A comprehensive and detailed checklist for performing a readiness assessment to achieve HITRUST e1 certification, expanded with examples and further explanations for each step

HITRUST e1 Readiness Checklist

HITRUST e1 Readiness Assessment Checklist (Detailed with Examples)

HITRUST
Authorized
External Assessor

Palindrome Technologies

1 Introduction

Achieving HITRUST e1 demonstrates a foundational commitment to cybersecurity, building trust with partners and customers, especially in industries handling sensitive data. The e1 assessment is an excellent entry point, focusing on 44 critical security controls, and can serve as a stepping stone to more comprehensive HITRUST certifications like the i1 or r2.

Why a Readiness Assessment is Crucial for e1 Certification

While the e1 assessment is less demanding than its counterparts, a readiness assessment is still vital. It acts as a pre-audit, allowing your organization to identify and address security gaps *before* the formal validated assessment. This proactive approach saves time, resources, and significantly increases your chances of a successful certification.

Key benefits of a readiness assessment include:

- **Gap Identification:** Pinpoint areas where your current security controls, policies, and procedures fall short of HITRUST requirements.
- **Efficiency:** Streamline the certification process by understanding your security posture and addressing issues proactively, reducing back-and-forth during the validated assessment.
- **Resource Optimization:** Avoid wasting resources on ineffective security measures and focus on what's truly needed for compliance.
- **Informed Decision-Making:** Gain precise knowledge of your security posture to make informed decisions about remediation efforts.

This checklist is designed to help your company systematically prepare for a HITRUST e1 validated assessment. The e1 assessment provides a 1-year certification and focuses on a single-scored maturity level: Implemented, specifically designed to demonstrate essential cybersecurity hygiene.

2 How to prepare

Embarking on your HITRUST e1 certification journey can seem like a significant undertaking, but breaking it down into manageable phases makes the process clear and achievable. This guide is designed to walk you through each critical stage of your readiness assessment, ensuring you're well-prepared for a successful certification.

We've structured the journey into three distinct, yet interconnected, phases:

1. **Phase 1: Understanding & Scoping** - This initial phase is all about laying the groundwork. You'll gain a deep understanding of the HITRUST e1 requirements and precisely define the boundaries of your assessment.
2. **Phase 2: Gap Analysis & Remediation** - Here's where you'll roll up your sleeves! You'll rigorously evaluate your current security posture against the e1 controls, identify any areas needing improvement, and then actively work to close those gaps.
3. **Phase 3: Final Review & Preparation for Validated Assessment** - The final stretch involves a thorough internal review to ensure everything is in order before you engage your external assessor for the official validation.

By systematically moving through these phases, your organization will build a robust foundation for cybersecurity and confidently approach its HITRUST e1 certification.

2.1 Phase 1: Understanding and Scoping

This foundational phase is the first and most critical step in the HITRUST e1 certification journey. It's all about establishing a clear plan and defining the precise boundaries of your project before the technical work begins. By thoroughly understanding the specific e1 requirements and determining which parts of your organization will be assessed, you create a solid blueprint for a smooth and efficient certification process. Successfully completing this phase prevents wasted effort and ensures your team's resources are focused on what truly matters.

2.1.1 Understand the HITRUST e1 Scope and Requirements

Before you can measure your organization's security, you must first know the yardstick. This initial step is dedicated to understanding the precise target you are aiming for. The HITRUST e1 certification is intentionally focused, designed to validate an organization's mastery of **44 fundamental security controls**.

These controls represent a vital baseline of cyber hygiene and form the core of a strong security posture. The goal here is for your team to become thoroughly familiar with each of these 44 requirements, understanding the objective behind each control before you begin to assess how they are implemented within your own environment.

1. [ ] **Access and familiarize yourself with the HITRUST CSF (Common Security Framework).**
   - **Details:** The CSF is the overarching framework that harmonizes existing controls and requirements from various standards, regulations, and best practices. Although you're focusing on e1, understanding the broader CSF provides context for future certifications.
   - **Example:** Download the latest version of the HITRUST CSF from the HITRUST Alliance website.
2. [ ] **Thoroughly review the specific requirements for each of the 44 essential cybersecurity controls in the HITRUST e1 assessment.**
   - **Details:** The e1 assessment focuses on a prescriptive set of controls, often covering areas like endpoint protection, network security, access control, vulnerability management, incident management, and basic data protection.
   - **Example:** For a control like "Endpoint Protection," identify specific requirements such as anti-malware installation, regular scanning, and automatic updates on all workstations and servers.
3. [ ] **Understand that the e1 assessment focuses primarily on the "Implemented" maturity level.**
   - **Details:** Unlike r2 assessments which can consider up to five maturity levels (Policy, Process, Implemented, Measured, and Managed), the e1 assessment strictly evaluates if controls are *implemented*.
   - **Example:** When reviewing controls, focus on whether the security measures are actively in place and functioning, rather than just documented policies or procedures (though these are often prerequisites for implementation).
4. [ ] **Recognize that e1 controls are threat-adaptive.**
   - **Details:** The e1 assessment is designed to leverage threat intelligence and best practice controls to address relevant practices and active cyber threats.

