

Leading strategies
for HITRUST success

The Best of the
Ostendio

**HITRUST Master
Class Series**



A Comprehensive Guide to Mastering HITRUST



OSTENDIO



Introduction

For many organizations, pursuing HITRUST certification can seem like a daunting task. However, if you're considering taking the leap, look no further than this eBook. Filled with top strategies and expert advice from auditors and HITRUST experts - including a HITRUST representative and a CEO whose organization has already achieved HITRUST - this guide is the perfect resource to help you navigate the process with confidence.

This eBook provides a behind-the-scenes look into practical applications to achieve HITRUST certification, derived from transcriptions from Ostendio's HITRUST Audit Master Class series.

Table of Contents

1. Intro to HITRUST
2. HITRUST Expectations vs. Reality
3. A Quick Guide to Validated Assessments
4. Real-World HITRUST Implementation Recounts
5. Expert Takeaways


Ostendio is the first HITRUST readiness licensed team of experts with a dynamic GRC platform to power your HITRUST compliance.



Featured contributors:

HITRUST
Michael Parisi
VP of Adoption

Aprio
Powell Jones
Partner

 **A-LIGN**
Blaise Wabo
Healthcare &
Financial Services
Director

360ADVANCED
Chris Gudzak
Practice Director

 **wellth**
Alec Zopf
CTO and Co-Founder

Intro to HITRUST



FEATURED CONTRIBUTOR:

Michael Parisi

Vice President of Adoption, HITRUST

Michael has led over 500 controls-related engagements primarily in the healthcare and financial services industries. He has extensive experience with third-party assurance reporting including HITRUST readiness, HITRUST certification, SOC 1, SOC 2, SOC 3, Agreed Upon Procedure and customized AT-101 engagements.

A brief history on HITRUST

[HITRUST] started with a number of organizations coming together looking at security and compliance related activities and identifying that the processes were broken. There were a lot of duplicative efforts going on across these healthcare organizations, and they were looking for a better way to not only complete their audits, but to provide assurances more efficiently and more effectively.

This group came together and started HITRUST with the goal to help organizations manage risk, and at the same time, provide assurance over information, security, privacy, and then also cover compliance.

Today, HITRUST is not just for healthcare—we are industry agnostic.

There are a lot of new use cases focused on specific compliance initiatives where organizations are using HITRUST assurances to provide reliability and comfort over particular standards.

Exploring the origins of HITRUST i1 and r2 assessments

HITRUST was a one-trick pony for quite some time. We had the highest level of certification that we now refer to as the “r2”. At a point in time, that was the only HITRUST certification that organizations could obtain.

The market had been asking us for quite some time to have additional options available for organizations that still could result in a certification. When you think about the level of assurance and reliability, i1 is a lower level of assurance compared to the r2, but that’s okay. We introduced this concept of inherent risk, recognizing that all organizations aren’t created equal relative to



In 2023, HITRUST launched a third assessment, e1 (HITRUST Essentials) to help organizations show progress toward i1 or r2. The e1 Assessment is a 1-Year Validated Assessment that is beneficial to organizations who would like to get started with HITRUST by implementing foundational controls and allowing them to easily move into i1 or r2 assessments when ready.

the level of inherent risk that they introduce to their customers and stakeholders. That could be based upon what type of service offering they have or the size of that particular offering.

Recognizing that, we said we need to introduce this concept of a moderate assurance mechanism. When you look at the assurance mechanisms that exist within the marketplace today, we're talking about assessments—independently validated assessments that provide trust, reliability, and comfort to stakeholders. There was a big gap between an r2 and a SOC 2, and as we know, a SOC 2 is still probably the most widely-used assurance mechanism relative to information security.

We tried to provide an equivalent in the form of an i1. But that assurance mechanism gives you additional data points around program maturity, insight into fourth parties, and a lot of the elements that a SOC 2 will not give you. We had a lot of service providers in the marketplace where the r2 was kind of like killing a mosquito with a cannon.

So we said, how do we meet organizations where they are?

