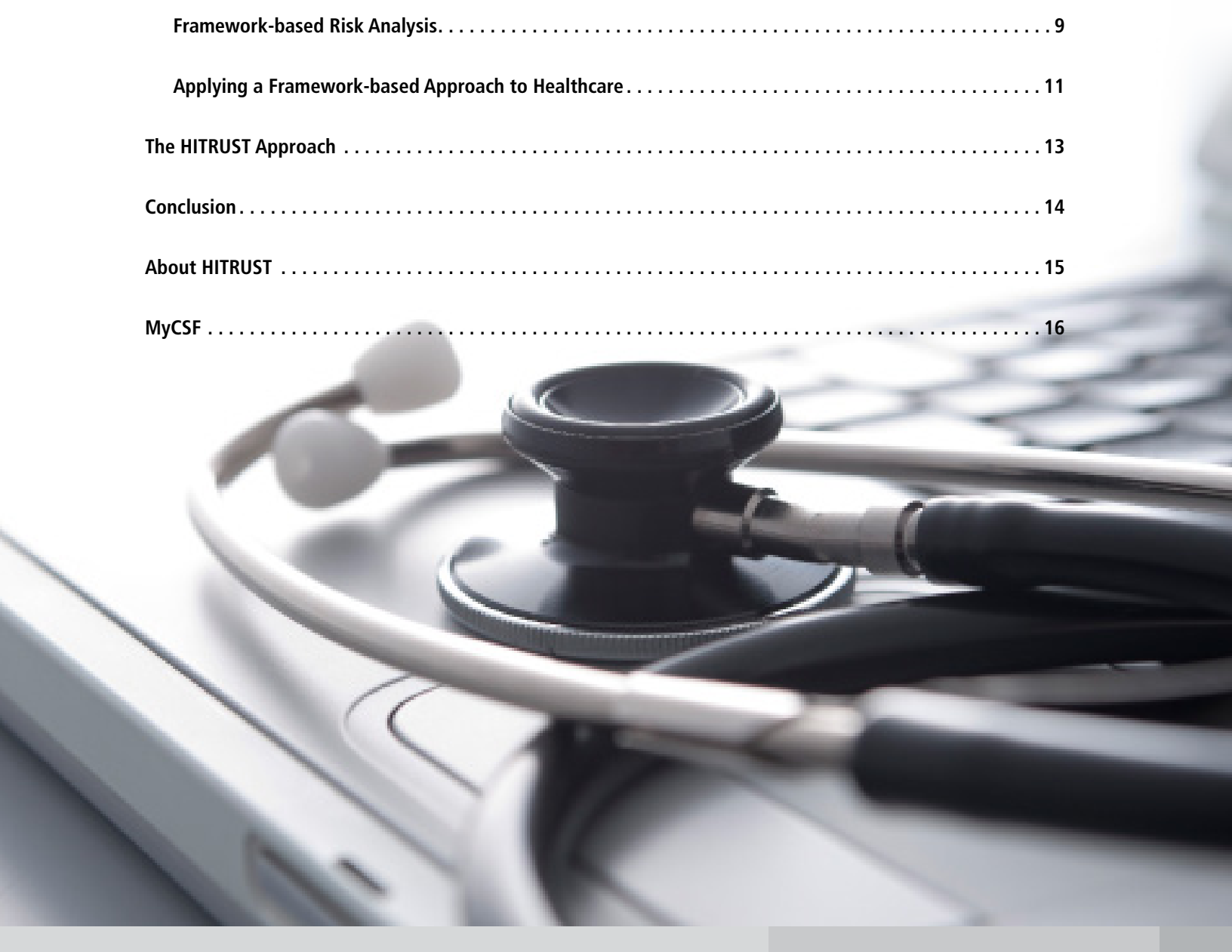
HITRUST

Understanding HITRUST's Approach to Risk vs. Compliance-based Information Protection

Why framework-based risk analysis is crucial to HIPAA compliance and an effective information protection program

April 2018

Contents



Introduction

HITRUST is commonly asked why it aligned the CSF and CSF Assurance program with a risk assessment versus a compliance assessment methodology. This document aims to provide some insights into various related concepts and HITRUST's approach to the CSF and the CSF Assurance program. Healthcare organizations face a multitude of challenges with regards to information security and privacy. At the forefront of these challenges is the need to apply "reasonable and appropriate" safeguards to provide "adequate" protection of sensitive information in order to demonstrate compliance with a growing number of continuously evolving federal, state and industry requirements. However, given the general lack of definition and prescriptiveness of these requirements, organizations are left with the task of deciding what actions would be considered "reasonable and appropriate" and what level of protection would be "adequate" in the eyes of federal, state and industry regulators and ensure compliance.

