cloudticity

BEYOND LLC
one-to-one healthcare compliance

Conquering the HITRUST Mountain

Build a strong, talented, motivated team to achieve HITRUST CSF Certification

Table of Contents

THE METAPHOR.
What's Everest got to do with it?

If you're in the healthcare business, you're in the HITRUST business — whether you know it or not. In just over a decade, HITRUST has steadily grown in importance to the healthcare industry. Due to recent IT trends such as multicloud environments and increasingly sophisticated cyberthreats, to say nothing of events such as massive information breaches and Covid-19, interest in HITRUST is accelerating at a fever pitch.

HITRUST certification offers a range of benefits such as streamlined audits, competitive advantage and more, but the certification comes at a price. To put it bluntly, HITRUST certification is hard. The process itself is complex and difficult for newcomers to navigate. There are substantial costs involved, from out-of-pocket expenses ranging from process development of your information security program to hiring the right assessor firm, to say nothing of substantial time investment by people throughout the organization. Without the right preparation, organizations can see their validation rejected by the HITRUST Alliance — a demoralizing outcome with the need of additional time, resources and investments.

To help you better understand what you're up against and how you can be successful in achieving HITRUST Certification, Cloudticity and BEYOND LLC offer this ebook. We organized this document around the metaphor of climbing Mount Everest (if you're keeping score, 29,029 feet high) because we see similarities:

- Both processes are challenging endeavors with little margin for error.
- Both have exceptional payoffs for success.
- Each requires the help of an experienced expert (Lead Sherpa/External Assessor).
- You probably won't make it to the top unless you have assembled the right team.

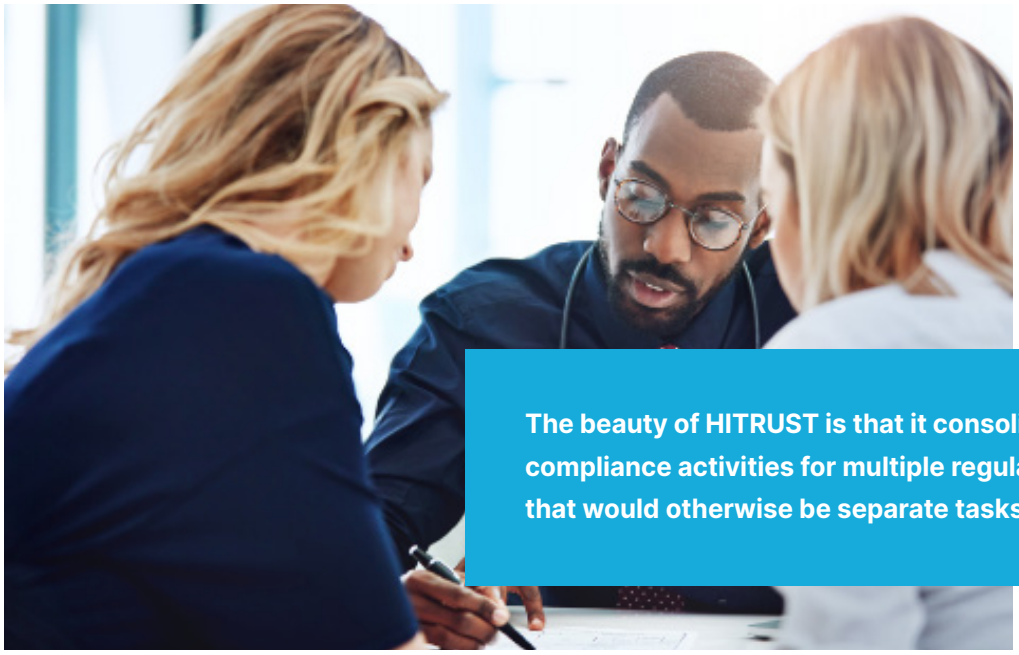
So grab your ice axes, strap on those crampons, and let's get started!

THE TERRAIN.
What Is HITRUST?

The term HITRUST is shorthand for the Health Information Trust Alliance, a privately held company located in Frisco, Texas, United States. Founded in 2007, the HITRUST Alliance creates programs to safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. HITRUST was developed initially for the healthcare industry, and now, other industries have taken note and are moving to adopt the HITRUST framework in their information security programs.

The HITRUST Alliance certifies that companies meet a customized set of requirements from HITRUST CSF[1], a comprehensive framework for addressing security, privacy, and regulatory requirements. CSF offers a unified approach to managing compliance with HIPAA as well as a range of globally recognized standards, regulations, and business requirements formulated by organizations such as ISO, GDPR, NIST, and PCI.

1 CSF originally stood for Common Security Framework



The beauty of HITRUST is that it consolidates compliance activities for multiple regulations that would otherwise be separate tasks.

HITRUST IS NOT HIPAA

HITRUST and HIPAA often get conflated and it's not hard to understand why, because they both relate to security and privacy in healthcare. But it's the differences that matter.

For starters, HIPAA is a mandatory law of the United States that applies to all healthcare organizations. In contrast, HITRUST is a voluntary certification, although many hospitals and other institutions require their vendors to be HITRUST certified — not exactly voluntary if you want to stay in business.

When it comes to organizational compliance, there is no such thing as HIPAA certification[2]. In contrast, HITRUST certification establishes that the organization is HIPAA compliant because the HIPAA requirements are embedded in HITRUST CSF.

