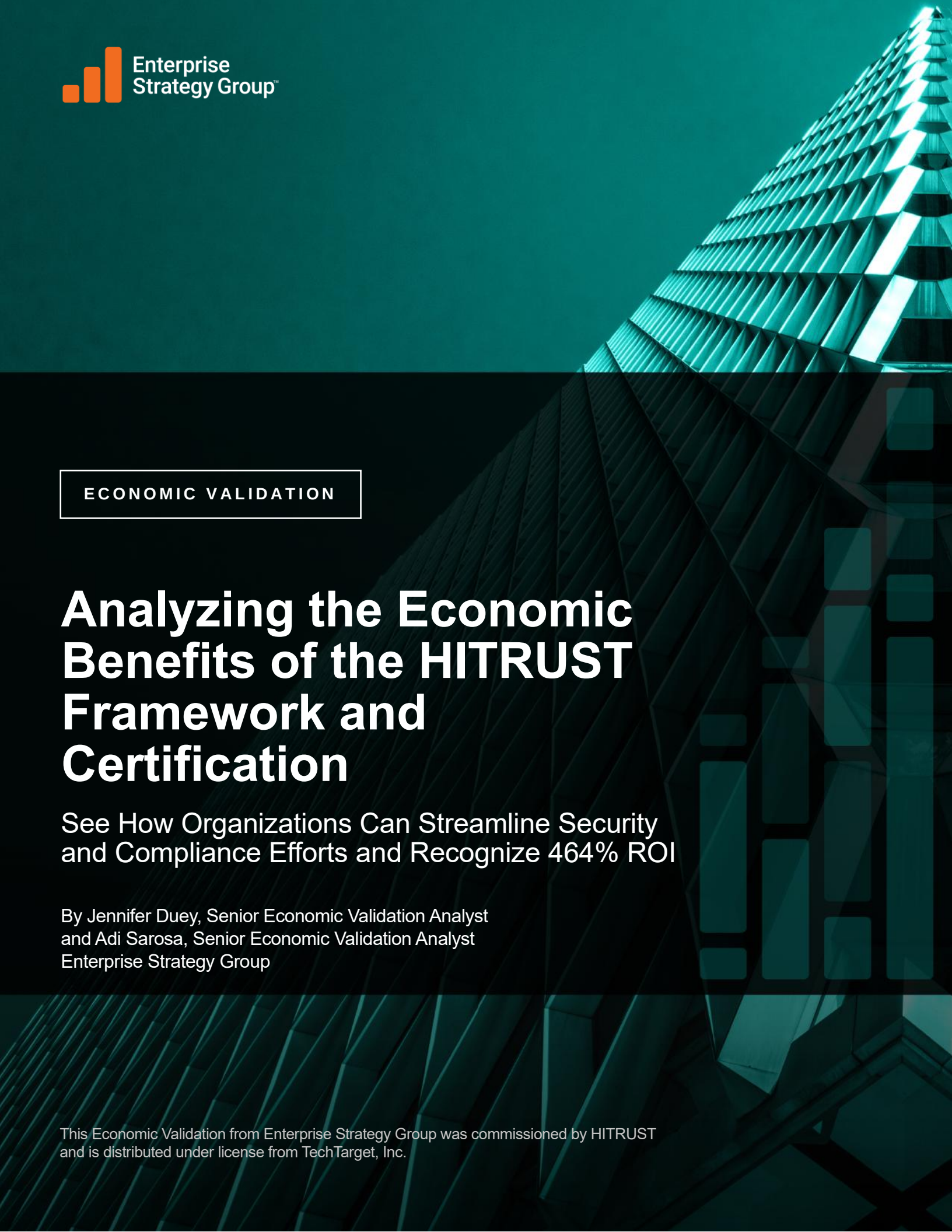


Enterprise Strategy Group™

ECONOMIC VALIDATION

Analyzing the Economic Benefits of the HITRUST Framework and Certification

See How Organizations Can Streamline Security and Compliance Efforts and Recognize 464% ROI

By Jennifer Duey, Senior Economic Validation Analyst
and Adi Sarosa, Senior Economic Validation Analyst
Enterprise Strategy Group

Contents

Enterprise Strategy Group Economic Validation: Key Findings Summary

Validated Benefits with HITRUST certification

464% Return on Investment (modeled)

Significantly lower risk of a security breach, non-compliance, and business disruption

63% increase in operational efficiency related to certification and audit activities

- **Impact business growth** by strengthening customer trust, accelerating procurement and renewal cycles, and supporting revenue retention in highly regulated industries. HITRUST certification serves as a credible, third-party validation of an organization's security posture, helping reduce sales friction, differentiate from competitors, and improve pipeline conversion.
- **Reducing risk** in today's evolving threat landscape requires more than a one-time compliance effort. HITRUST provides an actively maintained framework that helps them strengthen defenses, align with regulatory requirements, and minimize exposure to breaches and penalties. By implementing consistent controls, enforcing advanced access safeguards, and maintaining oversight across both internal operations and third-party relationships, organizations use HITRUST to take a proactive stance on risk management.
- **Increase operational efficiency** by leveraging both the prescriptive harmonization of controls across frameworks and detailed assessment of control maturity, enabling teams to reduce redundancy, align audit efforts, and streamline collaboration across compliance, security, and IT functions.

