HITRUST CSF

Pentesting Requirements - Including r2 Deep Dive

A practical guide for security leaders, healthcare organizations, and SaaS teams navigating HITRUST e1, i1, and r2 certifications - with specific control domain references, maturity model mapping, and a detailed breakdown of r2 penetration testing requirements.

Contents

01 Quick Summary

WHAT SECURITY LEADERS NEED TO KNOW

HITRUST CSF (Common Security Framework) is the most comprehensive certifiable security framework in healthcare and increasingly across SaaS and enterprise technology. Unlike frameworks that imply penetration testing, HITRUST r2 assessments explicitly require it as part of the on-site validation process. The framework's three assessment tiers - e1, i1, and r2 - have meaningfully different penetration testing expectations:

AT A GLANCE

- HITRUST CSF v11 (current: v11.7.0, with v11.8 released June 2026) has three assessment options: e1 (~44 controls), i1 (182 controls), and r2 (200-800+ tailored controls).
- r2 is the only HITRUST assessment where penetration testing is explicitly validated during the on-site assessment phase.
- r2 requires five maturity levels to be addressed: Policy, Procedure, Implemented, Measured, and Managed.
- The HITRUST framework maps to 60+ authoritative sources including HIPAA, NIST, ISO 27001, PCI DSS, GDPR, and SOC 2.
- 99.62% of HITRUST r2-certified environments reported no breach in 2025 - the strongest breach-free record of any certification framework.
- HITRUST r2 is selected by TEFCA as the required certification for Qualified Health Information Networks (QHINs).
- SaaS and technology companies now account for 37% of all HITRUST certifications - well beyond healthcare alone.
- r2 certification is valid for 2 years with a mandatory interim assessment at the 12-month mark.

02 What Is HITRUST CSF?

BACKGROUND AND CONTEXT

The HITRUST Common Security Framework (CSF) is a certifiable, risk-based security framework developed by the Health Information Trust Alliance (HITRUST). First published in 2007 and now on version 11.7.0 (December 2025), the HITRUST CSF is purpose-built to help organizations manage information risk and demonstrate compliance through a single, comprehensive assessment - rather than separate audits for HIPAA, ISO 27001, SOC 2, PCI DSS, and other frameworks simultaneously.

Who Uses HITRUST?	Examples and Context
Healthcare providers and payers	Hospitals, health systems, insurers, pharmacy benefit managers - the original and still core HITRUST constituency
SaaS and technology companies	37% of all HITRUST certifications in 2024 - enterprise SaaS increasingly required by healthcare and regulated enterprise customers
Business services firms	~19% of certifications - consulting, BPO, managed service providers processing client data

Government and public sector	TEFCA requires HITRUST r2 for Qualified Health Information Networks (QHINs)
Life sciences and pharma	Clinical trial data, regulated research, CROs processing patient-adjacent data
Financial services	HITRUST increasingly adopted alongside SOC 2 for organizations processing both financial and health data

What Makes HITRUST Different

The key differentiator of HITRUST relative to SOC 2, ISO 27001, and other frameworks is its prescriptive, measurable control maturity model. Where SOC 2 asks 'do you have a control?', HITRUST r2 asks 'how mature is your control across five dimensions?'. This produces:

- A quantified maturity score (1-5 scale) for each control domain - not a binary pass/fail.
- A minimum score threshold (62/100 per domain) that must be met for certification.
- Corrective Action Plans (CAPs) for controls below threshold - organizations must remediate before certification.
- An inheritance model - organizations can inherit controls from certified cloud providers (AWS, Azure, GCP), reducing assessment scope.
- A cyber-threat adaptive engine - HITRUST updates control requirements based on real-world threat intelligence and breach data.

Key Terms

Term	Plain English Meaning
HITRUST CSF	The Common Security Framework - the master control library with 14 control categories, 19 domains, 49 control objectives, and 2,000+ requirement statements.
myCSF	HITRUST's online portal where assessments are managed, evidence uploaded, and scores submitted for HITRUST QA review.
External Assessor	A HITRUST-authorized third-party firm that conducts validated assessments. Required for all three assessment types.
Control Reference	A specific HITRUST control (e.g., 09.ab - Penetration Testing). The atomic unit of the CSF.
Maturity Level	One of five evaluation dimensions: Policy, Procedure, Implemented, Measured, Managed.
CAP	Corrective Action Plan - required remediation when a control scores below threshold. Must be resolved before certification is granted.
Inheritance	Reusing a certified third party's controls in your own assessment - reduces scope for controls the provider has already certified (e.g., AWS infrastructure controls).
Interim Assessment	Required at the 12-month mark for r2 certifications - a mid-cycle check to confirm controls are still operating effectively.
TEFCA	Trusted Exchange Framework and Common Agreement - US national health information exchange framework that requires HITRUST r2 for QHIN designation.