- **Example:** The set of 44 controls is not static; it evolves to address emerging cyber threats actively being targeted.

5. [ ] **Understand that the e1 assessment serves as a stepping stone to a validated assessment.**
    - **Details:** A readiness assessment helps identify gaps *before* the formal validated assessment, saving time and resources.
    - **Example:** Completing an e1 readiness assessment allows your organization to remediate deficiencies and refine its security posture, making the subsequent validated assessment smoother and more likely to result in certification.

2.1.2 Define Your Assessment Scope

After understanding *what* you're being assessed against, the next step is to define *where*. This is where you draw a clear, unambiguous boundary around the specific parts of your organization that will be included in the HITRUST assessment.

Think of it as putting a fence around the exact systems, applications, facilities, and personnel that create, access, or store the sensitive data you're protecting. This decision is critical as it directly dictates the amount of effort, evidence collection, and resources required for the entire project. A well-defined scope ensures that your team's efforts are focused, efficient, and aligned with your certification goals.

1. [ ] **Clearly diagram data flows for protected information entering, moving, and exiting your environment (in motion, at rest, in use).**
    - **Details:** This helps identify all systems and processes that handle sensitive data, ensuring comprehensive coverage.
    - **Example:** Create a diagram showing how customer Personally Identifiable Information (PII) is collected via a web application, stored in a database, processed by an internal system, and transmitted to a third-party billing service.
2. [ ] **Identify and list all in-scope systems and assets (servers, networks, endpoints, applications, cloud services, etc.) that handle or store protected data.**

- **Details:** HITRUST certifies *implemented systems*, not just facilities, people, services, or products. The CSF controls apply to all information systems regardless of classification or function.
- **Example:** List specific servers (e.g., Web Server 01, Database Server 02), applications (e.g., CRM, ERP), network devices (e.g., Firewall A, Router B), and cloud instances (e.g., AWS S3 bucket for data storage).

3. [ ] **Ensure all systems included in scope have been fully installed and configured within the control environment for at least 90 days.**
   - **Details:** This is a crucial "incubation period" requirement for implemented controls to demonstrate consistent operation. [111111]
   - **Example:** For a new security information and event management (SIEM) system implemented for logging, verify that it has been operational and collecting logs for at least 90 days before the assessment period begins.
4. [ ] **Engage key client management to define the scope, considering business units, related systems, facilities, and service providers.**
   - **Details:** Scoping is the most important step for any HITRUST assessment, and client management is responsible for defining it. [12]Consider primary scope components (applications, databases, networks, facilities, operating systems) and secondary scope components (endpoints, portable media, mobile devices, etc.).
   - **Example:** Conduct interviews with IT, legal, and business unit leaders to confirm which systems and processes handle sensitive data and align with business objectives for the certification. For instance, define if the scope is "Enterprise," "IT Service/Platform-focused," "Enclave-focused," "Shared IT services," or "Follow-the-data."
5. [ ] **Begin setting up your organizational information and assessment object in the HITRUST MyCSF tool.**
   - **Details:** The MyCSF tool is essential for managing your assessment, including defining your organization, scope, and tracking progress. [15151515]

- **Example:** Log into MyCSF, create a new assessment object, and input basic organizational details like name, location, number of employees, and overview of your security organization. Specify the assessment type as "e1 Validated Assessment."

2.2 Phase 2: Gap Analysis and Remediation

With your roadmap in hand from Phase 1, this next phase marks the transition from planning to direct action. This is the "heavy lifting" portion of your certification journey, where you hold a mirror up to your organization's security practices and then actively work to strengthen them.

This critical phase is a two-part process. First, the **Gap Analysis** involves systematically comparing your current controls against the 44 e1 requirements to pinpoint any areas that fall short. Second, **Remediation** is the hands-on work of developing and implementing Corrective Action Plans (CAPs) to close those identified gaps. This is where you transform your security posture from its current state to a compliant one, gathering the evidence needed to prove it.

