HITRUST®

HITRUST® CSF Risk Factors

How HITRUST uses risk factors to help healthcare organizations dynamically tailor CSF controls to meet their information protection needs

February 2018

Introduction

The Health Information Trust Alliance (HITRUST) was formed in mid-2007 to ensure that information security is a core pillar of, rather than an obstacle to, the healthcare industry. The original HITRUST Board of Directors, which included Chief Information, Security and Privacy Officers from leading healthcare providers, insurers and vendors, understood that information security was critical to the broad adoption of healthcare technologies and systems necessary to provide a greater quality of care.

With the advent of the CSF, organizations were given a consensus-driven solution to address problems with security in the industry. The CSF not only provides the prescriptiveness needed for healthcare organizations to effectively implement controls to meet regulatory, third party and business requirements, it did so in a way that was scalable based on key organizational, system and regulatory risk factors. These factors, which were developed through industry working groups, representing a variety of healthcare sectors, allow large, highly complex healthcare insurers as well as smaller, resource-constrained providers to adopt an approach to security that may be tailored to their risk and compliance needs.

This paper presents the concept of tailoring a general baseline to create an industry sector or sub-sector overlay, consistent with federal guidance, and how the CSF leverages this concept to allow users of the CSF to dynamically create a new baseline from the CSF that is custom to the types of healthcare entities defined by their risk factors. We then present the CSF risk factors as they were defined since the CSF's inception, followed by a description of changes to organizational risk factors as recommended by a HITRUST-sponsored working group made up of various stakeholder organizations within the healthcare industry.

Contents

Introduction 2

Baselines 4

Tailoring 5

Overlays 6

Original Risk Factors 8

Updated Risk Factors 10

- Risk Factors Working Group 10
- Revised Risk Factors 10
  - General 10
  - Payer 11
  - Hospital / Inpatient Facility 11
  - Pharmacy / Pharmacy Benefit Management (PBM) 11
  - Physician Practice 11
  - Health Information Exchange (HIE) 11
  - Service Provider (Information Technology, IT) 11
  - Service Provider (Non-IT) 12
  - Deleted Vertical 12

Conclusion 14

Baselines

It's well-understood in the healthcare industry that the Health Information Portability and Accountability Act (HIPAA) Administrative Simplification[1] requires covered entities and business associates to "ensure the confidentiality, integrity, and availability of all electronic protected health information [ePHI] the covered entity or business associate creates, receives, maintains, or transmits [and] protect against any reasonably anticipated threats or hazards to the security or integrity of such information."[2] To do so, these organizations must "implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level,"[3] which in turn is determined by conducting "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability [CIA] of [ePHI] held by the covered entity or business associate."[4]

What's not well-understood—as evidenced from the first round of OCR audits—is how these organizations should go about complying with the Rule's requirements for a risk analysis, as well as what constitutes a reasonable and appropriate level of protection.

Although the Department of Health and Human Services describes a traditional, "built-from-scratch" approach to conducting a risk analysis in its Final Guidance on Risk Analysis,[5] conducting such an analysis can be difficult for many organizations.[6] In fact, the federal government actually takes a different approach to ensuring reasonable and appropriate protection, and they do this by leveraging a common risk management framework (RMF) developed by the National Institute of Standards and Technology (NIST) to determine a minimum acceptable baseline set of security safeguards called controls. Depending on the CIA requirements of the information being protected, agencies may select one of three minimum security baselines from NIST Special Publication (SP) 800-53.[7]

However, while this obviates the need for an agency or other organization relying on a NIST baseline to conduct a traditional risk analysis, there's more work that needs to be done.

1. *http://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf*
2. *HIPAA § 164.306(a)(1)-(2)*
3. *HIPAA § 164.308(a)(ii)(B)*
4. *HIPAA § 164.308(a)(ii)(A)*
5. *http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalintro.html*
6. *https://hitrustalliance.net/documents/csf_rmf_related/RiskAnalysisGuide.pdf*
7. *http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf*

Tailoring

Once a minimum security baseline is selected, organizations are expected to do a smaller, arguably more tractable risk analysis of its unique business and system environment.

