Introduction to the HITRUST CSF

Version 11.3.0

HITRUST

© 2024 HITRUST Services Corp. All rights reserved.

April 2024

Table of Contents

Executive Summary

HITRUST Alliance, Inc. (“HITRUST”) recognizes that most, if not all, organizations today are part of one or more "ecosystem" in which they need to interact with customers, third parties, and other trading partners. Core to these interactions is the exchange of information, much of which is sensitive. Furthermore, such exchange is only possible when the parties have confidence in one another. Essential to HITRUST's *One Framework, One Assessment, Globally*™ mission is to make it easy for organizations to give and obtain said assurances.

Fundamental to our mission is the availability of a common security and privacy framework that provides the structure, transparency, guidance, and cross-references to global authoritative sources that organizations need to be certain of their own data protection compliance as well as that of the many organizations with whom they interoperate. By collaborating with information security and privacy professionals, HITRUST developed a common security and privacy framework, the HITRUST CSF (“CSF”), that allows organizations in any sector to confidently create, access, store, or transmit information safely and securely.

The CSF’s core structure is based on ISO/IEC 27001 and 27002, published by the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC). It incorporates more than 40 other security and privacy-related regulations, standards, and frameworks providing comprehensive and prescriptive coverage. HITRUST has done extensive work to harmonize each of the current authoritative sources while continually evaluating new sources for inclusion. Through the lifecycle of each release, we integrate and normalize relevant requirements and best practices, as needed, while better aligning and eliminating redundant requirements within the framework.

Adopting a common security and privacy framework is necessary, but not sufficient by itself to confidently ensure coverage and compliance. To bolster the CSF, HITRUST offers the HITRUST Assurance Program and MyCSF. The HITRUST Assurance Program provides simplified compliance assessment reporting using a common approach to managing security assessments while creating efficiencies and containing costs associated with multiple and varied assurance requirements. As a result, MyCSF, as a software as a service (SaaS) information risk management platform, delivers an efficient solution for assessing, managing, and reporting information risk and compliance.

HITRUST is driving adoption and widespread confidence in the CSF, enabling sound risk mitigation practices throughout the HITRUST Community, and providing awareness, education, advocacy, support, knowledge-sharing, leadership, and additional outreach activities. HITRUST understands data protection and compliance and the challenges of assembling and maintaining the many and varied programs they require, which is why our integrated approach ensures that components are aligned, maintained, and comprehensive to support your organization’s unique information security management program.

© 2024 HITRUST

Introduction

No organization is immune to the inherent challenges posed when protecting data in today's ever-changing environment; these challenges include:

- Rapidly changing business, technology, and regulatory environments;
- Public and regulatory concerns over the increasing number of breaches and cyberattacks;
- Progression and increasing precision of computer abuse and computer crime;
- Increasing scrutiny from regulators, auditors, underwriters, customers, and business partners;
- Increasing public and community concern about the potential risks of evolving technologies, such as Artificial Intelligence
- Ineffective and inefficient internal compliance management processes;
- Inconsistent business partner requirements and compliance expectations;
- Inconsistent adoption of minimum controls for reliance; and
- Gaining the assurances needed to allow organizations to safely engage with their customers and trading partners.

In addition, all organizations face resource constraints, and none want to invest unwisely. Nowhere is this more critical than when it comes to security, privacy, and risk management. To maximize the risk reduction benefits from investments in security, organizations are better served focusing on the design and deployment of controls and leaving the development and maintenance of their control framework to a team of specialists whose only objective is to ensure your framework is current and all-encompassing of what is important to you, now.

Organizations must be prepared to answer:

- Where do we begin?
- What is our current compliance posture?
- What is our current technology posture?
- What is our current security posture?
- What is our current privacy posture?
- What is our current risk exposure?
- How do we compare to other organizations in our industry?
- Where do we need to be?
- How do we know what to do?
- How do we know if what we are doing is effective and sufficient?
- What level of resources do we need to allocate?
- To whom and how should we organize around security and privacy?
- What do we do first?
- To whom do we need to provide assurances, and how?
- What do our customers expect of us?
- What do we need to do to fulfill our due diligence expectations?
- From whom do we need to obtain assurances?
- What level of residual risk is acceptable?
- What do we need to do to qualify for cyber insurance?
- How might we reduce our insurance premiums?
- Are the answers to these questions the same for data entrusted to us as they are for data we own?
- What additional requirements would we need to meet to expand into a new geographic market?
- What would be expected of us if we started supporting a new industry sector?
- How do we support all of this in the most cost-effective manner?