2.2.1 Conduct a Comprehensive Gap Analysis (Self-Assessment)

This is the moment of truth, where you meticulously compare your current security reality against the established HITRUST e1 standard. Think of this step as a thorough diagnostic exam for your security program.

The objective is to systematically go through each of the 44 e1 controls and honestly assess whether your organization's existing policies, procedures, and technical implementations meet the requirement. The deliverable from this process is not a fix, but a detailed and honest report, a list of every identified "gap" between where you are and where you need to be. This gap list will become the official to-do list that drives your entire remediation effort in the steps to come.

1. [ ] **For each of the 44 e1 controls, evaluate your existing policies, procedures, and actual implementation against the requirement statements.**

   - **Details:** Assess if your current practices meet the prescriptive requirements of each control. This includes reviewing whether policies are documented, procedures exist to support them, and whether they are actually implemented. [18]

- **Example:** For a requirement related to access control, review your user access policy, the procedure for granting and revoking access, and then inspect system logs to verify that access changes are performed according to procedure.

2. [ ] **Gather sufficient evidence for each control, demonstrating its operation for at least 90 days.**

    - **Details:** Evidence is critical and should show consistent operation over the required incubation period. [19]Evidence types include verbal information (interviews), observed information (screenshots, data center visits), paper documents (signed policies), and electronic information (system logs, scanned forms). [20]

    - **Example:** For an access review control, collect the access review policy (paper document/electronic), documented procedures for conducting reviews (paper document/electronic), screenshots of the system demonstrating the review process (observed/electronic), and meeting minutes of review discussions (paper document).

3. [ ] **Document all identified gaps where current practices deviate from HITRUST e1 requirements.**

    - **Details:** A "gap" is a deficiency against one or more requirement statements and corresponding maturity levels. [21] Document these clearly to inform remediation efforts.

    - **Example:** If vulnerability scans are performed quarterly but not consistently covering all in-scope systems, identify this as a gap for the "Vulnerability Management" control.

4. [ ] **(Highly Recommended) Engage a HITRUST Authorized External Assessor for readiness assessment, as they can provide expert guidance and templates for documentation.**

    - **Details:** External Assessors bring expertise, can provide templates for policies and procedures, and offer invaluable guidance on the level of detail required by HITRUST. [22] This can significantly reduce remediation efforts later.

- **Example:** Partner with an assessor firm to perform a "mock audit" where they review your self-assessment, identify weaknesses, and advise on necessary improvements before the official validated assessment.

5. [ ] **Ensure internal assessments are performed by CCSFP-certified personnel.**

   - **Details:** Internal assessors must be certified CSF Practitioners (CCSFP) and independent of the organization's IT security control design and operation. [23]

   - **Example:** Verify that the internal audit team members conducting the readiness assessment have valid CCSFP certifications.

6. [ ] **If internal assessor results are used, ensure the external assessor performs procedures to establish a suitable basis of reliance, including participation in control walkthroughs.**

   - **Details:** While external assessors can rely on the work of internal assessors, they must still validate the scoring and participate in control walkthroughs. [24]

   - **Example:** If your internal team performs initial testing, the external assessor might re-perform a sample of those tests to verify accuracy.

2.2.2 Develop and Execute Corrective Action Plans (CAPs)

With a comprehensive list of gaps from your analysis, the focus now shifts from *finding* problems to actively *fixing* them. This step is the core of the remediation process, where plans are made and real, tangible improvements to your security posture are implemented.

For each deficiency you identified, you will first **develop** a formal Corrective Action Plan (CAP). This plan acts as a mini-project, detailing the specific tasks, responsible owners, required resources, and a timeline for resolution. Then comes the most critical part: you must **execute** that plan. This is the hands-on work of reconfiguring systems, updating policies, and training staff to close every identified gap. This is where your organization's commitment to security becomes a demonstrable reality, turning weaknesses into certifiable strengths.

1. [ ] **For each identified gap, develop a detailed Corrective Action Plan (CAP).**

   - **Details:** CAPs are management's formal response to deficient requirement statements.

- **Example:** For the vulnerability scanning gap, a CAP might state: "Implement an automated scanning tool to ensure monthly vulnerability scans cover 100% of in-scope systems by Q4 2025."

2. [ ] **Each CAP must define:**

    - [ ] **Who is responsible for remediation.**

        - **Example:** John Doe, IT Security Manager.