Compliance

Regulatory compliance may be viewed as an adherence to the laws, regulations, standards, guidelines and other specifications relevant to an organization's business. Subsequently compliance risk—or perhaps more accurately the risk of noncompliance—is associated with civil punishment, either through regulatory penalties or possible tort action as the result of negligence due to a general failure to comply with applicable requirements. Typical compliance requirements include legislation such as the Dodd-Frank Act, regulations such as the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification,[1] and industry specifications such as the Payment Card Industry Digital Security Standard (PCI-DSS). And, in some cases, there may be a risk of criminal punishment, as with Sarbanes-Oxley (SOX).

Subsequently, organizations manage the risk of noncompliance simply by complying with the requirements. For example, if a covered entity is required to have a privacy officer, then it either has one or it doesn't. It's essentially a 'Yes or No' proposition. For more complex requirements, such as with the encryption of portable devices that contain sensitive information, an organization could very well be partially compliant if, for example, it cannot demonstrate that all devices that contain such information are encrypted.

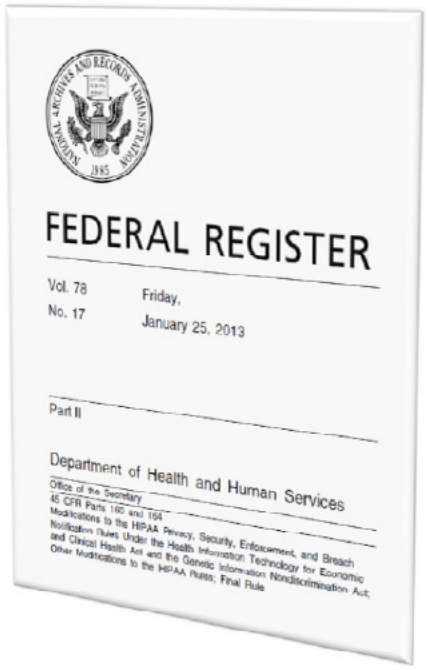
When considering whether or not to comply with a law, regulation, standard, guideline or specification, most organizations typically weigh the operational and financial impact from implementing the requirement against the likelihood of noncompliance being discovered and the subsequent operational, financial and reputational impact.

Other types of risk—such as the operational, financial and reputational financial risks from an actual loss of confidentiality, integrity and availability—are simply not a normal part of the compliance equation.

---

[1] U.S. Department of Health and Human Services (2013). HIPAA Administrative Simplification Regulation Text: 45 CFR Parts 160, 162,and 164. Retrieved from https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf

HIPAA Compliance


FEDERAL REGISTER
Vol. 78
No. 17
Friday,
January 25, 2013
Part II
Department of Health and Human Services
Office of the Secretary
45 CFR Parts 160 and 164
Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

"HIPAA compliance" and "HIPAA compliant" have probably been some of the most overused yet least understood terms in the healthcare industry. This is because the HIPAA Security Rule provides numerous standards and implementation specifications for administrative, technical and physical safeguards that, despite what the terms imply, lack the prescription necessary for actual implementation by a healthcare organization.

However, this approach was necessary as no two healthcare organizations are exactly alike, which means no single set of information protection requirements could possibly apply across the entire industry. In other words, one size truly does not fit all. Regardless, this lack of prescription along with a general lack of guidance from HHS on how organizations should interpret 'reasonable and appropriate safeguards' and 'adequate protection' resulted in wildly varying information protection programs amongst healthcare entities, including those of similar size and scope. Yet all these organizations likely believed they were "HIPAA compliant" because they had done something around each of the HIPAA standards and implementation specifications. By checking the box against the general requirements in the HIPAA Security Rule, organizations subsequently 'checked the box'—albeit inappropriately—for the one requirement that sets the Rule apart from many other information protection regulations—the risk analysis—without actually conducting one.

When asked at the 2014 Health Care Compliance Association (HCCA) Conference in San Diego, Linda Sanches, Senior Advisor and Health Information Privacy Lead, stated that the Office for Civil Rights (OCR) would not accept an assessment based on the original OCR Audit Protocol developed by KPMG as a valid risk assessment because—although the Protocol addressed each of the Security Rule's standards and implementation specifications—the controls reviewed would not sufficiently address all reasonably anticipated threats, as required by HIPAA. This supports the notion that focusing on the HIPAA Security Rule's standards and implementation specification language is flawed and would not constitute an acceptable risk analysis.

The HIPAA Administrative Simplification states covered entities and business associates must "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information [created, received, maintained or transmitted to][2] … protect against any reasonably anticipated threats or hazards to the security or integrity of such information."[3]

[2] *HIPAA Administrative Simplification, 45 C.F.R. § 164.308(a)(1) (2013)*
[3] *HIPAA Administrative Simplification, 45 C.F.R. § 164.306(a)(2) (2013)*

The problem organizations encounter by not performing such a risk analysis can best be demonstrated by looking at how the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-66 revision 1 (r1), "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,"[4] maps the HIPAA Security Rule requirements against the comprehensive control framework specified in NIST SP 800-53 revision 3[5] , "Recommended Security Controls for Federal Information Systems and Organizations," which is based on such a risk analysis. Of all controls listed (regardless of a particular baseline), only about half of them are mapped to HIPAA. The table below provides the number of controls (n) that map to the HIPAA Security Rule as a percentage of all controls (N) that are selected for each baseline.

