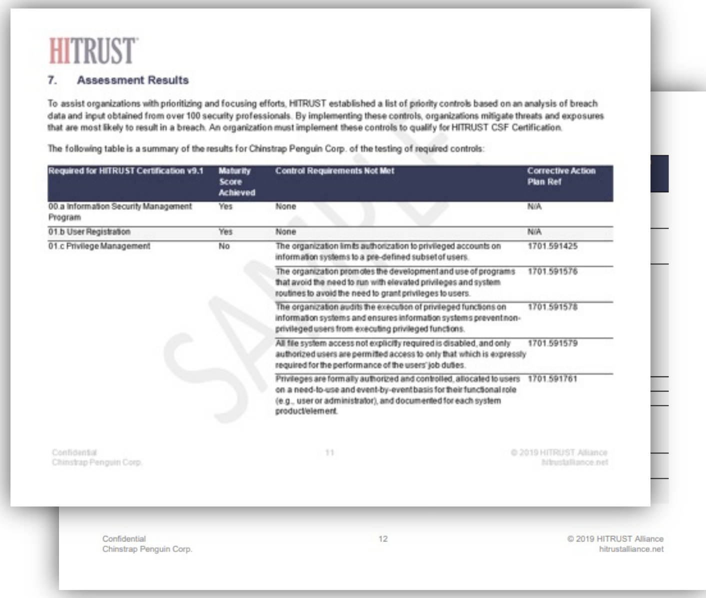
Additional information regarding Chinstrap Penguin Corp.'s security program:

Types of Security Tools Deployed	• Laptop encryption • Anti-malware (Microsoft System Center Endpoint Protection) • Anti-spam and web filtering • JAMF MDM • OWASP web application assessments • Microsoft SQL Server Transparent Database Encryption • Forced TLS • Access control/Active Directory • CHEF for Configuration Management • Splunk Log Analysis for SIEM • JIRA ticket system for change management
Third-party Assessments	• HITRUST CSF Certified Assessment Report – 17-Feb-2017 Performed by Assessor ID • HITRUST CSF Certified Interim Assessment – 16-Feb-2018 Performed by Assessor ID • External Pen Test – December 14th, 2018 Performed by Assessor ID

Confidential
Chinstrap Penguin Corp.
10
© 2019 HITRUST Alliance
[illegible]

- This section is intended to provide the reader with a concise summary of the assessed entity's:
  - Information protection program
  - Information protection organization
- It also provides detailed information on:
  - The security and privacy tools and technology the entity deploys in the scoped environment
  - Relevant independent assessments by external consulting and professional services firms (e.g., a PCI audit, SSAE 18 SOC 2®, or a vendor's penetration test of the corporate perimeter)

7. Assessment Results



HITRUST

7. Assessment Results

To assist organizations with prioritizing and focusing efforts, HITRUST established a list of priority controls based on an analysis of breach data and input obtained from over 100 security professionals. By implementing these controls, organizations mitigate threats and exposures that are most likely to result in a breach. An organization must implement these controls to qualify for HITRUST CSF Certification.

The following table is a summary of the results for Chinstrap Penguin Corp. of the testing of required controls:

Required for HITRUST Certification v9.1	Maturity Score Achieved	Control Requirements Not Met	Corrective Action Plan Ref
00.a Information Security Management Program	Yes	None	N/A
01.b User Registration	Yes	None	N/A
01.c Privilege Management	No	The organization limits authorization to privileged accounts on information systems to a pre-defined subset of users.	1701.591425
		The organization promotes the development and use of programs that avoid the need to run with elevated privileges and system routines to avoid the need to grant privileges to users.	1701.591576
		The organization audits the execution of privileged functions on information systems and ensures information systems prevent non-privileged users from executing privileged functions.	1701.591578
		All file system access not explicitly required is disabled, and only authorized users are permitted access to only that which is expressly required for the performance of the users' job duties.	1701.591579
		Privileges are formally authorized and controlled, allocated to users on a need-to-use and event-by-event basis for their functional role (e.g., user or administrator), and documented for each system product/element.	1701.591761

SAMPLE

Confidential
Chinstrap Penguin Corp.
11
© 2019 HITRUST Alliance
hitrustalliance.net

Confidential
Chinstrap Penguin Corp.
12
© 2019 HITRUST Alliance
hitrustalliance.net

- Organizations must generally implement all requirements in all 135 security-related CSF controls (or more if privacy requirements are included) as tailored by its applicable risk factors and any subsequent risk analysis to:
  – Provide a complete set of reasonable and appropriate controls
  – Address all reasonably anticipated threats
  – Provide adequate protection of ePHI, and subsequently
  – Minimize risk at an acceptable level
- However, consistent with NIST guidelines (http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf), "organizations can use targeted risk assessments, in which the scope is narrowly defined, to produce answers to specific questions … or to inform specific decisions…."
- HITRUST CSF validated assessments provide a reasonable level of assurance at a reasonable cost by selecting specific:
  – High risk controls (based on an analysis of breach data and subject matter expert input)
  – High interest controls
- The current CSF Assurance Program requires the assessment of 75 CSF controls for the purposes of certification and basic third-party assurance
- This section lets the reader of the report identify which of these 75 controls meet or do not meet certification requirements, whether a CAP is required, and the specific identifier for the weakness/CAP
- For more information on HITRUST's risk vs. compliance-based approach to information protection and the overall approach to supporting attestations, refer to https://hitrustalliance.net/documents/csf_rmf_related/RiskVsComplianceWhitepaper.pdf & https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf

8. Overall Program Summary

HITRUST

8. Overall Security Program Summary

HITRUST leverages the concepts and rating scheme of the NISTIR 7358 standard - Program Review for Information Security Management Assistance (PRISMA) to assess an organization's security management program. The methodology is a proven and successful scalable process and approach to evaluating an organization's information security program. The structure of a PRISMA Review is based upon the Software Engineering Institute's (SEI) former Capability Maturity Model (CMM), where an organization's developmental advancement is measured by one of five maturity levels. The rating is an indicator of an organization's ability to protect information in a sustainable manner.

Maturity Level	Rating Description
Level 1-	Few if any of the control specifications included in the assessment scope are defined in a policy or standard and may not be implemented as required by the HITRUST CSF.
Level 1	Many of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.
Level 1+	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.
Level 2-	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard but few if any of the requirements are supported with organizational procedures or implemented as required by the CSF.
Level 2	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, many of the requirements are supported with organizational procedures, but few if any are implemented as required by the CSF.
Level 2+	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, but few if any are implemented as required by the CSF.
Level 3-	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and some are implemented as required by the CSF.
Level 3	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and many are implemented as required by the CSF.
Level 3+	Most if not all of the control specifications included in the assessment scope are defined in a policy or standard, supported with organizational procedures, and implemented as required by the CSF.

Confidential
Christmas Penguin Corp

1

© 2019 HITRUST Alliance
hitrustalliance.net

- Boilerplate that presents the 15-point scale used by HITRUST to communicate the maturity of a control's implementation
  - Controls are evaluated using a 5-level maturity model
  - HITRUST scores the controls
  - HITRUST converts the scores to a 15-point rating for the purpose of CSF certification
- For more information, refer to: https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf

Maturity Scoring Approach

Compliance with a maturity level's requirements is indicated by:

- **Non-compliant** (NC, 0%) – **Very few if any** of the control requirements are implemented for the maturity level assessed (e.g., Policy)
- **Somewhat Compliant** (SC, 25%) – **Some** of the control requirements are implemented for the maturity level assessed (e.g., Policy)
- **Partially Compliant** (PC, 50%) – **About half** of the control requirements are implemented for the maturity level assessed (e.g., Policy)
- **Mostly Compliant** (MC, 75%) – **Many** of the control requirements are implemented for the maturity level assessed (e.g., Policy)
- **Fully Compliant** (FC, 100%) – **Most if not all** of the control requirements are implemented for the maturity level assessed (e.g., Policy)

Scores are computed as the sum of the points awarded for each level

5-level Control Maturity Model

Assurance the control has been properly implemented is indicated by:

1. **Policy** (15 pts.) – Does an organization know what it's supposed to do?
2. **Process** (sometimes referred to as Procedure) (20 pts) – Does the organization know how to do what it's supposed to do?
3. **Implemented** (40 pts.)– Does the organization implement all the elements of a specified control and does it implement it everywhere it's supposed to be implemented?

Assurance the control will continue to be effective is indicated by:

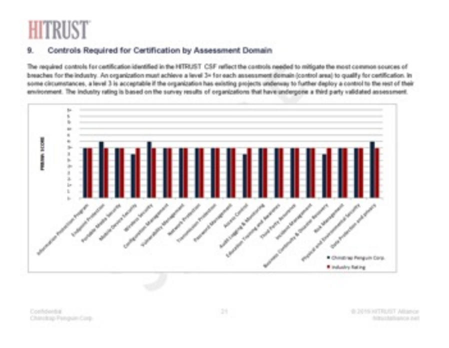
4. **Measured** (10 pts.) – Does the organization monitor the effectiveness of the control?
5. **Managed** (15 pts.) – Does the organization correct any problems that are identified while monitoring the effectiveness of the control?

