HITRUST®

Improving Information Risk Management and Assurance in a Cyber World

August 2019

Executive Summary

As regulatory expectations increase the minimum standard of care, organizations face a growing need to seek better and more efficient methods to evaluate and mitigate risk associated with safeguarding sensitive information; they also know this risk extends beyond their own environment to include service providers and other third parties. As a result, some organizations have turned to security scorecard or reputational assessment services in an attempt to gain quick visibility into their third parties' information security posture; however, such methods have limited utility as they are based on circumstantial rather than direct evidence of the actual state of information protection.

Assessing the maturity of an organization's information protection program, including the status of its information security policies, procedures, and implementation of controls, continues to be the gold standard of assurance and the only legitimate method of measure for an information risk profile, specifically because it is based on direct rather than circumstantial evidence. Such assessments, when done by leveraging a comprehensive and consistently applied methodology, are far more likely to be indicative of the actual level of protection an organization affords to sensitive information and subsequently their level of residual risk.

Further, the more mature an organization's information protection program, specifically whether their information security controls have reached a maturity level where they demonstrate proficiency of operation, management, and reporting, (1) the more likely an organization is to continue to operate those controls in a similar manner into the future, (2) the less likely that the organization will suffer a breach, and (3) the more likely the organization will be able to contain and minimize the impact of a breach, should one occur.

Further still, organizations who implement a robust information security continuous monitoring (ISCM) program to continually assess the state of their information security controls not only achieve higher levels of maturity but also make better and more timely risk-based decisions. Additional benefits of this type of monitoring include:

- On-demand, near real-time insight into organizational security and compliance risk posture
- Better prioritization of remediation activities
- More consistent adoption of best practices
- A higher level of assurance, both now and in the future

Ongoing certification (OC) of an organization's information protection program based on a continuous monitoring approach provides numerous efficiencies and cost benefits as well, including:

- Longer periods between comprehensive control gap assessments
- Reduced time and effort needed to maintain certification
- Reduced lifecycle costs for maintaining certification
- Higher levels of assurance and trust with and amongst external stakeholders such as regulators, business partners, and customers.

Based on the evidence in support of implementing ISCM and OC programs, specifically that organizations with mature information security controls pose less information risk and will likely operate those controls in a similar manner in future, HITRUST is establishing the HITRUST CSF Ongoing Certification Program.

Coupling ISCM and OC with the consistency and integrity of the HITRUST CSF Assurance Program will allow the findings in the CSF Assessment Report to be truly prospective, basing its foresight on evidence rather than anecdotal or circumstantial information.

Organizations that are already achieving high maturity scores for ‘measured’ and ‘managed’ will likely have little additional work to qualify their internal programs for the HITRUST CSF Ongoing Certification Program beyond addressing ISCM program-related control requirements in the HITRUST CSF.

Organizations that do not have viable metrics in place and subsequently do not score well for the ‘measured’ and ‘managed’ levels of maturity can and should draft an ISCM program strategy, develop corrective action plans (CAPs), and begin implementing both the strategy and CAPs.

The HITRUST Alliance is the only standards development organization (SDO) which provides all the elements needed for an effective and efficient ongoing privacy and security certification program. Primary elements of the HITRUST Approach include the HITRUST CSF, a comprehensive yet highly tailorable privacy and security control framework, and the HITRUST CSF Assurance Program, a robust approach to independent privacy and security assessment and certification.

The HITRUST Approach also includes numerous other products, services, and tools as part of a complete security and privacy risk and compliance ‘ecosystem’ designed to help organizations implement, assess, certify, and share assurances about their information protection programs. Examples include the HITRUST Threat Catalogue, the HITRUST MyCSF, the HITRUST Assessment XChange, and the Risk Triage Methodology.

HITRUST is working towards a 2020 launch for the HITRUST CSF Ongoing Certification Program by establishing an industry working group (WG) to help develop the ISCM-based approach. We are encouraging organizations with mature ISCM programs to volunteer for both the WG and future pilot-related activities.