> *The security controls in the [NIST] catalog with few exceptions, have been designed to be policy- and technology-neutral. This means that security controls and control enhancements focus on the fundamental safeguards and countermeasures necessary to protect information during processing, while in storage, and during transmission…. Application specific areas are addressed by the use of the tailoring process.*[8]

Tailoring a baseline allows organizations to achieve cost-effective, risk-based security that supports operational and business needs,[9] and the process is relatively straightforward. First, organizations should identify and designate common controls in a baseline; apply scoping considerations to the remaining baseline security controls; select alternate (compensating) controls, if needed; assign specific parameters if a control doesn't provide them; supplement the baseline with additional control requirements, if needed; and provide additional information to support implementation, if needed.[10]

This tailoring of a minimum security baseline is consistent with HIPAA requirements for reasonable and appropriate protection as HIPAA also states covered entities and business associates may "use any security measures that… reasonably and appropriately implement the standards and implementation specifications"[11] by taking into consideration its size, complexity and capabilities; its technical infrastructure, hardware and software security capabilities; the costs of security measures, and the probability and criticality of potential risks to ePHI.[12] Note risk analysis is one of those implementation specifications.[13]

The tailoring process may be performed for and by a single organization for a specific system, or it may be performed more broadly to create an overlay.

8. *NIST SP 800-53 r4, p. ix*
9. *Ibid, p. 31*
10. *Ibid, pp. 30-31*
11. *HIPAA § 164.306(b)*
12. *HIPAA § 164.306(b)(i) thru (iv)*
13. *HIPAA § 308(a)(ii)(A)*

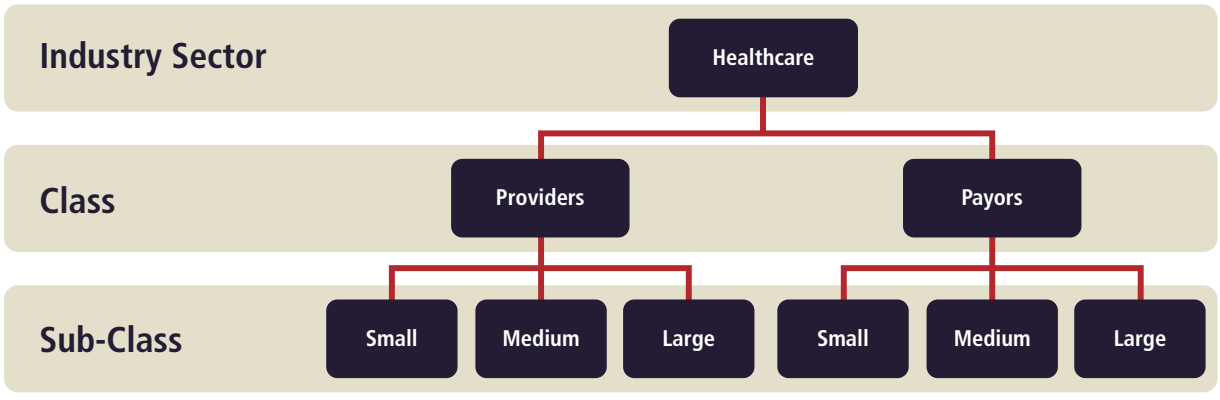
Overlays

An overlay is "a fully specified set of security controls, control enhancements, and supplemental guidance derived from the application of tailoring guidance … for community-wide use or to address specialized requirements, technologies, or unique missions/environments of operation."[14] Tailored baselines can be developed for "unique circumstances/environments and promulgated to large communities of interest—thus achieving standardized security capabilities, consistency of implementation, and cost-effective security solutions."[15]

In developing the CSF, HITRUST integrated and harmonized requirements from multiple healthcare-related authoritative sources and applied the tailoring process to create all the controls in the framework, which in NIST terms constitutes an overlay for the healthcare industry but for all intents and purposes becomes its initial baseline. At this point, healthcare organizations would be expected to tailor this baseline to address their specific needs. However, HITRUST helps organizations with this tailoring process by using specific risk factors to tailor the initial comprehensive baseline and create overlays—essentially new baselines—for specific sub-classes of organizations that are defined by those factors.

We do this by defining healthcare as the industry sector and verticals within healthcare, such as providers and payers, as classes within the sector. Subsequently, we may then examine what makes these classes different and tailor a baseline defined for healthcare into multiple overlays, one for each class of healthcare. However, not all organizations within a common vertical will present the same risks. For example, the risks posed by a large, geographically-diverse health system that exchanges information with multiple business partners may not present the same level of risk that a small, independent community clinic with no information exchange. Thus healthcare organizations within a vertical or class may be further subdivided based on other criteria, such as their size, the type of architectures and/or technologies in the environment, and the type of regulatory and other requirements to which healthcare organizations may be subject.