15-point Rating Scheme for Certification

Maturity Level	1-	1	1+	2-	2	2+	3-	3	3+	4-	4	4+	5-	5	5+
Cut-off Score	<10	<19	<27	<36	<45	<53	<62	<71	<79	<83	<87	<90	<94	<98	≤100

- Scores for a control requirement can range from 0 to 100
- A total score of 72 to 79 (a "3+", or a solid "C" in academics) is considered the standard for a fully implemented control
- Scores over 80 generally indicate at least some aspect of the control requirements are monitored and/or managed to help ensure the control continues to remain fully implemented and effective

9. Breakdown by Control Areas



HITRUST

9. Controls Required for Certification by Assessment Domain

The required controls for certification identified in the HITRUST CSF reflect the controls needed to mitigate the most common sources of breaches for the industry. An organization must achieve a level 3+ for each assessment domain (control area) to qualify for certification. In some circumstances, a level 3 is acceptable if the organization has existing projects underway to further deploy a control to the rest of their environment. The industry rating is based on the survey results of organizations that have undergone a third party validated assessment.

Confidential
Chinstrap Penguin Corp.
21
© 2019 HITRUST Alliance
hitrustalliance.net

- This section provides a summary of the assessment results in terms of 19 topical control areas, which HITRUST refers to as CSF assessment domains
  - Facilitates the actual assessment process by grouping requirements that are typically handled by a specific office
  - Provides a more focused view on areas of particular interest to organizational leadership and external third parties
- The first page provides a histogram comparing assessment averages for each domain with the respective averages for all entities that have completed a validated assessment
- By reporting against standardized requirements, the organization can benchmark itself against other organizations and help ensure it is providing an appropriate level of due care and due diligence for the protection of its information assets

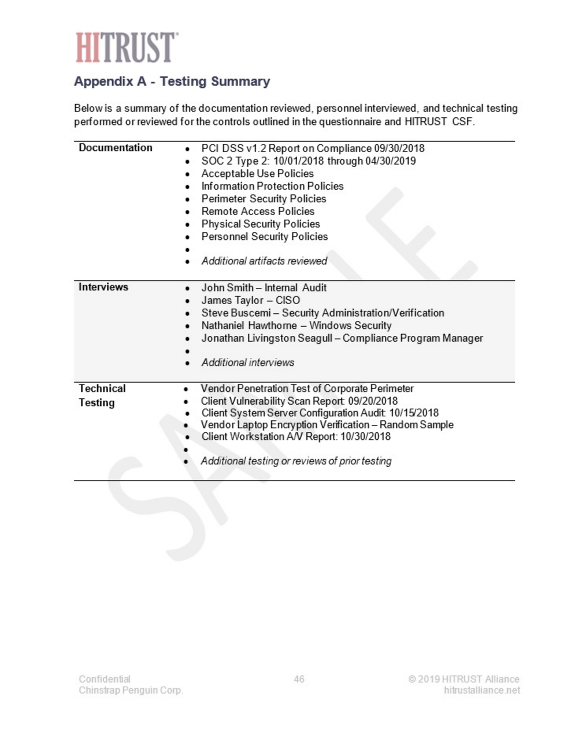
HITRUST

CSF Assessment Domain	Rating	Comments
01 Information Protection Program	3+	The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed. The information protection program is formally documented and actively monitored, reviewed and updated to ensure program objectives continue to be met. User security roles and responsibilities are clearly defined and communicated. The organization formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its human resources security protection program. The organization has an information security workforce improvement program. The organization ensures plans for security testing, training and monitoring activities are developed, implemented, maintained and reviewed for consistency with the risk management strategy and response priorities. Management ensures users are briefed on their security role(s)/responsibilities, conform with the terms and conditions of employment prior to obtaining access to the organization's information systems; are provided with guidelines regarding the security expectations of their roles; are motivated to comply with security policies; and continue to have the appropriate skills and qualifications for their role(s). The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures and notifies defined personnel within a defined time frame when a formal sanction process is initiated, identifying the individual sanctioned and the reason for the sanction. Further, the organization includes specific procedures for license, registration, and certification denial or revocation and other disciplinary action. Information security objectives, approach, scope, importance, goals and principles for the organization's security program are formally identified, communicated throughout the organization to users in a form that is relevant, accessible and understandable to the intended reader, and supported by a controls framework that considers legislative, regulatory, contractual requirements and other policy-related requirements. The security policies are regularly reviewed and updated to ensure they reflect leading practices, and communicated throughout the organization. The organization ensures individuals may make complaints concerning the information security policies, procedures, or the organization's compliance with its policies and procedures, documents the complaints and requests for changes, and records their disposition, if applicable. A senior-level information security official is appointed and is responsible for ensuring security processes are in place, communicated to all stakeholders, and consider and address organizational requirements. Senior management assigns an

Confidential
Chinstrap Penguin Corp.
22
© 2019 HITRUST Alliance
hitrustalliance.net

- The remaining pages provide a table with a detailed summary of the assessor's findings for each of the 19 CSF assessment domains
- The first column provides the CSF assessment domain that is addressed in the other two columns
- The second column provides the overall rating for the CSF assessment domain based on the 15-point maturity scale discussed earlier
- The third column in provides the assessor's comments for the CSF assessment domain
  - Summary of the assessor's findings based on the evaluation of each CSF control requirement that maps to the CSF assessment domain
  - High-level recommendations on how the organization can achieve a higher rating for the CSF assessment domain, which can help improve implementation of the HITRUST CSF control requirements and further mitigate excessive residual risk to the organization's information assets

Appendix A – Testing Summary



HITRUST

Appendix A - Testing Summary

Below is a summary of the documentation reviewed, personnel interviewed, and technical testing performed or reviewed for the controls outlined in the questionnaire and HITRUST CSF.

Documentation	• PCI DSS v1.2 Report on Compliance 09/30/2018 • SOC 2 Type 2: 10/01/2018 through 04/30/2019 • Acceptable Use Policies • Information Protection Policies • Perimeter Security Policies • Remote Access Policies • Physical Security Policies • Personnel Security Policies • • *Additional artifacts reviewed*
Interviews	• John Smith – Internal Audit • James Taylor – CISO • Steve Buscemi – Security Administration/Verification • Nathaniel Hawthorne – Windows Security • Jonathan Livingston Seagull – Compliance Program Manager • • *Additional interviews*
Technical Testing	• Vendor Penetration Test of Corporate Perimeter • Client Vulnerability Scan Report: 09/20/2018 • Client System Server Configuration Audit: 10/15/2018 • Vendor Laptop Encryption Verification – Random Sample • Client Workstation A/V Report: 10/30/2018 • • *Additional testing or reviews of prior testing*

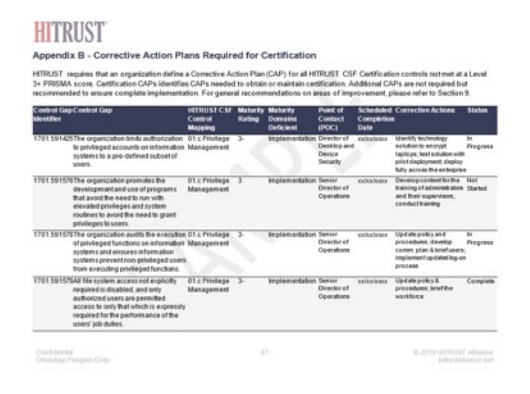
Confidential
Chinstrap Penguin Corp.

46

© 2019 HITRUST Alliance
hitrustalliance.net

- HITRUST recognizes three (3) types of testing (or evaluation):
  - The review of applicable documentation, such as an organization's written policies and procedures, organization charts, and network diagrams. It also includes the observation of processes or the implementation of certain controls, e.g., observing the amount of time it takes for a session to be automatically terminated or whether or not employees adhere to the organization's clear/clean desk policy. This type of evaluation may also be referred to as "examination."
  - Interviews with leadership, technical personnel, general users and other workforce members to identify actual practices (as opposed to written procedures) and gain other information relevant to the assessment
  - The conduct of technical testing, such as vulnerability scans, or the review of other independent testing such as that performed by an internal audit function or a third-party professional services (PS) firm
- The appendix simply provides a laundry list of all the testing performed by the assessor organization
- HITRUST uses this information to help determine if testing could reasonably support the evaluation and scoring/rating of the controls required for CSF certification
- For more information on the HITRUST assessment methodology employed by an assessor organization, see https://hitrustalliance.net/content/uploads/CSFAssessmentMethodology-1.pdf

Appendix B – Corrective Action Plans Required for Certification & Appendix C – Additional GAPs Identified



HITRUST

Appendix B - Corrective Action Plans Required for Certification

HITRUST requires that an organization define a Corrective Action Plan (CAP) for all HITRUST CSF Certification controls not met at a Level 3+ PRISMA score. Certification CAPs identifies CAPs needed to obtain or maintain certification. Additional CAPs are not required but recommended to ensure complete implementation. For general recommendations on areas of improvement, please refer to Section 9.