03 The Three Assessment Types: e1, i1, and r2

CHOOSING THE RIGHT ASSESSMENT AND HOW PENTEST REQUIREMENTS DIFFER

HITRUST CSF v11 offers three validated assessment paths. Each provides a different level of assurance, requires a different number of controls, and has meaningfully different penetration testing and security testing expectations. Organizations often progress from e1 to i1 to r2 as their security program matures and customer requirements increase.

Attribute	e1 - Essentials	i1 - Implemented	r2 - Risk-Based (2-Year)
Purpose	Foundational cybersecurity hygiene - entry level	Moderate assurance - current/emerging threat focus	Highest assurance - comprehensive risk-based
Controls in scope	~44 controls (43 in v11.7+)	182 controls	200-800+ tailored controls (risk-based selection from 2,000+ library)
Certification period	1 year	1 year (rapid recertification in year 2)	2 years (interim assessment at 12 months)
Maturity levels tested	Implemented only	Implemented only	Policy, Procedure, Implemented (+ optional Measured, Managed)
Penetration testing required?	Not explicitly required	Not explicitly required	YES - assessors validate pentest evidence during on-site r2 assessment
Vulnerability scanning required?	Basic controls included	Yes - in-scope controls	Yes - required with documented cadence and remediation SLAs
Assessor on-site testing	Limited	Moderate	Full on-site risk assessment including pentest evidence review
Who chooses this	Low-risk orgs, early-stage startups, basic due diligence	Mid-market orgs, moderate risk, stepping stone to r2	High-risk orgs, healthcare, enterprise contracts, TEFCA/DoD
Average CAPs required (2024)	~25% need remediation	~89% need at least one CAP	~8.6 CAPs average per assessment
Breach-free rate (2024)	Part of 99.41% HITRUST overall	Part of 99.41% HITRUST overall	99.62% certified breach-free (2025)

r2 IS THE ONLY ASSESSMENT WHERE PENTESTING IS EXPLICITLY VALIDATED

For e1 and i1 assessments, penetration testing may contribute evidence for certain control statements, but it is not explicitly evaluated during the assessor's on-site review. For r2, the on-site assessment explicitly includes penetration testing evidence review as part of the validation process - alongside interviews, documentation sampling, and vulnerability scan results. If your organization is pursuing r2 certification, an annual penetration test with documented remediation is a practical requirement - not an optional best practice.

The r2 Maturity Model in Detail

The r2 assessment evaluates five maturity levels for each control. A minimum score of 3 (Implemented) across all three mandatory levels - Policy, Procedure, and Implemented - is required for certification. The Measured and Managed levels are optional for r2 but increase the maturity score.

Maturity Level	What It Means	Pentest Relevance
1 - Policy	Formal, documented policies exist and are communicated to staff. 'Shall' and 'will' language. Covers the security control in writing.	Pentest policy and scope definition. Rules of engagement documentation. Testing authorization policy.
2 - Procedure	Step-by-step procedures exist for implementing the policy. Operational runbooks and work instructions are current.	Pentest methodology documented. Remediation SLA procedures. Retest procedures.
3 - Implemented	Controls are consistently implemented across all applicable systems. Evidence of actual operation required. Minimum required level.	Active pentest program operating. Vulnerability scan results. Remediation evidence. Retest confirmation.
4 - Measured	Control effectiveness is quantified and tracked over time. Metrics, KPIs, and trend data exist. (Optional for r2 certification.)	Pentest trend analysis across multiple years. Remediation SLA compliance metrics. Vulnerability density tracking.
5 - Managed	Controls are continuously improved based on measurement data. Formal improvement cycles. Executive reporting. (Optional for r2.)	Executive security reporting incorporating pentest findings. Formal risk treatment decision records. Program improvement evidence.