The following diagram provides a graphical depiction of what this would look like if subclasses for payers and providers were limited to small, medium and large organizations.



14. NIST SP 800-53 r4, p. 40

15. Ibid.

The key to creating the sub-classes is to identify risk factors that will provide a reasonable and meaningful categorization of relative risk between sub-classes, so that the resulting baselines present an appropriate number and rigor of controls to reduce the residual risk for each subcategory to a similar level.

> *Risk models define the risk factors to be assessed and the relationships among those factors. Risk factors are characteristics used in risk models as inputs to determining levels of risk in risk assessments. Risk factors are also used extensively in risk communications to highlight what strongly affects the levels of risk in particular situations, circumstances, or contexts. Typical risk factors include threat, vulnerability, impact, likelihood, and predisposing condition [emphasis added].*[16]

NIST defines a predisposing condition as one that "exists within an organization, a mission or business process, enterprise architecture, information system, or environment of operations, which affects (i.e., increases or decreases) the likelihood that threat events, once initiated, result in adverse impacts to organizational operations and assets, individuals, [or] other organizations."[17]

Type	Example	Effect on Risk
Physical	Flood Plain	Increased likelihood of exposure to hurricanes or floods
Technical	Stand-alone System	Decreased likelihood of exposure to a network-based attack
Administrative	Gap in Contingency Plans	Increased likelihood of exposure to a disruption in operations

Table 1: Predisposing Conditions

HITRUST leverages this concept of predisposing conditions along with scoping considerations (e.g., system functionality and public access in the operational environment) to help categorize the relative risk between healthcare organizations, their architecture/technology, and their legislative, regulatory and contractual requirements to create the subclasses and their respective overlays—new baselines—as defined by their respective risk factors.

16. *NIST SP 800-30 r1, p. 8*
17. *Ibid, p. 10*

Original Risk Factors

HITRUST defines a risk factor—for the purposes of producing custom baselines (overlays) for the specific subclasses of healthcare organizations specified by all risk factors—as a listing of organizational, system, and regulatory factors that drive requirements for a higher level of control, for which the CSF has three general implementation levels and multiple industry segments for unique requirements, such as for Health Insurance Exchanges, to address increasing levels of inherent risk.

The following is an extract from the 2015 CSF version 7.0, which provides the list of factors by type as determined by the industry working group that created the CSF circa 2008:[18]

Organizational Factors: The Organizational Factors are defined based on the size of the organization and complexity of the environment as follows:

- Volume of business
  - Health Plan / Insurance – Number of Covered Lives
  - Medical Facilities / Hospital – Number of Licensed Beds
  - Pharmacy Companies – Number of Prescriptions Per Year
  - Physician Practice – Number of Visits Per Year
  - Third Party Processor – Number of Records Processed Per Year
  - Biotech Companies – Annual Spend on Research and Development
  - IT Service Provider / Vendor – Number of Employees
  - Health Information Exchange – Number of Transactions Per Year
- Geographic scope
  - State
  - Multi-state
  - Off-shore (outside U.S.)

Regulatory Factors: The regulatory factors are defined based on the compliance requirements applicable to an organization and systems in its environment:

- Subject to PCI Compliance
- Subject to FISMA Compliance
- Subject to FTC Red Flags Rules

18. https://hitrustalliance.net/hitrust-csf/

- Subject to the State of Massachusetts Data Protection Act
- Subject to the State of Nevada Security of Personal Information Requirements
- Subject to the State of Texas Medical Records Privacy Act
- Subject to Joint Commission Accreditation
- Subject to CMS Minimum Security Requirements (High-level Baseline)
- Subject to MARS-E Requirements
- Subject to FTI Requirements

System Factors: The system factors are defined considering various system attributes that would increase the likelihood or impact of a vulnerability being exploited. These factors are to be assessed for each system or system grouping to determine the associated level of control.

- Stores, processes, or transmits PHI
- Accessible from the Internet
- Accessible by a third party
- Exchanges data with a third party/business partner
- Publicly accessible
- Mobile devices are used
- Connects with or exchanges data with a Health Information Exchange (HIE)
- Number of interfaces to other systems
- Number of users
- Number of transactions per day

For example, let's assume that, for a system to increase from a level 1 implementation requirement to a level 2 or 3 implementation requirement, the system must be processing ePHI AND include at least one of the other system factors associated with the control. For example, if a system is accessible from the Internet, exchanges data with a business partner, and has the level 2 threshold number of users, but DOES NOT process ePHI, that system is only required to meet the level 1 implementation requirements. However, if another system DOES process ePHI AND is accessible from the Internet, then that system must meet an implementation requirement level higher than level 1.