Table of Contents

Introduction

While there has been some volatility in the relative number of breaches and total records breached year after year, the trend has been and continues to be a general increase over time. And the trend does not show any real signs of slowing down anytime soon. A recent report from the Identity Theft Center indicates that, although the total number of data breaches was down in 2018 over 2017, the total number of records exposed more than doubled.[i] "The variety of industries and types of businesses impacted by breaches in 2018 opened the eyes of many consumers to the fact that breaches have become 'the new normal'. It is not so much a matter of 'if' a breach will happen, but 'when' a breach will happen."[ii]

Corresponding expectations around the level of protection organizations must afford personal data have also continued to increase over time. In addition to the 'morality' behind protecting personal data, such as the duty to prevent harm, informational injustice, and discrimination, all of which are posited in the Stanford Encyclopedia of Philosophy,[iii] organizations face increasing expectations around a legal standard of care[1] for personal data protection. As regulatory expectations increase the minimum standard of care, organizations face a growing need to seek better and more efficient methods to evaluate and mitigate risk associated with safeguarding sensitive information.

According to the National Conference of State Legislatures, the number of U.S. states with "data security laws [have] doubled since 2016, reflecting growing concerns about computer crimes and breaches of personal information."[iv]

> *Most of these data security laws require businesses that own, license, or maintain personal information about a resident of that state to implement and maintain 'reasonable security procedures and practices' appropriate to the nature of the information and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure…. States also have other data security laws that apply to state agencies or other governmental entities.*[v]

U.S. state law is also becoming more stringent, increasingly "[mirroring] some of the protections provided by Europe's newly enacted General Data Protection Regulation ('GDPR') … [which] are intended to provide consumers with greater transparency and control over their personal data."[vi]

[1] **Standard of care** may be defined as "the degree of care or competence that one is expected to exercise in a particular circumstance or role" (https://www.merriam-webster.com/legal/standard%20of%20care; https://dictionary.findlaw.com/legal-terms/s.html), where standard may be defined in this context as the "something established by authority, custom, or general consent as a model, example, or point of reference [… of the reasonable person]" (https://dictionary.findlaw.com/definition/standard.html).

Security Scorecards Fall Short of the Mark

Rather than employ traditional means of assessment and certification of an organization's information protection program and then sharing the results of such assessments with external stakeholders, some organizations have moved to cybersecurity risk scorecards, or reputational assessment services, which are based on publicly accessible information—what a cyber attacker can see—rather than an in-depth review of internal controls.[2] While useful, such an approach is limited (similar to a narrowly-scoped external penetration test) and is arguably unique for each organization's network.

> *Security professionals have some concerns, however, about whether a single score can capture all the nuances of a security program, whether score issuers are comparing the same security metrics to produce a score, and if companies can even be compared to one another given that no two networks are the same.*[vii]

It is further recognized that each scorecard vendor uses a proprietary approach to collecting data as well as proprietary analytics when computing the scores or ratings. In addition to the challenges inherent in their opacity, any changes to these proprietary approaches can change an organization's score, sometimes dramatically, when there has been no discernible change in their actual security posture.[viii] This is because the type of evidence collected for these scorecards is circumstantial and statements made about the actual state of the organization's security posture must be inferred rather than directly observed.

Subsequently, while security scorecards based on publicly accessible information can help inform an organization's understanding of its cyber risk, boards and other key stakeholders must recognize the inherent limits of these scores and draw correspondingly limited conclusions regarding a program's effectiveness. Simply put, security scorecards cannot replace the level of assurance provided by a thorough assessment of an organization's information protection program, including its overall approach to risk and risk management as well as detailed reviews of its privacy and security controls.

[2] For example, see https://securityscorecard.com/, https://www.normshield.com/security-cyber-risk-scorecard-safe-not/, and https://www.upguard.com/articles/bitsight-vs-securityscorecard.

Control Maturity Provides Better Assurance

'Secure-ability' or 'securability' is "the characteristic of being securable [or] the extent to which something is securable, especially the ability of a system to provide different levels of secure access."[ix] From a systems engineering perspective, securability, like reliability and usability, is generally considered a quality-related attribute. This makes it possible for organizations to apply concepts and methodologies from quality improvement programs, such as Total Quality Management and the Carnegie Melon Software Engineering Institute's (CM-SEI's) Capability Maturity Model (CMM), to information security engineering and management. For example, organizational implementation of information systems security engineering methodologies is similar to that of quality-based methodologies[x]; the National Institute of Standards and Technology (NIST) provides a 'quality' approach to evaluating the maturity of an organization's information security in its Program Review for Information Security Assistance (PRISMA) methodology.[xi]

"The structure of a PRISMA Review is based upon the [CMM], where an organization's developmental advancement is measured by one of five maturity levels"[xii]: (1) Policies (does the organization know what it needs to do?), (2) Procedures (does the organization know how to do it?), (3) Implementation (has the organization done it?), (4) Testing (does the organization ensure it is working properly?), and (5) Integration (are the activities in the first four levels well integrated?).[3] Assessing the maturity of an organization's information protection program by leveraging a comprehensive and consistently applied methodology, including assessing the status of its information security policies, procedures, and controls implementation, provides better assurance because it is based on direct rather than circumstantial evidence and therefore is more indicative of the actual level of protection the organization provides sensitive information like personal data, making it the only legitimate method of measuring an organization's information risk profile.