Control Gap Identifier	Control Gap	HITRUST CSF Control Mapping	Maturity Rating	Maturity Domains Deficient	Point of Contact (POC)	Scheduled Completion Date	Corrective Actions	Status
1701.591425	The organization limits authorization to privileged accounts on information systems to a pre-defined subset of users.	01.c Privilege Management	3-	Implementation	Director of Desktop and Device Security	xx/xx/xxxx	Identify technology solution to encrypt laptops; test solution with pilot deployment; deploy fully across the enterprise	In Progress
1701.591576	The organization promotes the development and use of programs that avoid the need to run with elevated privileges and system routines to avoid the need to grant privileges to users.	01.c Privilege Management	3	Implementation	Senior Director of Operations	xx/xx/xxxx	Develop content for the training of administrators and their supervisors; conduct training	Not Started
1701.591578	The organization audits the execution of privileged functions on information systems and ensures information systems prevent non-privileged users from executing privileged functions.	01.c Privilege Management	3-	Implementation	Senior Director of Operations	xx/xx/xxxx	Update policy and procedures; develop comm. plan & brief users; implement updated log-on process	In Progress
1701.591579	All file system access not explicitly required is disabled, and only authorized users are permitted access to only that which is expressly required for the performance of the users' job duties.	01.c Privilege Management	3-	Implementation	Senior Director of Operations	xx/xx/xxxx	Update policy & procedures; brief the workforce	Complete

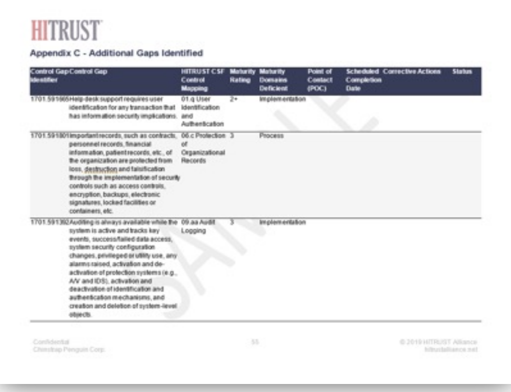
Confidential
Chinstrap Penguin Corp.

47

© 2019 HITRUST Alliance
hitrustalliance.net

- These appendices provide two (2) tables that list the corrective actions needed to address the identified control gaps
  - Certification CAPs: identifies CAPs needed to meet the criteria for CSF Certification
    - "3+" in all CSF Assessment Domains
    - "3+" for all controls; "3" plus CAPs or risk acceptance
    - CAPs will not be created for Gaps identified at the policy/procedure level if there is no corresponding Gap at the implementation level
  - Additional Gaps: Identified CAPs needed to ensure control requirements are fully implemented across the breadth and depth of the organization but do not adversely impact the criteria for CSF certification

For more information on CSF certification, see https://hitrustalliance.net/content/uploads/CSFAssuranceProgramRequirements-2.pdf



HITRUST

Appendix C - Additional Gaps Identified

Control Gap Identifier	Control Gap	HITRUST CSF Control Mapping	Maturity Rating	Maturity Domains Deficient	Point of Contact (POC)	Scheduled Completion Date	Corrective Actions	Status
1701.591665	Help-desk support requires user identification for any transaction that has information security implications.	01.q User Identification and Authentication	2+	Implementation				
1701.591801	Important records, such as contracts, personnel records, financial information, patient records, etc., of the organization are protected from loss, destruction and falsification through the implementation of security controls such as access controls, encryption, backups, electronic signatures, locked facilities or containers, etc.	06.c Protection of Organizational Records	3	Process				
1701.591392	Auditing is always available while the system is active and tracks key events, success/failed data access, system security configuration changes, privileged or utility use, any alarms raised, activation and de-activation of protection systems (e.g., A/V and IDS), activation and deactivation of identification and authentication mechanisms, and creation and deletion of system-level objects.	09.aa Audit Logging	3	Implementation				

Confidential
Chinstrap Penguin Corp.

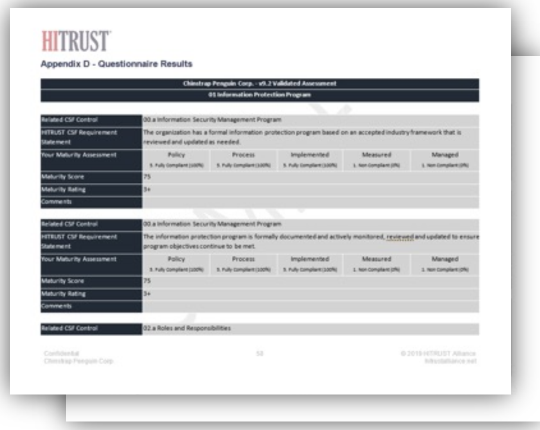
55

© 2019 HITRUST Alliance
hitrustalliance.net

- **Control Gap Identifier** – The tracking number the organization assigns to the CAP entry to help distinguish one control gap (weakness or deficiency) from another
- **Control Gap** –The control gap that was identified and for which the organization needs to take action; this is expressed in the language of the CSF requirement that was assessed
- **HITRUST CSF Control Mapping** – The CSF control that contains/addresses the requirement that was found to have a gap (a weakness or deficiency) in its implementation
- **Maturity Rating** – This is the overall maturity rating computed for the control based on its assessment
- **Maturity Domains Deficient** – This identifies which maturity domains resulted in a lower maturity rating
- **Point of Contact (POC)** – The individual or office that is responsible for addressing the control gap
- **Scheduled Completion Date** – The estimated date when all work associated with the corrective action will be finished and the CAP closed (marked completed) for the identified gap
- **Corrective Actions**– This is a brief description of the various actions or activities the organization will take to address the control gap; the actions are most often some form of remediation or "fix" but can be a formal acceptance of the excessive residual risk caused by the gap, if warranted.
- **Status** – Identifies whether the work has not yet been started, is ongoing, on hold, or completed

For more information on risk and CAP prioritization, refer to https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf

Appendix D – Questionnaire Results



Appendix D - Questionnaire Results

Chinstrap Penguin Corp. - v9.2 Validated Assessment

01 Information Protection Program

Related CSF Control	00.a Information Security Management Program				
HITRUST CSF Requirement Statement	The organization has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.				
Your Maturity Assessment	Policy 5. Fully Compliant (100%)	Process 5. Fully Compliant (100%)	Implemented 5. Fully Compliant (100%)	Measured 1. Non Compliant (0%)	Managed 1. Non Compliant (0%)
Maturity Score	75				
Maturity Rating	3+				
Comments					

Related CSF Control	00.a Information Security Management Program				
HITRUST CSF Requirement Statement	The information protection program is formally documented and actively monitored, reviewed and updated to ensure program objectives continue to be met.				
Your Maturity Assessment	Policy 5. Fully Compliant (100%)	Process 5. Fully Compliant (100%)	Implemented 5. Fully Compliant (100%)	Measured 1. Non Compliant (0%)	Managed 1. Non Compliant (0%)
Maturity Score	75				
Maturity Rating	3+				
Comments					

Related CSF Control	02.a Roles and Responsibilities

Confidential
Chinstrap Penguin Corp.

58

© 2018 HITRUST Alliance
hitrustalliance.net

- This appendix is generated from the MyCSF online assessment tool after the assessor submits the assessment for HITRUST validation and (possible) certification

- For more information on MyCSF, including downloadable brochures, refer to https://hitrustalliance.net/mycsf/

- For access to videos that describe various capabilities within MyCSF, refer to https://hitrustalliance.net/mycsfvideos/

- ***Title*** – Provides the name of the organization subject to the assessment and the CSF version used

- ***Subtitle*** – Provides the number and name of the CSF Assessment Domain for the controls that follow

- **Related CSF Control** - Provides the number and name of the CSF control from which the HITRUST CSF Requirement Statement is derived

- **HITRUST CSF Requirement Statement** – The CSF control requirement that was evaluated and the subject of the Maturity Assessment, Maturity Score, Maturity Rating, and Comments that follow.
- **Your Maturity Assessment** – The percentage of compliance with the requirements for each level of the maturity model: Policy, Process, Implemented, Measured and Managed

- **Maturity Score** – The raw score for the requirement computed as the sum of the percentage of the points awarded for each maturity level (as indicated by the percentages contained in the maturity assessment above.) Note the maximum points for each maturity level are: Policy – 15 pts, Process – 20 pts, Implemented – 40 pts, Measured – 10 pts, and Managed – 15 pts. In this example, the score was computed as (1)(15) + (1) (20) + (1)(40) + (0)(10) + (0)(15) = 75

- **Maturity Rating** – The maturity rating of the control requirement derived from the maturity score. In this case, 75 falls between 71 and 78, which results in a 3+. (Refer to the table in the previous slide addressing Section 8)

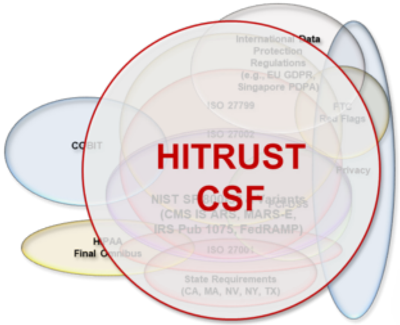
- **Comments** – A summary of the testing (evaluation) performed for the specified control requirement, or if the requirement is scored as N/A, the reason why it is not applicable

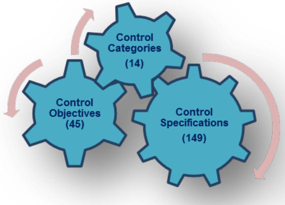
For more information on the maturity model and scoring approach, refer to https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf

Section 3

HOW IT DESCRIBES AN ORGANIZATION’S SECURITY POSTURE

Multiple Requirements but One Information Protection Program


International Data Protection Regulations (e.g., EU GDPR, Singapore PDPA)
ISO 27799
FTC Red Flags
COBIT
ISO 27002
HITRUST CSF
Privacy
NIST SP 800-53 Variants (CMS IS ARS, MARS-E, IRS Pub 1075, FedRAMP)
PCI-DSS
HIPAA Final Omnibus
ISO 27001
State Requirements (CA, MA, NV, NY, TX)



Sample of Included Standards, Frameworks & Other Authoritative Sources

ISO/IEC 27001:2005, 2013, 27002:2005, 2013, 27799:2008
21 CFR Part 11
COBIT 4.1; 5.0
NIST SP 800-53 Revision 4
NIST Cybersecurity Framework (CSF)
DHS Cyber Resilience Review

NIST SP 800-66 Revision 1
PCI DSS version 3
FTC Red Flags Rule
FFIEC IT InfoSec Examination
201 CMR 17.00 (State of Mass.)
NRS 603A (State of Nev.)

