HITRUST services

Fit for all
Securing trust
Ensuring compliance

pwc

Table of contents

Introduction

India Inc. finds itself at a crossroads where regulatory compliance, risk management and technology developments must come together to enhance its resilience and sustainability. Strategic technology trends will help shape industries and redefine how we interact with the digital world. Therefore, staying up to date about these developments and adopting a proactive approach to innovation will be the key to success.

Emerging shifts in healthcare

Digital healthcare in India is revolutionising service delivery through telemedicine, digital health records and mobile apps, thus enhancing its quality and efficiency. As healthcare becomes increasingly data-driven, organisations must securely and seamlessly share data, while necessitating robust governance, cybersecurity and trust. To this end, several ambitious national-level initiatives have been launched, such as:

- Ayushman Bharat Digital Mission (ABDM)
- Ayushman Bharat Health Account (ABHA) and e-Sanjeevani
- Ayushman Bharat

Digitally evolving landscape

Regulators keep emphasising on data security, building trust in data safety, validity and integrity to update the regulations ensuring that these innovations around emerging technologies are secure and compliant. Several ambitious national-level initiatives have been launched such as:

- Digital Personal Data Protection Act (DPDPA) 2023
- Digital India Act 2023 (Draft)
- National Artificial Intelligence (AI) Policy (Draft)

Organisations are under increasing pressure to prove they use security and privacy practices capable of managing information risks in an ever-changing threat and regulatory environment. The HITRUST assessment and certification process enables organisations to foster trust among their stakeholders and regulators in their risk management and compliance programmes.

Overview of HITRUST

In a world where the integrity of digital systems is continually tested, being certified by a body that epitomises reliability and relevance is not just an advantage – it is a necessity.

HITRUST offerings are designed to be accessible, scalable and suitable for organisations as they:

- offer a **comprehensive** suite of security, compliance and risk management solutions that serve a wide array of industries, including healthcare
- incorporate **44 relevant standards, best practice frameworks and regulations**
- integrate six essential principles of **transparency, scalability, consistency, accuracy, integrity and efficiency**
- use an **'assess once, report many'** assessment model based on selected authoritative sources and insight reports
- provide a centralised digital solution **(MyCSF platform)** for organisations to have a continuous oversight on assessment processes
- allow them to use **inheritance** which results in lower certification costs and faster times to achieve HITRUST certification.

HITRUST assessments: An overview

Who can opt for a HITRUST certification?

As of 2019, the HITRUST Common Security Framework (CSF) became industry-agnostic which implies that organisations from any industry, size or risk profile can pursue HITRUST certification.

The HITRUST CSF provides a comprehensive framework for protecting sensitive information, such as electronic protected health information (ePHI), personally identifiable information (PII), payment card information (PCI), proprietary information and other sensitive data. While the healthcare industry remains the primary beneficiary of HITRUST, organisations from various sectors can also benefit from this certification.

Other sectors

- IT/ITeS companies
- Business services
- E-commerce
- Financial services

Health and pharma sector

- Insurance companies
- Business associates
- Clearing-houses
- Hospitals, pharmacies and wellness centres
- HealthTech start-ups

Why HITRUST?

44+

authoritative sources can be mapped to HITRUST requirements

75%

of Fortune 20 companies use the HITRUST CSF

8 out of 10

top cloud service providers use the HITRUST CSF

100%

of submitted assessments undergo HITRUST quality review

187%

increase in i1 submissions from 2022 to 2023

173%

increase in e1 submissions from 2022 to 2023

100%

of the techniques, tactics and procedures (TTPs) included in the MITRE ATT&CK framework are covered

0.6%

of the organisations with HITRUST certifications reported a breach in 2022 and 2023 (which is very low as compared organisations using other frameworks)

Assessment options

HITRUST r2 – 2-year Validated Assessment

The r2 certification is best suited for organisations that need to demonstrate regulatory compliance with authoritative sources, or ones that require expanded tailoring of controls based on other identified risk factors. It is the most comprehensive and robust HITRUST assessment.

HITRUST i1 – 1-year Validated Assessment

The i1 certification is a good fit for organisations that already have robust information security programmes in place and are ready to demonstrate leading security practices. It allows for a baseline validated assessment and certification based on 182 foundational security controls.