If a control contains more than one category of factors, the organization must adhere to the highest level of implementation requirements driven by the factors. For example, if a health plan is at the level 2 threshold for a control based on their number of covered lives but must also be FISMA compliant (implementing and adhering to the controls specified in NIST SP 800-53), the organization must implement the Level 3 requirements of the CSF if FISMA is a Level 3 regulatory factor for that control.

In this way, users of the CSF are able to create—in a very dynamic way—a custom baseline for their subclass of healthcare organizations based on their applicable risk factors.

Updated Risk Factors

Risk Factors Working Group

Since the CSF was first published for use in 2009, HITRUST has endeavored to maintain its relevance by regularly reviewing changes in source frameworks and best practices, changes in the regulatory or threat environment, and the analysis of breach incidents to determine the root cause and any potential impact to the CSF. The CSF is updated no less than annually, which is much timelier than other standards and best practice frameworks like ISO/IEC 27001, NIST SP 800-53, or PCI DSS. Updates to these other standards and framework may also not reflect new federal or state regulations or legislation relevant to healthcare (e.g., the HIPAA Omnibus and TX HB 300). The ongoing enhancements and maintenance to the CSF provide continuing value to healthcare organizations, sparing them from much of the complexity and expense of integrating and tailoring these multiple requirements and best practices into a custom framework of their own.

In August of 2014, as part of this ongoing maintenance of the CSF, HITRUST chartered an industry working group to examine the current risk factors and make recommendations for improvement if needed. Upon review, the working group determined that modifications to the volume of business in the organizational factors were needed.

Revised Risk Factors

General: The consensus of working group members was that a significant determinant of relative risk amongst organizations is the number of individual records that they hold and/or process, regardless of the class (or vertical) in which the organization resides. The rationale is based primarily on common use of the average cost of a breach per individual record compromised to estimate the costs of a specific breach. Further, the total number of individual records that could potentially be compromised then provides an estimate of the organization's maximum exposure in the event of such a catastrophic breach.

However, since in HITRUST's experience not all healthcare organizations can provide a precise estimate of the total number of individual records they hold, the working group decided to provide an alternative risk factor based on the number of individual records processed annually. While not the best indicator for the organization's maximum exposure due to a catastrophic breach of all records held, the two are reasonably correlated.

Working group members determined that changes to the system and regulatory risk factors are not needed at this time.

We now present specific changes, if any, to the organizational risk factors by healthcare vertical.

Payer: This vertical was previously titled "Health Plan / Insurance." Payers are covered entities identified as "Health Plans" under HIPAA, and are defined as an individual or group plan that provides, or pays the cost of, medical care.[19] Health Insurance Exchanges (HIXs) are also considered payers for this purpose.[20] The Working Group kept the existing risk factor for number of covered lives as another means of classifying a payer's volume of business.

Hospital / Inpatient Facility: This vertical was previously titled "Medical Facilities / Hospital." Hospitals and other inpatient facilities are identified as "Providers" under HIPAA, and are generally defined as a place for receiving medical or surgical care, usually as an inpatient (resident). The Working Group added another new risk factor in addition to record counts. Entitled "Number of Admissions," the members based the implementation level cut-offs on an average of 6318 annual admissions.[21]

Pharmacy / Pharmacy Benefit Management (PBM): This vertical was previously titled "Pharmacy Companies." Pharmacies are identified as "Providers" under HIPAA, and are generally defined as a place where medicines are prepared, compounded, dispensed or sold. The Working Group kept the existing risk factor for annual number of prescriptions as another means of classifying a pharmacy or PBM's volume of business.

Physician Practice: Physician practices are identified as "Providers" under HIPAA, and are defined as medical practices comprised of two or more physicians organized to provide patient care services (regardless of its legal form or ownership).[22] The working group modified the original factor for the number of patient encounters and added a factor for the number of physicians in the practice. Cutoffs for each of the three possible CSF levels for both factors were determined by the working group leveraging information contained in a 2013 American Medical Association survey.[23]

Health Information Exchange (HIE): HIE is a term used to describe both the sharing of health information electronically among two or more entities and also a health information exchange organization that provides services that enable the sharing electronically of health information.[24] The Working Group kept the existing risk factor for volume of data exchanged as another means of classifying a non-IT service provider's volume of business.