04 The 19 HITRUST Domains

CONTROL DOMAIN OVERVIEW

The HITRUST CSF assessment is organized into 19 domains aligned with common IT and security process areas. These domains contain 135 security controls (plus 14 privacy controls) broken into specific requirement statements. The r2 assessment tailors which domains and controls apply based on an organization's risk profile, system type, and regulatory requirements.

Domain	Name	Key Focus	Pentest Relevance
01	Information Security Management Program	Governance, policies, risk management, information classification	Pentest policy, risk register, program governance - Policy maturity evidence
02	Endpoint Protection	Desktops, laptops, servers, mobile devices, AV, patching, hardening	Endpoint exploitation testing, lateral movement from workstations, AV bypass
03	Portable Media Security	USB drives, removable media, encryption, access controls	Data exfiltration via media, DLP control validation
04	Mobile Device Security	Smartphones, tablets, MDM, remote wipe, app security	Mobile application testing, MDM bypass, remote access security
05	Wireless Security	WiFi security, rogue access points, encryption standards	Wireless network testing, rogue AP detection, WPA2/3 validation
06	Configuration Management	Secure baselines, hardening, change management, patch management	Configuration review, hardening validation, insecure default detection
07	Vulnerability Management	Vulnerability scanning, remediation timelines, patch verification	Vulnerability scanning evidence, pentest findings and remediation SLAs
08	Network Protection	Firewalls, segmentation, DMZ, intrusion detection, network controls	External/internal network pentest, segmentation testing, IDS validation
09	Transmission Protection	Encryption in transit, TLS, secure protocols, VPN security	TLS/SSL testing, cleartext detection, VPN security testing
10	Password Management	Password policies, complexity, MFA, privileged account controls	Credential security testing, MFA bypass, brute force resistance
11	Access Control	Identity management, least privilege, access reviews, termination	Access control testing, privilege escalation, orphaned account testing
12	Audit Logging and Monitoring	Log generation, SIEM, alerting, log integrity, retention	Detection validation, log bypass testing, SIEM alert coverage
13	Education, Training and Awareness	Security awareness, phishing training, role-based training	Social engineering simulation, phishing testing (where in scope)
14	Third Party Assurance	Vendor risk, BAAs, supplier security assessments, contracts	Third-party API testing, supplier security validation
15	Incident Management	Incident detection, response, reporting, post-incident review	IR trigger testing, incident response simulation alongside pentest
16	Business Continuity and Disaster Recovery	BCP/DR planning, backup integrity, recovery testing	Backup security testing, DR system access control

17	Risk Management	Risk assessment, risk treatment, risk register, risk monitoring	Risk analysis incorporating pentest findings, treatment plan validation
18	Physical and Environmental Security	Physical access, facility controls, equipment security, data center	Physical penetration testing (where in scope), badge cloning, tailgating
19	Data Protection and Privacy	Data classification, retention, disposal, privacy controls, consent	Data exfiltration testing, classification enforcement validation

05 Control Domains and Pentest Mapping

SPECIFIC HITRUST CONTROL REFERENCES WITH TESTING RELEVANCE

The HITRUST CSF uses a numbered control reference system (e.g., 09.ab) tied to control categories and objectives. The controls below are the most directly relevant to penetration testing programs. Control references reflect the HITRUST CSF v11 structure used across current assessments.

Domain 07 - Vulnerability Management

CORE PENTEST DOMAIN: 07.a and 07.b

Domain 07 is the primary vulnerability management domain and the strongest regulatory anchor for penetration testing in HITRUST. Control 07.a (Technical Vulnerability Management) explicitly requires documented penetration testing as part of the vulnerability identification and assessment process. For r2, auditors validate: documented pentest scope and methodology, pentest reports within the assessment window, evidence of remediation tracking, retest results, and a risk-based remediation SLA program.

Control Reference	Pentest Testing Requirement
07.a - Technical Vulnerability Management	Requires timely identification, evaluation, and remediation of technical vulnerabilities. Penetration testing is explicitly listed in ISO 27002 implementation guidance referenced by HITRUST. r2 assessors validate pentest reports and remediation evidence.
07.b - Patch Management Controls	Patch management effectiveness is validated by pentest - unpatched systems discovered during testing represent direct 07.b findings. SLA compliance for critical/high patches must be demonstrated.