Introduction

This Economic Validation from Enterprise Strategy Group focused on the quantitative and qualitative benefits organizations can expect by using HITRUST's framework and certification to reduce their risk profile and ensure the highest levels of security risk management, rather than leveraging alternative assessment and assurance frameworks that are static or less comprehensive.

Challenges

As organizations continue through their digital transformation, both related to their internal operations and external interactions, having the right cyber and information security posture is paramount. Thus, to succeed in today's marketplace, organizations must find ways to demonstrate that they have implemented necessary robust security infrastructure and processes. In fact, some organizations demand proof of adequate security standards and posture before partnering with others or procuring services from vendors. Without the ability to quickly validate their security posture, organizations risk delayed or lost opportunities, resulting in real financial impact.

However, proving this level of security can be complex. Various parts of the business might require other certifications or assessments, each with its own scope and requirements. Over time, managing these parallel efforts becomes a significant and ongoing operational burden. Research from Enterprise Strategy Group showed that 21% of respondents identified the need to perform cybersecurity assessments regularly to be one of the most challenging risk management activities for their organization, followed by managing identities, access policies, entitlements, etc. (20%) and integrating data from multiple systems to get a comprehensive view of cyber-risks (18%).[1]

Figure 1. Top 5 Most Challenging Risk Management Activities

Source: Enterprise Strategy Group, now part of Omdia

According to Enterprise Strategy Research, 65% of organizations believe cyber-risk management to be more difficult than it was two years ago. To that end, organizations are increasingly looking for ways to provide credible assurances to stakeholders, whether leadership, partners, or customers, that they are taking meaningful steps to

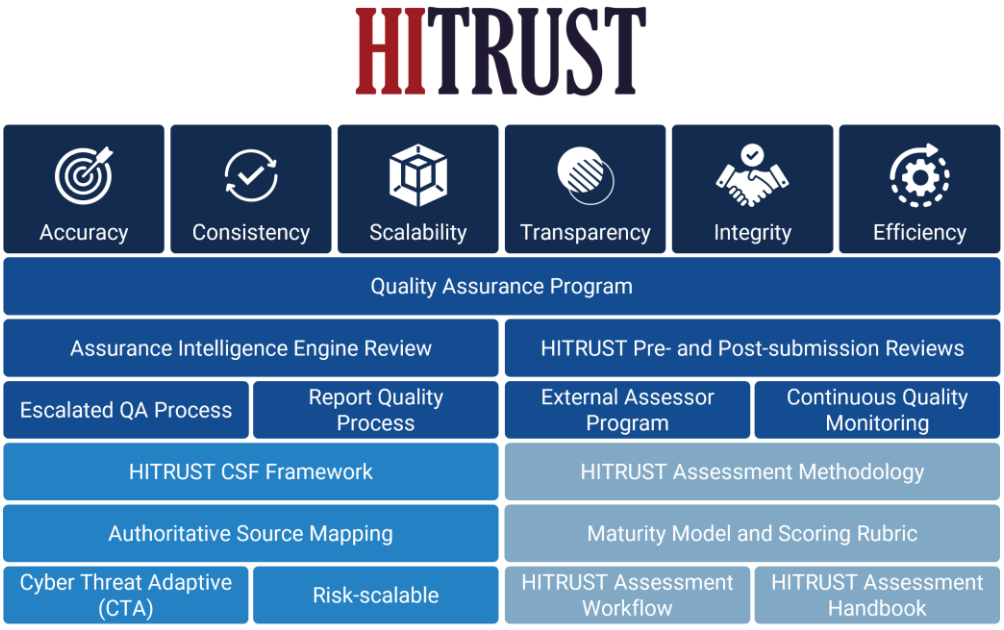
[1] Source: Enterprise Strategy Group Research Report, *Cyber-risk Management Best Practices*, December 2024. All Enterprise Strategy Group research references and charts in this Economic Validation are from this report.

protect sensitive information and manage risk effectively. Organizations need a recognizable, trusted validation that demonstrates their security posture has been independently assessed and continues to evolve in step with the modern threat landscape. At the same time, organizations are seeking comprehensive programs that eliminate the need to pursue multiple, time-consuming individual certifications, freeing up valuable resources for more strategic initiatives.

The Solution: HITRUST Framework and Certification

HITRUST, the leader in enterprise risk management, information security, and compliance assurances, offers a certification system for the application and validation of security, privacy, and AI controls, informed by over 60 standards and frameworks. The company's threat-adaptive approach delivers the most relevant and reliable solution, including multiple selectable and traversable control sets, over 100 independent assessment firms, centralized quality reviews and certification, and a powerful SaaS platform enabling its program and ecosystem. For over 17 years, HITRUST has led the assurance industry and, today, is widely recognized as the most trusted solution to establish, maintain, and demonstrate security capabilities for risk management and compliance.