We introduced another assurance mechanism that's focused on good cybersecurity hygiene. The same standard civic controls are applicable to every shape, size, color, organization around a good information security program derived from NIST 801-71, not the full 853 (as we know that's really too big for a lot of organizations).

Again, the goal was to provide an additional option leveraging inherent risk methodology, aligning to more moderate size organizations, providing a stepping stone as they move along the assurance continuum to maybe get an r2 over a period of time, and being more industry-agnostic around information security program.



FEATURED CONTRIBUTOR:

Blaise Wabo

Healthcare & Financial Services
Director, A-LIGN

Blaise is the Healthcare and Financial Services Knowledge Leader at A-LIGN and has over 12 years of experience in Security Compliance and Risk Management. He joined A-LIGN in 2013 and started the HITRUST/HIPAA and Healthcare Services practice in 2015. Having a very unique background as a CPA, CISA and CCSK, Blaise has performed over 500 SOC attestation reviews and over 300 HITRUST/HIPAA assessments for Global 1000 and Fortune 500 clients in various industries.

How HITRUST supports scalable security

The CSF framework is reviewed and updated at least annually as well to address emergent threats and risks.

[HITRUST] is very different from most other standards out there that are typically reviewed every three years, or in some cases, five years or more. The two validated HITRUST assessments are risk-based, and are very comprehensive and scalable.

From a comprehensiveness standpoint, the CSF maps to over 40 standards out there. From a security and privacy perspective, it maps to the likes of ISO 27001, PCI, NIST, CMMC, GDPR, CCP... and the list goes on.

HITRUST CSF also offers a niche cybersecurity framework, certification and scorecard. HITRUST is the only body that offers a cybersecurity certification, and I think that's pretty unique as well from a scalable perspective.

Navigate HITRUST Compliance like a Pro: Looking for a HITRUST Readiness Licensee? Get the HITRUST cheat sheet to help you choose the right vendor.

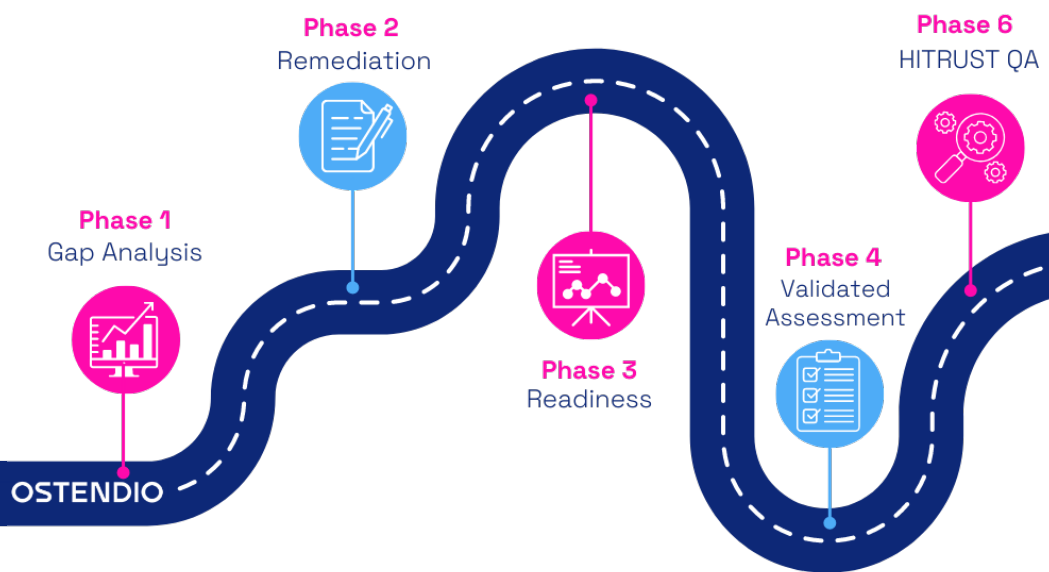
[Grab the cheat sheet](#)



What is the HITRUST CSF Certification Process?