2 Confusingly, the term "HIPAA certification" means that an individual has completed a HIPAA compliance class, but does not mean that the organization itself is HIPAA compliant.

THE OBSTACLES.
Chasms, Icefalls Ahead

To choose their ascent route, mountaineers need a clear picture of the terrain ahead. The same is true of HITRUST certification, and the place to start is understanding the central role of controls.

Controls are the atoms of HITRUST CSF, each encapsulating a specific requirement for security or privacy. HITRUST CSF currently has 156 security controls and 75 control objectives. HITRUST controls are broken into 19 separate domains — similar to how a business is built. This partitioning benefits the project manager because the domain areas tend to match up to a single group or SME, making task assignments easier. It also makes reporting more granular and digestible because the PM can report the status of domains (subject matter) to executives.

The number of controls that a company must meet varies depending on organizational, data, and systems factors. A scoping exercise early in the process allows HITRUST to determine the subset of requirements specific to that organization — more on the process later. A small healthcare vendor may have 200+ requirements to meet for certification, while a large enterprise could have 600 or more.

1. Information Protection Program		
2. Endpoint Protection	8. Network Protection	14. Third-Party Assurance
3. Portable Media Security	9. Transmission Protection	15. Incident Management
4. Mobile Device Security	10. Password Management	16. Business Continuity & Disaster Recovery
5. Wireless Security	11. Access Control	17. Risk Management
6. Configuration Management	12. Audit Logging & Monitoring	18. Physical & Environmental Security
7. Vulnerability Management	13. Education, Training & Awareness	19. Data Protection & Privacy

Figure 1. HITRUST control domains

SECTION 1.
ASSEMBLING YOUR TEAM

Before you can climb the mountain — or achieve HITRUST certification — you need a core group of key players to be successful. This section lays out some basic principles to follow as you make these key decisions.

"Climbing the big mountains demands three key principles: flexibility, patience, and respect."

— Alan Arness, veteran climber, "The Four Phases of Everest"

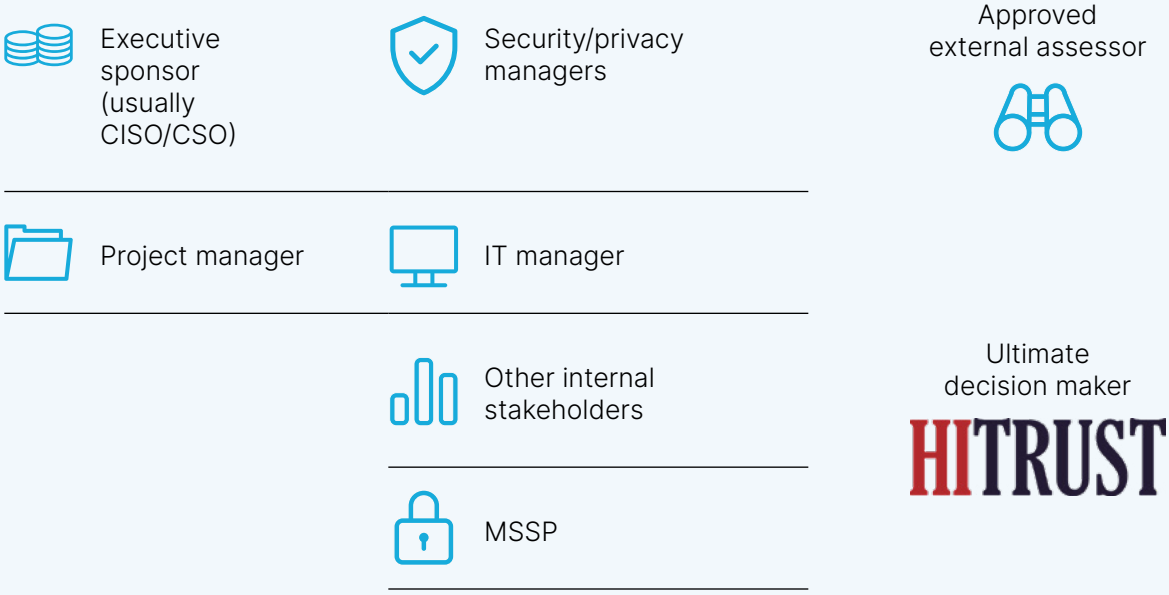


Figure 2. Typical HITRUST Team Members

THE LEADERS.
Cooperation gets you up the mountain

Everest ascents have a single guide who is solely responsible for the climbers and the climb. In the HITRUST certification process, however, three leaders must work closely to achieve the ultimate goal of HITRUST certification. The triad includes the executive sponsor, the CSF assessor, and the HITRUST Alliance (see figure 4).