Figure 2. HITRUST Framework and Certification



Source: Enterprise Strategy Group, now part of Omdia

Enterprise Strategy Group Economic Validation

Enterprise Strategy Group completed a quantitative economic analysis of HITRUST's framework and certification. Our process is a proven method for understanding, validating, quantifying, and modeling a product or solution's value propositions. The process leverages Enterprise Strategy Group's core competencies in market and industry analysis, forward-looking research, and technical/economic validation.

Enterprise Strategy Group conducted in-depth interviews with end users to better understand and quantify how the HITRUST framework and certification has impacted their organization, particularly when compared to alternative assessments that are not as robust. We conducted a comprehensive evaluation encompassing vendor-generated technical documentation, established case studies, independent analyses, and our team's expert insights into the

industry, markets, and alternative technologies. The qualitative and quantitative data were then used for a simple economic analysis comparing the costs and benefits of implementing HITRUST's framework and certification.

HITRUST Framework and Certification Economic Overview

Enterprise Strategy Group's economic analysis of the HITRUST framework and certification validated that it provided its customers with significant savings and benefits in the following categories:

- **Business growth.** The framework demonstrates a credible, third-party validated security posture that builds customer trust, reduces sales friction, and strengthens competitive differentiation. It helps organizations retain and expand client relationships, accelerate procurement cycles, and convert more opportunities into long-term revenue.
- **Reduced risk.** By enforcing consistent, up-to-date security controls and extending them to vendors and subsidiaries, organizations minimize the risk of breaches, compliance violations, and costly penalties, and might qualify for lower cyber insurance premiums.
- **Operational efficiency.** Through reusable documentation, coordinated audit efforts, and improved cross-team collaboration, organizations streamline compliance tasks, reduce manual effort, shorten certification timelines, and strengthen their cyber-risk profile for insurers.

Business Growth

Prioritizing HITRUST framework and certification helps organizations across all industries meet the rising expectations for security and compliance especially in highly regulated sectors such as the healthcare and financial services industries. This proactive approach enables organizations to retain key customers, satisfy third-party risk requirements, and accelerate procurement and renewal processes. HITRUST strengthens these efforts by providing a standardized, independently validated framework that demonstrates a mature security posture. Organizations strengthen their market position and drive growth when they simplify vendor assessment frameworks and minimize redundant audits. This approach improves efficiency and builds stakeholder trust. As one customer put it, **"We've doubled our revenue since getting HITRUST certified; it's really driven a lot of growth for us."** Customers reported savings and benefits in the following categories:

- **Strengthened customer trust.** As customer expectations for data protection grow and regulatory demands intensify, HITRUST framework and certification helps organizations strengthen trust by demonstrating a validated, industry-recognized commitment to security and compliance. For healthcare organizations and others handling sensitive data, HITRUST is widely regarded as the gold standard, offering assurance that systems and processes have undergone a rigorous, standardized audit. Customers increasingly require HITRUST certification in RFPs, recognizing it as a critical indicator of security maturity and a key factor in vendor selection. Organizations with HITRUST framework and certification reported fewer breaches compared to industry averages, reinforcing customer confidence in the safety of their data. One customer noted that clients specifically expressed comfort using their solutions, citing HITRUST as a decisive factor in trusting the company's environment and capabilities.

> **"HITRUST certification has become the Gold Standard; without it, expanding into regulated markets or competing for certain contracts simply isn't possible."**

- **Accelerated procurement and renewal cycles.** By satisfying third-party risk assessment requirements and offering a recognized benchmark for security, HITRUST framework and certification helps organizations accelerate procurement and renewal cycles. While many customers still require security questionnaires, HITRUST provides a trusted foundation that reduces the need for additional validation or follow-up, helping

buyers feel more confident in moving forward. One customer shared that a prospective client initially planned to conduct a full audit of their product, but accepted HITRUST certification in its place, significantly speeding up the deal. Another customer emphasized how HITRUST has become an essential asset in their sales process, especially in healthcare, where clients increasingly expect this certification as a standard requirement. In highly regulated markets, HITRUST signals credibility, maturity, and alignment with industry expectations, helping organizations build trust and reduce friction in the buying process.

- **Revenue growth and market differentiation.** As security and compliance expectations continue to rise, organizations need trusted frameworks to support revenue retention and expansion within tightly controlled industries. HITRUST framework and certification addresses this need by providing a recognized and standardized approach to demonstrating strong security and compliance practices, which helps organizations meet client requirements and maintain existing relationships. Customers shared that HITRUST certification gives their clients greater confidence in continuing business, especially when contracts come up for renewal or competitive alternatives are being considered. By reducing uncertainty around data protection and regulatory alignment, HITRUST helps organizations defend their market position, expand within key accounts, and avoid revenue risk tied to compliance concerns. The certification serves as a credible third-party assurance, helping organizations distinguish their offerings from competitors' and reducing concerns about data protection during the sales process. By addressing security questions early and with confidence, organizations can reduce sales friction, increase client engagement, and improve pipeline conversion rates.