Domain 08 - Network Protection

Control Reference	Pentest Testing Requirement
08.a - Network Controls	Network security controls must be validated through testing. External and internal network pentests directly satisfy this control's implementation maturity evidence requirement.
08.b - Security of Network Services	Network service security testing - validation of network service agreements with providers and testing of network service security features.
08.c - Segregation of Networks	Network segmentation testing validates that VLAN boundaries, DMZ controls, and environment isolation are enforced. Lateral movement testing is the primary technique.
08.d - Electronic Messaging	Secure messaging and email security testing - relevant to phishing simulation and email gateway security validation.

Domain 09 - Transmission Protection

Control Reference	Pentest Testing Requirement
09.aa - Audit Logging	Logging systems must be tested to confirm they capture security-relevant events - including pentest activity. Failure of SIEM to alert during pentest is a direct 09.aa finding.
09.ab - Monitoring System Use	Detection and monitoring validation - do monitoring systems detect adversarial behavior? Pentest provides the evidence.
09.s - Information Exchange Policies	Data transmission security testing - TLS validation, secure file transfer testing, API transport security.
09.y - On-Line Transactions	Web application and API security testing for transactional systems. Directly maps to web application pentest scope.

Domain 10 - Password Management

Control Reference	Pentest Testing Requirement
10.a - Information Access Restriction	Access control technical testing - validates that access restrictions are enforced at the system level, not just in policy.
10.f - Password Management System	Password policy enforcement testing - validates complexity, lockout, history, and MFA controls. Brute force and credential stuffing resistance testing.
10.g - Key Management	Cryptographic key management testing - validates secure key storage, rotation, and access controls. Hardcoded keys and exposed secrets are in scope.

Domain 11 - Access Control

Control Reference	Pentest Testing Requirement
11.a - Access Control Policy	Technical access control enforcement is validated through penetration testing - policy alignment with technical implementation.
11.b - User Registration and De-registration	Orphaned account testing - validates that terminated users and deprovisioned accounts cannot access systems. Access lifecycle management.
11.c - Privilege Management	Privilege escalation testing - validates that standard users cannot gain administrative access through misconfiguration or application flaws.
11.d - User Password Management	Password testing for privileged and standard accounts - validates enforcement of password policy at the system level.
11.i - Teleworking	Remote access security testing - VPN security, remote desktop protocols, cloud access security, split tunneling risks.

06

r2 Deep Dive: Penetration Testing Requirements

WHAT THE R2 ASSESSMENT SPECIFICALLY REQUIRES

The HITRUST r2 (Risk-Based, 2-Year) assessment is the most rigorous cybersecurity certification available for organizations handling sensitive data. It is the only HITRUST assessment where penetration testing is explicitly validated during the on-site assessment process. This section covers everything specific to r2 pentest requirements.

How Penetration Testing Is Evaluated in r2

In an r2 validated assessment, the external assessor conducts a comprehensive on-site evaluation that explicitly includes:

- Interviews with key personnel including the security team, IT operations, and executive sponsors.
- Documentation review - policies, procedures, pentest reports, remediation evidence, risk register.
- Sampling - testing a representative subset of systems against stated controls.
- Penetration testing evidence review - assessors examine pentest scope, methodology, findings, and remediation.
- Vulnerability scan review - assessors examine scan results, coverage, and remediation timelines.

r2 PENTEST EVIDENCE: WHAT ASSESSORS EXAMINE

HITRUST r2 assessors do not conduct the penetration test themselves. They review and validate evidence that your organization has conducted an appropriate pentest program. Evidence must demonstrate all three required maturity levels:

Policy (Level 1): Penetration testing policy exists, is formally documented, and covers scope, frequency, methodology, authorization, and remediation SLAs.

Procedure (Level 2): Step-by-step operational procedures exist for executing the pentest program - from scope definition through findings tracking and retest confirmation.