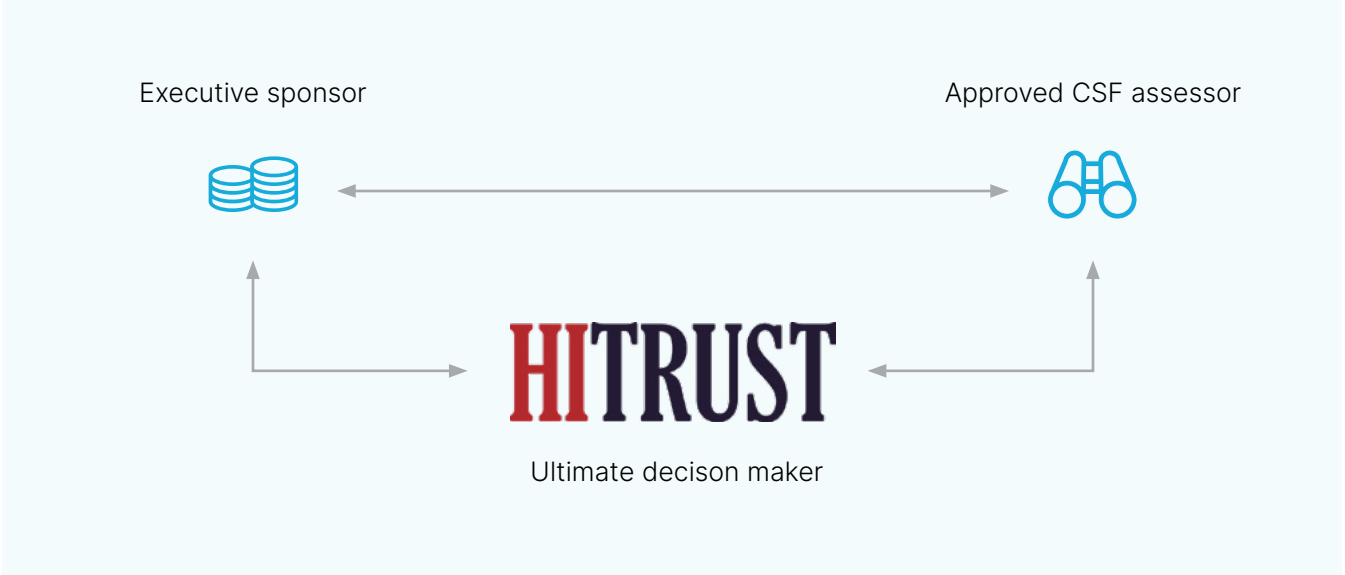


Figure 3. Leaders of the HITRUST Certification Project

Executive Sponsor: Usually the chief security officer (CISO or CSO) but can also be senior director level. This executive needs to have significant domain knowledge about security and privacy and be strongly motivated to drive the certification process to a successful outcome. While not a day-to-day participant — that responsibility falls to the project manager as discussed below — the sponsor must have the organizational clout to break interdepartmental logjams and get the project back on track when it falters.

External Assessor: Organizations that have been approved by HITRUST for performing assessment and services. BEYOND LLC is the approved External Assessor used by Cloudticity for their own HITRUST certification and works with many of Cloudticity's clients.

HITRUST Assessment Reviewer: HITRUST reviews the assessment details submitted by the External Assessor. The External Assessor will work with HITRUST directly as this review is conducted.

THE ASSESSOR (1): BASIC QUALIFICATIONS. Been there, done that

Expertise: Every assessor organization brings expertise to the table — but is it the kind that you need? When evaluating potential assessors, look for three specific kinds of expertise:

- Domain: Healthcare lives in a unique and demanding regulatory climate, one that has to be experienced to be understood. Prefer a firm that specializes in and derives the bulk of their revenue from the healthcare sector.
- Cybersecurity: A high-quality assessor firm should have at least one high-ranking official who has managed security within a medium-sized or larger organization at an executive level — CISO, CSO, senior director of security. Enterprise cybersecurity simply can't be learned from a Cybersecurity for Dummies book.
- Auditing: Your assessor firm should include an individual with extensive hands-on experience auditing risk management and regulatory compliance in a medium-sized to large enterprise as well as a thorough understanding of the HITRUST process.

Track record: When evaluating candidates, ask about the firm's success rate. Don't be afraid to set the bar high. As one data point, BEYOND LLC has never failed to achieve certification for their clients — a 100% success rate.

Framework: If your assessor team shows up for the kickoff meeting with yellow legal pads and a bunch of #2 pencils, you're in trouble. Given the massive size of the task — even a modest audit scope for a medium-size company can require hundreds or thousands of screen shots — the assessor should come to the table with a tested and proven approach. There are many ways to successfully reach the top of the mountain, but winging it is not one of them.

THE ASSESSOR (2): CUSTOMER EXPERIENCE. Hold my hand

Flexibility: If ever there were an industry where cookie-cutter approaches don't work, it would be healthcare. Just as treatment plans are tailored to the needs of the individual patient, HITRUST certification plans must be scoped to fit the needs of the client. Lean toward an assessor organization that will adapt their process to accommodate your individual circumstances. Ask them to be specific about how they work, and what you can expect. Ultimately, your decision will rely on a huge dose of gut feeling, so the more interaction during the selection process, the better.

Transparency: The entire HITRUST process is built on transparency. Your assessor's business model should be too. If they spoon-feed you information about their team structure, workflow ,or their fee structure, beware. Look for firms who are forthcoming right from the first call through the entire selection process and check references to learn the experience of others. Please remember some details will not be known until your assessment is scoped, but once that is complete, all information should be on the table before you move forward.

Continuity: The assessor-client relationship requires trust, something that builds over time through multiple interactions between the same team members. For that reason, you should base your decision on interviews and communication with the actual members who will be assigned to your account. Furthermore, those people should continue to be your contacts throughout the certification project and beyond.