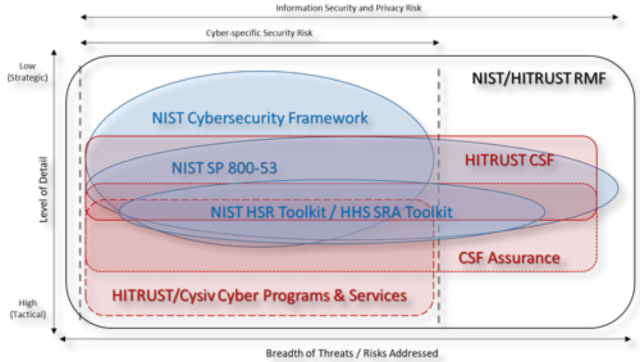
CSA Cloud Controls Matrix version 3.1
CIS CSC version 6 (SANS Top 20)
CMS IS ARS version 3.1
MARS-E version 2
IRS Pub 1075 v2014
FedRAMP
NY
GDPR

CSF Control Categories (Based on ISO 27001:2005)

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

A Model for Cybersecurity

- HITRUST provides a risk management framework (RMF) consistent with the NIST Cybersecurity Framework and also addresses non-cyber threats
  - NIST Cybersecurity Framework categorizes security controls according to an incident response process as opposed to the topical arrangement provided in a traditional RMF
  - HITRUST CSF provides an integrated, harmonized set of requirements specific to h as compared to individual references to controls in NIST and other frameworks
  - HITRUST CSF Assurance Program provides a standardized evaluation and reporting approach fully supported by an integrated maturity model
  - HITRUST CSF Assurance Program provides a pool of vetted assessor organizations and centralized quality assurance processes to ensure consistent and repeatable results

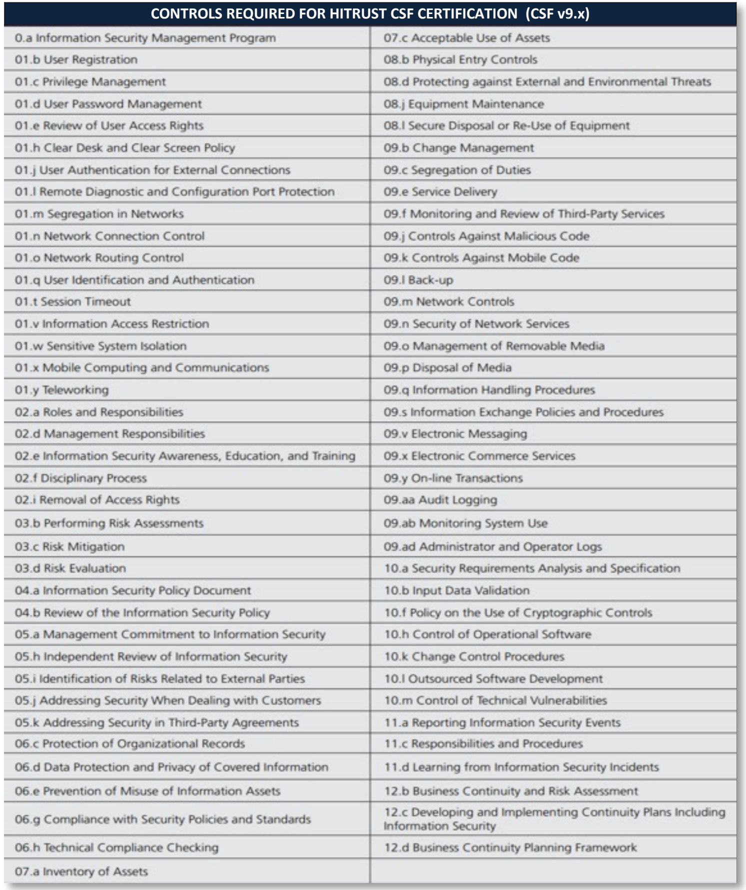

Information Security and Privacy Risk
Cyber-specific Security Risk
Low (Strategic)
Level of Detail
High (Tactical)
NIST/HITRUST RMF
NIST Cybersecurity Framework
NIST SP 800-53
HITRUST CSF
NIST HSR Toolkit / HHS SRA Toolkit
CSF Assurance
HITRUST/Cysiv Cyber Programs & Services
Breadth of Threats / Risks Addressed

The MyCSF Security Assessment

- Two major assessment types are available in the MyCSF GRC-based assessment management tool to support the HITRUST CSF Assurance Program
  - Security
    - Used to support HITRUST CSF Self-Assessment Reports, Validated Reports, and Certified Reports (“CSF Certification”)
    - Supports generation of a partial compliance scorecard that minimally addresses each of the HIPAA Security Rule’s standards and implementation specifications, if the HIPAA regulator factor is selected
    - Supports partial scorecards for other authoritative sources such as the AICPA Trust Services Criteria or NIST Cybersecurity Framework
  - Comprehensive
    - Used as the basis for an organization’s entire information protection program
    - Provides the ability to assess 100% of the HITRUST CSF control requirements
    - Supports the generation of various scorecards, e.g., a complete compliance scorecard for the HIPAA Security Rule or AICPA Trust Services Criteria, or a HITRUST certification and scorecard based on the NIST Cybersecurity Framework
- CSF v9.x certification is based on a MyCSF security assessment
- A security assessment addresses 75 of 135 security-specific CSF controls (or 149 controls if privacy-specific controls are included), which are considered:
  - “High risk”” based on the analysis of breach data and industry input
  - “High interest” based on the need to cover mainline security requirements
- Provides a reasonable level of assurance about the state of an assessed entity’s information protection program at a reasonable cost
- NIST specifically allows for the use of this type of approach to targeted assessments

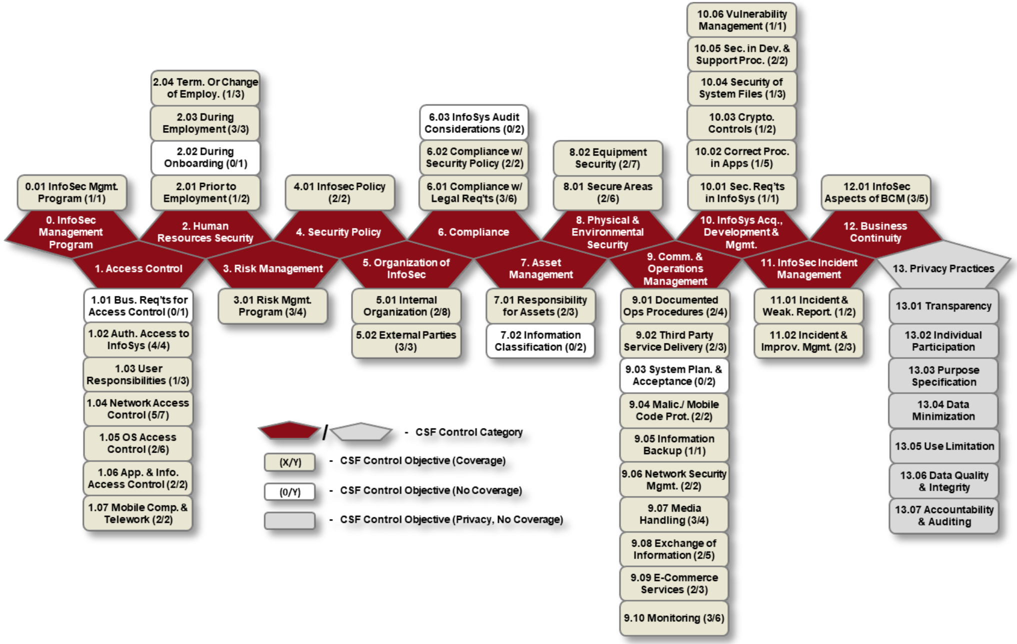
“Organizations can use targeted risk assessments, in which the scope is narrowly defined, to produce answers to specific questions … or to inform specific decisions[,] … have maximum flexibility on how risk assessments are conducted, … [and] are encouraged to use [NIST] guidance in a manner that most effectively and cost-effectively provides the information necessary to senior leaders/executives to facilitate informed decisions.”