© 2024 HITRUST

To enable organizations to confidently answer these questions and more, HITRUST developed the HITRUST CSF, a certifiable framework that provides organizations with a comprehensive, flexible, and efficient approach to regulatory compliance and risk management. The CSF rationalizes relevant regulations and standards into a single overarching security framework. Because the CSF is both risk- and compliance-based, organizations of varying risk profiles can customize the security and privacy control baselines as applicable through a variety of factors, including organization type, size, systems, and compliance requirements.

By adopting the CSF, organizations:

- increase trust and transparency among business partners and consumers;
- streamline compliance interactions in and out of the organization;
- provide a single benchmark to facilitate internal and external measurements that incorporate security and privacy requirements of applicable standards and regulations; and
- contain the cost of compliance and the number, complexity, and degree of variation in security audits or reviews.

The strategic organization of the HITRUST CSF, supported by the comprehensive HITRUST Approach, which includes the assurance programs and the MyCSF integrated online tool, empowers organizations to implement a formal information security management program with intent and focused purpose.

© 2024 HITRUST

Organization of the HITRUST CSF

The HITRUST CSF is a framework that normalizes security and privacy requirements for organizations, including federal legislation (e.g., HIPAA), federal agency rules and guidance (e.g., NIST), state legislation (e.g., California Consumer Privacy Act), international regulation (e.g., GDPR), and industry frameworks (e.g., PCI, COBIT). Then, it simplifies this myriad of requirements by providing a single-source solution tailored to the organization's needs. The CSF is the only framework built to provide scalable security and privacy requirements based on the different risks and exposures of each unique organization.

Key Components

The CSF was designed with security and privacy professionals in mind. By taking an abstraction of what is core to and common across most dominant frameworks, the architecture was deliberately chosen to facilitate straightforward understanding and easy consumption. Each control category in the CSF includes control objectives and control specifications, leveraging the primary categories from the ISO/IEC framework, as well as the inclusion of specific categories for an information security management program and risk management practices which collectively help to ensure organizational, regulatory compliance, and system controls are properly specified and implemented. The core structure is then integrated with various authoritative sources, along with the experience and leading practices of the HITRUST Community, to create specific implementation requirements for each control. All requirements are mapped to the related framework, standard, or regulation, and noted as an authoritative source.

Control Categories

The CSF contains 14 control categories, comprised of 49 control objectives and 156 control specifications. The CSF control categories, accompanied with their respective number of control objectives and control specifications for each category are:

1. Information Security Management Program (1, 1)
2. Access Control (7, 25)
3. Human Resources Security (4, 9)
4. Risk Management (1, 4)
5. Security Policy (1, 2)
6. Organization of Information Security (2, 11)
7. Compliance (3, 10)
8. Asset Management (2, 5)
9. Physical and Environmental Security (2, 13)
10. Communications and Operations Management (10, 32)
11. Information Systems Acquisition, Development, and Maintenance (6, 13)
12. Information Security Incident Management (2, 5)
13. Business Continuity Management (1, 5)
14. Privacy Practices (7, 21)

It should be noted that the order of the control categories does not imply importance; all security and privacy controls

© 2024 HITRUST

should be considered important. However, the full implementation of an information security management program (Control Category 0) will allow an organization to better identify, define, and manage the processes and resources that are necessary for proper data protection, which can be measured with the CSF.

The architecture of each control category is as follows:

- Control Objective: Statement of the desired result, or purpose to be achieved, by one or more control within the control category.
- Control Reference: Control number and title.
- Control Specification: Policies, procedures, guidelines, practices, or organizational structures, which can be managerial, operational, technical, or legal in nature, required to meet the control objective.
- Risk Factor Type: Predefined organizational, compliance, or system risk factors that increase the inherent risk to an organization or system, necessitating a higher level of compliance.