NIST Control Family	Low Baseline			Moderate Baseline			High Baseline		
	n	N	%	n	N	%	n	N	%
Access Control (AC)	5	11	45%	9	15	60%	9	16	56%
Awareness & Training (AT)	4	4	100%	4	4	100%	4	4	100%
Audit & Accountability (AU)	5	10	50%	5	11	45%	5	12	42%
Security Assessment & Authorization (CA)	6	6	100%	6	6	100%	6	6	100%
Configuration Mgmt. (CM)	1	6	17%	1	9	11%	1	9	11%
Contingency Planning (CP)	6	6	100%	9	9	100%	9	9	100%
Identification & Authentication (IA)	5	7	71%	6	8	75%	6	8	75%
Incident Response (IR)	6	7	86%	7	8	88%	7	8	88%
Maintenance (MA)	3	4	75%	4	6	67%	4	6	67%
Media Protection (MP)	2	3	67%	5	6	83%	5	6	83%
Physical & Environmental Protection (PE)	6	11	55%	10	18	56%	10	18	56%
Planning (PL)	2	4	50%	3	5	60%	3	5	60%
Personnel Security (PS)	8	8	100%	8	8	100%	8	8	100%
Risk Assessment (RA)	3	4	75%	3	4	75%	3	4	75%
System & Services Acquisition (SA)	2	8	25%	2	11	18%	2	13	15%
System and Communications Protection (SC)	2	8	25%	4	20	20%	4	23	17%
System & Information Integrity (SI)	4	5	80%	7	11	64%	7	12	58%
Program Management (PM)	0	11	0%	0	11	0%	0	11	0%
Totals	**70**	**123**	**57%**	**93**	**170**	**55%**	**93**	**178**	**52%**

[4] Scholl, M., Stine, K., Hash, J., Bowen, P., Johnson, A., Smith, C. D., and Steinberg, D. (2008). An Introductory Resource Guide for Implementing the [HIPAA] Security Rule. NIST: Gaithersburg, MD. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf

[5] NIST SP 800-66 r1 has not been updated to include changes to the security controls in NIST SP 800-53 r4

While HIPAA maps readily to some areas, such as Awareness & Training (AT), the standards and implementation specifications map poorly to others, such as Configuration Management (CM), System & Services Acquisition (SA), and System & Information Integrity (SI). This means that a 'check-the-box' approach to compliance with the HIPAA Security Rule would result in a failure to address all the threats a federal healthcare organization might reasonably anticipate. The following suggests this is true for non-federal organizations as well.

The HITRUST CSF harmonizes multiple, relevant information security and privacy regulations, frameworks and best-practice standards relevant to healthcare, including the controls contained in NIST SP 800-53 r4. But despite the additional healthcare-relevant content, only 98 of 135 or 73% of HITRUST CSF controls in 2014 mapped directly to the HIPAA Security Rule[6,7]. Exceptions included 01.w, Sensitive System Isolation; 05.f, Contact with Authorities; 09.ac, Protection of Log Information; 09.af, Clock Synchronization; and 10.k, Change Control Procedures, among others. In addition, there are 55 specific NIST SP 800-53 r4 controls[8] —also common to r3—that are referenced by the NIST Framework for Improving Critical Infrastructure Cybersecurity version 1 (also known as the Cybersecurity Framework)[9,10] but do not map to the HIPAA standards and implementation specifications in NIST SP 800-66 r1.

The position that the HIPAA Security Rule's standards and implementation specifications do not prescribe a comprehensive information protection program in and of themselves also appears to be supported by HHS. In its Guidance on Risk Analysis Requirements under the HIPAA Security Rule, HHS states that "conducting a risk analysis is the first step in identifying and implementing safeguards that comply with and carry out the standards and implementation specifications in the Security Rule." In other words, implementing the standards and implementation specifications will not ensure compliance with the risk analysis requirement; but a risk analysis will help ensure compliance with the standards and implementation specifications.

Risk Analysis

NIST defines risk analysis as "the process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment."[11] As NIST considers the term to be synonymous with risk assessment, we provide that definition as well.