(NIST SP 800-30 r1, p. 22)



CONTROLS REQUIRED FOR HITRUST CSF CERTIFICATION (CSF v9.x)	
0.a Information Security Management Program	07.c Acceptable Use of Assets
01.b User Registration	08.b Physical Entry Controls
01.c Privilege Management	08.d Protecting against External and Environmental Threats
01.d User Password Management	08.j Equipment Maintenance
01.e Review of User Access Rights	08.l Secure Disposal or Re-Use of Equipment
01.h Clear Desk and Clear Screen Policy	09.b Change Management
01.j User Authentication for External Connections	09.c Segregation of Duties
01.l Remote Diagnostic and Configuration Port Protection	09.e Service Delivery
01.m Segregation in Networks	09.f Monitoring and Review of Third-Party Services
01.n Network Connection Control	09.j Controls Against Malicious Code
01.o Network Routing Control	09.k Controls Against Mobile Code
01.q User Identification and Authentication	09.l Back-up
01.t Session Timeout	09.m Network Controls
01.v Information Access Restriction	09.n Security of Network Services
01.w Sensitive System Isolation	09.o Management of Removable Media
01.x Mobile Computing and Communications	09.p Disposal of Media
01.y Teleworking	09.q Information Handling Procedures
02.a Roles and Responsibilities	09.s Information Exchange Policies and Procedures
02.d Management Responsibilities	09.v Electronic Messaging
02.e Information Security Awareness, Education, and Training	09.x Electronic Commerce Services
02.f Disciplinary Process	09.y On-line Transactions
02.i Removal of Access Rights	09.aa Audit Logging
03.b Performing Risk Assessments	09.ab Monitoring System Use
03.c Risk Mitigation	09.ad Administrator and Operator Logs
03.d Risk Evaluation	10.a Security Requirements Analysis and Specification
04.a Information Security Policy Document	10.b Input Data Validation
04.b Review of the Information Security Policy	10.f Policy on the Use of Cryptographic Controls
05.a Management Commitment to Information Security	10.h Control of Operational Software
05.h Independent Review of Information Security	10.k Change Control Procedures
05.i Identification of Risks Related to External Parties	10.l Outsourced Software Development
05.j Addressing Security When Dealing with Customers	10.m Control of Technical Vulnerabilities
05.k Addressing Security in Third-Party Agreements	11.a Reporting Information Security Events
06.c Protection of Organizational Records	11.c Responsibilities and Procedures
06.d Data Protection and Privacy of Covered Information	11.d Learning from Information Security Incidents
06.e Prevention of Misuse of Information Assets	12.b Business Continuity and Risk Assessment
06.g Compliance with Security Policies and Standards	12.c Developing and Implementing Continuity Plans Including Information Security
06.h Technical Compliance Checking	12.d Business Continuity Planning Framework
07.a Inventory of Assets	

HITRUST CSF Coverage of a MyCSF Security Assessment



0. InfoSec Management Program
0.01 InfoSec Mgmt. Program (1/1)

1. Access Control
1.01 Bus. Req'ts for Access Control (0/1)
1.02 Auth. Access to InfoSys (4/4)
1.03 User Responsibilities (1/3)
1.04 Network Access Control (5/7)
1.05 OS Access Control (2/6)
1.06 App. & Info. Access Control (2/2)
1.07 Mobile Comp. & Telework (2/2)

2. Human Resources Security
2.01 Prior to Employment (1/2)
2.02 During Onboarding (0/1)
2.03 During Employment (3/3)
2.04 Term. Or Change of Employ. (1/3)

3. Risk Management
3.01 Risk Mgmt. Program (3/4)

4. Security Policy
4.01 Infosec Policy (2/2)

5. Organization of InfoSec
5.01 Internal Organization (2/8)
5.02 External Parties (3/3)

6. Compliance
6.01 Compliance w/ Legal Req'ts (3/6)
6.02 Compliance w/ Security Policy (2/2)
6.03 InfoSys Audit Considerations (0/2)

7. Asset Management
7.01 Responsibility for Assets (2/3)
7.02 Information Classification (0/2)

8. Physical & Environmental Security
8.01 Secure Areas (2/6)
8.02 Equipment Security (2/7)

9. Comm. & Operations Management
9.01 Documented Ops Procedures (2/4)
9.02 Third Party Service Delivery (2/3)
9.03 System Plan. & Acceptance (0/2)
9.04 Malic./Mobile Code Prot. (2/2)
9.05 Information Backup (1/1)
9.06 Network Security Mgmt. (2/2)
9.07 Media Handling (3/4)
9.08 Exchange of Information (2/5)
9.09 E-Commerce Services (2/3)
9.10 Monitoring (3/6)

10. InfoSys Acq., Development & Mgmt.
10.01 Sec. Req'ts in InfoSys (1/1)
10.02 Correct Proc. in Apps (1/5)
10.03 Crypto. Controls (1/2)
10.04 Security of System Files (1/3)
10.05 Sec. in Dev. & Support Proc. (2/2)
10.06 Vulnerability Management (1/1)

11. InfoSec Incident Management
11.01 Incident & Weak. Report. (1/2)
11.02 Incident & Improv. Mgmt. (2/3)

12. Business Continuity
12.01 InfoSec Aspects of BCM (3/5)

13. Privacy Practices
13.01 Transparency
13.02 Individual Participation
13.03 Purpose Specification
13.04 Data Minimization
13.05 Use Limitation
13.06 Data Quality & Integrity
13.07 Accountability & Auditing

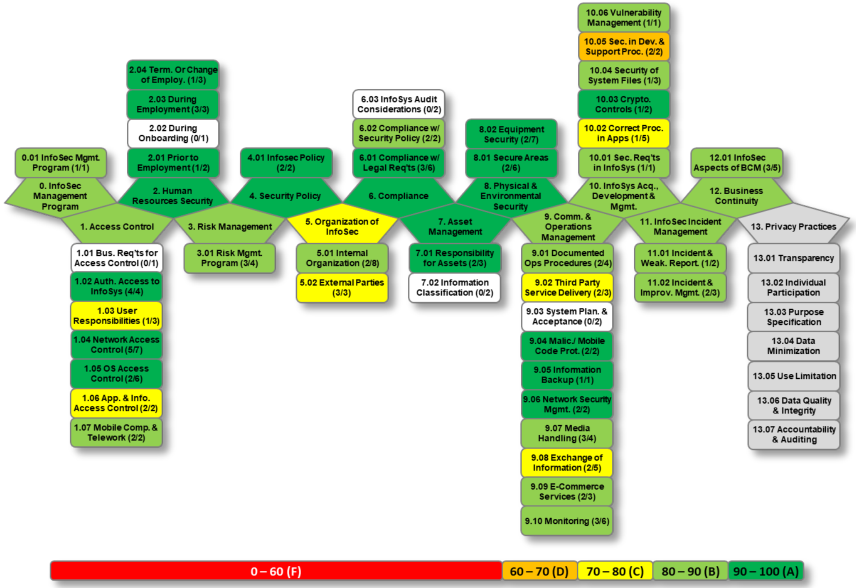
▰ / ▱ - CSF Control Category
(X/Y) - CSF Control Objective (Coverage)
(0/Y) - CSF Control Objective (No Coverage)
▭ - CSF Control Objective (Privacy, No Coverage)

DEPENDING ON THE RELYING ORGANIZATON's ASSURANCE NEEDS, ALL CSF CONTROLS ARE AVAILABLE AND MAY BE EVALUATED VIA THE SELECTION OF A <u>COMPREHENSIVE</u> ASSESSMENT

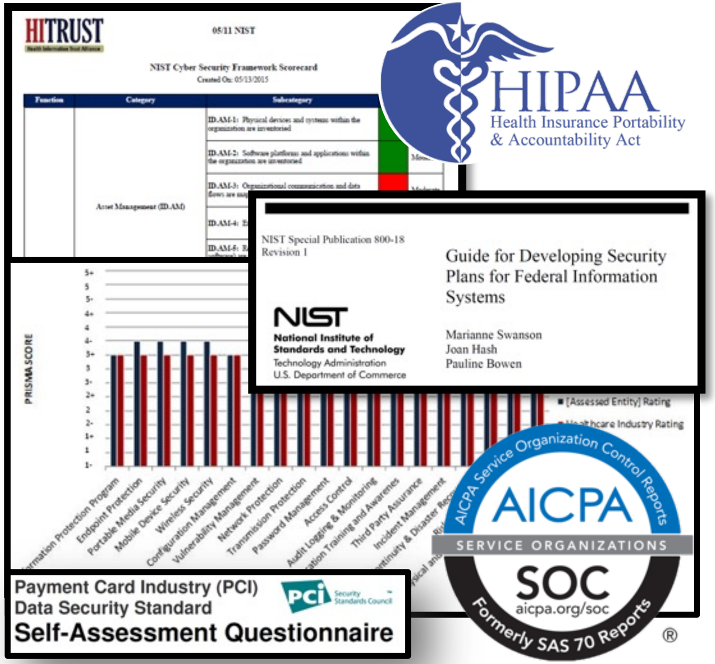
- Focused on "high risk, high interest" control requirements
- Covers controls in 37 of 42 security-specific control objectives, indicated by (x/y) in the figure to the left
- For those control objectives not specifically covered:
  - 1.01 Business Requirements for Access Control contains 1 control, 01.a Access Control Policy, which is not assessed
  - 2.02 During On-boarding contains 1 control, 02.c Terms & Conditions of Employment, which is not assessed
  - 6.03 Information System Audit Consideration contains 2 controls, 06.i Information System Audit Controls and 06.j Protection of Information System Audit Tools; note auditing and monitoring are addressed in in great detail via 09.10 Monitoring, which is addressed
  - 7.02 Information Classification contains 2 controls, 07.d Classification Guidelines and 07.e Information Labeling and Handling; note classification is a required element for 07.a, Inventory of Assets, which is addressed
  - 9.03 System Planning & Acceptance contains 2 controls, 09.h Capacity Mgmt. and 09.i System Acceptance, which are not assessed
- For the controls not specifically covered in the assessment regardless of control objective, the evaluation of 0.01 Information Security Mgmt. Program and 3.01 Risk Mgmt. Program will provide evidence of any gaps the organization has identified via internal and external assessments and audits, security incidents, data breaches and other sources, and whether or not the organization has taken corrective action
- Domain 13 Privacy Practices is not currently addressed