Organizational Factors include, but are not limited to, the amount of sensitive information an organization holds and/or processes, the annual number of transactions, the relative size of the organization based on a relevant estimator, the volume of business or data, and geographic scope e.g., state, multi-state, or international (outside the U.S.).

Compliance Factors focus on the compliance requirements applicable to an organization and systems in its environment, for example, compliance with PCI, FISMA, EU GDPR, and/or the Personal Data Protection Act.

System Factors consider the various system attributes that would increase the likelihood or impact of a vulnerability being exploited including assessing each system or system grouping to determine the associated level of compliance, for example, whether system(s) store, process, or transmit security and privacy information, are accessible from the Internet, are accessible by a third party, exchange data with a third party/business partner, are publicly accessible; if mobile devices are used, number of interfaces to other systems, and, number of users.

- Topics: Keywords indicating relevant categories associated with the control reference.
- Implementation Requirements: Detailed information to support the implementation of the control to meet the control objective. Requirements are defined based on relevant factors through three progressive implementation levels or by specific segment.

Implementation Requirement Levels: The CSF's risk-based approach applies security resources commensurate with the level of risk, or as required by applicable regulations or standards, by defining multiple levels of implementation requirements, which increase in restrictiveness. Three levels of requirements are defined based on organizational, regulatory compliance, or system risk factors. Level 1 provides the minimum baseline control requirements; each subsequent level encompasses the lower level and includes additional requirements commensurate with increasing levels of risk.

Segment-Specific Requirement Levels: Certain industries, or segments of industries, have specific requirements to address risks that do not apply to others or would not be considered reasonable and appropriate to mitigate from a general controls perspective. As a result, the CSF contains specific implementation levels that provide additional requirements for these segments, e.g., cloud service providers, FedRAMP, EU GDPR.

- Control Standard Mapping by Level: Documented mapping to related authoritative source(s).
- AI-based Standards Tooling: As part of the CSF v11 release, HITRUST built a new Artificial Intelligence enabled toolkit that precisely describes control relationships and allows for greater efficiency when mapping the CSF framework to other standards and regulations. Leveraging AI, these new tooling capabilities allow adding and maintaining new authoritative sources faster and more efficiently to keep the HITRUST CSF up to date.

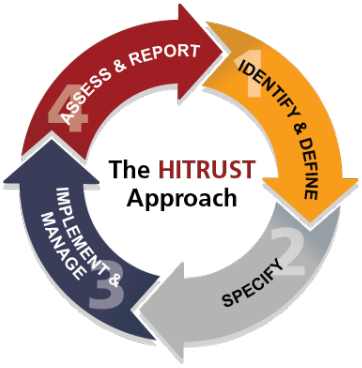
The HITRUST Approach

Adopting the HITRUST CSF is only one component of an effective data protection program. HITRUST understands information risk management and compliance and the challenges of assembling and maintaining the many and varied programs required, which is why our integrated approach ensures the components are aligned, maintained, and comprehensive to support an organization's information risk management and compliance program, including after the framework is implemented.

Designed to leverage the best-in-class components for a comprehensive information risk management and compliance program, the HITRUST Approach integrates and aligns the following:

HITRUST CSF®—a robust privacy and security controls framework
HITRUST MyCSF®—an assessment and corrective action plan management SaaS platform
HITRUST Assurance Program™—a scalable and transparent way to provide reliable assurances to internal and external stakeholders
HITRUST Threat Catalogue™—a list of reasonably anticipated threats mapped to specific CSF controls
HITRUST Assessment XChange™—an automated means of obtaining third-party assurances between organizations
HITRUST Shared Responsibility Program™—a matrix of CSF requirements identifying service provider and customer control sharing responsibilities
HITRUST Third-Party Assurance Program—a third-party risk management process

To further expand on the advantages of the interconnected relationships between the CSF and the different aspects of the HITRUST Approach, below is an introduction to two of the framework's key partners: the HITRUST Assurance Program and MyCSF.