    - [ ] **When the deficiency will be resolved (consider committing to a project plan if full resolution takes longer).**

        - **Example:** Target Completion Date: 2025-12-31. If it's a large project, the CAP might initially target "Completion of Project Plan by 2025-09-30."

    - [ ] **What steps will be taken to resolve the deficiency.**

        - **Example:** "Research and select automated scanning tool; procure licensing; deploy agents to all systems; configure scan schedules; train staff on tool usage."

    - [ ] **The current status of the remediation effort (Not Started, In Progress, or Complete).**

        - **Example:** Status: "In Progress - Tool Selection Phase."

3. [ ] **Implement all necessary changes and maintain meticulous records of all remediation efforts.**

    - **Details:** Documenting remediation is crucial for demonstrating progress and eventual compliance.

    - **Example:** Keep a log of tool deployment dates, configuration changes, training sign-offs, and any internal audit reports verifying the new process.

4. [ ] **Ensure documented policies and procedures are up-to-date, comprehensive, and accurately reflect your implemented controls.**

    - **Details:** Policy and procedure documentation is vital. A policy defines the mandatory nature of requirements, and a procedure details ***how*** to implement those requirements.

- **Example:** Update your "Vulnerability Management Policy" to include the new scanning tool and frequency, and revise the "Vulnerability Scan Procedure" to detail its operation.

5. [ ] **Note that the scoring of the requirement statement should reflect its status as originally found, even if the CAP is fully resolved during the assessment.**

   - **Details:** HITRUST looks at the state of controls during the review period, not just at the time of submission.

   - **Example:** Even if the new scanning tool is fully deployed two weeks before the validated assessment, the initial readiness assessment score should reflect the original deficiency. The CAP progress will demonstrate improvement.

6. [ ] **CAPs should be entered by management into the MyCSF tool and submitted to HITRUST.**

   - **Details:** CAPs are typically created and managed by the assessed entity, not the external assessor. [31]They are reviewed by HITRUST for reasonableness.

   - **Example:** The CISO or compliance officer is responsible for formally entering the CAPs into the MyCSF platform.

2.3 Phase 3: Final Review and Preparation for Validated Assessment

Having completed the intensive work of closing your security gaps, you now enter the final phase of the HITRUST e1 journey. This stage is all about verification, quality control, and preparing for the formal audit. The focus shifts from internal remediation to proving your compliance to an independent third party.

Think of this as the "dress rehearsal" before opening night. It begins with a thorough internal quality assurance check to ensure all your documentation is in order and the evidence is compelling. Following this, you will engage an authorized HITRUST External Assessor who will validate your work. This entire phase is designed to package your efforts into a flawless submission, paving the way for a smooth review by HITRUST and, ultimately, a successful certification.

2.3.1 Final Review and Internal Quality Assurance

Before you present your work to an external party, the first critical step is to be your own toughest critic. This internal review is your organization's chance to perform a meticulous quality assurance (QA) check on the entire submission package, ensuring everything is in place for a successful validation.

Think of it as proofreading a final paper before submitting it for a grade. The goal is to have a fresh set of eyes review the evidence, test the descriptions in MyCSF for clarity, and confirm that every remediated gap is now fully supported by documentation. This internal audit is designed to catch any errors, omissions, or inconsistencies *before* your external assessor sees them, saving you valuable time and resources down the line and ensuring you put your best foot forward.

1. [ ] **Conduct a thorough internal review of all documentation and evidence.**
    - **Details:** Before engaging the external assessor for the validated assessment, perform a final internal check to catch any remaining issues.
    - **Example:** Have a separate internal team (e.g., internal audit or a different IT security team member) review all evidence, policies, and procedures against the e1 requirements.
2. [ ] **Ensure all responses and evidence are accurately uploaded and linked within the MyCSF platform.**
    - **Details:** MyCSF serves as the central repository for all assessment-related information. [33333333]
    - **Example:** Verify that every scored requirement statement has supporting documents linked correctly to the appropriate maturity levels (Policy, Procedure, Implemented). [34343434]
3. [ ] **Confirm that policies cover all facilities and systems within scope and procedures are detailed enough for implementation.**
    - **Details:** Policies must explicitly state the mandatory nature of requirements for all in-scope elements. Procedures must provide sufficient detail for a knowledgeable individual to perform the requirement. [35353535]

- **Example:** Double-check that your access control policy clearly states that all in-scope applications and servers must adhere to the principle of least privilege, and that the associated procedure outlines specific steps for configuring roles and permissions on each system type.