Assess Once and Report Many Times in Many Ways

- Cross-references allow granular scores at the requirement level to be “rolled up” in many and varied ways, both
  - Internal to the CSF, e.g., CSF control assessment domains (shown bottom right), CSF control objectives/categories (such as depicted below) and
  - External to the CSF, e.g., against the NIST Cybersecurity Framework, HIPAA, AICPA Trust Services Principles & Criteria, or PCI (as seen on the right)


2.04 Term. Or Change of Employ. (1/3)
2.03 During Employment (3/3)
2.02 During Onboarding (0/1)
2.01 Prior to Employment (1/2)
0.01 InfoSec Mgmt. Program (1/1)
4.01 Infosec Policy (2/2)
6.03 InfoSys Audit Considerations (0/2)
6.02 Compliance w/ Security Policy (2/2)
6.01 Compliance w/ Legal Req'ts (3/6)
8.02 Equipment Security (2/7)
8.01 Secure Areas (2/6)
10.06 Vulnerability Management (1/1)
10.05 Sec. in Dev. & Support Proc. (2/2)
10.04 Security of System Files (1/3)
10.03 Crypto. Controls (1/2)
10.02 Correct Proc. in Apps (1/5)
10.01 Sec. Req'ts in InfoSys (1/1)
12.01 InfoSec Aspects of BCM (3/5)
0. InfoSec Management Program
2. Human Resources Security
4. Security Policy
6. Compliance
8. Physical & Environmental Security
10. InfoSys Acq., Development & Mgmt.
12. Business Continuity
1. Access Control
3. Risk Management
5. Organization of InfoSec
7. Asset Management
9. Comm. & Operations Management
11. InfoSec Incident Management
13. Privacy Practices
1.01 Bus. Req'ts for Access Control (0/1)
1.02 Auth. Access to InfoSys (4/4)
1.03 User Responsibilities (1/3)
1.04 Network Access Control (5/7)
1.05 OS Access Control (2/6)
1.06 App. & Info. Access Control (2/2)
1.07 Mobile Comp. & Telework (2/2)
3.01 Risk Mgmt. Program (3/4)
5.01 Internal Organization (2/8)
5.02 External Parties (3/3)
7.01 Responsibility for Assets (2/3)
7.02 Information Classification (0/2)
9.01 Documented Ops Procedures (2/4)
9.02 Third Party Service Delivery (2/3)
9.03 System Plan. & Acceptance (0/2)
9.04 Malic./ Mobile Code Prot. (2/2)
9.05 Information Backup (1/1)
9.06 Network Security Mgmt. (2/2)
9.07 Media Handling (3/4)
9.08 Exchange of Information (2/5)
9.09 E-Commerce Services (2/3)
9.10 Monitoring (3/6)
11.01 Incident & Weak. Report. (1/2)
11.02 Incident & Improv. Mgmt. (2/3)
13.01 Transparency
13.02 Individual Participation
13.03 Purpose Specification
13.04 Data Minimization
13.05 Use Limitation
13.06 Data Quality & Integrity
13.07 Accountability & Auditing
0 – 60 (F)
60 – 70 (D)
70 – 80 (C)
80 – 90 (B)
90 – 100 (A)

- No matter what the question about an entity’s information protection program, a CSF validated assessment can help provide the answers


HITRUST
05/11 NIST
NIST Cyber Security Framework Scorecard
Created On: 05/13/2015
Function
Category
Subcategory
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 ma
ID.AM-4:
ID.AM-5:
HIPAA
Health Insurance Portability & Accountability Act
NIST Special Publication 800-18 Revision 1
Guide for Developing Security Plans for Federal Information Systems
NIST
National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce
Marianne Swanson
Joan Hash
Pauline Bowen
PRISMA SCORE
5+
5
5-
4+
4
4-
3+
3
3-
2+
2
2-
1+
1
1-
Endpoint Protection
Portable Media Security
Mobile Device Security
Wireless Security
Configuration Management
Vulnerability Management
Network Protection
Transmission Protection
Password Management
Access Control
Audit Logging & Monitoring
Third Party Assurance
Incident Management
[Assessed Entity] Rating
Healthcare Industry Rating
Payment Card Industry (PCI)
Data Security Standard
Self-Assessment Questionnaire
PCI Security Standards Council
AICPA Service Organization Control Reports
AICPA
SERVICE ORGANIZATIONS
SOC
aicpa.org/soc
Formerly SAS 70 Reports

All product names, logos, and brands are property of their respective owners and used for identification purposes only, and are in no way associated or affiliated with HITRUST. Use of these names, logos, and brands does not imply endorsement.

Section 4

HOW YOU CAN ALIGN IT WITH YOUR CURRENT APPROACH

Actively Reading HITRUST CSF Validated and Certification Reports (1)

- **Step 1*** – Confirm the organization name on the title page is correct or is an acceptable alternative (e.g., the Incorporated name versus the fictitious name). If not, request the organization provide the correct report.
- **Step 2** – Confirm the existence of (1) the Letter of Certification (or Validation, as appropriate) in Section 2 and (2) the Representation Letter from Management in Section 3. If either of these are missing, reject the report and request a complete/corrected copy of the report.
- **Step 3** – Review the assessment context in Section 4 and confirm (1) the name of the organization for which the report was prepared and (2) the date of the report match the name and date on the title page. If not, reject the report and request a corrected copy.
- **Step 4** – Make note of the organizational, regulatory and system risk factors identified in Section 4 and ensure these factors are appropriate to the intended scope of the assessment. If the factors do not adequately describe the scope of the assessment, determine what control gaps may exist and whether assurances around their implementation are needed. If needed, either request additional information from the assessed entity to address these gaps or reject the report and request a new one.
- **Step 5** – Review the scope of the assessment in Section 5 and determine if all the organizational business units, information systems, and outsourced services of interest, i.e., those for which assurances are required, are covered by the assessment. If not, determine what gaps may exist and request additional information to provide the necessary assurances. Alternatively, reject the report and request one with the required scope.

** Note that not all steps or the actions described in each step are necessarily sequential; e.g., concerns/issues identified in any one step may be addressed together after the complete review/reading of the report.*

Actively Reading HITRUST CSF Validated and Certification Reports (2)

- **Step 6** – Review the breadth and depth of the assessed organization’s information protection program in Section 6, including the types of technology deployed and the number and variety of independent assessments. Ensure level of program maturity is consistent with your expectations given the inherent risk the assessed organization presents. If not, review the findings for CSF Assessment Domain 1, Information Protection Program in Section 9 and determine if the scores and observations are consistent with your understanding of its maturity. Make note of the recommended actions for improving the overall maturity score for this domain and any CAPs that may exist for CSF controls 0.a, 03.b and 03.c in Section 7 and Appendix B. Determine if the proposed corrective actions adequately address any concerns about the assessed organization’s information protection program, including any controls/requirements that are not specifically addressed by the assessment. Discuss any concerns you may have with the assessed organization and determine if additional corrective action will be taken or, if not, whether your organization is willing to accept any additional residual risk you perceive. (You may also wish to consider how the assessed organization compares to the rest of the industry via the benchmark information in Section 9.)

- **Step 7** – Review the remaining CSF Assessment Domains in Section 9. Verify the ratings match those in the benchmark diagram. If not, you may wish to request a corrected report. Ensure the ratings and the summaries for each CSF Assessment Domain adequately describe these areas. If not, review the findings for each relevant CSF control in Appendices D to determine if any perceived gaps in the Section 9 summaries are adequately addressed and/or consider requesting additional information from the assessed entity (based on the perceived level of excessive risk to your organization). Review the recommendations for improvement and, based on the domain score, compare the recommendations to the corrective actions identified in Appendices B and C, and/or those for individual controls identified in Section 7 and Appendix D. If you believe there are gaps that have not been addressed to bring a CSF control requirement or CSF Assessment Domain score in line with certification requirements (generally a 3+ or a 3 with CAPs or formal acceptance of excessive residual risk), consider discussing the issue(s) with the assessed organization and obtain additional information/assurances as needed.

Actively Reading HITRUST CSF Validated and Certification Reports (3)

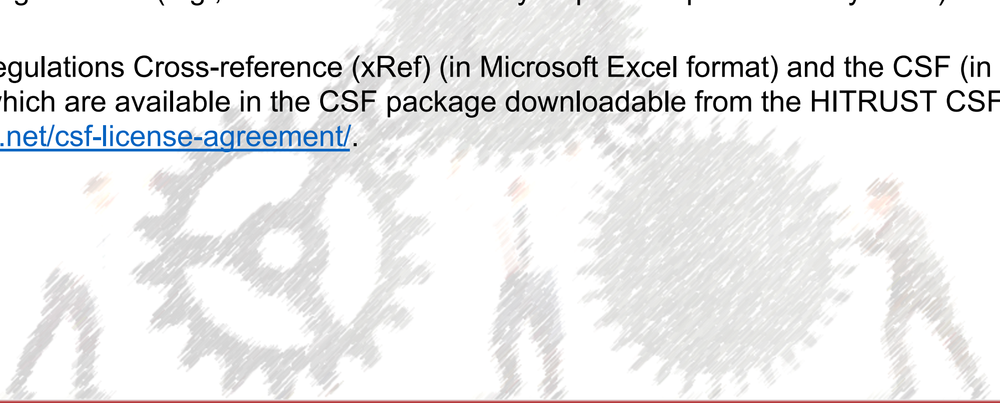
- **Step 8** – Review the results in Appendix D for any controls not reviewed in Steps 6 and 7, as needed, to address any particular concerns your organization may have regarding a specific requirement. For example, some organizations may have a particular interest in segmenting certain devices from the rest of the network or restricting removable media to company-only devices. If these specific concerns are not adequately addressed by or documented in the report, consider requesting additional information/assurances from the assessed organization.

