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

Why risk analysis is crucial to HIPAA compliance and an overall information protection program
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Introduction</td>
<td>3</td>
</tr>
<tr>
<td>Compliance</td>
<td>3</td>
</tr>
<tr>
<td>HIPAA Compliance</td>
<td>4</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>6</td>
</tr>
<tr>
<td>HITRUST Approach</td>
<td>9</td>
</tr>
<tr>
<td>Conclusion</td>
<td>11</td>
</tr>
<tr>
<td>About HITRUST</td>
<td>12</td>
</tr>
<tr>
<td>MyCSF</td>
<td>12</td>
</tr>
</tbody>
</table>
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 the various concepts and HITRUST’s approach regarding the CSF and CSF Assurance programs. 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 to ensure compliance.

Compliance
Regulatory compliance refers to the adherence to laws, regulations, guidelines and 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 Simplification1 and industry specifications such as the Payment Card Industry Digital Security Standard (PCI-DSS). Furthermore, 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, 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, reputational and financial risks from an actual loss of confidentiality, integrity and availability—are simply not a normal part of the compliance equation.

HIPAA Compliance

In recent times, “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 Rule’s implementation specifications, organizations subsequently checked the box—albeit inappropriately—for the risk analysis without actually conducting one.

When asked at the 2014 Health Care Compliance Associate (HCCA) Conference in San Diego, Linda Sanchez, 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. Although the Audit 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 45 CFR § 164.308(a)(1)
3 45 CFR § 164.306(a)(2)
The problem organizations encounter by not performing such a risk analysis can best be demonstrated by looking at 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.” This maps the HIPAA Security Rule⁴ requirements against the comprehensive control framework specified in NIST SP 800-53 revision 3, “Recommended Security Controls for Federal Information Systems and Organizations,” which is based on such a risk analysis. Of all controls listed, regardless of the selection for 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 a particular baseline.

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


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 Common Security Framework (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 Common Security Controls map directly to the HIPAA Security Rule6,7. Exceptions include but are not limited to 01.w, Sensitive System Isolation; 05.f, Contact with Authorities; 05.j, Addressing Security When Dealing with Customers; 08.m, Removal of Property; 09.y, On-line Transactions; 09.ac, Protection of Log Information; 09.af, Clock Synchronization; 10.b, Input Data Validation; 10.e, Output Data Validation; 10.h, Control of Operational Software, and 10.k, Change Control Procedures. In addition, there are 55 specific NIST SP 800-53 r4 controls8—also common to r3—that are referenced by the Framework for Improving Critical Infrastructure Cybersecurity9 but do not map to the HIPAA standards and implementation specifications in NIST SP 800-66 r1.

The position that simply focusing on the HIPAA standards and implementation specifications will not yield a valid risk analysis also appears to be supported by HHS, which states in their Guidance on Risk Analysis Requirements under the HIPAA Security Rule 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.” Implementing the standards and 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

The Committee for National Security Systems Instruction (CNSSI) 400910, National Information Assurance Glossary, defines a risk analysis as an examination of information to identify the risk to an information asset, but as the term is a candidate for deletion it also refers to the definition of a risk assessment:

> The process of identifying, prioritizing, and estimating risks. This includes determining the extent to which adverse circumstances or events could impact an enterprise. Uses the results of threat and vulnerability assessments to identify risk to organizational operations and evaluates those risks in terms of likelihood of occurrence and impacts if they occur. The product of a risk assessment is a list of estimated, potential impacts and unmitigated vulnerabilities. Risk assessment is part of risk management and is conducted throughout the Risk Management Framework (RMF).

---


7 Note the CSF maps to 100% of the Security Rule’s standards and implementation specifications.


The Glossary goes on to provide a definition of risk assessment from NIST SP 800-53 r4:

*The process of identifying risks to organizational operations (…), 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.*

Regardless of the specific model 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 when 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 impact
- Risk expressed as control effectiveness
- No documentation of risk treatments, especially of risk acceptance
- Failure to address corrective actions for all risks requiring mitigation

Of these, the threat and impact analyses are perhaps the most difficult. From a quantitative viewpoint, the process of determining the likelihood of a threat occurrence is virtually impossible for most—if not all—organizations, and is 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 of the threat source and the difficulty or cost associated with exploiting one or more vulnerabilities to achieve the actor’s objectives.

An alternative to this traditional approach to risk analysis is to rely on a comprehensive control framework, which is already built upon a broad analysis of threats faced by a specific type of organization with specific types of information, using similar 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 with their respective information security control and risk management frameworks. To understand how this works, one must understand how risk analysis supports the overall risk management process. Although several models exist, the activities can be distilled into a basic four-step model.

---

11 Formerly three separate control framework, they are currently in the process of being consolidated into a single framework for all federal agencies including the IC and DOD under a general NIST umbrella.
Step 1—Identify Risks and Define Protection Requirements
This is the risk analysis, 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.

Step 3—Implement and Manage Controls
Controls are implemented through an organization's normal operational, 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 to focus on the first two steps. 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. By applying a baseline set of controls from a comprehensive control framework developed from an analysis of common 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, 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 as discussed in NIST SP 800-53 r4, 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.
HITRUST Approach

From its inception, HITRUST chose to use a risk-based approach rather than compliance-based approach to information protection and to 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 Business Impact Analysis (BIA) on all systems with ePHI (criticality)
- Categorize and evaluate these systems based on sensitivity and 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 and 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.\textsuperscript{12}

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\textsuperscript{13}. 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 Cyber Threat Intelligence and Incident Coordination Center (C\textsuperscript{3})\textsuperscript{14}, 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\textsuperscript{15} to learn more about RMFs and the relationship between NIST and the HITRUST CSF, and the Risk Analysis Guide for HITRUST Organizations & Assessors\textsuperscript{16} to further 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.

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

\textsuperscript{12} \url{http://omnibus.healthcareinfosecurity.com/how-texas-boosting-hipaa-compliance-a-6800}
\textsuperscript{13} \url{http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf}
\textsuperscript{14} \url{http://hitrustalliance.net/cyber-threat-intelligence/}
\textsuperscript{15} \url{http://hitrustalliance.net/content/uploads/2014/05/HITRUST-RMF-Whitepaper2.pdf}
\textsuperscript{16} \url{http://hitrustalliance.net/content/uploads/2014/05/Risk-Analysis-Guide.pdf}
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

The Health Information Trust Alliance (HITRUST) was born out of the belief that information security should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST, in collaboration with healthcare, business, technology and information security leaders, has established the Common Security Framework (CSF), a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information. Beyond the establishment of the CSF, HITRUST is also driving the adoption of and widespread confidence in the framework and sound risk management practices through awareness, education, advocacy and other outreach activities.

For more information, visit 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 hitrustalliance.net/mycsf.