> *The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, [and] other organizations … resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.*

[6] *Cline, B. (2014). HITRUST CSF to HIPAA Relationship Matrix v1.1. HITRUST: Frisco, TX. Retrieved from http://hitrustalliance.net/content/uploads/2014/05/CSF-HIPAA-Matrix-v3-CSF-HIPAA-Primary_Secondary.pdf.*

[7] *Note the CSF maps to 100% of the Security Rule's standards and implementation specifications.*

[8] *Joint Task Force Transformation Initiative (2013). Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4 (NIST SP 800-53, r4). Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.*

[9] *National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0 (NIST Cybersecurity Framework, v1.0). Author: Gaithersburg, MD. Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.*

[10] *A new NIST Cybersecurity Framework, version 1.1, was released in April 2018 and is available at https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf.*

[11] *Kissel, R (Ed.) (2013). Glossary of Key Information Security Terms, Revision 2 (NISTIR 7298, r2). NIST: Gaithersburg, MD. Retrieved from https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf*

But regardless of the specific term used, risk analysis is generally the first step in the risk management process. This step is supported by seven sub-processes, which range from the classification of information assets to the development of specific risk treatments.

This sub-process model is also consistent with HHS' Guidance on Risk Analysis Requirements under the HIPAA Security Rule, which requires an organization to:

- Scope the assessment to include all ePHI
- Identify & document all assets with ePHI
- Identify & document all reasonably anticipated threats to ePHI
- Assess all current security measures
- Determine the likelihood of threat occurrence
- Determine the potential impact of a threat occurrence
- Determine the level of risk
- Document assigned risk levels and corrective actions

However, many organizations fall short in conducting their risk analysis for many reasons, some of which include but certainly aren't limited to the following:

- Incomplete asset inventory
- Failure to categorize assets properly
- Limited or no understanding of asset value
- Failure to enumerate/address all reasonably anticipated threats

- Unable to determine likelihood of a threat occurrence or its impact
- Risk expressed as control effectiveness based on an evaluation of its implementation
- No documentation of risk treatments, especially of risk acceptance
- Failure to address corrective actions for all risks requiring mitigation

Of these, the threat, vulnerability and impact analyses are perhaps the most difficult for many organizations, especially in healthcare, often due to a lack of skilled resources or, as in the case of many smaller organizations such as physician practices and clinics, the budget needed to outsource the analysis to a third-party consultant or professional services firm. Consider threat identification, for example. There is no generally accepted list of common threats to healthcare organizations, and resources that provide more general threat information are often inconsistent with one another (e.g., the Bundesamt fur Sicherheit in der Informationstechnik (BSI) IT-Grundschutz-Catalogues[12] and the European Union Agency for Network and Information Security (ENISA) Threat Taxonomy[13]) or incomplete (e.g., NIST SP 800-30 [14]). And from a quantitative viewpoint, the process of determining the likelihood of a threat occurrence is virtually impossible for most—if not all—organizations, and not always due to a lack of expertise. Unless 'actuarial-type' information is available, the likelihood a threat-source will successfully exploit one or more vulnerabilities cannot be calculated with any level of precision. In the case of a human threat actor, likelihood is also dependent on the motivation and capability of the actor and the difficulty or cost associated with exploiting one or more vulnerabilities to achieve the actor's objectives. The final few steps involve calculating the risk, ranking the risks in order of severity, and developing an overall strategy to address the risks, which generally involves avoidance, acceptance, transfer and mitigation.

The U.S. Department of Health and Human Services (HHS) takes a slightly different approach by incorporating a controls gap analysis in the risk analysis process.[15] This approach presumes organizations already have at least some security controls in place before conducting their first analysis, but a complete set of security controls must still be specified. HHS includes this control specification in the last step along with specific remediation plans based on the control gap analysis.

Risk Analysis in the Risk Management Process

The risk management process can be represented by a general four-step process model,[16] which includes identifying risks and information protection requirements, specifying controls, implementing and managing controls, and assessing and reporting on the controls.

---

[12] Bundesamt fur Sicherheit in der Informationstechnik, BSI (2013). IT-Grundschutz-Catalogues, Version 13. Author: Bonn, GE. Retrieved from https://download.gsb.bund.de/BSI/ITGSKEN/IT-GSK-13-EL-en-all_v940.pdf.

[13] European Union Agency for Network and Information Security, ENISA (2016). ENISA Threat Taxonomy. Author: Heraklion, GR. Retrieved from https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/enisa-threat-landscape/etl2015/enisa-threat-taxonomy-a-tool-for-structuring-threat-information.

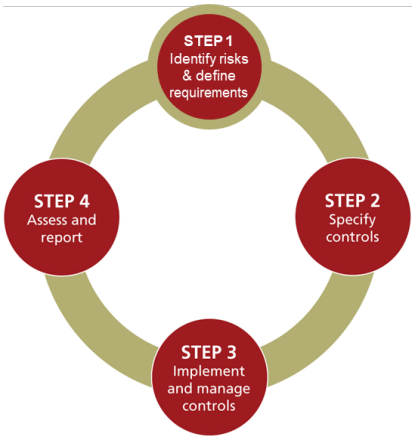
[14] Joint Task Force Transformation Initiative (2012). Guide for Conducting Risk Assessments, Revision 1. (NIST SP 800-30, r1.) NIST: Gaithersburg, MD. Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

[15] U.S. Department of Health and Human Services (2010). Guidance on Risk Analysis under the HIPAA Security Rule. Author: Washington, D.C. Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf?language=es.