HITRUST e1 – 1-year Validated Assessment

The e1 certification is ideal for start-ups and companies with limited risk profiles or less complexity. It allows for an entry-level validated assessment and certification based on 44 controls for establishing foundational cybersecurity.

Note: Please refer to **Annexure A** for key characteristics and differences between these assessments.

Unlocking the HITRUST potential – PwC India perspective

Amidst the myriad of compliance frameworks and assurance reports, distinguishing between superficial validation and genuine security assurance is a challenge that demands urgent attention.

PwC India draws on the HITRUST 2024 Trust report[1] (for study 1) and the mappings with authoritative sources (for study 2) to compare different security standards (such as International Organization for Standardization [ISO], National Institute of Standards and Technology [NIST], American Institute of Certified Public Accountants [AICPA], Payment Card Industry [PCI] Data Security Standard) in order to obtain quantitative results that serve as a useful baseline for understanding the effectiveness of the HITRUST CSF.

Study 1: This study evaluates selected key security standards (widely adopted in the industry) based on the parameters mentioned below. We've provided our view on how each standard performs in these areas. To do this, we employed a three-point scale – high [100], medium [60], low [30] – to compare these standards across different parameters.

Scalability: Ability of the security standard to achieve multiple compliance requirements through a single comprehensive assessment

Transparency: Presence of clear, detailed requirement statements and a well-defined scoring methodology that ensures consistent evaluations

Reliability: Reflects the level of trust it offers to stakeholders

Cyber threat adaptivity: Ability of the security standard to evolve with emerging threats, irrespective of the changing cyber threat landscapes

Results: HITRUST provides a comprehensive framework which describes the process, requirements and scoring methodology for all HITRUST assessments and enables organisations to cross reference any requirement with their corresponding authoritative source. The HITRUST CSF differentiates from other standards by providing accurate scoring of controls rather than an opinion-based pass/fail model.

1. https://hitrustalliance.net/trust-report

Study 2: In this study, we used HITRUST requirements as the baseline, systematically identifying which of these requirements were **not** met by other security standards considered in this study. This approach highlights the additional layers of protection and assurance that HITRUST provides, offering a clear perspective on the unique value it brings to organisations as compared to other standards.

	HITRUST CSF v11.3.0	NIST CSF v1.1	NIST SP 800-53 r5	PCI DSS v4.0	Health Insurance Portability and Accountability Act (HIPAA) Security Rule
HITRUST control categories	**Number of requirements**	**Count of control requirements not covered by above standards**			
00 - Information security management program	01	*	*	*	*
01 - Access control	25	09	02	12	01
02 - Human resources security	09	02	01	05	*
03 - Risk management	04	*	01	02	*
04 - Security policy	02	*	02	*	*
05 - Organisation of information security	11	01	03	07	01
06 - Compliance	10	*	01	04	02
07 - Asset management	05	02	*	02	01
08 - Physical and environmental security	13	01	03	09	03
09 - Communications and operations management	32	05	03	11	04
10 - Information systems acquisition, development and maintenance	13	03	01	04	04
11 - Information security incident management	05	*	*	02	*
12 - Business continuity management	05	*	01	04	*

* Highlights no differences in the control requirements noted in the comparative study.

Please refer to **Annexure B** for more details on the comparison presented in study 2.

Note: We have intentionally left out one of the control categories (13-Privacy practices) as it caters to various privacy regulations which were not in the scope of the above analysis.

PwC India – a trusted and certified HITRUST external assessor

Your journey to security starts with our HITRUST expertise.

Our portfolio of services	r2 Assessment	i1 Assessment	e1 Assessment
Readiness/preparedness	●	●	●
Validated assessment	●	●	●
Interim assessment	●		
Bridge assessment	●		
Rapid recertification assessment		●	
Remediation assistance	●	●	●
Training and brainstorming sessions	●	●	●
We also help organisations to set up an internal HITRUST CSF.			