4. [ ] **Confirm that testing for implemented controls covers all facilities, systems, and supporting infrastructure within scope and adheres to HITRUST population and sampling methodology.**

   - **Details:** Implementation testing must demonstrate consistent application across the entire scope, and if sampling is used, it must follow HITRUST's guidelines (e.g., random, systematic, or haphazard, with random being recommended). [36363636]

   - **Example:** For a patch management control, verify that the evidence (e.g., patch deployment reports) shows successful patching on all in-scope workstations and servers, not just a subset. If you have 500 workstations, ensure your sample size meets HITRUST's guidelines (which can be calculated using their online calculators). [37]

2.3.2 Engage and Confirm External Assessor

With your internal preparations complete, it's time to bring in the experts. This step marks the formal transition from self-assessment to independent validation. To earn a credible, certified assessment, you must partner with a **HITRUST Authorized External Assessor**, an independent firm that has been vetted and approved by HITRUST to perform these specific audits.

The goal here is to select and formally engage the right partner for your organization. This assessor will not only perform the official testing of your controls but will also serve as your guide through the final, crucial stages of the submission process. Confirming your assessor solidifies the team that will review your hard work and attest to its compliance, making their selection a critical decision on the path to certification.

1. [ ] **Formally engage and confirm your chosen HITRUST Authorized External Assessor for the validated assessment.**

   - **Details:** The external assessor is responsible for validating the existence and operation of attested controls. You can find authorized assessors on the HITRUST website or simply contact Palindrome Technologies.

- **Example:** Sign an engagement letter with a HITRUST Authorized External Assessor firm, outlining the scope and terms of the validated assessment.

2. [ ] **Work with your assessor to schedule the HITRUST QA review date via the MyCSF Reservation System.**

    - **Details:** Assessed entities are required to schedule the Quality Assurance (QA) review date themselves, which can be done up to a year in advance. This ensures HITRUST has allocated resources for your assessment review.

    - **Example:** Log into MyCSF, navigate to the "Reservation System" and select a suitable date for HITRUST's QA review.

3. [ ] **Understand that if the assessment is not submitted by the reserved date, the reservation may be canceled, requiring a new one.**

    - **Details:** Strict adherence to the submission date is required to maintain the QA reservation. [42]

    - **Example:** Monitor your progress closely and communicate any potential delays to your assessor and potentially reschedule your QA slot if necessary.

3 Key Considerations and Best Practices

While the HITRUST e1 certification process is a structured journey, navigating it efficiently requires more than just following the steps. This section outlines the key strategic considerations and best practices that can significantly influence the success, speed, and cost-effectiveness of your certification effort.

Moving beyond the "what" of the process, we now focus on the "how." This includes foresight in planning, diligence in execution, and a proactive mindset. By embracing these principles, you can avoid common pitfalls, such as improper scoping and under-resourcing, which can lead to significant delays and budget overruns. Adopting these best practices will help transform the certification from a mere compliance exercise into a genuine opportunity to strengthen your organization's security posture and build lasting trust with your stakeholders.

Your action plan:

- **Start Early:** HITRUST certification, even for e1, takes time. Begin your readiness assessment well in advance of your desired certification date.
- **Leadership Buy-in:** Secure strong support from senior management. Their commitment is crucial for allocating necessary resources and driving the initiative.
- **Dedicated Team:** Assign a dedicated team or individual to champion the HITRUST certification process.
- **Leverage MyCSF:** The MyCSF platform is designed to guide you through the assessment process. Utilize its features for scoping, answering requirements, and uploading evidence.
- **Evidence Management:** Maintain meticulous records of all evidence and ensure it is readily available and properly linked in MyCSF.
- **Corrective Action Plans (CAPs):** Understand that CAPs are required for controls with scores below specific thresholds (for e1, a score below 75 is a gap, requiring a CAP if it falls below 75).
- **N/A Justification:** Ensure all N/A classifications are adequately supported with detailed rationale. Some controls, especially those related to monitoring, should never be marked N/A.
- **Continuous Monitoring:** Cybersecurity is an ongoing process. Once certified, maintain continuous monitoring of your controls to ensure ongoing compliance.
- **External Assessor Independence:** Ensure your chosen external assessor meets all independence requirements as defined by HITRUST.
- **Report Delivery:** Reports are delivered via the MyCSF tool, and the Point of Contact (POC) on the assessment will be notified via email when a report is ready.

Palindrome Technologies
ASSURANCE | TRUST | CONFIDENCE

HITRUST®
Authorized
External Assessor