Evidence suggests that the more mature an organization's information protection program, specifically their information security controls which demonstrate proficiency of operation, management, and reporting, the more likely an organization will be to continue to operate those controls in a similar manner in the future. Further, it can also be shown that mature organizations are less likely to suffer a breach and, should a breach occur, the more likely these organizations will be able to contain it and minimize the impact. This is because controls that have been implemented at a high level of maturity are simply less likely to fail than controls that are implemented poorly. For example, Forrester Consulting has shown organizations that implement a CMM-based maturity model and have the highest level of maturity—even when limited to the area of identity and access management—incur roughly "half the number of breaches as the least mature … [and save] 40% in technology costs and an average of $5 million in breach costs."[xiii]

[3] For more information on the PRISMA maturity levels, see https://csrc.nist.gov/Projects/Program-Review-for-Information-Security-Assistance/Security-Maturity-Levels.

Benefits of Continuous Monitoring and Assessment

To achieve these higher levels of maturity, it is clear from the NIST PRISMA model that testing must be conducted as a matter of routine, the frequency and rigor of which must be based on the risks posed by the controls not operating as intended.[xiv] Fortunately, the concept of monitoring information security controls in this manner is not new and "has long been recognized as sound management practice."[xv] The information obtained from monitoring controls in a continuous manner helps organizations continually assess the state of their information security controls and subsequently the amount of additional and potentially unacceptable residual risk the organization may be incurring. This 'ongoing' evaluation of control effectiveness is an integral part of what's known as information security continuous monitoring.[xvi]

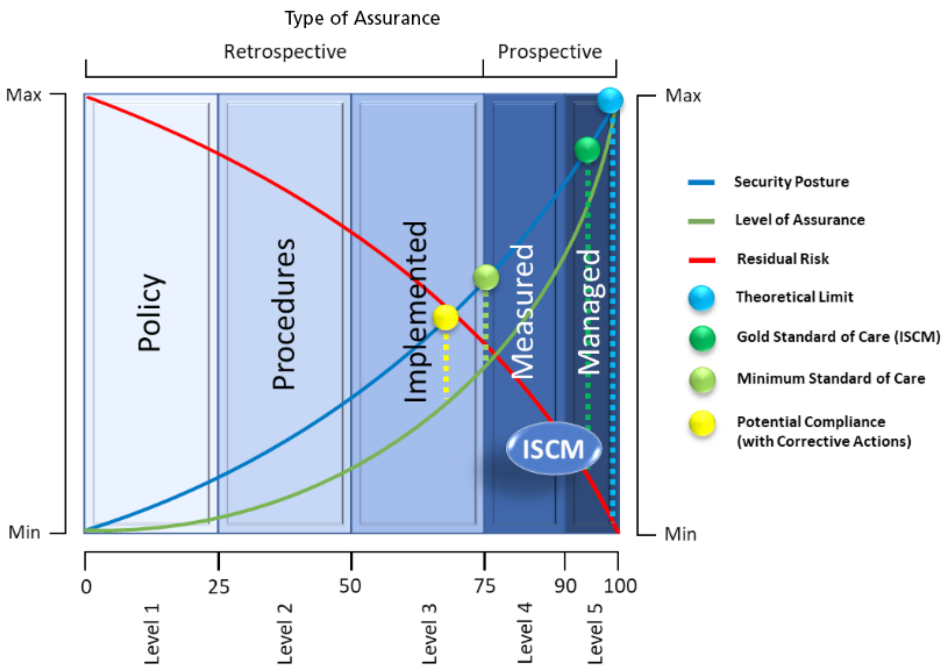

Figure 1. Relationship Between Control Maturity, Security Posture, Residual Risk and Level of Assurance

Figure 1 shows the general relationship between security posture, residual risk, and the level of assurance provided by the HITRUST CSF control maturity and scoring model. Organizations that have higher control maturity generally have a higher level of security, as shown by the blue line, which results in lower levels of residual risk to the organization, as shown by the red line, and can subsequently provide higher levels of assurance to relying parties, as shown by the green line. It is also clear that organizations with robust ISCM programs in place have the highest levels of security and assurance with the lowest levels of excessive risk.