Differentiated offerings

At PwC, our reputation is defined by **building trust and achieving quality and sustainable value.** We believe in winning work on the merits of the quality and value we deliver to our clients. We're **qualified and eager to promote you to the PwC audit experience.**

- **Sharp focus on risks that matter**
- **Enhanced quality**
- **Transparent issues management**
- **Clear communication**
- **Efficient and tech-enabled project management**
- **Client-centric and customisable approach**
- **Credentialed and recognised problem solvers**
- **Proven methodology**

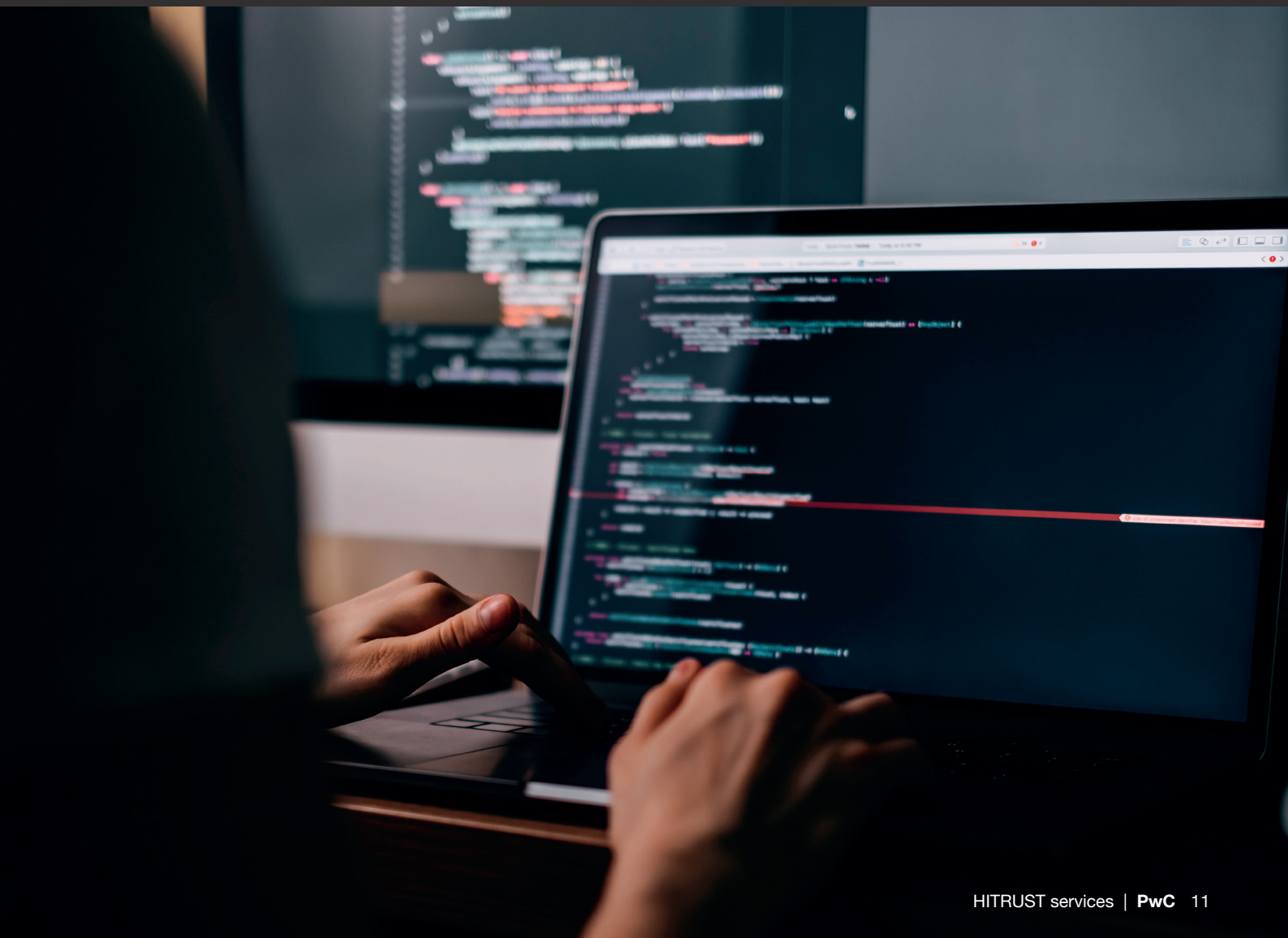
Value for you: Our diverse and experienced delivery team