[16] Cline, B. (2018). Risk Analysis Guide for HITRUST Organizations & Assessors. HITRUST: Frisco, TX. Retrieved from https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf.

Step 1—Identify Risks and Define Protection Requirements

This first step is essentially the 7-step risk analysis process described earlier, the output of which is essentially a list of risks and proposed risk treatments.



Step 2—Specify Controls

The next step after the risk analysis is to determine a set of reasonable and appropriate safeguards an organization should implement in order to adequately manage information security risk. The end result should be a clear, consistent and detailed/prescriptive set of control recommendations that are customized for the healthcare organization. Whether control specification occurs at the end of the risk analysis as in the HHS model or just after the risk analysis in the model presented here, control specification follows information classification, asset categorization, threat analysis, vulnerability analysis, and the calculation, ranking and treatment of risk.

Step 3—Implement and Manage Controls

Controls are implemented through an organization's normal operational and capital budget and work processes with board-level and senior executive oversight using existing governance structures and processes.

Step 4—Assess and Report

The objective of this last step is to assess the efficacy of implemented controls and the general management of information security against the organization's baseline.

This process is then repeated by evaluating the effectiveness of existing safeguards and any new threats that may have materialized, which then results in the selection of new safeguards and/or the improvement of existing ones. For the purpose of this white paper, however, we only need focus on the first two steps.

Framework-based Risk Analysis

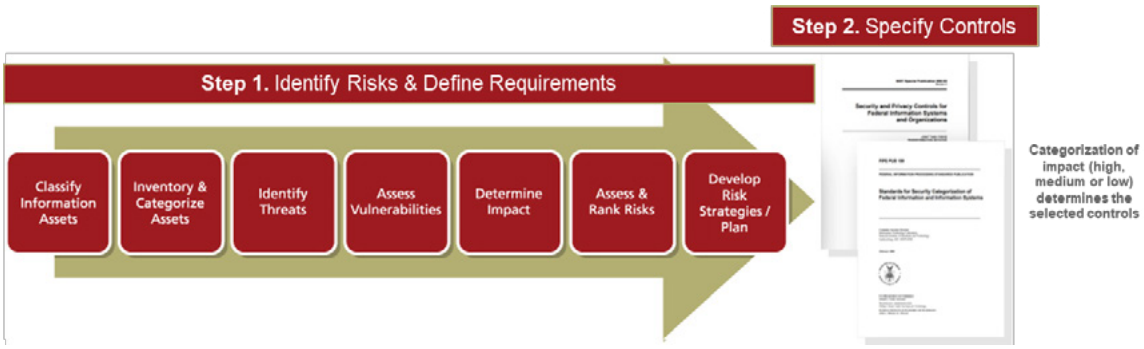
As with any process model, the output of one step is the input of the second. Subsequently, one can see that the whole point of conducting a risk analysis is to determine a specific set of reasonable and appropriate controls that will provide adequate information protection, as HIPAA requires.

But as mentioned earlier, the risk analysis requirement is problematic for many organizations, especially in healthcare. In fact, OCR cites an incomplete or inaccurate risk analysis for fully two-thirds of the organizations evaluated against the first OCR Audit Protocol,[17] conducted as part of a program mandated under the Health Information Technology for Economic and Clinical Health (HITECH) Act.[18]

Fortunately, there is a viable alternative for this traditional approach to the risk analysis requirement, which is to rely on a comprehensive control framework that has been built upon a broad analysis of reasonably anticipated threats faced by similar organizations with specific types of information using common information technologies. This is the approach employed by the U.S. intelligence community (IC), Department of Defense (DoD) and civilian agencies of the federal government.[19]

Rather than perform a more traditional risk analysis as first described, Federal agencies categorize their information systems based on a more limited analysis focused on identifying "one of three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity or availability)."[20] Agencies then simply select a security control baseline appropriate for the categorization.

This is possible because major elements of the risk analysis have already been performed. For all intents and purposes, NIST conducted a general risk analysis of a typical Federal agency with typical threats to typical vulnerabilities of typical information assets and specified three security control baselines to address three levels of risk. The risk level—and subsequently the control baseline that should be selected—is determined when an agency categorizes the impact of a potential breach as low, moderate or high.[21] This greatly simplifies the risk analysis process for Federal Agencies and provides an "80 percent solution" for control specification.[22]



[17] Sanches, Linda (2012). 2012 HIPAA Privacy and Security Audits. 2012 NIST-OCR HIPAA Security Conference. Retrieved from http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-2_lsanches_ocr-audit.pdf.

[18] The Health Information Technology for Economic and Clinical Health (HITECH) Act, Public Law 11-5, U.S. Statutes at Large 123 (2009): 226-279. Retrieved from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/coveredentities/hitechact.pdf.