HITRUST Assurance Program

The HITRUST Assurance Program provides simplified and consistent compliance assessments and reporting against the HITRUST CSF and the authoritative sources upon which it is built. This risk- and compliance-based approach, which is governed and managed by HITRUST, provides organizations with an effective, standardized, and streamlined assessment process to manage compliance across a multitude of standards, regulations, and frameworks. The HITRUST Assessments utilize a maturity level scoring model and risk ratings, which provide more accurate, consistent, and repeatable scoring, and help organizations prioritize remediation efforts. As a result, the HITRUST Assurance Program is a more effective process than that used by other assessment approaches and toolkits, which only support limited compliance requirements and use classic checkbox approaches.

The HITRUST Assurance Program allows entities to be assessed by independent third parties and receive a validated report based on their compliance with the HITRUST Certification requirements. The HITRUST Assurance Program recognizes both internal and external assessors.

- Internal Assessors are trained personnel who facilitate the HITRUST Assessment process by performing in-house testing in advance of an External Assessor's validated assessment fieldwork.
- External Assessors are organizations that have been approved by HITRUST to perform assessments and services associated with the HITRUST Assurance Program, also known as a HITRUST Authorized Assessor Organization.

Organizations can perform a self-assessment, which in turn generates a HITRUST Readiness Assessment Report. While this report cannot be certified; it can be used as a stepping-stone to a validated assessment. HITRUST offers two validated assessments: HITRUST Validated and HITRUST Validated + Certification. Validated Assessments are performed on-site by a HITRUST Authorized External Assessor.

The unique approach of the HITRUST Assurance Program affords numerous oversight and quality advantages over other assurance programs and certifying bodies, most notably that HITRUST has centralized the assurance and compliance aspects for all assessment reporting. This results in HITRUST Assessment Reports being more consistent and more reliable than other reports, which do not centralize robust reporting and review processes.

Through the HITRUST Assurance Program, organizations have a common security baseline and mechanism for communicating validated security and privacy controls to various business partners, without redundant, overlapping, frequent, and costly audits.

MyCSF

The HITRUST information risk management platform, MyCSF, is an online tool that organizations use to effectively and efficiently create a custom set of requirements based on the HITRUST CSF and tailored to their environment. This fully integrated, optimized, and powerful tool integrates the content and methodologies of the HITRUST CSF and Assurance Program with the technology and capabilities of a governance, risk, and compliance (GRC) tool. The user-friendly MyCSF tool provides organizations of all types and sizes a secure, web-based solution for accessing the CSF, performing assessments, managing remediation activities, and reporting and tracking compliance. Managed and supported by HITRUST, MyCSF provides organizations with up-to-date content, accurate and consistent scoring, reports validated by HITRUST, and benchmarking data, surpassing what traditional GRC tools can offer. Organizations can easily collaborate and work with HITRUST Authorized External Assessor Organizations to share documentation directly in the tool, incorporate necessary corrective action plans, and monitor progress.

MyCSF goes a step further by providing assessment guidance, referred to as 'illustrative procedures' in the tool. Illustrative procedures provide clarity to those adopting the CSF and assessor organizations when validating the security and privacy controls implemented by the organization. This guidance includes examination of documentation, interviewing of personnel, and testing of technical implementation. Integrating the illustrative procedures with the requirement statements provides a clear starting point when performing an assessment and developing a test plan.

MyCSF increases the efficiency with which organizations can implement and assess against the CSF by utilizing advanced workflows, custom criteria and notifications, and enhanced navigation and search tools. The MyCSF platform also provides a user-friendly interface, with the availability of dashboards and reports, and acts as a central repository for managing documents, system scoping, test plans, and corrective action plans.

MyCSF includes the following modules: risk assessment, corrective action plan (CAP) management, policy management, exception management, and incident management. Please visit the HITRUST website for current information on the various modules and other functionality available in MyCSF.

HITRUST Authoritative Sources

A broad base of U.S. federal and international regulations, security and privacy standards and frameworks were used to ensure the HITRUST CSF addresses all areas of data protection governance and control. The CSF integrates and normalizes these different authoritative sources, incorporating key objectives under one umbrella framework. The CSF v11.3.0 integrates 51 major security and privacy-related standards, regulations, and frameworks as authoritative sources, ensuring appropriate coverage, consistency, and alignment:

- 16 CFR Part 681 – FTC "Red Flag" Identity Theft Rules [16 CFR 681]
- 201 CMR 17.00 – State of Massachusetts Data Protection Act: Standards for the Protection of Personal Information of Residents of the Commonwealth [201 CMR 17.00]
- American Institute of Certified Public Accountants (AICPA) Trust Services Principles and Criteria: Security, Confidentiality and Availability, 2017 [AICPA TSP 100]
- Asia-Pacific Economic Cooperation (APEC) Cross Border Rules for the APEC Privacy Framework, 2005 [APEC]
- California Consumer Privacy Act (CCPA) [CCPA 1798]
- Center for Internet Security (CIS) Critical Security Controls (CSC) v8: Critical Security Controls for Effective Cyber Defense [CIS Controls v8]
- CMS Information Security ARS 2013 v3.1: CMS Minimum Security Requirements for High Impact Data [CMS ARS v3.1]
- COBIT 5: Deliver and Support Section 5 – Ensure Systems Security [COBIT 5]
- Electronic Health Network Accreditation Commission (EHNAC) [EHNAC]
- Federal Financial Institutions Examination Council (FFIEC) Information Technology (IT) Examination Handbook – Information Security, Sept ember 2016 [FFIEC IS]
- Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) [FFIEC CAT]
- Federal Register 21 CFR Part 11: Electronic Records; Electronic Signatures, 2003 [21 CFR 11]
- Federal Risk and Authorization Management Program (FedRAMP) Revision 5 [FedRAMP r5]
- General Data Protection Regulation (GDPR) European Union [EU GDPR]
- Guidance Specifying the Technologies and Methodologies That Render Protected Health Information Unusable, Unreadable, or Indecipherable to Unauthorized Individuals for Purposes of the Breach Notification Requirements [OCR Guidance for Unsecured PHI]
- The United States Department of Health and Human Services (HHS) Cybersecurity Performance Goals [HHS Cybersecurity Performance Goals]
- Health Industry Cybersecurity Practices (HICP) 2023 edition [HICP 2023]
- Health Information Trust Alliance (HITRUST) De-Identification (De-ID) Framework: De-identification Controls Assessment (DCA) [HITRUST De-ID Framework v1]
- HIPAA – Federal Register 45 CFR Part 164, Subpart C: HIPAA Administrative Simplification: Security Standards for the Protection of Electronic Protected Health Information (Security Rule) [45 CFR HIPAA.SR]
- HIPAA – Federal Register 45 CFR Part 164, Subpart D: HIPAA Administrative Simplification: Notification in the Case of Breach of Unsecured Protected Health Information (Breach Notification Rule) [45 CFR HIPAA.BN]
- HIPAA – Federal Register 45 CFR Part 164, Subpart E: HIPAA Administrative Simplification: Privacy of Individually Identifiable Health Information (Privacy Rule) [45 CFR HIPAA.PR]
- IRS Publication 1075 v2021: Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for protecting Federal Tax Returns and Return Information [IRS Pub 1075 (2021)]
- ISO/IEC 23894: Information technology – Artificial intelligence – Guidance on risk management [ISO/IEC 23894:2023]
- ISO/IEC 27001:2022: Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements [ISO/IEC 27001:2022]
- ISO/IEC 27002:2022: Information Security, Cybersecurity and Privacy Protection – Information Security Controls [ISO/IEC 27002:2022]