- **Step 9** – When conducting Steps 6 thru 8, you may wish to refer to Appendix A (as needed) to ensure testing adequately supports the assessment results documented in Sections 7 and 9 and in Appendix D. If not, consider discussing possible discrepancies with the assessed organization and obtain additional information/assurances.

- **Step 10** – Consistent with your overall third-party assurance program requirements, formally document your “analysis” of the HITRUST CSF assessment report along with summaries of additional discussions, either internally or with the assessed organization, along with any recommendations and/or courses of action required.

Aligning Reports to Your Current Approach

- Relying organizations that already use the HITRUST CSF as the basis for their information protection program should have little difficulty in leveraging a HITRUST CSF assessment report to:
  - Provide assurances to internal stakeholders (e.g., executive leadership or internal audit) or external third parties (e.g., regulators).
  - Obtain assurances about a third-party organization’s information protection program.
- However, organizations that do not already use or are otherwise unfamiliar with the HITRUST CSF may have difficulty relating the CSF controls to their own information security controls (safeguards), whether it’s based on another third party framework (e.g., PCI DSS) or it was built as a custom specification for the organization (e.g., based on the risk analysis process prescribed by NIST).
- You’ll need the HITRUST CSF v9.x Standards and Regulations Cross-reference (xRef) (in Microsoft Excel format) and the CSF (in Adobe PDF format) to facilitate your work, copies of which are available in the CSF package downloadable from the HITRUST CSF License Agreement Webpage at https://hitrustalliance.net/csf-license-agreement/.



More on the Documents You'll Need

HITRUST CSF®

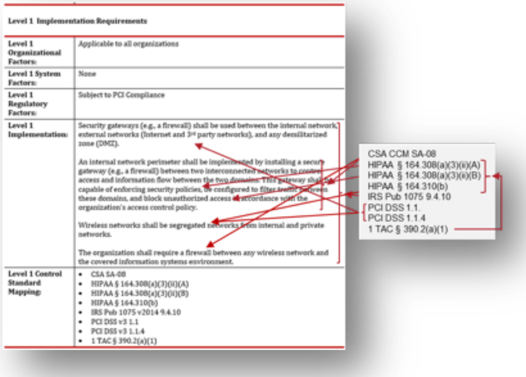
Version 9.2

January 2019

HITRUST

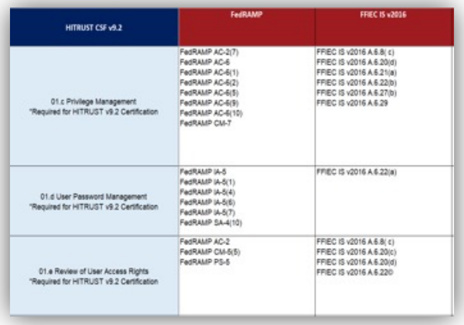
CSF PDF

- The CSF in Adobe PDF format provides a narrative description of all the control requirements, and is structured along the lines of ISO/IEC 27001:2005
  - 14 Control Categories
  - 46 Control Objectives parsed amongst the Categories
  - 149 Controls parsed amongst the Objectives
- Each control contains up to 3 implementation levels and may include 1 or more industry segments following the last level, which support
  - Special data requirements like card data and federal tax information
  - Special organizational requirements such as Health Information Exchanges
  - Other special requirements such as GDPR



Level 1 Implementation Requirements	
Level 1 Organizational Factors:	Applicable to all organizations
Level 1 System Factors:	None
Level 1 Regulatory Factors:	Subject to PCI Compliance
Level 1 Implementation:	Security gateways (e.g., a firewall) shall be used between the internal network, external networks (Internet and 3rd party networks), and any demilitarized zone (DMZ). An internal network perimeter shall be implemented by installing a secure gateway (e.g., a firewall) between two interconnected networks to control access and information flow between the two domains. This gateway shall be capable of enforcing security policies, be configured to filter traffic between these domains, and block unauthorized access in accordance with the organization's access control policy. Wireless networks shall be segregated networks from internal and private networks. The organization shall require a firewall between any wireless network and the covered information systems environment.
Level 1 Control Standard Mapping:	• CSA SA-08 • HIPAA § 164.308(a)(3)(ii)(A) • HIPAA § 164.308(a)(3)(ii)(B) • HIPAA § 164.310(b) • IRS Pub 1075 v2014 9.4.10 • PCI DSS v3 1.1 • PCI DSS v3 1.1.4 • 1 TAC § 390.2(a)(1)

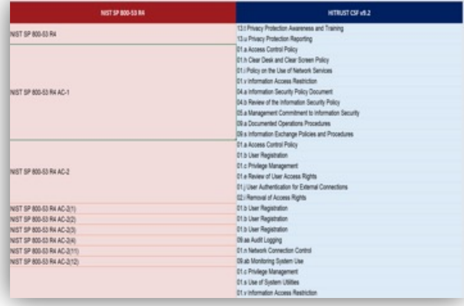
CSA CCM SA-08
HIPAA § 164.308(a)(3)(ii)(A)
HIPAA § 164.308(a)(3)(ii)(B)
HIPAA § 164.310(b)
IRS Pub 1075 9.4.10
PCI DSS 1.1.
PCI DSS 1.1.4
1 TAC § 390.2(a)(1)



HITRUST CSF v9.2	FedRAMP	FFIEC IS v2016
01.c Privilege Management *Required for HITRUST v9.2 Certification	FedRAMP AC-2(7) FedRAMP AC-6 FedRAMP AC-6(1) FedRAMP AC-6(2) FedRAMP AC-6(5) FedRAMP AC-6(9) FedRAMP AC-6(10) FedRAMP CM-7	FFIEC IS v2016 A.6.8(c) FFIEC IS v2016 A.6.20(d) FFIEC IS v2016 A.6.21(a) FFIEC IS v2016 A.6.22(b) FFIEC IS v2016 A.6.27(b) FFIEC IS v2016 A.6.29
01.d User Password Management *Required for HITRUST v9.2 Certification	FedRAMP IA-5 FedRAMP IA-5(1) FedRAMP IA-5(4) FedRAMP IA-5(6) FedRAMP IA-5(7) FedRAMP SA-4(10)	FFIEC IS v2016 A.6.22(a)
01.e Review of User Access Rights *Required for HITRUST v9.2 Certification	FedRAMP AC-2 FedRAMP CM-5(5) FedRAMP PS-5	FFIEC IS v2016 A.6.8(c) FFIEC IS v2016 A.6.20(c) FFIEC IS v2016 A.6.20(d) FFIEC IS v2016 A.6.22©

HITRUST xRef Spreadsheet

- The xRef has multiple tabs, the first of which provides a cross-reference matrix from all the authoritative sources mapped to the HITRUST CSF at the control implementation level (see figure to the left)
- The remaining tabs provide mappings from individual authoritative sources to the HITRUST CSF at the control level (see figure to the right)
- Note mappings down to the individual MyCSF requirement statement (the level at which CSF assessments occur) are only available in the MyCSF assessment tool at this time

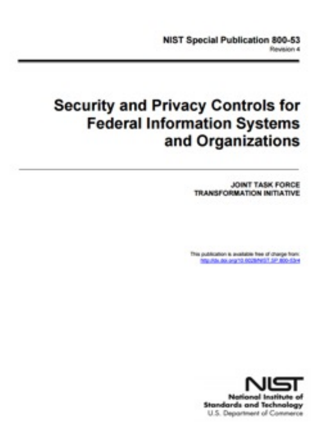


NIST SP 800-53 R4	HITRUST CSF v9.2
NIST SP 800-53 R4	13.t Privacy Protection Awareness and Training 13.u Privacy Protection Reporting
NIST SP 800-53 R4 AC-1	01.a Access Control Policy 01.h Clear Desk and Clear Screen Policy 01.i Policy on the Use of Network Services 01.v Information Access Restriction 04.a Information Security Policy Document 04.b Review of the Information Security Policy 05.a Management Commitment to Information Security 09.a Documented Operations Procedures 09.s Information Exchange Policies and Procedures
NIST SP 800-53 R4 AC-2	01.a Access Control Policy 01.b User Registration 01.c Privilege Management 01.e Review of User Access Rights 01.j User Authentication for External Connections 02.i Removal of Access Rights
NIST SP 800-53 R4 AC-2(1)	01.b User Registration
NIST SP 800-53 R4 AC-2(2)	01.b User Registration
NIST SP 800-53 R4 AC-2(3)	01.b User Registration
NIST SP 800-53 R4 AC-2(4)	09.aa Audit Logging
NIST SP 800-53 R4 AC-2(11)	01.n Network Connection Control
NIST SP 800-53 R4 AC-2(12)	09.ab Monitoring System Use
	01.c Privilege Management 01.s Use of System Utilities 01.v Information Access Restriction