ISCM subsequently changes the "point-in-time" nature of traditional security assessments to one of an ongoing,[4] prospective nature by providing the organization a view into the status of its controls "with a frequency sufficient to make ongoing, risk-based decisions… ."[xvii] The end result is improved organization-wide risk management and continual improvement of its information security program limited only by the speed with which the organization can collect information and respond to findings."[xviii]

[4] The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. Data collection, no matter how frequent, is performed at discrete intervals.

Organizations that implement a robust ISCM program do so generally because of the numerous benefits they receive, such as:

- On-demand, near real-time insight into their security and compliance risk posture[xix] (visibility into how well stuff is protected)
- The ability to make quick, risk-based decisions on system security in near real-time[xx] (helps minimize the impact from bad things happening)
- Better prioritization of remediation activities and corrective actions[xxi] (helps identify the problems that need to be fixed first)
- Consistent, continuous adoption of cybersecurity best practices[xxii] (ensures extant and emerging threats continue to be addressed appropriately)
- A higher level of assurance that personal data and individual privacy will continue to be protected and risk appropriately managed in the future (management can sleep better at night)

Better Assurance through Ongoing Certification

The conventional approach to information security certification[5] is to require organizations to undergo a conformity assessment[6] against a standard, which in turn results in a gap analysis between 'what is' and 'what should be.' As a result, they are considered static or 'point-in-time' assessments, i.e., they describe the state of the controls relative to the standard at the time of the assessment. A certification that could take advantage of an organization's ISCM program would therefore be a 'game changer' for those organizations seeking higher levels of assurance around the state of their internal programs as well as the programs of their third parties.