The HITRUST certification process is built out in five phases over the course of 20-24 months:

- Phase 1: Gap Analysis
- Phase 2: Remediation
- Phase 3: Readiness
- Phase 4: Validated Assessment (e1, i1 or r2)
- Phase 5: HITRUST Quality Assurance



Ostendio helps you eliminate costs and save time on audits by mapping evidence across multiple frameworks.

80%

Time Savings on Audit Prep

150+

Built-In Security Frameworks

90+

Policy Templates

Ready to get
started
with HITRUST?

Review your security maturity with one of Ostendio's HITRUST Readiness Licensees.

[Chat with an expert](#)

HITRUST Expectations vs. Reality



FEATURED CONTRIBUTOR:

Powell Jones

Partner, Aprio

Powell is a Partner at Aprio, helping clients achieve sustainable information risk management, control costs and gain efficiencies in managing multiple compliance frameworks and requirements. Powell's specialties include SOC reporting, HITRUST CSF Certification, and third-party risk management.

Not your average audit “check box” exercise

The comprehensive nature of CSF is what makes HITRUST so unique. It's not a “check-the-box” exercise. People need to realize that, you can get a SOC 2 report, and it may have 60 or 70 controls in it—but that's more of a checkbox exercise than HITRUST is. When you look at the HITRUST r2 requirements for policy, procedure, and implementation, it drives a lot more time and preparation.

You have to address policy and procedure for each of the illustrated procedures, and implement controls for each of the requirement statements in scope. The i1 takes some complexity out by reducing some policy and procedure needs, limiting the set of requirement statements in scope, and reducing implementation needs for some controls. But it's not as high a level of assurance as the r2.

How much preparation time should an organization budget for HITRUST?

Companies need to realize that the HITRUST certification is extremely comprehensive, and there's no comparable certification in the marketplace. You need 10 to 18 months of preparation just to be ready for your certification, and then controls must operate for a minimum of three months before you can move to a validated assessment. The comprehensive nature, scope, and scale of CSF drive the preparation time and effort required for becoming HITRUST compliant.



FEATURED CONTRIBUTOR:

Michael Parisi

Vice President of Adoption, HITRUST

HITRUST is a high-level assurance security certification

Organizations are treating information security as if it's a compliance exercise. They don't equal each other.

We're seeing a commoditization of certain assurance mechanisms within the marketplace: "Get your SOC 2 in two weeks for \$10,000." You can automate evidence collection and compliance to a certain extent with configuration controls. But you can't replace the concept of reliability and independent validation.

What worries me with a lot of these platforms and organizations is what their customers or assessed entities are getting. It really isn't even worth the paper it's written on. We're seeing a movement in the stakeholder and related party space that's starting to identify that. We need higher levels of assurance. We all need to elevate and step our game up as it relates to the level of transparency we're getting relative to those business partners that we're working with.

The market will continue to correct itself. The general concept would be: buyer beware. Make sure you're making the appropriate investments in your information security program in providing assurances over that information security program because it's really that level of reliability that's going to differentiate you within the marketplace.



You can automate evidence collection and compliance to a certain extent with configuration controls. But you can't replace the concept of reliability and independent validation.

MICHAEL PARISI | HITRUST



FEATURED CONTRIBUTOR:

Chris Gudzak

Practice Director, 360 Advanced

Chris is a licensed CPA and holds multiple certifications including being a HITRUST Certified CSF Practitioner. His area of interests include building strong foundations of trust with his clients and mentoring colleagues who are new to the profession. His primary areas of expertise are SOC, risk management, HIPAA, data privacy, and incident response.

Maturity plays a key role in readiness

It all really starts at the prospect level with introductory conversations: Who are you, what's your goal? Why HITRUST? is always my first question. Then we start to navigate timelines for certification.

Then we typically ask:


- Do you need to find an external consulting partner?
- Do you have the internal resources?
- Do you understand the amount of time that it will take to build the program?
- Do you have the resources to maintain the program and continue to manage it?

Essentially, what HITRUST does on their QA, we do internally ourselves, [reviewing documents, checking the test plan, and ensuring controls have been implemented thoroughly] before it ever gets to HITRUST. We want to find the issues and correct them before it's ever presented to HITRUST. In the audit world, once you see something, you can't unsee it. So we want to make sure that we have everything that crosses the T's and dots the I's.