> **"I see HITRUST as a growth enabler. It plays a critical role in expanding business with existing clients and staying competitive in regulated markets. Without it, we'd likely spend far more time navigating RFPs or risk losing opportunities where HITRUST is a client requirement."**

Reduced Risk

Reducing organizational risk requires a consistent, well-defined approach to security and compliance, especially in industries like healthcare and financial services where the stakes are high. HITRUST framework and certification provide a comprehensive, prescriptive framework that helps organizations identify gaps, enforce controls, and align with evolving regulatory standards. Customers reported that having HITRUST in place gave them greater confidence in their ability to withstand audits, avoid compliance violations, and reduce the likelihood of breaches. With fewer uncertainties around security readiness, organizations not only lower their exposure to legal and financial penalties but also protect their reputation and ensure operational continuity. Customers reported savings and benefits in the following categories:

- **Comprehensive risk management.** Comprehensive risk management requires organizations to actively secure their environments and reduce vulnerabilities across both internal operations and external partnerships. Many organizations use the HITRUST framework to apply consistent, rigorous controls when onboarding new subsidiaries or managing third-party vendors. One customer explained that they now incorporate HITRUST controls during subsidiary onboarding to ensure security alignment from day one, even if a full certification isn't pursued. For vendor management, organizations require high-risk partners, particularly those with access to personally identifiable information (PII), to provide either a SOC 2 or HITRUST assessment, with a clear preference for

> **"HITRUST gives you a much deeper view into the controls needed to strengthen security across your organization. It's based on NIST but goes further, and it's in high demand, especially in healthcare and increasingly in other industries, too."**

HITRUST due to its depth. When risk levels are especially high, HITRUST certification becomes a specific requirement, as it has proven to significantly reduce the chance of breaches through third-party access.

"With so many compliance requirements now, HITRUST helps us stay on track and avoid fines. It keeps us focused on the right controls, like access and asset monitoring, so we don't miss anything that could put us at risk."

- **Holistic regulatory compliance.** Holistic regulatory compliance is essential for organizations operating under federal and state regulations, where failure to meet requirements can result in serious financial and operational consequences. Noncompliance with Medicaid and Medicare requirements, for example, ranging from data protection to service delivery, can lead to liquidated damages and fines from both state agencies and managed care organizations. Organizations must monitor everything from user access and external network connections to hardware ownership and facility-level infrastructure to stay ahead of increasing scrutiny. HITRUST plays a key role in identifying security gaps and establishing controls that help avoid penalties tied to noncompliance or data breaches. Customers told us during interviews that, by aligning with HITRUST's comprehensive framework, they not only protect sensitive member information but also reduce their liability and financial exposure. Repeated fines can severely limit growth and put operations at risk, making structured compliance efforts not just a regulatory necessity but a business imperative.

"I really believe HITRUST adds an extra layer of protection. It strengthens our network boundaries and helps reduce the surface area for potential attacks."

- **Stronger security posture.** A stronger security posture requires more than periodic compliance checks; it demands a continuous, structured approach to risk management and threat mitigation. HITRUST supports this by requiring regular updates to security controls and ongoing validation across a broad set of domains, ensuring that organizations actively adapt to evolving risks. One customer we spoke to described how they aligned their security programs with HITRUST's 19 assessment domains by organizing their efforts into four key focus areas: protection, defense, response, and recovery. Within the protection domain, for example, they implement identity and access management practices that extend beyond basic login credentials, including single sign-on, two-factor authentication, and VPN access for sensitive systems, all in alignment with HITRUST's access control requirements. This approach helped them maintain a proactive security stance by embedding modern controls into everyday operations, not only strengthening defenses against internal and external threats but also keeping security practices relevant and resilient as risks evolve.
- **Strengthened risk posture and enhancing insurability.** By enforcing standardized, up-to-date security controls across internal systems, vendors, and third parties, HITRUST helps organizations reduce their exposure to data breaches, regulatory violations, and associated penalties. This stronger risk posture not only minimizes the likelihood and severity of incidents but also improves an organization's insurability. Many insurers recognize HITRUST certification as evidence of mature cybersecurity practices, which can lead to lower premiums and more favorable policy terms. These avoided costs contribute directly to the overall risk-adjusted return on investment.

Operational Efficiency

Increasing operational efficiency remains a top priority for organizations navigating complex and overlapping compliance requirements. HITRUST supports this goal by providing a structured approach that helps teams reduce redundancy, improve coordination, and optimize the use of internal resources. Organizations save time and effort not only by reusing the evidence, control mappings, and assessment artifacts developed through HITRUST, but also by streamlining audit preparation and eliminating duplicated effort through consistent, prescriptive guidance.