[19] Formally three separate control frameworks, they are now consolidated into a single framework for all federal agencies including the IC and DOD under a general NIST umbrella.

[20] National Institute of Standards and Technology (2004). Standards for Security Categorization of Federal Information and Information Systems (FIPS Pub 199). Author: Gaithersburg, MD. Retrieved from http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf.

[21] Categorization is determined by the greatest impact to the organization from a loss of confidentiality, integrity and availability (referred to as the "high-water mark").

[22] In the vein of the "80/20" or Pareto Rule, organizations can obtain a minimum security control baseline that will address a majority (80%) of its risks for a relatively small (20%) effort from categorizing its information and information system(s).

Agencies are then expected to further tailor the baseline to ensure their unique information protection requirements are addressed. The tailoring process [23] includes additional scoping to eliminate unnecessary controls, selecting compensating controls, assigning parameters for organization-defined parameters, adding controls and enhancements, and providing any additional information required for control implementation. This process can be used granularly on a specific system or organizational element, or it can be used to create an overlay for general use, such as a general type of information system or organization.

Applying a Framework-based Approach to Healthcare

Healthcare organizations can create their own overlay of a NIST SP 800-53 baseline by going through the tailoring process. While daunting for some organizations, it is arguably a more tractable approach than specifying a complete set of security controls based on a traditional risk analysis.

- First, scale the controls by selecting an appropriate baseline from which to begin. This helps ensure time and effort is not wasted on implementing controls that aren't necessary for the level of risk mitigation required.

- Second, scope the scaled baseline by adding or enhancing controls, as needed, to address applicable regulatory, legal, contractual and other business-related requirements unique to your organization. Controls may also be removed based on organizational and financial constraints; however, no control should be removed simply as a matter of convenience.

- Third, specify compensating controls for baseline controls that cannot be implemented, e.g., due to technical, architectural or financial reasons. Ensure the compensating controls address a similar type and amount of risk as the baseline controls.

- Fourth, continue the tailoring process by reviewing the organization-defined parameters to ensure the values are consistent with best practices and industry due care and due diligence requirements.

- And finally, review the resulting overlay periodically, or otherwise as needed, to ensure the overlay continues to address extant and emerging threats to your information assets.

The healthcare industry already leverages the overlay concept to great benefit. For example, the Centers for Medicare and Medicaid Services (CMS) produces an overlay of all three NIST SP 800-53 control baselines for their use and that of their contractors.[24] CMS also produces a separate overlay of the NIST SP 800-53 moderate control baseline for Health Insurance Exchanges (HIXs).[25] And the HITRUST Alliance—a leading privacy and security standards and information risk management organization—produces an overlay of the NIST moderate baseline for the industry and incorporates mechanisms to help further tailor the overlay to an organizational type based on defined risk factors.[26]

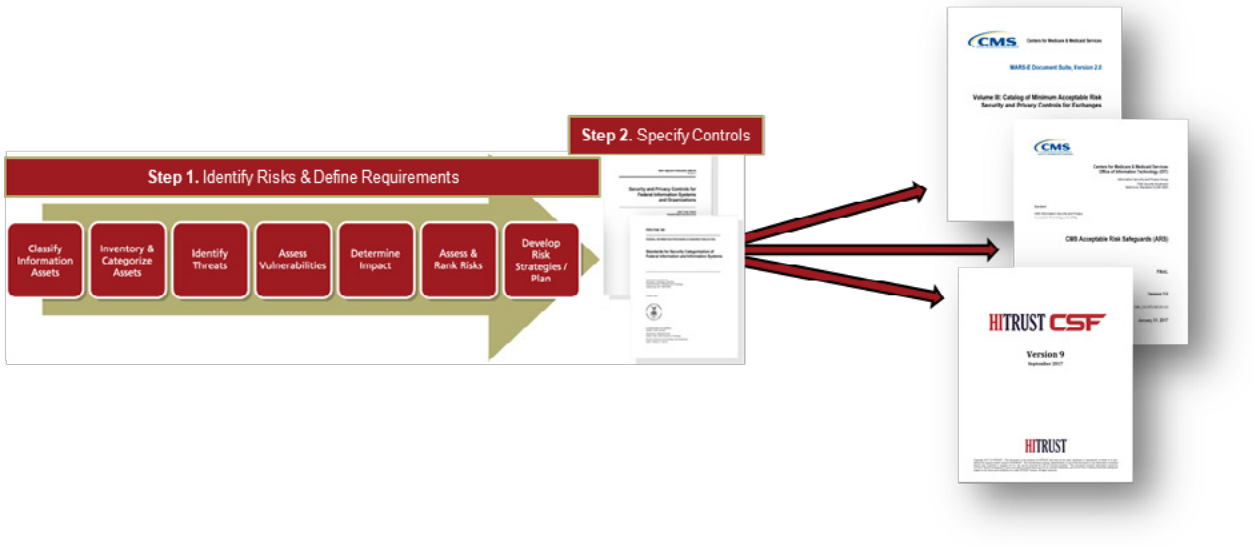
---

[23] The tailoring process, including its use in the development of overlays, is discussed extensively in NIST SP 800-53, Chapter 3.