THE ASSESSOR (3): FRIEND OR FOE?
Hold my hand

One common concern within the organization is what exactly is the assessor's role here? Are they going to help us improve our systems (friend) or find the flaws and inadequacies of our current system (foe)?

The short answer is both. In the readiness assessment and implementation stages, the tone needs to be friendly. All interactions should be professional, collegial, and cooperative. Early on, a good assessor firm will leave you with the impression that they will play a constructive role, not find fault or blame anyone.

However, during the validation process, the assessor needs to take on a more adversarial role — for your sake. As one customer put it, they try to "break your HITRUST submission" as a way to determine controls that require additional documentation to pass the scrutiny of the HITRUST Alliance. The assessor's value-add at this point is to look at each control the way HITRUST will and convince themselves that your evidence will hold up.

What you can do to help is to be open and transparent during the readiness assessment. It may be painful to talk about the parts of your security implementation plan (SIP) that are less than stellar, but the assessor needs to have the complete picture to do the best job possible. Come clean early to avoid problems down the road.

A final thought: If anyone on your team feels uncomfortable or intimidated about being honest with your assessor, then you probably have the wrong assessor or the wrong team members working on this project.

THE PROJECT MANAGER.
Lead Sherpa

For many organizational projects, the PM is primarily a spreadsheet jockey, tallying the tasks as they are completed and nudging laggards to catch up. However, a HITRUST PM wears many more hats, and that makes it a difficult yet vital position to fill (see figure 4).

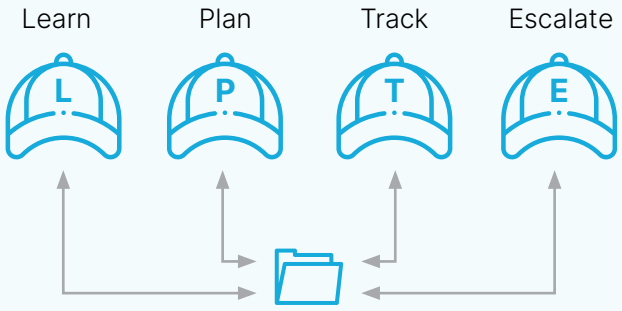


Figure 4. Typical tasks of a HITRUST PM

Learning: Unless he or she has participated in a HITRUST certification process, the PM should start with self-education or ask for guidance from the assessor organization. PMs must understand the HITRUST controls and taxonomy well enough to assess the accuracy of information coming from stakeholders. The PM is the single source of truth about the project and must maintain that position start to finish. Some organizations have team members obtain their CCSFP to have a stronger understanding of the project at hand.

Planning: HITRUST certifications are complex activities, so it is essential to create a phased project plan and timeline that allows stakeholders to understand what is expected of them and budget their time accordingly. The plan serves as a touchpoint for executive oversight and needs to be constantly updated to reflect the true situation on the ground.

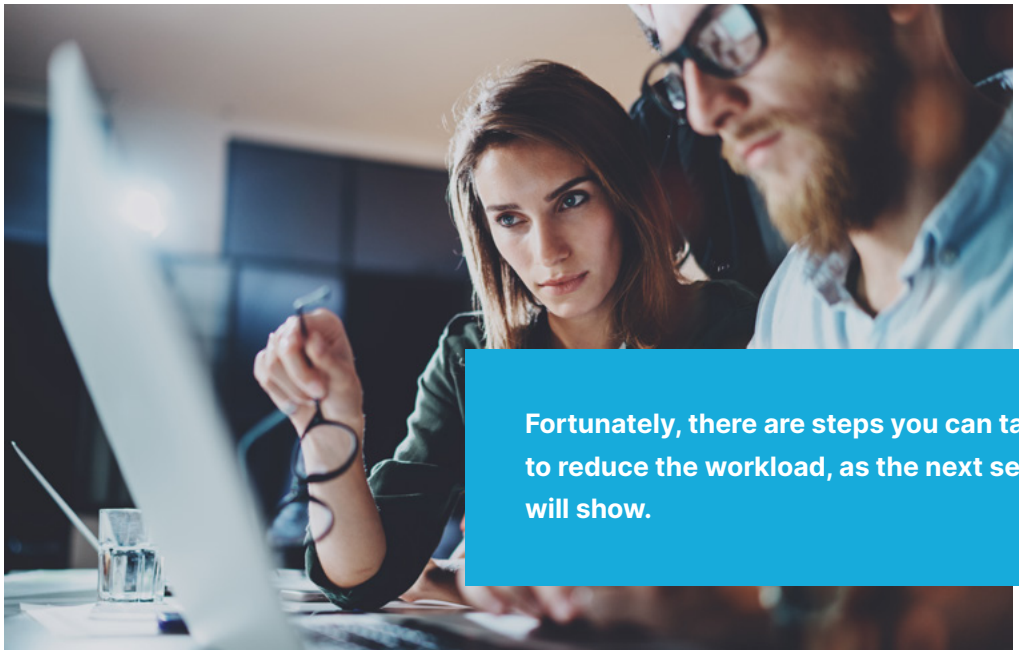
Tracking: The core activity of the PM is maintaining accurate records of the certification status for each of the hundreds of controls that apply to the company. For some PMs, the best tool is a spreadsheet, although it can also be a formal project management software package such as monday.com, SmartSheet, Hive or Teamwork. However, a better approach is to take advantage of purpose-built tools provided by the assessor organization. BEYOND always develops a custom test plan for just this purpose.