The HITRUST framework also drives more effective collaboration between compliance, security, IT, and operations teams, ensuring that responsibilities are aligned and processes are well-coordinated. Customers reported savings and benefits in the following categories:

- **Streamlined compliance management.** Streamlined compliance management is increasingly important as organizations face growing demands from overlapping regulatory frameworks. HITRUST offers a comprehensive and prescriptive framework that maps to regulatory requirements like HIPAA, attestation frameworks such as SOC 2, and certifiable standards including NIST, and ISO 27001, enabling organizations to address multiple compliance requirements through a single, unified approach. The HITRUST framework helps organizations organize and align their compliance activities more effectively, making it easier to demonstrate adherence to other standards. By building around the HITRUST framework, customers were able to create a centralized and repeatable approach that improves consistency and reduces fragmentation across compliance initiatives. This structured methodology ensures that compliance requirements are met systematically while minimizing redundancy in documentation and processes.

- **Reduced audit preparation time.** Preparing for audits traditionally requires significant manual effort, especially when responding to multiple regulatory bodies with similar but non-identical requirements. Customers we spoke to stated that the documentation and controls developed during the HITRUST process enable them to streamline related audits and certifications significantly. The comprehensive nature of HITRUST documentation often covers overlapping requirements for other certifications, leading to reduced assessment fees and accelerated timelines. Customers noted that, by aligning HITRUST with other initiatives, such as SOC 2 attestations, they were able to reduce the overall audit preparation time by 30%. This coordination reduces redundant work, eases the burden on internal teams, and enables a more efficient path to demonstrating compliance across multiple frameworks.

> **"The evidence I gather for HITRUST gets me about 80% of the way through HIPAA, at least 60% for PCI and SOC2, maybe more."**

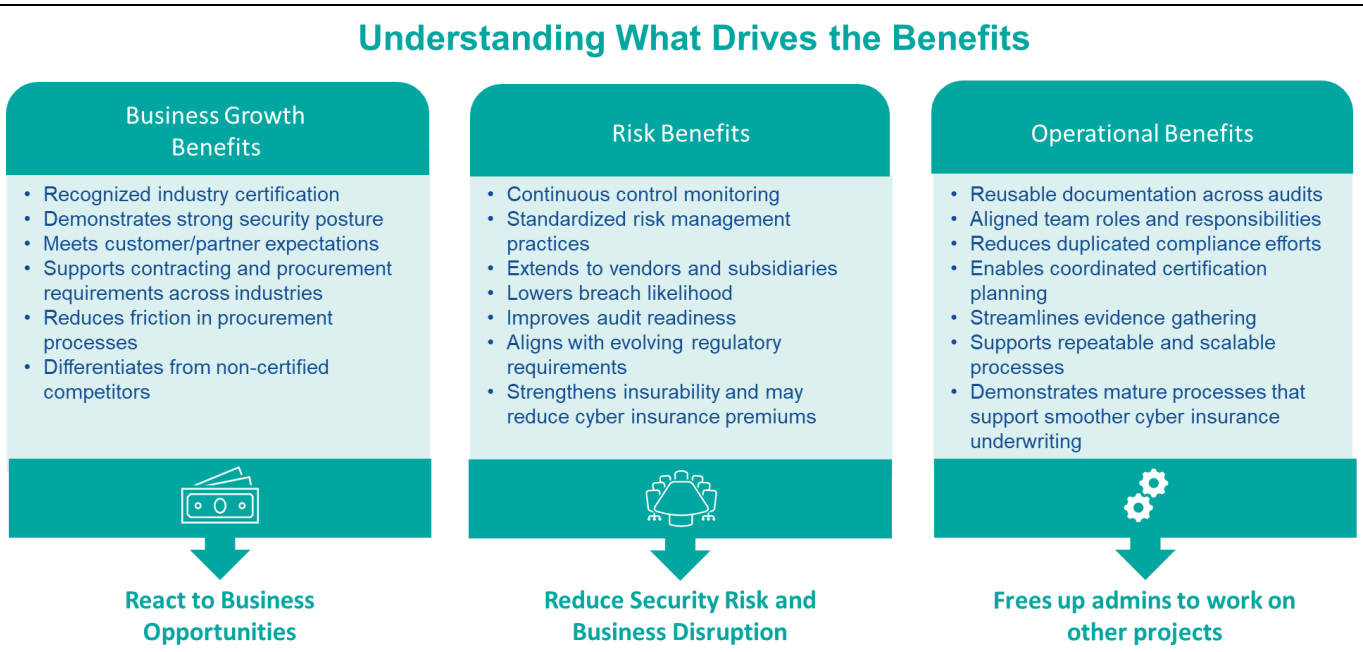
- **Improved cross-team coordination.** HITRUST assessments promote stronger collaboration by providing teams with a common framework and shared security language. The framework helps to align roles and responsibilities across security, compliance, IT, and operations teams, effectively breaking down organizational silos and streamlining workflows. Teams coordinate more effectively through joint planning, shared documentation, and regular cross-functional communication. This integrated approach fosters collective ownership of security and compliance goals, encouraging knowledge sharing and reducing duplicate efforts across departments. By embedding security and compliance into daily operations, organizations can support continuous improvement and ensure long-term program sustainability. The framework's structured approach helps teams work together more efficiently, leading to better resource utilization and more effective program management.