Mapping Your Controls to the HITRUST CSF

- If the controls you've specified for your information protection program are based on a framework like the Cloud Security Alliance's Cloud Control Matrix (CSA CCM) or the Payment Card Industry Digital Security Standard (PCI DSS), the process of mapping your controls to the HITRUST CSF is generally straightforward
- This will also work if you have proprietary controls based on a NIST-type risk analysis as long as you've already mapped them to one of the more comprehensive authoritative sources that are also mapped by HITRUST to the CSF (NIST SP 800-53 being one of the best)
- Mappings can be done using a more high-level framework like AICPA's Trust Services Principles and Criteria and even the NIST Cybersecurity Framework, but it will require some work searching through the CSF for key terms, similar to the process described in the next example for proprietary programs
- However, if you use a custom set of controls and you do not currently map them to a recognized standard like NIST, PCI DSS or CSA CCM, the mapping exercise will be more difficult and time-consuming

Framework-based Program



NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for
Federal Information Systems
and Organizations

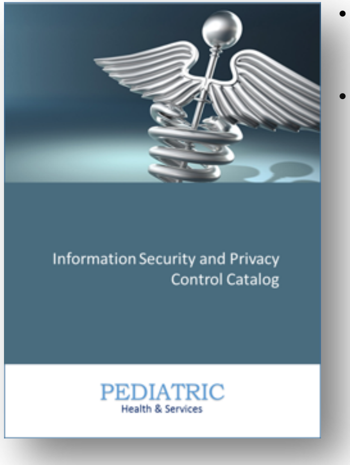
JOINT TASK FORCE
TRANSFORMATION INITIATIVE

This publication is available free of charge from:
http://dx.doi.org/10.6028/NIST.SP.800-53r4

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

- Determine if your framework controls have an authoritative source in common with the HITRUST CSF, e.g., NIST SP 800-53 r4
- If not, consider mapping your controls to a common standard, such as NIST SP 800-53 r4
- Cross-walk your controls to the CSF based on the common standard by:
  - Selecting a subset of controls or control requirements in the HITRUST CSF that have the same mapping to the control you wish to map, e.g., NIST AC-1
  - Review the language in the subset of controls or control requirements and determine the best match

Proprietary Program



Information Security and Privacy
Control Catalog

PEDIATRIC
Health & Services

- If you've mapped your controls to a common standard like NIST SP 800-53 r4, follow the directions for a framework-based program
- If not, you'll need to map your controls directly to the HITRUST CSF by:
  - Identifying the appropriate CSF Control Category for the proprietary control, e.g., 01. Access Control
  - Selecting the CSF Control Objective for the proprietary control that fits best, e.g., 01.02 Access to Information Systems
  - Reviewing the language in your control and identifying the CSF control that is the best match based on intent/content, e.g., 01.e Review of User Access Rights, or
  - If unable to determine a match, searching the CSF based on one or more key words or phrases

Mapping a Framework-based Program to the CSF

NIST Special Publication 800-53
Revision 4

Security and Privacy Controls for Federal Information Systems and Organizations

JOINT TASK FORCE
TRANSFORMATION INITIATIVE

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Example – NIST-based Controls

- Assume your information protection requirements, including those for your third parties, are based on the controls contained in NIST SP 800-53 r4
- Assume your organization wants the events you've identified in your audit standard to reasonably support an investigation should a security incident occur
- You also know this requirement is derived from NIST SP 800-53 control AU-2 Audit Events, subparagraph (c), which states the organization:

  > *Provides a rationale for why the auditable events are deemed to be adequate to support after-the-fact investigations of security incidents.*

- Referring to the "NIST SP 800-53" tab in the HITRUST CSF xRef spreadsheet, we see that AU-2 maps to the following CSF controls:
  - 01.p Secure Log-on Procedures
  - 01.s Use of System Utilities
  - 06.i Info. System Audit Controls
  - 09.aa Audit Logging
  - 09.ad Admin. and Operator Logs
  - 09.ae Fault Logging
- By looking up the CSF controls in the first tab of the xRef, "CSF Cross-Reference," we note that AU-2 is mapped at levels 1, 2, 2, 2, 1 and 1 for CSF controls 01.p, 01.s, 06i, 09.aa, 09.ad and 09.ae, respectively
- On inspection of the narrative for CSF control 09.aa, level 1 in the CSF PDF document, we find the relevant language:

  > *The organization provides a rationale for why the auditable events are deemed adequate to support after the fact investigations of security incidents and which events require auditing on a continuous basis in response to specific situations.*

Payment Card Industry (PCI)
Data Security Standard

Requirements and Security Assessment Procedures
Version 3.1
April 2015

Example – PCI-based Controls

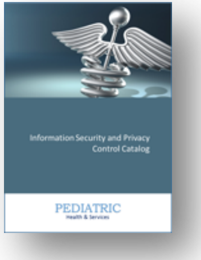
- Assume you're interested in specific information protection requirements for a system that processes credit card information, and this regulatory requirement is within scope of the CSF assessment report you're reviewing
- Subsequently you need to determine which CSF controls map to your controls that are tied directly to PCI DSS v3.2
- So let's find where these requirements are located within the CSF by way of an example, such as the need to ensure the importance of cardholder data security is part of the security training & awareness program
- PCI DSS v3.2 control 12.6 states the organization must:

  > *Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures*

- Referring to the "PCI DSS v3.2" tab in the HITRUST CSF xRef spreadsheet, we see that 12.6 maps to CSF control 02.e Information Security Awareness, Education & Training
- By looking up the CSF control 02.e in the first tab of the xRef, "CSF Cross-Reference," we note that PCI DSS 12.6 maps to 02.e level 2
- On inspection of the narrative in level 2, we note the language does not exist; subsequently, we look in the industry segment for PCI and find the relevant language:

  > *The organization ensures that all personnel are aware of the cardholder data security policy and procedures as part of the formal security awareness program.*

Mapping a Proprietary Program to the CSF



- When organizations establish their own custom or proprietary controls, the number of controls and their specificity can vary significantly
- When the organization's proprietary controls have been mapped to an industry-recognized or "best practice" control framework, the process of mapping them to their respective HITRUST CSF controls is relatively straightforward and can generally follow the same process for framework-based programs, which we outlined previously
- However, when the proprietary controls have not been mapped to such a control framework, the process becomes much more of a manual exercise, which may be performed by either (1) selecting a relevant CSF control category, objective and control to help narrow the search for an equivalent requirement, or (2) simply reviewing the results of one or more key word searches of the entire CSF

Example – Proprietary Controls

- Consider the following requirement:

  Information containing sensitive information is not left in the open, unattended and unsecured.
- Although the requirement appears fairly specific, there are actually several issues that it could potentially cover; in addition to the typical "clear desk" or "clean desk" requirement, we might also wish to consider the security of documents left out on printers and facsimile machines as well as the security of portable media (assuming these other issues are not addressed elsewhere in your proprietary control framework)
- Clear/clean Desk – This is an access control requirement, CSF Control Category 1.0; is generally a user responsibility, which is addressed by CSF Control Objective 01.03; and appears to be addressed by CSF control 01.h Clear Desk and Clear Screen Policy
- The control specification for 01.h states, "A clear desk policy for papers and removable storage media and a clear screen policy for information assets shall be adopted," which indicates the first and third of our concerns are addressed by the control
- By reviewing the 01.h level 1 control specification, it's clear that the second of our concerns, the security of printers and facsimile machines, is also addressed
- Alternatively, one could search the CSF PDF on the following key terms to locate relevant control language: "clean desk" (0 matches), "desk" (31 matches), "clear desk" (6 matches), "printer" (5 matches), "facsimile" (8 matches), "fax" (8 matches), "portable media" (0 matches) and/or "removable media" (19 matches)

Section 5

WHERE YOU CAN FIND MORE INFORMATION

HITRUST Resources

Healthcare Sector Cybersecurity Framework Implementation Guide

October 2015

HITRUST

Healthcare Sector CsF Implementation Guide

Discusses healthcare's implementation of the NIST Cybersecurity Framework based on the HITRUST CSF and CSF Assurance Program

https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf

HITRUST

Understanding HITRUST's Approach to Risk vs. Compliance-based Information Protection

Risk vs. Compliance-based Protection

Discusses the difference between compliance and risk-based information protection programs and shows how controls are selected based on a risk analysis, after which their implementation becomes a compliance exercise

https://hitrustalliance.net/documents/csf_rmf_related/RiskVsComplianceWhitepaper.pdf

HITRUST

Risk Analysis Guide for HITRUST Organizations & Assessors

Risk Analysis Guide

Provides a detailed discussion of HITRUST's NIST-based control implementation maturity model, HITRUST's scoring model, and additional information on risk treatments, including remediation planning for control deficiencies

https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf

HITRUST

HITRUST MyCSF vs. GRC Tools

Understanding the Differences and Total Cost of Ownership

HITRUST MyCSF® vs. GRC Tools

Provides a discussion of the differences between a "typical" GRC tool and HITRUST MyCSF, which was primarily designed to automate HITRUST's assessment validation and certification process

https://hitrustalliance.net/documents/content/MyCSFVsGRCTool.pdf

HITRUST

Risk Management Frameworks

Risk Management Frameworks Whitepaper

How HITRUST provides an efficient and effective approach to the selection, implementation, assessment and reporting of information security and privacy controls

https://hitrustalliance.net/documents/campaigns/HITRUST-RMF-Whitepaper-FM.pdf

HITRUST

CSF Assurance Program Requirements

CSF Assurance Program Requirements

Provides an overview of the CSF Assurance Program, the various types of assessments available, and the process of obtaining and maintaining certification

https://hitrustalliance.net/documents/assurance/csf/CSFAssuranceProgramRequirements.pdf

For more resources, visit the HITRUST Blog at https://blog.hitrustalliance.net

HITRUST®

Visit www.HITRUSTAlliance.net for more information

To view our latest documents, visit the
Content Spotlight