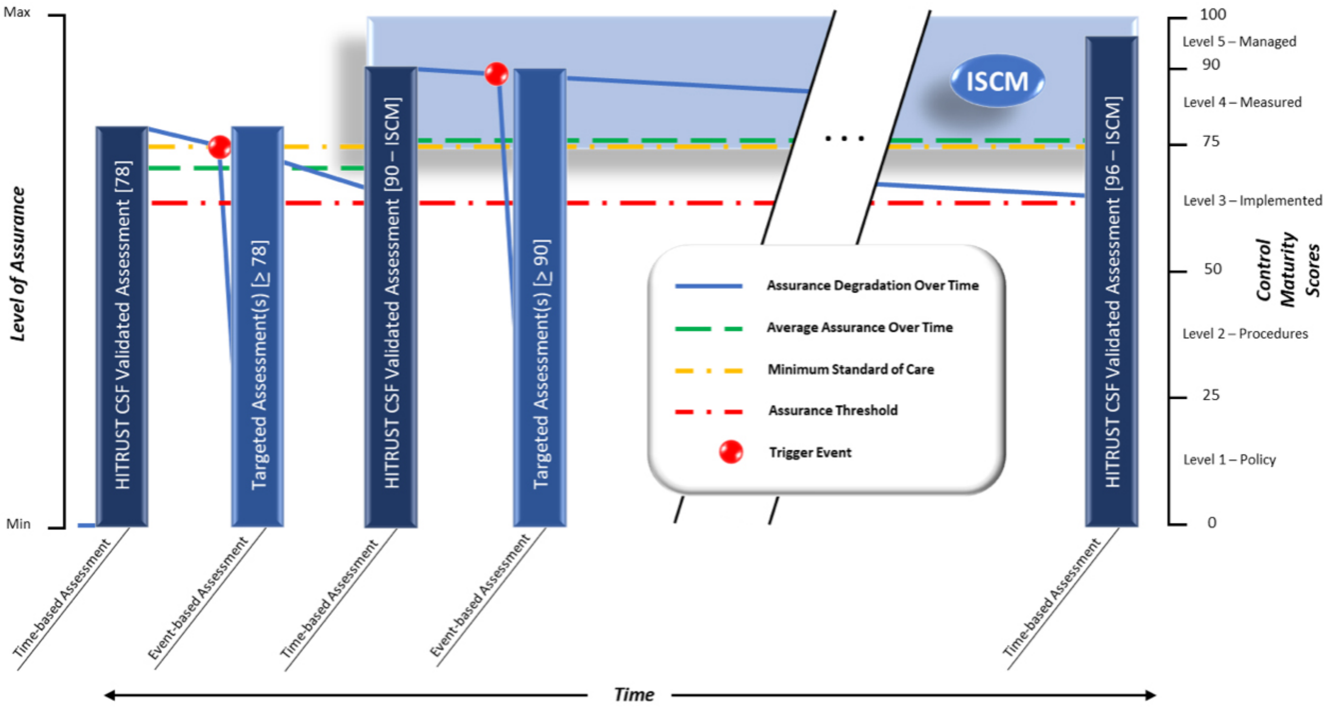

Figure 2. Relative Degradation of Assurance Over Time – ISCM vs. Non-ISCM-based Assessment

Figure 2 depicts how an organization can go from a traditional, retrospective conformity assessment with a moderate level of assurance, as shown on the left, to a continuous assessment (CA) approach with higher scores on the HITRUST CSF control maturity model associated with a formal ISCM program, as shown on the right. The rate of decline or degradation in the level of assurance is generally less pronounced when an ISCM program is in place than it would for a traditional assessment that becomes 'stale' or outdated over time, as shown by the solid blue lines. This allows the organization to undergo fewer, regularly scheduled comprehensive assessments even though targeted assessments may be needed to address an event trigger, such as patching levels exceeding a defined threshold. These targeted assessments provide the additional assurances needed to maintain a normal rate of degradation in assurance over time, regardless of the assessment and certification approach used by the organization. However, the average level of assurance provided by ISCM-based OC is generally greater for ISCM-based OC than traditional assessment and certification despite fewer time-based assessments, as shown by the dashed green lines.

[5] Certification may be defined as "the act of certifying; the state of being certified" (https://dictionary.findlaw.com/definition/certification.html) or "the provision by an independent body of written assurance (a certificate) that the product, service or system in question meets specific requirements" (https://www.iso.org/certification.html), where certify (-fied, -fying) may be defined as "to state authoritatively: as [a.] to give assurance of the validity of [corporate records], [b.] to present in formal communication (as an order) …, [c.] to state as being true or as reported or as meeting a standard (https://dictionary.findlaw.com/definition/certify.html).

[6] The International Standards Organization roughly defines a conformity assessment as "a set of processes that show [an organization's] product, service or system meets the requirements of a standard" (https://www.iso.org/conformity-assessment.html).

This is because the "continuous assessment … of security control effectiveness supports [certification] over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and … business processes,"[xxiii] by allowing an organization to evaluate relevant information "as it becomes available … [and] make adjustments to security requirements or individual controls as needed to maintain [certification] decisions."[xxiv] Such a dynamic, near real-time approach to CA and 'ongoing certification' of an organization's information protection program would provide:

- Longer periods between comprehensive control gap assessments (fewer interruptions at work)
- Reduced time and effort needed to maintain certification (ability to focus on the real work)
- Reduced lifecycle costs for maintaining certification (more money for other work)
- Higher levels of assurance and trust with and amongst external stakeholders such as regulators, business partners, and customers (everyone can sleep better at night)

The HITRUST Approach

HITRUST's rationale for organizations to move from a traditional to an ongoing certification process is centered around the concept of trustworthiness, i.e., the ability to rely on the evidence provided[xxv] by the certification. This trustworthiness or 'rely-ability' of certification is, in turn, based on the "***methodologies*** [emphasis added] and ***metrics*** [emphasis added] that allow us to measure the degree of confidence [or trust] we can place in an assessed entity."[xxvi]

The methodologies used to create the HITRUST CSF, tailor the control requirements to a particular organization, and assess the implementation of those requirements with accuracy and precision are solidly grounded upon NIST methodologies for the creation of industry overlays,[xxvii] how risk factors inform control specifications,[xxviii] and the measurement of control effectiveness by the maturity of its implementation.[xxix] Combined with the level of oversight provided by the HITRUST CSF Assurance[xxx] and Assessor[xxxi] programs, the HITRUST approach to control specification, implementation, assessment, and certification provide a level of transparency, accuracy, precision, consistency, and overall "rely-ability" unparalleled by any other approach in the industry. It is no wonder that HITRUST has become a leading private-sector SDO[xxxii] for security and privacy and the HITRUST CSF is well on its way to becoming one of the most widely adopted security and privacy control frameworks in the industry.[xxxiii]