> **"HITRUST has definitely helped improve collaboration across security, compliance, and operations. It gets everyone aligned around the same goals."**

- **Streamlined compliance and insurance incentives.** HITRUST enhances operational efficiency by aligning compliance activities across multiple frameworks through reusable documentation, coordinated audit cycles, and improved collaboration between security, compliance, and IT teams. This consolidation significantly reduces the time and manual effort required to meet diverse regulatory obligations. Additionally, by streamlining security governance and demonstrating a proactive compliance posture, organizations could benefit from

lower cyber insurance premiums, reflecting insurers' confidence in their reduced risk profile and strong internal controls.

Figure 3. Unlocking the Value Drivers



Source: Enterprise Strategy Group, now part of Omdia

Enterprise Strategy Group Analysis

Enterprise Strategy Group leveraged the information collected through vendor-provided material, public and industry knowledge of economics and technologies, and the results of customer interviews to create a return on investment (ROI) model that compares the costs and benefits of implementing HITRUST's framework and certification. Our interviews with customers who have this framework and certification, combined with experience and expertise in economic modeling and technical validation of HITRUST framework and certification helped to form the basis for our modeled scenario.

Enterprise Strategy Group developed a financial model to evaluate the potential costs and benefits associated with using HITRUST's framework and certification compared to alternative, less comprehensive compliance and security certification frameworks. The model is based on a representative scenario involving a midsize organization with the following characteristics: $20 million in annual revenue, 100,000 PII records under management, five administrators supporting the framework, certification, and audit activities, a $5 million cybersecurity insurance policy, and a HITRUST r2 certification with a count of 50 systems or assets.

Why This Matters

Managing multiple compliance frameworks and security requirements independently creates significant operational overhead, redundant work, and increased risk of gaps or inconsistencies.

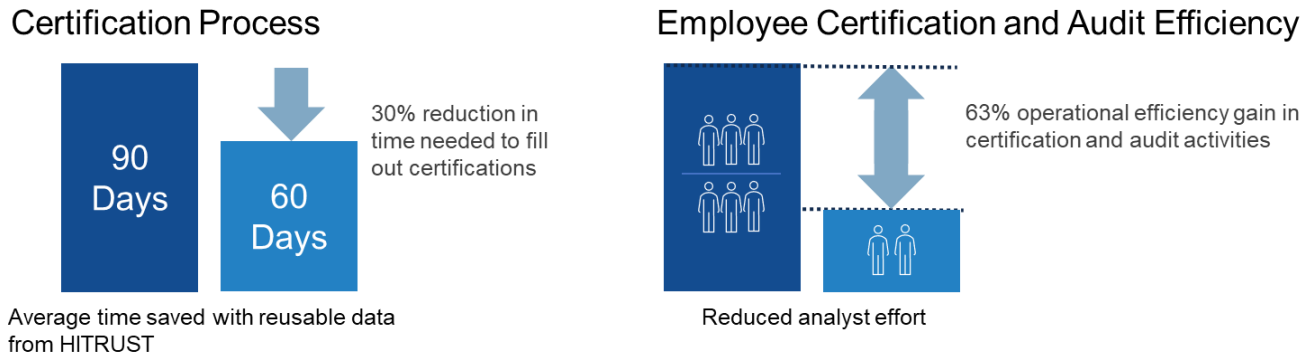
HITRUST framework and certification provides a unified, comprehensive framework that streamlines compliance efforts, reduces duplicate work, and delivers a structured approach to security that can be leveraged across multiple regulatory requirements and business objectives.

Operational Efficiency

We based our model on insights from interviews with customers who have implemented HITRUST's framework and certification. These customers emphasized the operational advantages of HITRUST's structured, rigorous approach, particularly the ability to repurpose its comprehensive documentation across multiple frameworks such as HIPAA, SOC 2 attestations, and NIST and ISO 27001 certifiable standards. This reuse reduced redundant effort and enabled faster certification timelines. Customers reported saving approximately 30% in preparation time per audit cycle, cutting the process from 90 days to 60.

Customers also shared that HITRUST's acceptance by external clients often eliminates the need for additional product-specific audits, further reducing the burden on internal teams. When combining the time saved from accelerated certification efforts and avoided audits, Enterprise Strategy Group calculated a 63% increase in operational efficiency related to certification and audit activities (see Figure 4).