Escalation: Most PMs prefer to deal with problems on their own — in fact, that's part of the job description. However, a good PM for HITRUST certification must realize when the project is veering significantly off-schedule and needs intervention from the executive sponsor.

THE EVIDENCE FINDERS.
Everybody on the rope

Once you know the list of requirements, it's time to gather the evidence — a process that touches a surprisingly large portion of the organization.

What constitutes evidence? Evidence will be dictated by HITRUST and the assessor organization. One example of evidence can be one or more screenshots proving that the control is in place. For example, you can prove that you have two-factor authentication by capturing screens of the login process that show the use of the authorization code. Needless to say, capturing and managing hundreds or even thousands of screenshots is a huge logistic challenge and significant time drain.



Fortunately, there are steps you can take to reduce the workload, as the next section will show.

The composition of the evidence finder's group depends on a range of factors including the number of controls, the unique roles and responsibilities within your organization, and the availability of resources. In general, the minimum subset includes the privacy officer, security officer, and IT manager — the bulk of the evidence gathering falls on these staff members (SME that works within each Domain). Other functional groups play a less time-consuming but vital role, for example, the HR manager could be tasked with providing evidence of HIPAA training.

Individual HITRUST domains can often be mapped to specific evidence finders as a way to simplify project management as shown in the figure below.

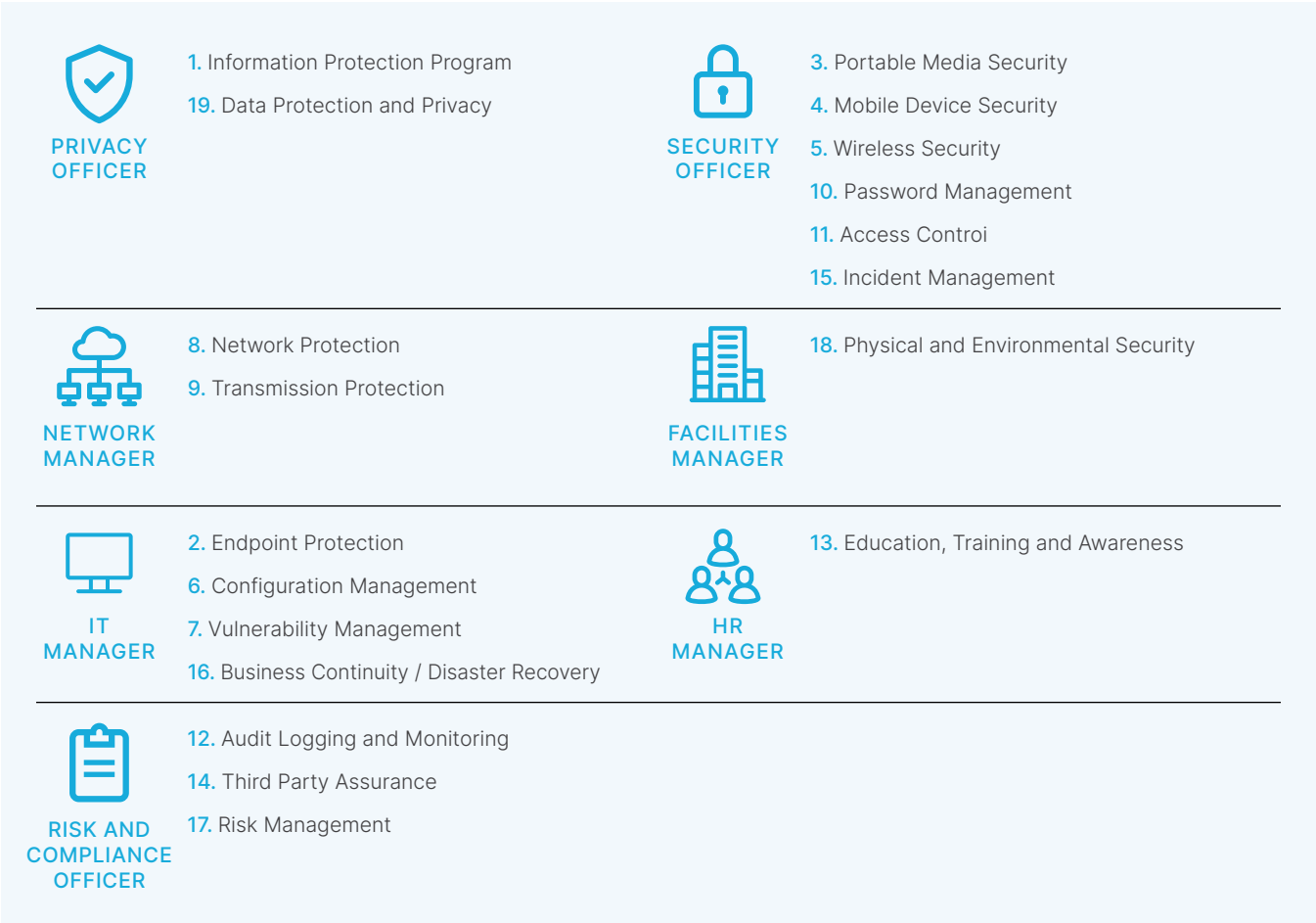


Figure 5. Typical domain responsibilities for HITRUST evidence gathering

THE MSSP.
Inheritance is a good thing

In theory, your managed security service provider (MSSP) — assuming you have one — has a limited role in the formal HITRUST certification process. However, there are several ways that having an MSSP can streamline the project.