Implemented (Level 3): Active evidence - pentest reports dated within the assessment window, vulnerability scan logs, remediation tracking records, and retest confirmation reports. Controls must have been operational for at least 90 days before the assessment submission.

r2 Pentest Cadence Requirements

Requirement	r2 Expectation
Annual penetration test	Annual pentest covering all in-scope systems is the baseline expectation. Evidence must fall within the assessment window.
Post-change testing	Significant changes - new applications, major infrastructure changes, cloud migrations - typically require targeted testing.
High-risk system frequency	Externally exposed systems and high-risk applications may warrant more frequent testing (semi-annual or quarterly).
Interim assessment (12 months)	At the one-year interim assessment, updated pentest evidence or confirmation of current program status is expected.
Vulnerability scanning cadence	Separate from pentesting - regular authenticated scanning (typically monthly or quarterly) with documented results and remediation SLAs.
Remediation SLAs by severity	Critical: typically 15-30 days. High: 30-60 days. Medium: 90 days. Low: 180 days. SLAs must be documented and tracked.

r2 Corrective Action Plans (CAPs) and Pentest Findings

One of HITRUST's most important mechanisms is the Corrective Action Plan (CAP). When a control scores below the certification threshold during an r2 assessment, a CAP is issued and the organization must remediate before certification is granted. Penetration testing findings directly feed the CAP process:

CAP Scenario	What It Means
No pentest evidence in assessment window	CAP issued for Domain 07 - must conduct and document pentest before certification can proceed
Pentest scope incomplete (missing key systems)	CAP issued - scope must cover in-scope systems per ISMS/assessment boundary

Critical findings not remediated	CAP issued - critical and high findings must be resolved with retest evidence before certification
No documented remediation SLAs	CAP issued for procedure maturity - policy alone is insufficient without operational procedures
Scan coverage gaps identified by assessor	CAP issued - authenticated scanning must cover all in-scope assets with documented results
Recurring findings across assessment cycles	Potential Managed maturity finding - absence of systemic improvement is a program gap

r2 INHERITANCE: REDUCING PENTEST SCOPE

Nearly 70% of r2 assessments in 2024 leveraged inheritance - reusing certified controls from cloud providers like AWS, Azure, and Google Cloud. Infrastructure-level controls (physical security, hypervisor isolation, data center controls) can often be inherited from a provider's HITRUST-certified environment. Important: Inheritance reduces scope but does not eliminate it. The application layer, configuration of cloud services, access management, and data flows remain in scope for your pentest - the inherited controls only cover what the provider has certified. Confirm what is and is not inheritable before scoping.

r2 vs. e1/i1: Penetration Testing Differences

Dimension	e1 / i1	r2
Pentest required for certification?	Not explicitly - pentest evidence may support certain controls but is not a validated requirement	YES - pentest evidence is explicitly reviewed and validated by the HITRUST-authorized assessor
Maturity levels evaluated	Implemented only - is the control in place?	Policy + Procedure + Implemented (minimum) - does a program exist, with procedures, operating with evidence?
Scope of evidence reviewed	Lighter evidence package - implemented controls demonstrated	Full documentation - policies, procedures, scan logs, pentest reports, remediation records, retest evidence
CAP risk from pentest gaps	Lower - control statements are fewer and more binary	High - missing pentest evidence is a direct CAP against Domain 07 (Vulnerability Management)
Vulnerability scanning	Required controls in scope	Required with authenticated scanning, documented cadence, and SLA-tracked remediation
Report requirements	Standard pentest report sufficient	Report must document scope, methodology, findings with severity, remediation evidence, and retest confirmation - mapped to HITRUST control references

07

Highlighted Control Areas

SECURITY TOPICS WITH HITRUST DOMAIN MAPPINGS

The following control areas map to specific HITRUST domains and include testing guidance for both standard and r2 assessments.

Password Hygiene and Credential Security

RELEVANT DOMAINS: Domain 10 (Password Management), Domain 11 (Access Control)

HITRUST Domain 10 contains explicit password management controls including system-enforced complexity, MFA requirements, and privileged account controls. The framework maps to HIPAA SS164.308(a)(5)(ii)(D), NIST SP 800-53 IA controls, and ISO 27001 A.8.5 simultaneously - satisfying multiple standards at once.