- **Healthcare domain knowledge:** Our capabilities and insights are driven by the knowledge we've gained from delivering information security and privacy services within the healthcare industry, including technology service providers, cloud platforms and software-as-a-service (SaaS) providers.
- **Subject matter specialists:** Our HITRUST engagements are delivered by a multidisciplinary team consisting of risk, information security, cyber and privacy professionals. Our specialists have deep expertise in using the MyCSF tool with hands-on experience and also have access to leaders in the fields of healthcare, cybersecurity, IT governance, emerging technology to keep themselves relevant.
- **Global presence:** We are a group of network firms working across geographies and delivering a range of information security and privacy services.

Annexure A: Characteristics and differences between the e1, i1 and r2 assessments

Characteristic	e1	i1	r2
Deliverables			
Can result in a HITRUST-issued certification (i.e. HITRUST certifiable)	Yes	Yes	Yes
Length of certification	1 year	1 year	2 years
Can result in a HITRUST-issued certification over the NIST Cybersecurity Framework	No	No	Yes
Final reports resulting from the assessment can be shared through the HITRUST Assessment XChange and assessment results can be shared through the HITRUST Results Distribution System.	Yes	Yes	Yes
Assessments			
Readiness assessments and validated assessments can be performed	Yes	Yes	Yes
Requires an authorised HITRUST External Assessor Organisation to inspect documented evidence to validate control implementation	Yes	Yes	Yes
Leverages the HITRUST Control Maturity Scoring Rubric	Yes	Yes	Yes
Assessor's validated assessment fieldwork window (maximum)	90 days	90 days	90 days
HITRUST CSF requirements performed by the assessed entity's service providers (such as cloud service providers) on behalf of the organisation can be excluded from consideration.	Yes	Yes	No
Personnel from the assessed entity, or its external assessors, are allowed to enter control maturity scoring and assessment scoping information	Yes	Yes	No
Requires an interim assessment	No	No	Yes
Can be bridged through a HITRUST bridge certificate	No	No	Yes
Assessed entities must achieve scores above a particular threshold to obtain a HITRUST certification	>83	>83	>62
Determining the level of compliance	Implemented	Implemented	PRISMA
Maturity levels	1	1	5

Characteristic	e1	i1	r2
Subject matter			
Threat-adaptive assessment	Yes	Yes	Yes
Includes a fixed number of HITRUST CSF requirement statements	Yes	Yes	No
Includes HITRUST CSF requirements specifically tailored to the assessment scope	No	No	Yes
Can be tailored to optionally convey assurances over dozens of information protection regulations and standards (e.g. HIPAA, NIST CSF, PCI DSS)	No	No	Yes
Can be tailored to include privacy	No	No	Yes
Must use the most current version of the CSF available at the time of assessment creation	Yes	Yes	No



Annexure B: Comparative study

HITRUST requirement	NIST Cybersecurity Framework v1.1	NIST SP 800-53 r5	PCI DSS v4.0	HIPAA Security Rule
00 - Information security management program	No differences	No differences	No differences	No differences
01 - Access control	01.f Password use 01.g Unattended user equipment 01.h Clear desk and clear screen policy 01.o Network routing control 01.r Password management system 01.s Use of system utilities 01.t Session time-out 01.u Limitation of connection time 01.v Information access restriction	01.h Clear desk and clear screen policy 01.u Limitation of connection time	01.a Access control policy 01.g Unattended user equipment 01.h Clear desk and clear screen policy 01.k Equipment identification in networks 01.o Network routing control 01.i Policy on the use of network services 01.r Password management system 01.s Use of system utilities 01.u Limitation of connection time 01.w Sensitive system isolation 01.x Mobile computing and communications 01.y Teleworking	01.s Use of system utilities
02 - Human resources security	02.f Disciplinary process 02.h Return of assets	02.h Return of assets	02.f Disciplinary process 02.a Roles and responsibilities 02.c Terms and conditions of employment 02.g Termination or change responsibilities 02.h Return of assets	No differences
03 - Risk management	No differences	03.d Risk evaluation	03.c Risk mitigation 03.d Risk evaluation	No differences
04 - Security policy	No differences	04.a Information security policy document 04.b Review of the information security policy	No differences	No differences