The HITRUST CSF has also become the control framework of choice for many organizations that wish to demonstrate compliance with the NIST Cybersecurity Framework.[7] In fact, a recent Government Accountability Office (GAO) report[xxxiv] supports HITRUST's position that the NIST framework[xxxv] requires the specification of more granular control to effectively implement its cybersecurity objectives. The GAO also "encourages the alignment of the NIST [Cybersecurity Framework] with existing cybersecurity guidelines currently in use within its respective sector." The GAO report continues, "[f]or example, the Healthcare and Public Health sector aligned the [HITRUST] Framework to the [NIST] cybersecurity framework,"[xxxvi] producing specific guidance[xxxvii] on how to leverage the HITRUST CSF in achieving successful outcomes." Department officials stated that the alignment of the [NIST] framework to the HITRUST [CSF] allows organizations to demonstrate compliance with NIST through their implementation of the pre-existing HITRUST framework."[xxxviii]

Metrics have long been a central component of HITRUST CSF Certification with our PRISMA-based maturity model, which is used to measure control effectiveness and evaluate the organization's use of metrics for each CSF control requirement, including how well the controls are maintained based on those metrics.[xxxix] HITRUST is further integrating metrics into the HITRUST CSF Certification process by moving towards the specification of monitoring frequencies for all HITRUST CSF control requirements and implementation of continuous monitoring requirements that will fully support an organization's transition from a traditional certification to an ongoing certification process.

[7] The NIST Cybersecurity Framework is an overarching or "umbrella" risk framework that depends on the custom specification of controls or the use of a control framework such as the HITRUST CSF to achieve the outcomes specified by the NIST Cybersecurity Framework's Core Subcategories.

HITRUST is the only SDO that provides all the elements needed to support an effective and efficient approach to leveraging ISCM to support continuous independent assessment and ongoing certification of an organization's privacy and security risk and compliance program.

- Our comprehensive yet highly tailorable privacy and security control framework, the HITRUST CSF, can be applied to any organization in any industry, nationally or globally.
- We take a robust approach to certification through the HITRUST CSF Assurance Program, which is supported by
    - A standardized assessment methodology based on a rigorous control implementation maturity and scoring model,
    - Qualified, independent assessor organizations with requisite training and experience in the HITRUST CSF and CSF Assurance Program, and
    - Formal oversight and review by HITRUST of every HITRUST CSF assessment submitted for validation and certification.

The HITRUST Approach also includes numerous other products, services, and tools as part of a complete security and privacy risk and compliance 'ecosystem' designed to help organizations implement, assess, certify, and share assurances about their information protection programs. Examples include the HITRUST Threat Catalogue, which enumerates common threats and maps them to HITRUST CSF controls, the HITRUST MyCSF, which provides automated support for CSF assessment and certification, the HITRUST Assessment XChange, which facilitates the sharing of HITRUST CSF reports with third parties, and the Risk Triage Methodology, which provides a standardized approach to evaluating inherent risk of a business relationship and assigning a required level of assurance.

Call to Action

Based on the outlined evidence and benefits, specifically that organizations with mature information security controls pose less information risk and will likely operate those controls in a similar manner in the future, HITRUST is currently exploring the requirements for developing and implementing an ISCM-based CA program and plans to pilot the program in late 2019 or early 2020 prior to a late 2020 release. Coupling ISCM, OA, CA, and OC as shown in Figure 3 with the consistency and integrity of the HITRUST CSF Assurance Program will allow the findings in the CSF Assessment Report to be truly prospective, basing its foresight on evidence rather than anecdotal or circumstantial information.

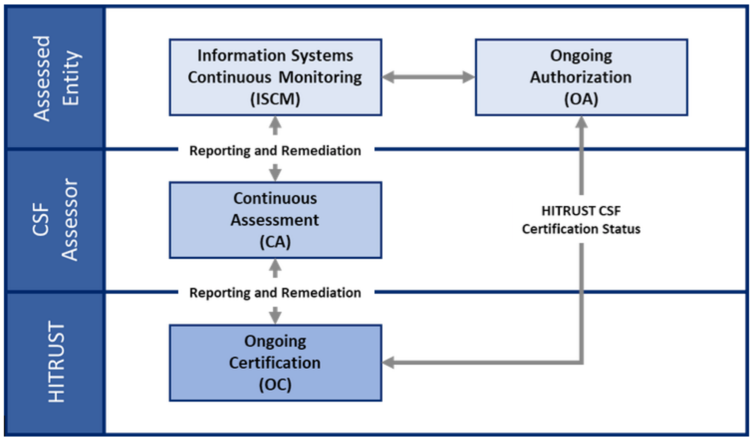
Assessed Entity
CSF Assessor
HITRUST
Information Systems Continuous Monitoring (ISCM)
Ongoing Authorization (OA)
Reporting and Remediation
Continuous Assessment (CA)
HITRUST CSF Certification Status
Reporting and Remediation
Ongoing Certification (OC)