Testing Area	HITRUST Domain / Control
Password complexity, history, and lockout enforcement	Domain 10 - Password Management; 10.f
Multi-factor authentication implementation and bypass	Domain 10, Domain 11 - MFA for remote and privileged access
Default credentials on systems and network devices	Domain 06 - Configuration Management; Domain 10
Privileged account credential controls	Domain 11 - Access Control; 11.c Privilege Management
Service account and API key exposure testing	Domain 11; Domain 07 - Vulnerability Management
Password reset and recovery security	Domain 10 - Password Management

Access Management

RELEVANT DOMAINS: Domain 11 (Access Control), Domain 01 (Information Security Management)

Domain 11 is one of the most control-rich domains in HITRUST, containing identity lifecycle management, least privilege enforcement, privileged access controls, and remote access security. HITRUST maps these to HIPAA SS164.308(a)(4), NIST AC controls, and ISO 27001 A.5.15/A.8.2 simultaneously.

Testing Area	HITRUST Domain / Control
Least privilege enforcement and role-based access control	Domain 11 - 11.a Access Control Policy; 11.c Privilege Management
Privilege escalation - vertical and horizontal	Domain 11 - 11.c Privilege Management
Broken authorization in applications and APIs (IDOR/BOLA)	Domain 11 - 11.a; Domain 09 - 09.y Online Transactions

Orphaned accounts - terminated employee and service account testing	Domain 11 - 11.b User Registration and De-registration
Remote access security - VPN, RDP, cloud console access	Domain 11 - 11.i Teleworking
Third-party and vendor access validation	Domain 14 - Third Party Assurance

Vulnerability Management

RELEVANT DOMAINS: Domain 07 (Vulnerability Management) - PRIMARY PENTEST DOMAIN

Domain 07 is the core vulnerability management domain and the primary HITRUST control anchor for penetration testing. For r2, this is the domain where missing pentest evidence directly results in a CAP. HITRUST maps Domain 07 to HIPAA SS164.308(a)(8), NIST RA-5, and ISO 27001 A.8.8.

Activity	Domain / Control Reference
Annual penetration test (r2: validated evidence required)	Domain 07 - 07.a Technical Vulnerability Management
Authenticated vulnerability scanning program	Domain 07 - 07.a; frequency and SLAs documented
Risk-based remediation with SLAs by severity	Domain 07 - 07.b Patch Management Controls
Retest confirmation after remediation	Domain 07 - 07.a; required before CAP closure in r2
Post-change testing after significant environment changes	Domain 07 - 07.a; re-evaluate after major changes
Third-party component vulnerability assessment	Domain 07; Domain 14 - Third Party Assurance

Network Segmentation and Protection

RELEVANT DOMAINS: Domain 08 (Network Protection), Domain 09 (Transmission Protection)

Domain 08 is the primary network security domain covering firewalls, DMZ, segmentation, and intrusion detection. HITRUST maps these to HIPAA physical and technical safeguards, NIST SC controls, and ISO 27001 A.8.20/A.8.22. Network segmentation is not optional for r2 - it is a required and validated control.

Testing Area	HITRUST Domain / Control
Network segmentation - VLAN boundary testing and lateral movement	Domain 08 - 08.c Segregation of Networks
Firewall rule review and bypass testing	Domain 08 - 08.a Network Controls
DMZ architecture validation	Domain 08 - 08.a, 08.c
Production vs. dev/test environment isolation	Domain 06 - Configuration Management; Domain 08

Cloud VPC, security group, and subnet configuration	Domain 08 - Network Controls (maps to cloud environments)
Intrusion detection effectiveness testing	Domain 08 - 08.a; Domain 12 - Audit Logging and Monitoring

Encryption and Transmission Security

RELEVANT DOMAINS: Domain 09 (Transmission Protection), Domain 10 (Password Management)

Domain 09 covers transmission protection - TLS, VPN, secure protocols, and encryption of data in transit. HITRUST maps these directly to HIPAA SS164.312(e) technical safeguards, NIST SC-28, and ISO 27001 A.8.24. Encryption testing is one of the most consistently found weaknesses in HITRUST assessments.

Testing Area	HITRUST Domain / Control
TLS/SSL configuration - cipher suites, protocol versions, certificate validity	Domain 09 - Transmission Protection; 09.s
Cleartext data detection in transit (internal and external)	Domain 09 - 09.s Information Exchange Policies
API encryption validation - HTTPS enforcement, payload encryption	Domain 09 - 09.y Online Transactions
VPN security testing - tunnel configuration, split tunneling	Domain 09; Domain 11 - 11.i Teleworking
Encryption key management and exposure testing	Domain 10 - 10.g Key Management
Database and backup encryption validation at rest	Domain 07; Domain 19 - Data Protection

Data Segregation and Protection

RELEVANT DOMAINS: Domain 19 (Data Protection), Domain 11 (Access Control)

Domain 19 is HITRUST's data protection and privacy domain. Combined with Domain 11 access controls, it governs how sensitive data is classified, protected, accessed, and disposed of. For healthcare organizations, ePHI data segregation is a core assessment focus.