[24] Centers for Medicare and Medicaid Services (2017). CMS Acceptable Risk Safeguards (ARS) (CMS_CIO-STD-SEC01-3.0). Baltimore, MD. Retrieved from https://www.cms.gov/Research-Statistics-Data-and-Systems/CMS-Information-Technology/InformationSecurity/Info-Security-Library-Items/ARS-30-Publication.html.

[25] Centers for Medicare and Medicaid Services (2015). Volume III: Catalog of Minimum Acceptable Risk Security and Privacy Controls for Exchanges. (MARS-E Document Suite, Version 2.0). Author: Baltimore, MD. Retrieved from https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/3-MARS-E-v2-0-Catalog-of-Security-and-Privacy-Controls-11102015.pdf.

[26] Health Information Trust Alliance (2018). HITRUST CSF Version 9.1. Author: Frisco, TX. Retrieved from https://hitrustalliance.net/csf-license-agreement/.



This approach is also used as the basis for Healthcare and Public Health (HPH) Sector guidance[27] on implementing the NIST Cybersecurity Framework,[28] published under the auspices of the Critical Infrastructure Protection Program.[29]

By applying a baseline set of controls from a comprehensive control framework developed from an analysis of reasonably anticipated threats to specific types of information using common technologies by similar organizations, one can be assured the organization is providing a known, minimally acceptable (i.e., adequate) level of protection for this information.

However, as indicated in the tailoring guidance provided earlier, organizations are also expected to address any unique threats it may face and address them accordingly. Fortunately, the selection of a control baseline reduces the problem space for the risk analysis required to create an organizationally-unique overlay for the baseline which makes the risk analysis more tractable. Successive iterations of the risk analysis, when required, are then limited to changes in the threat environment, as with the traditional approach.

Organizations can then focus on managing excessive residual risk— the risk that remains after all efforts have been made to mitigate, eliminate or transfer risks to their organization—by ensuring the selected safeguards are fully implemented and operating effectively.

---

[27] Joint Healthcare and Public Health Cybersecurity Working Group (2016). Healthcare Sector Cybersecurity Framework Implementation Guide. Critical Infrastructure Protection Advisory Council: Washington, D.C. Retrieved from https://www.us-cert.gov/ccubedvp/cybersecurity-framework#framework-guidance,

[28] National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cybersecurity Version 1.1. Author: Gaithersburg, MD. Retrieved from https://www.nist.gov/sites/default/files/documents////draft-cybersecurity-framework-v1.11.pdf.

[29] Sector guidance was developed and published by the Joint HPH Cybersecurity Working Group, as chartered by the Critical Infrastructure Protection Advisory Council. For more information, see https://www.dhs.gov/critical-infrastructure-sector-partnerships.

The HITRUST Approach

From its inception, HITRUST chose to use a risk-based rather than compliance-based approach to information protection and help mature the healthcare industry's approach to safeguarding information. By integrating NIST's moderate-level control baseline into the CSF, which is in turn built upon the ISO 27001:2005 control framework, HITRUST leverages the comprehensive threat analyses employed by these frameworks to provide a robust set of prescriptive controls relevant to the healthcare environment. The CSF also goes beyond the three baselines for specific classes of information and provides multiple control baselines determined by specific organizational, system and regulatory risk factors. These baselines can be further tailored through formal submission, review and acceptance by HITRUST of alternative controls, what PCI-DSS refers to as compensating controls, to provide healthcare with additional flexibility in the selection of reasonable and appropriate controls yet also provide assurance for the adequate protection of PHI.

The risk analysis guidance from HHS can subsequently be modified to support the use of a comprehensive control framework—built upon an analysis of common threats to specific classes of information and common technologies—as follows:

- Conduct a complete inventory of where ePHI lives
- Perform a BIA on all systems with ePHI (criticality)
- Categorize & evaluate these systems based on sensitivity & criticality
- Select an appropriate framework baseline set of controls
- Apply an overlay based on a targeted assessment of threats unique to the organization
- Evaluate residual risk
    - Likelihood based on an assessment of control maturity
    - Impact based on relative (non-contextual) ratings
- Rank risks and determine risk treatments
- Make contextual adjustments to likelihood & impact, if needed, as part of the corrective action planning process

Considering the reasonableness of this approach, one might ask why the use of a control baseline from a comprehensive control framework was not addressed in the original HIPAA Security Rule. The answer is quite simple: no healthcare-specific framework existed at the time. One might also ask why control baselines were not addressed in the Final Rule or by current OCR guidance. While not as simple, the answer is OCR does not currently endorse any framework, including their own—NIST. However, they do recognize the value added by such use.