Figure 3. ISCM-Based HITRUST CSF Ongoing Certification Process Model

Organizations that wish to benefit from HITRUST's ongoing certification of their information protection programs should first evaluate the state of their internal ISCM programs. If they are already achieving high maturity scores for 'measured' and 'managed' organizations will likely have little additional work to qualify their internal programs for the HITRUST CSF Ongoing Certification Program beyond addressing ISCM program-related control requirements in the HITRUST CSF; however, organizations that do not have viable metrics in place and subsequently do not score well for the 'measured' and 'managed' levels of maturity can and should draft an ISCM program strategy, develop corrective action plans (CAPs), and begin implementing the strategy and CAPs.

As we move forward with cultivating the HITRUST CSF Ongoing Certification Program, we intend to develop control requirements for organizations' internal ISCM and ongoing authorization programs, define reporting requirements between organizations and HITRUST CSF Assessors to support continuous assessment of the security controls, define reporting requirements between the HITRUST CSF Assessors and HITRUST, and develop OC criteria for maintaining certification or requiring the recertification or decertification of an assessed organization. HITRUST will also be establishing an industry working group (WG) to help develop the ISCM-based approach. We encourage organizations with mature ISCM programs to volunteer for the WG as well as future pilot-related activities.

About HITRUST

Since it was founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for global organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security, and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks as well as related assessment and assurance methodologies.

HITRUST understands the challenges of assembling and maintaining the many and varied programs needed to manage information risk and compliance. The HITRUST Approach[8] provides organizations a comprehensive information risk management and compliance program to provide an integrated approach that ensures all programs are aligned, maintained, and comprehensive to support an organization's information risk management and compliance objectives.

[8] For more information on **The HITRUST Approach**, refer to https://hitrustalliance.net/the-hitrust-approach/.

Endnotes

[i] Identity Theft Center (2019). ITRC 2018 End-of-Year Aftermath. Available from https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf.

[ii] IDC (2019), p. 5.

[iii] Privacy and Information Technology (2014, Nov 20). In Stanford Encyclopedia of Philosophy. Available from https://plato.stanford.edu/entries/it-privacy/.

[iv] National Conference of State Legislatures (N.D.). Data Security Laws I Private Sector: Overview. Available from http://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx.

[v] NCSL (N.D.).

[vi] Serrato, J. K., Cwalina, C., and Rudawski, A. (2019). US states pass data protection laws on the heels of the GDPR. Norton Rose Fulbright. Available from https://www.dataprotectionreport.com/2018/07/u-s-states-pass-data-protection-laws-on-the-heels-of-the-gdpr/.

[vii] CSO Online (2016, Aug 4) What's in a security score? Available from https://www.csoonline.com/article/3103293/what-s-in-a-security-score.html.

[viii] CSO Online (2016, Aug 4).

[ix] What does securability mean? (N.D.). In Definitions. https://www.definitions.net/definition/securability.

[x] Cline, B. (2009). Organizational Barriers to the Implementation of Security Engineering. 2009 Fifth International Conference on Information Assurance and Security, 2, 527-531.

[xi] Bowen, P. and Kissel, R. (2007, Jan). Program Review for Information Security Management Assistance (PRISMA) (NISTIR 7358). Available from https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7358.pdf.

[xii] Bowen & Kissel (2007, Jan), p. 2.

[xiii] Forrester Consulting (2017, Feb). Stop the Breach: Reduce the likelihood of an Attack through an IAM Maturity Model: A Forrester Consulting Thought Leadership Paper, p. 1. Commissioned by Centrify. Available from https://www.centrify.com/media/4594046/stop-the-breach.pdf.

[xiv] Bowen & Kissel (2007, Jan), p. 8.