For those who have lofty goals and not much in place, we're happy to have the conversation. We discuss some steps that they're going to need to take before we revisit and push forward through the actual validation phases. The biggest factor of those prospects who are not ready, is extending that timeline. The pathway to certification is a lot longer. Prospects that have the program in place, and it's fairly robust, you're shortening that timeline to validation.

Find out how Ostendio helped Kinetik reduce effort and time on HITRUST by **50%**.

[Read Full Case Study](#)



A Quick Guide to Validated Assessments

FEATURED CONTRIBUTOR:

Powell Jones

Partner, Aprio

HITRUST i1 VS. R2

A Closer Look into Control Requirements

Grab your free eBook

for a deeper dive into the two most common HITRUST assessments to determine which one is right for you.

Created in partnership with



How to choose between i1 or r2

It's interesting when you compare i1 and r2. If you look at a small scope r2 assessment and compare that to the i1, I would typically recommend my client go ahead and do the r2 at that point because, when you're talking at the smaller scope, you're going to have the i1 anyway.

What we see in a lot of the requirement statements is that an r2 assessment pulls in a lot of the level one, two, and three requirements into a single requirement statement. There's a reason the r2 exists and the i1 is different. You can customize it based on your scope for an r2. It's going to assess your level of risk depending on how you answer those scoping questions. It will adjust for the requirement statements that come into scope for you based on that level of risk as opposed to the i1, which doesn't necessarily take into consideration what your individual level of risk is because you're not answering the scoping questions. It's the same scope for everybody.

When you're comparing them, if your scope is very small on an r2, it's probably not that much less effort for you to go ahead and focus on the r2 rather than the i1. However, if you were to scope out an r2 assessment and you're talking 450-500 requirement statements, certainly in that case, the i1 is going to be less effort than the r2.

The question really comes down to: what do you want to be able to put out in the marketplace?

What are you capable of achieving at this point in time? Depending on how mature your organization is in regards to risk and compliance, it may not make sense to go to r2 at this point if you're not ready for it. It might be easier to get the i1 in place and then move towards the r2 as you grow and mature as an organization.

HITRUST in Action



FEATURED CONTRIBUTOR:

Alec Zopf

CTO & Co-founder, Wellth

Alec is CTO and Co-Founder of digital health company, Wellth. Prior to co-founding Wellth, Alec built innovative medical device technology at Northwestern University, helped algorithmic trading firms stay competitive in expanding options markets, and built data infrastructure and teams at a SaaS analytics startup to take it from 8 to 25 employees and to a successful acquisition.

–

Wellth became HITRUST certified in 2022, leveraging the Ostendio platform along with Ostendio Professional Services and 360 Advanced auditor services

Startup POV: Preparing for HITRUST

[Our] HITRUST preparation began from some of the earliest days of adopting the Ostendio platform. We were focusing on not necessarily, how do we pass HITRUST, but how do we pass our customers' security assessments? How do we make sure that when they send us 100 or 200-question Excel documents, we know how to answer them and we have the policies and procedures to show them.

In the very early days, we were making sure we had the basics in place to say, yes, we are doing the onboarding, the offboarding, and the access control... encrypting systems in the right ways, both on our endpoints and in our cloud systems.

We started out actually using some of Ostendio's off the shelf policy templates, which was a great way for us to get started—and also just to understand what a maturity security program should look like. That was really helpful for us to be able to get to that place before we started HITRUST—can we demonstrate to our customers that we have a mature security program or at least a sufficient security program for the type of data that they're going to be giving us and the volume of data that they're going to be giving us.

Then, over the course of our company's history, we really started ingesting more types of data. As we've moved up through different population sizes, the different complexities of data, we've had to increase our security program with that. When we were getting ready for HITRUST, we were looking at our policies and procedures and saying, we do most of what's in those documents, but we're missing some crucial pieces. Some of the things don't apply to the way we run our business anymore now that we've grown and changed as a startup. So we decided to start from scratch.