Figure 4. Operational Efficiency

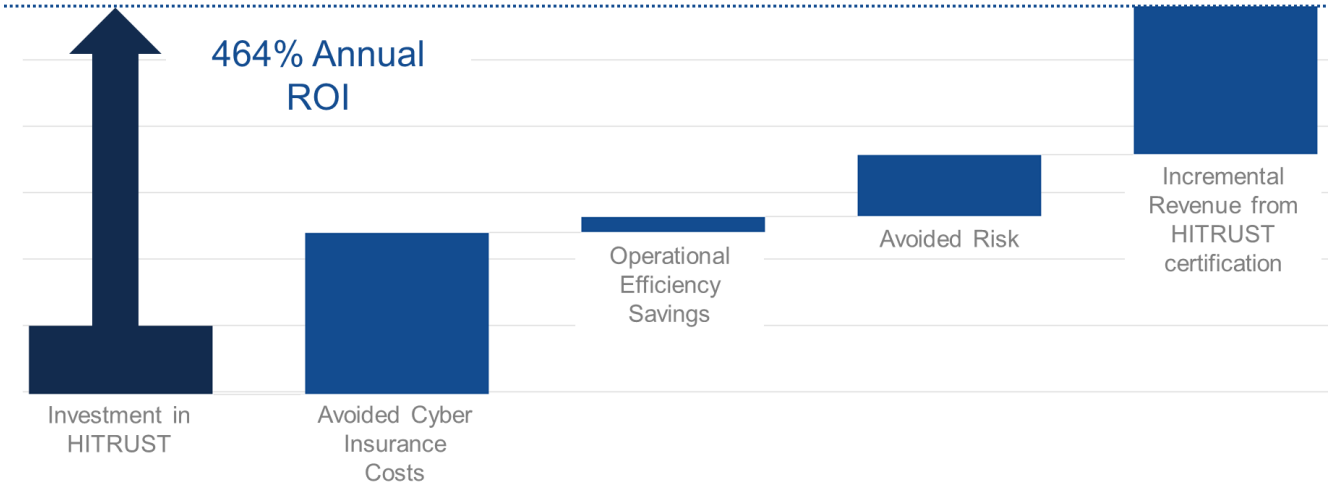


Source: Enterprise Strategy Group, now part of Omdia

Calculating the ROI

Enterprise Strategy Group conducted a comprehensive analysis to calculate ROI, leveraging proprietary financial models, industry-standard methodologies, and customer-reported data. The analysis applied conservative assumptions to assess the total cost of achieving HITRUST certification, including direct certification expenses and avoided costs. It also quantified a range of potential benefits, such as improved operational efficiency, reduced risk from fewer security breaches, enhanced regulatory compliance, minimized downtime, and incremental revenue opportunities driven by HITRUST certification. By capturing both cost savings and strategic value, the model provides a holistic view of HITRUST's overall economic impact. Based on this approach, Enterprise Strategy Group estimates a 464% ROI for organizations that adopt the HITRUST certification framework (see Figure 5).

Figure 5. Return on Investment



Source: Enterprise Strategy Group, now part of Omdia

What the Numbers Mean

Investment in HITRUST

The investment in HITRUST includes several key cost components that were considered in the ROI analysis. These include the initial certification fees, assessor costs for performing the validated assessment, and fees associated with application submission and scoring through HITRUST. In addition, we factored in internal labor costs related to preparing for the assessment, such as time spent by compliance, security, and administrative personnel to gather documentation, coordinate responses, and support the evaluation process. Together, these elements represent the total upfront and operational investment required to obtain and maintain HITRUST certification.

Avoided Cyber Insurance Costs

The ROI model accounts for avoided costs tied to discounted cyber insurance premiums available to organizations with valid HITRUST certifications. Based on program guidelines, these organizations receive a 25% reduction off standard premium rates, applied as a starting credit during the underwriting process. For this analysis, we assumed an average baseline premium of $65,000 and an r2 assessment with 50 systems or assets. Applying the 25% discount to that premium resulted in direct cost savings, which was factored into the overall ROI calculation. In addition to the premium reduction, HITRUST-certified organizations benefit from a faster, more streamlined underwriting process, as well as simplified renewals, a single-page exclusion model, access to cyber insurance limits exceeding $10 million, and enhanced terms and conditions. These advantages not only lower annual insurance costs but also improve coverage quality and administrative efficiency.

Operational Efficiency Savings

To reflect the operational impact of HITRUST, the ROI model includes measurable time and labor savings achieved through more streamlined framework, certification, and audit processes. Customers reported that HITRUST's structured approach enabled them to reuse documentation across frameworks, minimizing duplication and reducing the effort required for additional assessments. Many also noted that clients often accepted HITRUST certification in place of conducting separate audits, further easing internal workload. For this analysis, we assumed a team of five administrators with an average salary of $120,000, each dedicating 15% of their time to certification activities. Based on observed efficiencies, including reduced preparation timelines and audit avoidance, these organizations

achieved a 63% improvement in operational efficiency, which was captured in the model as a reduction in internal resource costs over time.

Risk Avoidance

The ROI model incorporates the value of avoided risk across three primary dimensions: reduced breach-related costs, minimized regulatory penalties, and avoided downtime. For this analysis, we modeled an organization with 100,000 PII records, applying a per-record cost of $179 based on industry benchmarks.[2] To provide both specific and aggregate perspectives on breach costs, we reference the IBM and Ponemon Institute's finding that healthcare data breaches average $9.77 million in cost.[3] These high costs are driven by the sensitive nature of protected health information, the need for uninterrupted care delivery, and the sector's stringent regulatory environment.