HITRUST requirement	NIST Cybersecurity Framework v1.1	NIST SP 800-53 r5	PCI DSS v4.0	HIPAA Security Rule
05 - Organisation of information security	05.e Confidentiality agreements	05.f Contact with authorities 05.h Independent review of information security 05.j Addressing security when dealing with customers	05.b Information security coordination 05.c Allocation of information security responsibilities 05.d Authorisation process for information assets and facilities 05.e Confidentiality agreements 05.f Contact with authorities 05.h Independent review of information security 05.j Addressing security when dealing with customers	05.e Confidentiality agreements
06 - Compliance	No differences	06.a Identification of applicable legislation	06.a Identification of applicable legislation 06.b Intellectual property rights 06.e Prevention of misuse of information assets 06.i Information systems audit controls	06.b Intellectual property rights 06.j Protection of information systems audit tools
07 - Asset management	07.b Ownership of assets 07.c Acceptable use of assets	No differences	07.b Ownership of assets 07.e Information labeling and handling	07.e Information labeling and handling

Annexure B: Comparative study

HITRUST requirement	NIST Cybersecurity Framework v1.1	NIST SP 800-53 r5	PCI DSS v4.0	HIPAA Security Rule
08 - Physical and environmental security	08.e Working in secure areas	08.e Working in secure areas 08.f Public access, delivery and loading areas 08.k Security of equipment off-premises	08.a Physical security perimeter 08.d Protecting against external and environmental threats 08.e Working in secure areas 08.f Public access, delivery and loading areas 08.h Supporting utilities 08.j Equipment maintenance 08.k Security of equipment off-premises 08.l Secure disposal or re-use of equipment 08.m Removal of property	08.d Protecting against external and environmental threats 08.f Public access, delivery and loading areas 08.h Supporting utilities
09 - Communications and operations management	09.r Security of system documentation 09.u Physical media in transit 09.y Online transactions 09.ae Fault logging 09.af Clock synchronisation	09.v Electronic messaging 09.g Managing changes to third-party services 09.ad Administrator and operator logs	09.c Segregation of duties 09.g Managing changes to third-party services 09.h Capacity management 09.i System acceptance 09.n Security of network services 09.r Security of system documentation 09.t Exchange agreements 09.x Electronic commerce services 09.y Online transactions 09.z Publicly available information 09.ae Fault logging	09.d Separation of development, test and operational environments 09.g Managing changes to third-party services 09.ae Fault logging 09.af Clock synchronisation

HITRUST requirement	NIST Cybersecurity Framework v1.1	NIST SP 800-53 r5	PCI DSS v4.0	HIPAA Security Rule
10 - Information systems acquisition, development and maintenance	10.e Output data validation 10.i Protection of system test data 10.j Access control to program source code	10.f Policy on the use of cryptographic controls	10.d Message integrity 10.e Output data validation 10.j Access control to program source code 10.l Outsourced software development	10.i Protection of system test data 10.e Output data validation 10.g Key management 10.l Outsourced software development
11 - Information security incident management	No differences	No differences	11.b Reporting security weaknesses 11.e Collection of evidence	No differences
12 - Business continuity management	No differences	12.d Business continuity planning framework	12.a Including information security in the business continuity management process 12.b Business continuity and risk assessment 12.d Business continuity planning framework 12.e Testing, maintaining and re-assessing business continuity plans	No differences

About PwC

At PwC, our purpose is to build trust in society and solve important problems. We're a network of firms in 151 countries with over 360,000 people who are committed to delivering quality in assurance, advisory and tax services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

Contact us:

Anirban Sengupta
Partner, Business and Technology Risk
PwC India
anirban.sengupta@pwc.com

Nebha Maheshwari
Partner, Business and Technology Risk
PwC India
nebha.maheshwari@pwc.com

pwc.in

Data Classification: DC0 (Public)

AW/November 2024 - M&C 41514