We decided to align ourselves completely to the HITRUST framework and say, what are all the controls that we're going to be certifying? And how do we make sure we have policies and procedures that address all of the elements of each of those controls and align our policies and procedures around those controls themselves?

Having the Ostendio platform to manage all those changes and documents over time, and prove that we're reviewing them was very helpful. We were able to gradually increase employee security involvement and make sure that they're doing all the right things, too. Then, as we started working with the professional services arm of Ostendio, we were able to understand what HITRUST controls we needed to write to, and then actually write all those policies and procedures that are truly mapping to the structure of our organization and the types of tools we use and processes we follow.

FEATURED CONTRIBUTOR:

Chris Gudzak

Practice Director, 360 Advanced

What to expect from your HITRUST auditor

It's important to understand early on what you have in place and what the path looks like to get remediations done. That's a big lift. But then once we step in and engage with a client, we build out that project plan to include many different steps.

Really, it's a crash course to understand our client and their business, the industry, what the platform does, what type of data, where's the risk, and having a good understanding of that to refine our understanding of the scope, and then agree to that scope. It's very important to do in that first phase.

The product of that readiness workshop is to identify where we're expecting to use to support each of these requirements within the 19 domains, and start building out some of the overview documentation that we're going to need to supply as far as the description of the scope, and then identifying any gaps or anything that might need to be remediated. Once you get that third-party perspective, it will illuminate some things.



HITRUST

Is it right for you?

Grab your free eBook

to learn more about HITRUST, the steps to getting certified, and whether or not it's right for your organization.

That's the wrap on phase one, and then going into phase two, which is consultation-type services, but mainly it's taking action items, and remediating them. When you have questions and need our assistance, we're there. The majority of the questions were, how deep do we really have to look at this? Do we really need to go through to this n level to tie it out? The answer is yes. Sometimes it's thinking about how we can apply it to your particular environment. That was primarily the type of questions that we were fielding with Alec at Wellth.


At the conclusion of that remediation phase, it's in the form of a mock assessment—taking a random sample of requirements across the entire assessment and let's see how you're doing. If there are major red flags or lack of documentation to support certain things, we're going to have to delay the other phases of the engagement because it'll be set up for failure, and we would never want to get into something, do all the work, and put Alec through all the rigors of pulling documentation and stressing over certain things, and then ultimately not achieve certification—because that is the end goal.

Once we break out of that remediation phase, that's when we're heavy into the actual execution of that validation. We're going live. We've done all the work, built out the policy, process, and implementation for each requirement, but now we have to collect it so it's prove it. We're going through completing our testing and then sending it through our QA process.



We started out actually using some of Ostendio's off the shelf policy templates, which was a great way for us to get started—and also just to understand what a maturity security program should look like.

ALEC ZOPF | WELLTH



Expert Takeaways

FEATURED CONTRIBUTOR:

Blaise Wabo

Healthcare & Financial Services
Director, A-LIGN

Build trust into your security program

I think most organizations have to take a step back, and try to be proactive versus reactive. What I mean by that is to try to design a well-thought out cybersecurity program.

We live in a world today where in any product or service, if you want to add a new feature, you have to make it secure. That security helps your stakeholders gain trust. It helps your customers gain trust.

Without that trust, they will not buy your product. It's critically important for organizations to align with their board of directors and executives to understand that security should be part of the conversation. It's not a second thought. You don't design a product and then you think about security or privacy later.

FEATURED CONTRIBUTOR:

Alec Zopf

CTO & Co-founder, Wellth

Employ professional services early

One of the things that was high leverage for us was starting to work with a professional services partner. When it comes to HITRUST and understanding all the controls, as a security professional starting out, you don't know what you don't know. I would have brought in some professional services help a little bit earlier and done a little bit more.