[xv] Dempsey, K., Chawla, N.S., Johnson, A., Johnston, R., Jones, A.C., Orebaugh, A., Scholl, M., and Stine, K. (2011, Sep). Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations [NIST SP 800-137]. Gaithersburg, MD: NIST, p. 2. Available from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-137.pdf.

[xvi] Dempsey, K., Ross, R., and Stine, K. (2014, Jun). Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management. Gaithersburg, MD: NIST, p. 3. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.06032014.pdf.

[xvii] Dempsey, et al. (2011, Sep), p. 2.

[xviii] Dempsey, et al. (2011, Sep), p. 6.

[xix] Eisensmith, J. (N.D.). Ongoing Authorization: Changing how Government does Security Compliance, CIO Review. Available from https://identity-governance-and-administration.cioreview.com/cxoinsight/ongoing-authorization-changing-how-government-does-security-compliance-nid-5608-cid-180.html.

[xx] Eisensmith (N.D.).

[xxi] Luu (2015). Implementing an Information Security Continuous Monitoring Solution—A Case Study. ISACA Journal (1). Available from https://www.isaca.org/Journal/Blog/Lists/Posts/Post.aspx?ID=264.

[xxii] Luu (2015).

[xxiii] Dempsey, et al. (2011, Sep), p. 10.

[xxiv] Dempsey, et al. (2011, Sep), p.10.

[xxv] Bishop, M. (2003). Computer Security: Art and Science. Boston, MA: Addison-Wesley, pp. 477-478. Cited in Gegick, M. and Barnum, M. (2013, May 10). Reluctance to Trust, US-CERT Cyber-Infrastructure. Available from https://www.us-cert.gov/bsi/articles/knowledge/principles/reluctance-to-trust.

[xxvi] Bishop (2003).

[xxvii] Joint Task Force Transformation Initiative (2013, Apr). Security and Privacy Controls for Federal Information Systems and Organizations [NIST SP 800-53 Rev 4]. Gaithersburg, MD: NIST, pp. 40-41. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[xxviii] Joint Task Force Transformation Initiative (2012, Sep). Guide for Conducting Risk Assessments [NIST SP 800-30 Rev 1]. Gaithersburg, MD: NIST, pp. 8-13. Available from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[xxix] Bowen, P. and Kissel, R. (2007, Jan). Program Review for Information Security Management Assistance (PRISMA) [NISTIR 7358]. Gaithersburg, MD: NIST, pp. 2-3. Available from https://csrc.nist.gov/publications/detail/nistir/7358/final.

[xxx] HITRUST (2019). CSF Assurance Program. Available from https://hitrustalliance.net/csf-assurance/.

[xxxi] HITRUST (2019). CSF Assessors. https://hitrustalliance.net/csf-assessors/

[xxxii] Cline, B. (2018). HITRUST as an Industry Standards Organization. Frisco, TX: HITRUST. Available from https://hitrustalliance.net/documents/content/The-HITRUST-Industry-Standards-Organization.pdf.

[xxxiii] HIMSS (2018). 2018 HIMSS Cybersecurity Survey. City, ST: Author, p. 18. Available from https://www.himss.org/sites/himssorg/files/u132196/2018_HIMSS_Cybersecurity_Survey_Final_Report.pdf.

[xxxiv] U.S. Government Accountability Office (2018, February). Report to Congressional Committees on Critical Infrastructure Protection: Additional actions are Essential for assessing Cybersecurity Framework adoption (Publication No. GAO -18-211 Critical Infrastructure Protection). Author: Washington, DC. Available from the GAO Reports & Testimonies Web page at https://www.gao.gov/products/GAO-18-211.

[xxxv] NIST (2018, Apr 16). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Author: Gaithersburg, MD. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[xxxvi] NIST (2018, Apr 16), p. 15.

[xxxvii] Joint HPH Cybersecurity Working Group (2016, May). Healthcare Sector Cybersecurity Framework Implementation Guide. Critical Infrastructure Partnership Advisory Council: Washington, DC. Available from the US-CERT Cybersecurity Framework Web page at https://www.us-cert.gov/ccubedvp/cybersecurity-framework#framework-guidance or directly from https://www.us-cert.gov/sites/default/files/c3vp/framework_guidance/HPH_Framework_Implementation_Guidance.pdf.

[xxxviii] Joint HPH CWG (2016, May).

[xxxix] Cline, B. (2018, Feb), pp. 9-12.

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net