> *While OCR does not endorse any particular credentialing or accreditation program, we certainly encourage covered entities and business associates to build strong compliance programs internally. Many of these credentialing/accreditation programs can help them do so…. OCR considers mitigation and aggravating factors when determining the amount of a civil monetary penalty, and these include the entity's history of prior compliance. An entity with a strong compliance program in place, with the help of a credentialing/ accreditation program or on its own, would have that taken into account when determining past compliance."*[30]

Assessments conducted under the HITRUST CSF Assurance Program have been successfully presented to OCR to support audits, investigations and resolution agreements on numerous occasions. HITRUST and the CSF have also been referenced as a resource by OCR in conducting a risk analysis per the HIPAA requirements.[31] But HITRUST believes more can be done in this area. HITRUST continues to evaluate the most efficient and effective methods for the selection, assessment, evaluation and reporting of information protection safeguards so that healthcare organizations can better manage cost, complexity and regulatory compliance. For example, future support for the HIPAA risk analysis requirement to identify all reasonably anticipated threats will be provided by the addition of a common threat catalog tied to the HITRUST CSF. Healthcare entities will subsequently be able to leverage the catalog to support their analysis of unique and changing threats. This information will also be tied to threat intelligence issued by the HITRUST Information Sharing and Analysis Organization (ISAO) to help organizations consume (utilize) the information, evaluate their cybersecurity preparedness, and ensure appropriate safeguards are in place.

Refer to the HITRUST white paper on Risk Management Frameworks[32] to learn more about RMFs and the relationship between NIST and the HITRUST CSF, and the Risk Analysis Guide for HITRUST Organizations & Assessors[33] to learn how HITRUST currently supports a HIPAA-compliant risk analysis and risk-based information protection.

Conclusion

The only thing constant about information security and privacy in the healthcare environment is change. New regulations, standards, guidance and tools continue to complicate the landscape, and organizations are left to determine how best to achieve compliance and provide an "adequate" level of protection.

[30] *Joint http://omnibus.healthcareinfosecurity.com/how-texas-boosting-hipaa-compliance-a-6800*
[31] *https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf*
[32] *https://hitrustalliance.net/documents/csf_rmf_related/HITRUST-RMF-Whitepaper.pdf*
[33] *https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf*

Healthcare organizations often do not have the skilled personnel or resources to develop a custom set of "reasonable and appropriate" safeguards. Instead, they often choose to adopt and adapt external information security control and risk management frameworks. But even this can be a difficult undertaking, requiring resources and expertise to integrate multiple international, federal and industry frameworks and best practice standards and adapt them to a healthcare environment. HITRUST was formed and the CSF was created in collaboration with the healthcare industry to establish a standard of due diligence and due care that can be tailored to an individual organization based upon their specific business requirements.

By leveraging the comprehensive analyses of common threats to specific classes of information and commonly used technologies, the CSF provides an easy yet effective way to ensure the implementation of a comprehensive set of information security controls that legitimately addresses threats that may be reasonably anticipated by healthcare organizations. The identification of unique threats and the selection of new controls or modification of existing controls then becomes a much simpler and more cost-effective risk analysis exercise for the organization.

Only by complying with the HIPAA risk analysis requirement—either by performing the analysis from scratch or relying on a risk analysis used to create a comprehensive controls framework such as NIST and the HITRUST CSF—can one legitimately support an assertion of compliance with the HIPAA Security Rule.

About HITRUST

Founded in 2007, HITRUST Alliance is a not-for-profit organization whose mission is to champion programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security and risk management leaders from both the public and private sectors, HITRUST develops, maintains and provides broad access to its widely adopted common risk and compliance management and de-identification frameworks; related assessment and assurance methodologies; and initiatives advancing cyber sharing, analysis and resilience.

HITRUST actively participates in many efforts in government advocacy, community building and cybersecurity education.

HITRUST is led by a seasoned management team and governed by a Board of Directors made up of leaders from across the healthcare industry and its supporters. These leaders represent the governance of the organization, but other founders also comprise the leadership to ensure the framework meets the short- and long-term needs of the entire industry.

For more information, visit www.HITRUSTalliance.net.

MyCSF

MyCSF is a fully integrated, optimized, and powerful tool that marries the content and methodologies of the HITRUST CSF and CSF Assurance Program with the technology and capabilities of a governance, risk and compliance (GRC) tool. The user-friendly MyCSF tool provides healthcare organizations of all types and sizes with a secure, Web-based solution for accessing the CSF, performing assessments, managing remediation activities, and reporting and tracking compliance. Managed and supported by HITRUST, MyCSF provides organizations with up-to-date content, accurate and consistent scoring, reports validated by HITRUST and benchmarking data unavailable anywhere else in the industry, thus going far beyond what a traditional GRC tool can provide.

For more information, visit http://www.hitrustalliance.net/mycsf.

HITRUST

855.HITRUST
(855.448.7878)
www.HITRUSTalliance.net