Going through customer security assessments was like readiness assessments that we had gradually done along the way, but I probably would've done a HITRUST readiness assessment earlier on, too. That could have been really helpful. We reinvented the wheel a few times and put a lot of thought into our security program, which is great, but some of those things were a little off. Could we have had someone come in who really knew the best way to do that? Yes, probably. Getting some early nudges in the right direction would've been great. We got there towards the end with Ostendio's Professional Services and 360 Advanced's direction, but understanding HITRUST better earlier on could have been great.



FEATURED CONTRIBUTOR:

Michael Parisi

Vice President of Adoption, HITRUST

Balance low effort with maximum security

We don't subscribe to the idea of HITRUST over something else, which is one of the main reasons why within the framework, we have a very "arms-open" approach. We want to work with everyone, recognizing that there isn't a silver bullet when it comes to compliance or building an information security program.

We need to ensure that we can encompass all the different standards and frameworks, which is one of the things that makes HITRUST unique. Although we're positioning ourselves as it relates to the level of reliability from an assurance mechanism perspective, we like to work with everyone as it relates to the framework.

The idea is to assess once and report many.

We want to put organizations in the place where they can leverage a framework to adapt, implement and build their information security program. They are then in a position to pivot and produce whatever reporting is necessary through the vernacular or lens of the particular compliance standard or other framework that their stakeholders are asking them to provide assurances over.

When you look at SOC 2, for example, what's the process? We've been collaborating with the AICPA for several years now, which is why you'll find the Service Principles included as an authoritative source within the framework.

Organizations can use their HITRUST adoption and assessment-related efforts to spin up or produce a SOC 2 report if that's something that they still need to produce above and beyond a HITRUST certification.

Even if you never have to get a HITRUST certification, the value is really in adopting and leveraging the framework from a management tool perspective and then providing validated assurances. If you meet a minimum necessary score, then you can submit for certification. We advise our customers and stakeholders and partners to focus on using the value of the framework and using this concept of validated assurances.



Ostendio takes governance, risk and compliance to the next level to strengthen your business operations, supply chain, and everyone you rely on with continuous security. Maintain policies and procedures, simplify onboarding and offboarding, keep up-to-date training and track organizational compliance all in one platform—freeing up valuable time to focus on critical security tasks.

That's how we advise most of our organizations: don't start with the idea of certification, start with the idea of managing your information security program, and adapting it more efficiently

What is HITRUST CSF?

We've received many questions about my CSF throughout the years. What's important to highlight, is defining what my CSF is and what it isn't by design. It is an assessment platform meant to help organizations manage the assessment process, tailor and scope assessments based on risk, and manage the process hand in hand with assessor organizations.

The platform manages the assessment and its results, but it is not a GRC platform. It is not a management implementation or documentation collection platform. We have customers who ask why it doesn't do what their GRC does, but it's not designed to be that.

We're finally at a point from a maturity perspective to start working on more integrated partnerships, particularly with evidence ingestion. We've migrated everything onto Azure, which has helped us to build the API ecosystem. HITRUST myCSF is not meant to be a GRC or management tool, despite being the only assessment platform that produces targeted assessments, validated assessments, certifications, and compliance insight reports.



When it comes to HITRUST and understanding all the controls, as a security professional starting out, you don't know what you don't know. I would have brought in some professional services help a little bit earlier and done a little bit more.

ALEC ZOPF | WELLTH



Conclusion

Additional HITRUST Resources:

Click the links below for more HITRUST resources

- [Blog: HITRUST Is it right for you?](#)
- [Cheat Sheet: HITRUST Cheat Sheet 8 Questions to Ask Your Preparer](#)
- [Case Study: How Ostendio Helped Kinetik Reduce HITRUST Timeline by 50%](#)
- [Blog: Are you ready for HITRUST?](#)
- [Blog: Keep humans in the loop for HITRUST success](#)

Everyone Secure.

Welcome to the next generation of security.

Ostendio is the only risk management platform that leverages the strength of your greatest asset. Your people. With deep customization, advanced intelligence, and flexible controls, you're always audit-ready, always secure, and always able to take on what's next.

[Set up your free HITRUST consultation](#)

AICPA Authorized Licensee
for SOC 1®, SOC 2®, SOC 3®

HITRUST
Authorized Readiness Licensee