Architecture: Organizations often bring in MSSPs during the system architecture phase to ensure that the new infrastructure has the components and interconnections needed to comply with HIPAA, PCI, and other regulations. As a result, these organizations can expect to have fewer control deficiencies from the beginning, reducing the number of controls that must be implemented and shortening the timeline.

Inheritance: HITRUST CSF recognizes the concept of inheritance, which means that your organization can inherit control compliance from a HITRUST certified third-party such as an MSSP or infrastructure provider such as AWS or Microsoft Azure. A typical MSSP may be certified for 200 controls, many of which can be inherited by the candidate organization through a dropdown menu on MyCSF, the customer portal for HITRUST. On the infrastructure provider side, all major providers — AWS, Microsoft Azure and Google Cloud Services — provide letters from HITRUST delineating their scope, which is the services that have been certified.

Evidence: As the candidate organization works its way through the evidentiary process, the MSSP can often help simplify the task, for example, pointing out where a single screenshot might be able to provide evidence for multiple controls. Don't hesitate to confer with your MSSP on matters related to your existing implementation.

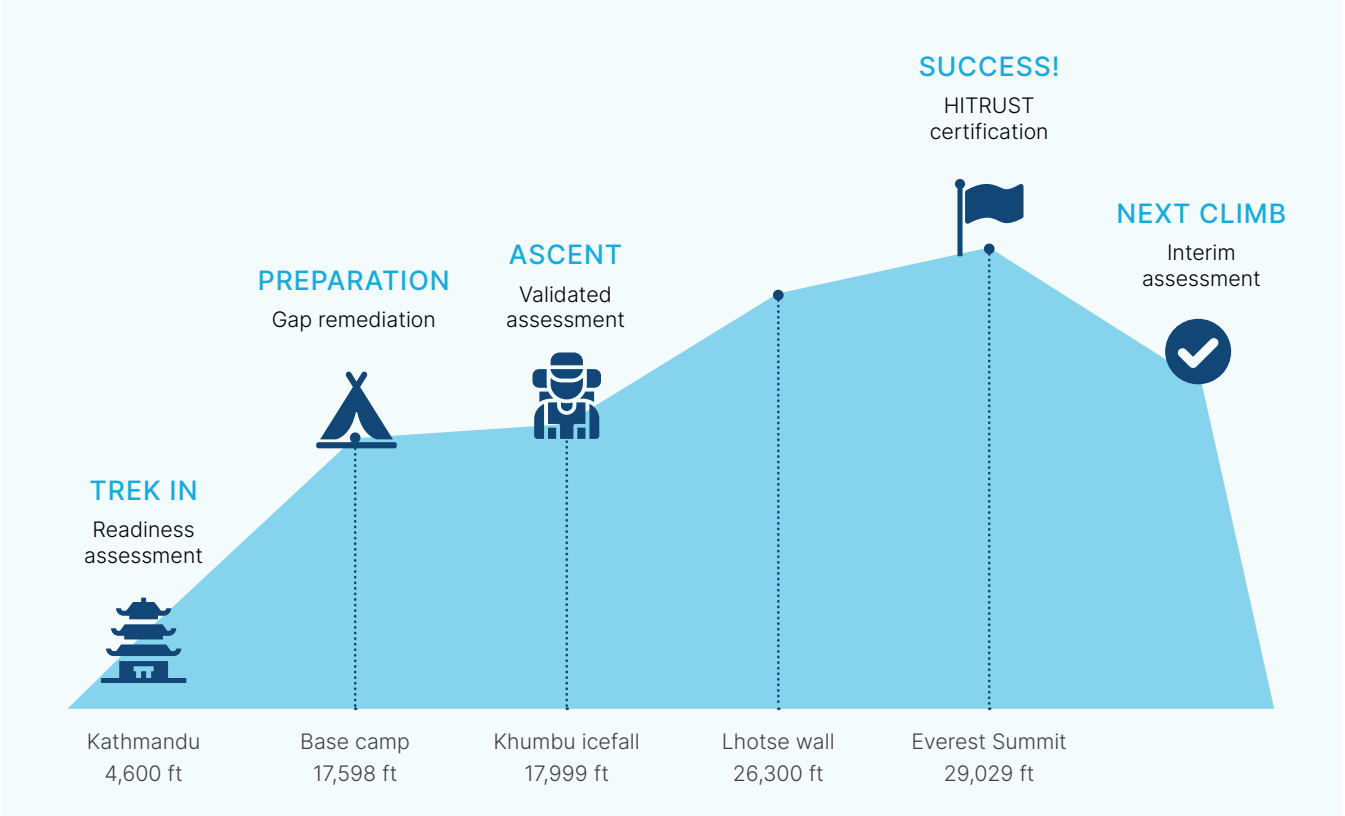
Value-Add Services: Top-tier MSSPs often offer solutions that can help simplify tasks in the HITRUST certification process. For example, Cloudticity offers a unified logging solution that allows multiple log sources to be aggregated into a single spot and queried — a HITRUST requirement. (The same consideration holds true for your assessor organization, for example, BEYOND offers a range of services to assist the client in obtaining HITRUST certification.)