To show the potential savings of proactive risk management, we compared breach scenarios involving only basic security controls with those using comprehensive frameworks like HITRUST certification. HITRUST demonstrates due diligence in compliance efforts and can significantly reduce an organization's risk exposure. This becomes especially important in the context of HIPAA regulations, for example, where violations can trigger fines ranging from $100 to $50,000 per incident, with annual caps of $1.5 million for repeat offenses.[4] Regulators calculate these penalties based on factors such as the number of individuals affected, the severity of negligence, and any history of ongoing noncompliance.

To account for operational disruptions, the model includes the cost of unplanned downtime. In the healthcare sector, these costs vary widely depending on the size of the organization, the nature of the incident, and whether the setting is a clinic or a hospital. Industry estimates range from hundreds to thousands of dollars per minute, with some incidents costing well into the millions. For this analysis, we used a benchmark of $9,000 per minute over a 60-minute outage, assuming one such event per year.[5] We then applied a conservative estimate of a 10% reduction in downtime based on HITRUST's enhanced security controls and improved incident response readiness compared to a typical security baseline.

HITRUST certification delivers comprehensive benefits beyond direct financial savings. In healthcare settings, downtime causes cascading disruptions, delayed patient check-ins, blocked EHR access, compromised data, and disrupted imaging services, all impacting productivity, recovery costs, and patient trust. By strengthening security posture and operational resilience, HITRUST reduces breach likelihood, lowers per-incident costs, strengthens legal defense against negligence claims, and minimizes regulatory penalties. These conservative estimates likely understate actual savings, which might include mitigated reputational damage, improved customer retention, and reduced legal and insurance expenses. The ROI model treats these avoided risks as cost offsets, reflecting HITRUST's role in enhancing organizational resilience and protecting both financial and clinical operations.

Incremental Revenue from HITRUST Certification

The ROI model includes revenue impact as a key benefit of HITRUST certification, based on both direct and indirect business gains reported by customers. During interviews, customers consistently stated that HITRUST certification positively influenced a substantial portion of their revenue, some attributing as much as 50% of their annual revenue to the ability to meet HITRUST requirements. For this analysis, we modeled an organization with $20 million in annual revenue and applied this insight to quantify the incremental revenue contribution. Direct revenue impacts included winning new business where HITRUST was a mandatory requirement, securing contract renewals that were contingent on certification, and successfully responding to RFPs that required HITRUST as a baseline qualification. Indirect revenue gains included faster sales cycles due to pre-validated security posture, competitive differentiation in regulated industries, and the ability to command premium pricing in certain contracts.

---

[2] Source: "Cost of a Data Breach Report 2024," IBM Security, 2024.
[3] Ibid.
[4] Source: "HIPAA Violations & Enforcement," American Medical Association, 2025.
[5] Source: David Flower, "The True Cost Of Downtime (And How To Avoid It)," Forbes.com, 2024.

These combined revenue impacts were incorporated into the ROI model to reflect HITRUST's strategic value beyond compliance and risk mitigation.

Issues to Consider

Enterprise Strategy Group's models are built in good faith upon conservative, credible, and validated assumptions; however, no single modeled scenario will ever represent every potential environment. The benefits received by an organization depend on the size of the organization, the nature of the business, and the capabilities of the current product or service being used, along with many more variables. Enterprise Strategy Group recommends that you perform your own analysis of available certifications and frameworks and consult with a HITRUST representative to understand and discuss the differences between certifications through your own proof-of-concept testing.

Conclusion

As organizations face increasing regulatory requirements and security risks, a structured and repeatable approach to compliance and risk management has become essential. HITRUST provides a comprehensive framework that supports alignment with multiple standards, while enabling operational improvements and reducing exposure to regulatory penalties and breach-related costs.

Enterprise Strategy Group's analysis found that HITRUST certification contributes to measurable financial benefits, including improved efficiency in audit and certification processes, lower risk-related costs, and increased revenue tied to client requirements and procurement eligibility. With a modeled ROI of 464%, the data suggests that HITRUST can provide both operational and financial value to organizations seeking to strengthen their security and compliance programs.

Beyond the quantifiable benefits, HITRUST certification positions organizations for long-term success in an evolving regulatory landscape. As compliance requirements continue to expand and cyberthreats grow more sophisticated, the value of a unified, comprehensive approach to security and compliance will likely increase. Organizations that invest in HITRUST certification today are not just addressing current needs but building a foundation for sustainable risk, security, and compliance management that can adapt to future challenges.

If your organization is looking to improve compliance readiness, reduce risk exposure, and streamline certification efforts across multiple frameworks, Enterprise Strategy Group recommends evaluating whether HITRUST certification aligns with your organization's security, regulatory, and operational objectives.

About Enterprise Strategy Group
Enterprise Strategy Group, now part of Omdia, provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

contact@esg-global.com
www.esg-global.com