Testing Area	HITRUST Domain / Control
Multi-tenant data isolation - cross-tenant data access testing	Domain 11 - Access Control; Domain 19 - Data Protection
ePHI access boundary testing - who can reach patient data?	Domain 11; Domain 19; mapped to HIPAA SS164.312(a)(1)
Data exfiltration path testing - can sensitive data leave the boundary?	Domain 19 - Data Protection; Domain 08 - Network controls

Non-production data masking validation	Domain 19 - Data Protection; Domain 06 - Configuration
Storage and file share access control testing	Domain 11 - Access Control; Domain 19
Audit trail integrity - can ePHI access logs be tampered with?	Domain 12 - Audit Logging and Monitoring

Third-Party and Supply Chain Security

RELEVANT DOMAINS: Domain 14 (Third Party Assurance)

Domain 14 requires that third-party relationships are assessed and managed. HITRUST maps this to HIPAA SS164.314 Business Associate requirements, NIST SA controls, and ISO 27001 A.5.19-A.5.23. Pentesting firms accessing in-scope environments are subject to Domain 14 controls - BAAs and vendor security assessments apply to testing firms as they would any other service provider.

Testing Area	HITRUST Domain / Control
Third-party API and integration security testing	Domain 14 - Third Party Assurance
Supplier access path testing - VPNs, portals, shared credentials	Domain 14; Domain 11 - Access Control
Pentesting firm BAA / vendor security assessment	Domain 14 - required for vendors with system access
Cloud provider inherited controls validation	Domain 14; r2 inheritance model - what is covered vs. your responsibility
Software supply chain component scanning (SCA)	Domain 07 - Vulnerability Management; Domain 14

08

Pentest Scope for HITRUST

WHAT SHOULD BE IN SCOPE?

HITRUST pentest scope is defined by the assessment boundary - the systems, applications, and infrastructure included in the HITRUST assessment object in myCSF. In practice, any system that processes, stores, or transmits data covered by the assessment (ePHI, PII, payment data, or other sensitive information) should be included.

Component	Typical Testing Focus	Relevant Domains
External network perimeter	Public-facing IPs, services, boundary controls, DNS, certificate management	Domain 08, 07
Web applications and APIs	Authentication, authorization, business logic, injection, OWASP Top 10, FHIR APIs	Domain 09, 11, 07
Internal network	Segmentation, lateral movement, inter-segment access, internal services	Domain 08

Cloud infrastructure	AWS/Azure/GCP IAM, storage, misconfigs, inherited vs. non-inherited controls	Domain 08, 07, 14
Identity and access management	SSO, MFA, directory, privilege escalation, lifecycle management	Domain 11, 10
Endpoints and workstations	Endpoint protection, hardening, lateral movement from workstations	Domain 02, 06
Database systems containing PHI/PII	Access controls, encryption at rest, SQL injection, query auditing	Domain 11, 19, 12
Medical devices (IoMT)	Default credentials, network isolation, firmware vulnerabilities	Domain 02, 08, 07
Backup and DR systems	Access controls, encryption validation, backup system security	Domain 16, 19
Logging and monitoring systems	Detection capability, log integrity, SIEM alert coverage	Domain 12

09 What Assessors Expect in Practice

EVIDENCE REQUIREMENTS FOR HITRUST VALIDATED ASSESSMENTS

r2 VALIDATED ASSESSMENT - EXPECTED	ALL ASSESSMENTS - RECOMMENDED
- Annual pentest - internal + external, within assessment window. - Web application / API security testing. - Cloud configuration review (where cloud services are in scope). - Authenticated vulnerability scanning with documented cadence. - Pentest policy (Level 1) + procedures (Level 2) + active evidence (Level 3). - Remediation SLAs documented by severity - critical/high/medium/low. - Retest evidence confirming critical and high findings remediated. - Risk-based scope covering all systems in assessment boundary. - Pentest reports retained in myCSF evidence package.	- Network segmentation validation testing (Domain 08). - Medical device (IoMT) security testing where applicable. - Social engineering / phishing simulation (Domain 13). - Detection and response validation (Domain 12 SIEM testing). - Third-party / supplier security testing (Domain 14). - Physical security testing where physical controls in scope (Domain 18). - Rolling testing schedule - network Q1, web app Q2-Q3, internal Q4.