SECTION 2.
CLIMBING THE MOUNTAIN

Now that you understand the terrain and obstacles and have put together a killer team, the time has come to actually climb the mountain. Just as the Everest ascent has milestones and checkpoints, so too does the HITRUST certification journey. In this section, we describe the BEYOND LLC phased approach that can be adapted to your individual needs to give you the best chance to reach the summit of HITRUST Certification.

"Never measure the height of a mountain until you reach the top. Then you will see how low it was."

— Dag Hammerskjold,
Swedish economist and diplomat



READINESS ASSESSMENT.
People, get ready

The typical Everest climb starts with a five-day walk from Kathmandu to base camp. While this part of the journey is not particularly strenuous compared to the actual ascent, it does help you and your guide determine your general level of fitness for the climb as well as the state of your equipment, for example, boots, backpack, and sun protection. Making it to base camp doesn't necessarily mean you're ready to push for the summit, but it's an important step.

The analogous activity in the HITRUST process is determining your organization's readiness to complete the validation assessment. While some organizations skip this step and just launch into the validated assessment, we believe that approach makes as much sense as a mountaineer skipping base camp and heading straight up the mountain. Through the Readiness Assessment, your assessor takes the lead by identifying gaps in your existing environment that could prevent HITRUST certification and providing recommendations, guidance, and timeline for developing an Information Security Program that meets the current HITRUST framework.

GAP REMEDIATION. Get your gear — and head — in tip-top condition

Base camp isn't a vacation, rather, it's a period of physical and mental preparation. The trek from Kathmandu has identified a number of equipment and technique issues. Before you start up the mountain, those issues have to be resolved. There is a mental side as well. By double-checking your gear and addressing any problems, you build your confidence that the climb will be successful.

It's the same with gap remediation in the HITRUST Readiness process. The list of deficiencies from the readiness assessment becomes the checklist for the gap remediation. The range of services that your assessor can perform is broad — some examples are functioning as a virtual CISO, creating a data classification protocol, and setting up a business continuity/disaster recovery strategy.

An important caveat: your assessor must enforce segregation between a) the team that completes the Readiness Assessment and helps with gap remediation, and b) the team that performs the validation. Otherwise, it would be like having students grade their own homework — an inherent conflict of interest.

VALIDATED ASSESSMENT. Up we go

The ascent phase of the Everest climb starts with a series of acclimation climbs, challenging shorter ascents that mimic the real thing.

In the same vein, the validated assessment looks at your submission from the HITRUST point of view. This phase is where your assessor's HITRUST experience — or lack thereof — comes into play. In this phase, the assessor takes on the role of the HITRUST Alliance evaluator, scrutinizing each of the hundreds of screenshots to see if they in fact demonstrate compliance with the corresponding control.

The validated assessment should not come off as a feel-good exercise. As described earlier, your assessor needs to be knowledgeable, thorough, and assertive throughout the validated assessment. That's the best way to optimize the probability of success.

Once the validated assessment is complete, the Assessor Organization will submit the details to HITRUST for their review. Make yourself comfortable — it can take 16-20 weeks for HITRUST to complete its review and rule on your submission. If you've chosen the right assessor and rigorously followed their advice, there's every reason to have the champagne on ice. You usually find out the results of the HITRUST review directly from your assessor, although they are also available within MyCSF.

HITRUST CERTIFICATION.
Sittin' on top of the world

Success! You've made it to the top — HITRUST certification — and it feels really, really good. But was it really worth the effort?

The answer is a resounding Yes. Here are three good reasons to invest the time, money, and energy necessary to achieve HITRUST certification.

1. **HITRUST Demonstrates Regulatory Compliance:** As an organization in the healthcare industry, you are subject to a range of regulations such as HIPAA, PCI, and HITECH. HITRUST CSF is based on those requirements, which means that HITRUST certification demonstrates that your organization is compliant. The HITRUST Alliance tracks changes to the regulations and ensures any changes are incorporated into CSF.

2. **HITRUST Reduces Cybersecurity Risk:** As hackers become smarter and more sophisticated, you must do the same. The HITRUST requirements embody a wealth of up-to-date information about today's cyberthreats and how to combat them. More than a checklist, HITRUST certification is a strategic tool to help you mitigate the risk of a high-profile breach that compromises your customers' PHI and PII as well as your reputation. In addition, your team will learn new techniques and security strategies to strengthen in-house knowledge.