© 2024 HITRUST

- ISO/IEC 27799:2016: Health Informatics – Information Security Management in Health using ISO/IEC 27002 [ISO/IEC 27799:2016]
- ISO/IEC 29100:2011: Information Technology – Security Techniques – Privacy Framework [ISO/IEC 29100:2011]
- ISO 31000: Risk management – Guidelines [ISO 31000:2018]
- Joint Commission Standards, The Joint Commission (formerly the Joint Commission on the Accreditation of Healthcare Organizations) [TJC]
- Minimum Acceptable Risk Standards for Exchanges (MARS-E) v2.2: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges [MARS-E v2.2]
- MITRE Adversarial Threat Landscape for Artificial-Intelligence Systems (ATLAS) Mitigations [MITRE ATLAS]
- New York State Department of Financial Services – Title 23 NYCRR Part 500 Second Amendment [23 NYCRR 500 Second Amendment]
- NIST Artificial Intelligence Risk Management Framework [NIST AI RMF 1.0]
- NIST Framework for Improving Critical Infrastructure Cybersecurity v1.1 [NIST Cybersecurity Framework v1.1]
- NIST Special Publication 800-53 Revision 4 (Final), including Appendix J – Privacy Control Catalog: Security Controls for Federal Information Systems and Organizations [NIST SP 800-53 R4]
- NIST Special Publication 800-53 Revision 5.1.1 Security and Privacy Controls for Information Systems and Organizations [NIST SP 800-53 R5]
- NIST Special Publication 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations [NIST SP 800-171 R2]
- NRS: Chapter 603A – State of Nevada: Security and Privacy of Personal Information [NRS 603A]
- NY DOH Office of Health Insurance Programs SSP v5.0 [NY OHIP Moderate-Plus Security Baseline v5.0]
- Office of Civil Rights (OCR) Audit Protocol April 2016 – HIPAA Security Rule [OCR Audit Protocol (2016)]
- Ontario, Canada Personal Health Information Protection Act, 2004 Chapter 3 [PHIPA]
- Organisation for Economic Co-Operation and Development (OECD) Privacy Framework, 2013 [OECD Privacy Framework]
- Open Worldwide Application Security Project (OWASP) AI Exchange [OWASP AI Exchange]
- Payment Card Industry (PCI) Data Security Standard Version 4: Requirements and Testing Procedures [PCI DSS v4]
- Personal Data Protection Act 2012 (PDPA) [PDPA]
- VA Directive 6500 VA Cybersecurity Program [VA Directive 6500]
- South Carolina Insurance Data Security Act (SCIDSA) – Title 38, Chapter 99 [SCIDSA 4655]
- StateRAMP Revision 5 Baselines [StateRAMP r5]
- Texas Risk and Authorization Management Program TX-RAMP 2.0 Control Baselines [TXRAMP r5]
- Title 1 Texas Administrative Code § 390.2 – State of Texas: Standards Relating to the Electronic Exchange of Health Information [1 TAC 15 390.2]

© 2024 HITRUST

HITRUST Community Supplemental Requirements

In developing a framework that can meet the needs of organizations locally, nationally, and globally, HITRUST recognizes that various organizations may have requirements imposed as a result of being part of a smaller community—such as a subset of an industry group or by a cooperative sharing agreement. In many cases, these may not be new security or privacy controls but more specific implementation requirements. Using the tailoring capabilities included in a HITRUST r2 Assessment, HITRUST provides the capability for these requirements to be incorporated, harmonized, and selected for inclusion during the assessment process and then included in the HITRUST Assessment Report, utilizing the MyCSF platform. The intent is to reduce any additional assessments by enabling organizations *to Assess Once, Report Many*™. The CSF now includes such community-specific authoritative sources, currently referred to as supplemental requirements (SR) or community supplemental requirements (CSR). HITRUST continues to evaluate the inclusion of others based on market demand.

HITRUST CSF Questions and Comments

HITRUST encourages organizations to provide comments to ensure the HITRUST CSF continues to evolve as the most relevant framework for data protection globally. Organizations who wish to provide HITRUST feedback on the CSF may submit comments via email to info@hitrustalliance.net.

About HITRUST

Since it was founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks, as well as related assessments and assurance methodologies.

HITRUST actively participates in government advocacy, community building, and security and privacy education. For more information, visit www.HITRUSTAlliance.net.

Reference Materials

For additional information on HITRUST, the HITRUST CSF, and related offerings, the following documentation can be found on the HITRUST website:

- About HITRUST
- HITRUST CSF Download (includes):
  - HITRUST CSF Authoritative Sources Cross-Reference
  - HITRUST Glossary of Terms and Acronyms
  - HITRUST CSF Summary of Changes
- HITRUST CSF Frequently Asked Questions
- HITRUST Threat Catalogue
- MyCSF Overview
- HITRUST CSF Assessors
- HITRUST Assurance & Related Programs

THANK YOU

855.HITRUST (855.448.7878)

www.HITRUSTAlliance.net

HITRUST®

Copyright 2024 © HITRUST Services Corp. This information contained in this document is the property of HITRUST Services Corp. Any reproduction in part or as a whole without the written permission of HITRUST Services Corp. is prohibited.