What a Compliant HITRUST Pentest Report Should Include

- Scope definition referencing the HITRUST assessment boundary and myCSF object.
- Methodology - NIST SP 800-115, PTES, or OWASP - documented and justified.

- Findings mapped to HITRUST control domains and control references (e.g., Domain 07, Domain 08).
- CVSS severity ratings with HITRUST-relevant business impact - PHI/PII at risk, regulatory exposure.
- Proof of exploitation - screenshots, request/response captures, attack chains demonstrating exploitability.
- Remediation guidance tied to specific HITRUST domains and control references.
- SLA tracking - findings tracked in a centralized risk register with target remediation dates by severity.
- Retest confirmation - before-and-after evidence for critical and high findings.
- Control Process Documentation - all steps from scoping through closure traceable for HITRUST QA review.
- Tester qualifications - relevant credentials (OSCP, CREST, CEH) and independence from the assessed organization.

HITRUST QA REVIEW: YOUR ASSESSOR'S ASSESSOR

Unlike SOC 2 or ISO 27001, HITRUST conducts its own Quality Assurance (QA) review of every validated assessment before issuing certification. HITRUST's QA team reviews the assessor's work and can reject or require additional evidence. This makes the evidence package quality critically important. Pentest reports submitted to myCSF must be thorough, current (within the assessment window), and demonstrate actual remediation - not just findings. HITRUST QA has rejected assessments where pentest evidence was incomplete, out of window, or where critical findings had not been addressed.

10 Resources

HITRUST CSF AND PENTESTING REFERENCES

HITRUST Alliance - Official Website hitrustalliance.net

Official source for the HITRUST framework, assessment options, and certification information. Download the HITRUST CSF (requires license agreement) and access the myCSF portal.

HITRUST r2 Assessment Overview hitrustalliance.net/r2

Official HITRUST r2 assessment page. Covers r2 requirements, controls, and the two-year certification cycle including interim assessment expectations.

HITRUST CSF Framework Overview hitrustalliance.net/hitrust-framework

Overview of the HITRUST CSF including the threat-adaptive engine, control library structure, and mapping to 60+ authoritative sources including HIPAA, NIST, ISO 27001, and PCI DSS.

HITRUST 2025 Trust Report hitrustalliance.net

Annual report on HITRUST certification outcomes including breach statistics, CAP rates, and assessment trends. Provides the 99.62% breach-free statistic and assessment maturity data.

Software Secured: NIST SP 800-115 and Pentesting softwaresecured.com

Explains how NIST SP 800-115 penetration testing methodology relates to HITRUST and other compliance frameworks. Useful for methodology documentation in your myCSF evidence package.

NIST SP 800-115: Technical Guide to Information Security Testing csrc.nist.gov

The most widely accepted penetration testing methodology standard. Referenced by HITRUST CSF as an implementation guide for vulnerability management controls. Free and authoritative.

HHS: HIPAA Security Rule Summary hhs.gov

HIPAA is the primary regulatory framework HITRUST maps to for healthcare. Understanding HIPAA Technical Safeguards (SS164.312) helps prioritize HITRUST pentest scope.

TEFCA: HITRUST r2 Requirement for QHINs healthit.gov

Official HHS/ONC page for the Trusted Exchange Framework. Confirms HITRUST r2 as the required certification pathway for Qualified Health Information Network (QHIN) designation.

OWASP Testing Guide v4.2 owasp.org

Industry-standard web application and API security testing methodology. Directly applicable to Domain 09 (Transmission Protection) and Domain 11 (Access Control) web-layer controls.

HITRUST CSF Inheritance Program hitrustalliance.net

Details on HITRUST's inheritance model - how to leverage certified cloud providers' controls to reduce your assessment scope. Nearly 70% of r2 assessments used inheritance in 2024.