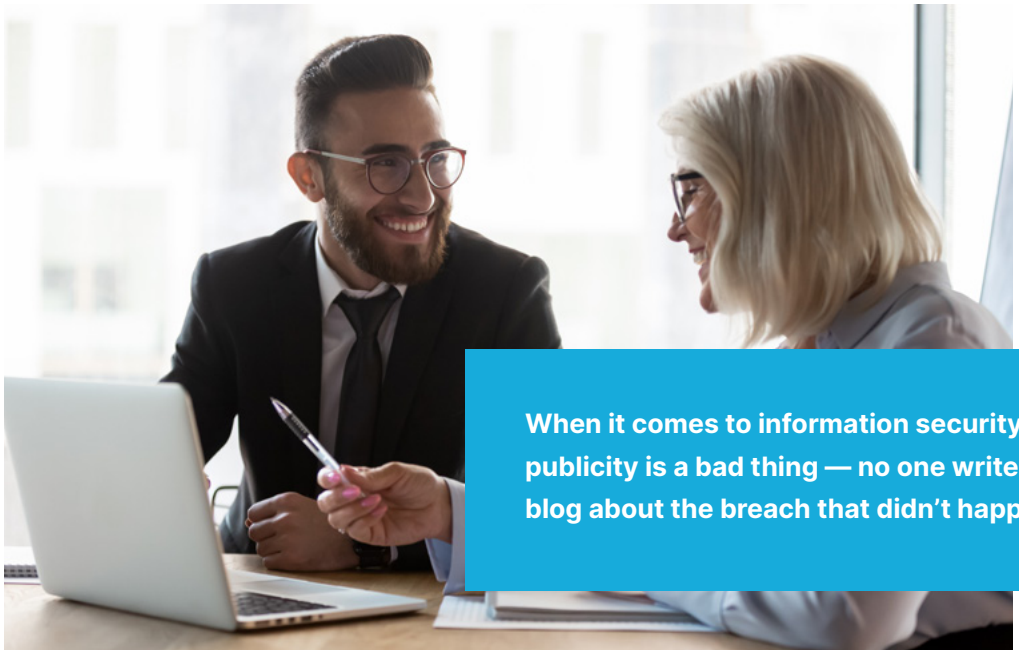
3. **HITRUST Certification Differentiates Your Organization:** When it comes to differentiation, there are two ways to look at HITRUST certification. If your competitors are certified and your organization is not, they automatically are perceived better than you — not the kind of differentiation you are looking for. If those roles are reversed, then you stand out from your rivals. In some cases, for example, hospital procurement, certification is table stakes — without HITRUST, you're still back at base camp.

INTERIM ASSESSMENT.
Congratulations! Now do it again.

Veteran mountaineers never rest. In fact, some say that they start planning their next climb during the Everest descent!

The HITRUST process is similar in that you can never rest on your laurels. While HITRUST certification is valid for two years, you must submit an interim assessment at the one-year mark. This review follows the same guidance as the validated assessment but has a limited set of requirements — typically, HITRUST asks for evidence of compliance for one requirement from each of the 19 domains.

Even though the interim assessment requires less overall effort than a full validation, the same high evidentiary standards still apply. In a sense, the interim assessment is a benefit to your organization because it provides another motivation to stay current on your security implementation plan. Of course, the primary motivation is to protect your sensitive information and IT infrastructure from breaches.



When it comes to information security, publicity is a bad thing — no one writes a blog about the breach that didn't happen.

FINAL THOUGHTS.
The assessor matters, big time

If you made it to the end of this ebook, congratulations! You may just have the stamina and motivation it takes to navigate the HITRUST certification process.

The one thing you should take away from this discussion is the critical role that the assessor plays in the HITRUST certification journey. When you select an assessor firm, you should approach the evaluation process as you would for a law or accounting firm. HITRUST certification is not a one-and-done project, but rather an ongoing commitment to your customers, employees, and brand.

When it comes to choosing your External Assessor, how do you find the right one? If you have an MSSP or a trusted contact at your cloud provider, ask for a referral. Otherwise, conduct an evaluation to winnow down the candidates and go through a formal selection process. The following checklist summarizes the main things you should look for.

- ☐ **Practice primarily in healthcare**
- ☐ **Executive-level cybersecurity experience**
- ☐ **Hands-on corporate auditing experience**
- ☐ **Excellent track record for HITRUST certification**
- ☐ **Proven, phased approach**
- ☐ **Transparency and staff continuity**

SPLIT PERSONALITY

When your assessor provides implementation services in addition to validation, there is a possibility for conflict of interest. In theory, the same person could evaluate a security measure that he himself put into place — with predictable results. To avoid even the appearance of such a conflict, look for a firm with internal segmentation, that is, one group handles the readiness assessment and gap remediation while a second team performs the validation assessment. This organizational strategy avoids conflicts of interest and helps ensure a rigorous and fair validation assessment.

About Cloudticity

Founded in 2011, Cloudticity focuses exclusively on helping healthcare organizations leverage the public cloud in order to revolutionize healthcare. Through our purpose-built, HITRUST-certified solutions and deep cloud expertise we help healthcare companies accelerate their HITRUST timeline by up to 50%, while reducing costs and complexity along the way.

Distinguished for having built some of the earliest and largest health systems on the cloud, including the first patient portal, the first health information exchange (HIE), the first and only FISMA high deployment on AWS GovCloud, and the first Meaningful Use 2 (MU2) compliance attestation for a large hospital system, Cloudticity enables healthcare to thrive in the digital era. Innovate faster, improve care, maintain compliance, and drive long-term growth with Cloudticity cloud-native solutions.

About BEYOND LLC

BEYOND LLC is a woman owned and operated consulting firm that is specific to performing HITRUST Assessment work by providing our clients with a personalized “one to one” approach to the highest level of service and quality at an affordable price.

As a HITRUST CSF Assessor, BEYOND LLC provides readiness, certification, and remediation services for healthcare organizations and their business associates to assess compliance with the industry security requirements and standards. With a 100% client success rate, BEYOND will work with each client and create solutions that help the organization align with the HITRUST Common Security Framework (CSF).