Service Provider (Information Technology, IT): This vertical was previously titled "IT Service Provider / Vendor." Service providers (IT) are generally entities that provides IT services, such as Cloud services and hosted IT infrastructure. The Working Group replaced the existing risk factor titled "Number of Employees" with a new risk factor titled "Data Volume," which is based on an estimated 80MB per person rounded to the nearest 5 TB.

19. *§2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)*
20. *http://obamacarefacts.com/obamacare-health-insurance-exchange/*
21. *http://www.aha.org/research/rc/stat-studies/fast-facts.shtml*
22. *https://questions.cms.gov/faq.php?id=5005&faqId=2327*
23. *http://www.nmms.org/sites/default/files/images/2013_9_23_ama_survey_prp-physician-practice-arrangements.pdf*
24. *http://www.hrsa.gov/healthit/toolbox/RuralHealthITtoolbox/Collaboration/whatishie.html*

Service Provider (Non- IT): This vertical was previously titled "Third Party Processor." Non-IT service providers are generally defined as business associates that provide non-IT services, such as transcription services and clearinghouses. The Working Group kept the existing risk factor for volume of data exchanged as another means of classifying a non-IT service provider's volume of business.

Deleted Vertical: The vertical titled "Biotech Companies" was deleted due to lack of demand for assessments since the CSF was first published.

The table below provides the ranges for each of the three general implementation levels for CSF controls by healthcare vertical and organizational risk factor for volume of business, and includes the general organizational risk factors for record count along with any new risk factors or changes to existing risk factors by healthcare industry vertical.

Risk Factor	Level 1	Level 2	Level 3
Payer			
Record Count: Total	< 10M	10M – 60M	> 60M
Record Count: Annual	< 180K	180K – 725K	> 725K
Number of Covered Lives	< 1M	1M – 7.5M	>
Hospital / Inpatient Facility			
Record Count: Total	< 10M	10M – 60M	> 60M
Record Count: Annual	< 180K	180K – 725K	> 725K
Number of Admissions: Annual	< 7500	7500 – 20K	> 20K
Number of Beds	< 200	200 – 750	> 750
Pharmacy/PBM			
Record Count: Total	< 10M	10M – 60M	> 60M
Record Count: Annual	< 180K	180K – 725K	> 725K
Number of Prescriptions: Annual	< 10M	10M – 60M	> 60M
Physician Practice			
Record Count: Total	< 10M	10M – 60M	> 60M
Record Count: Annual	< 180K	180K – 725K	> 725K
Number of Patient Encounters: Annual	< 40K	40K – 100K	> 100K
Number of Physicians	< 11	11 – 25	> 25
Health Information Exchange (HIE)			
Record Count: Total	< 10M	10M – 60M	> 60M
Record Count: Annual	< 180K	180K – 725K	> 725K
Transactions: Annual	< 1M	1M – 6M	> 6M
Service Provider (IT)			
Record Count: Total	< 10M	10M – 60M	> 60M
Record Count: Annual	< 180K	180K – 725K	> 725K
Data Volume	< 15TB	15TB – 60TB	> 60TB
Service Provider (Non-IT)			
Record Count: Total	< 10M	10M – 60M	> 60M
Record Count: Annual	< 180K	180K – 725K	> 725K
Volume of Data Exchanged: Annual	< 25MB	25MB – 100MB	> 100MB

Table 2: Organizational Factors: Volume of Business

Note, the CSF implementation level for an applicable CSF control is determined by one and only one risk factor of the multiple risk factors listed in the table for each healthcare vertical in the order of preference indicated. System risk factors only impact implementation level selection for system controls; however, regulatory factors can force selection of a higher implementation level for either organizational or system controls as previously discussed. The geographic scope factors described previously on page 8 are also retained.

Conclusion

Although DHS guidance on risk analysis specifies a traditional approach to risk analysis, the federal government uses a framework-based approach in which organizations are presented with a minimum baseline set of controls that addresses common threats to similar types of information used by similar types of organizations (in this case, federal agencies). Each organizations is then expected to tailor the selected baseline to better address those threats that may be unique to it.

HITRUST takes a similar approach and provides a prescriptive control framework, the CSF, which allows organizations to effectively implement a reasonable and appropriate set of controls that provides adequate protection of health information, as required by HIPAA, as well as meet other regulatory, third party and business requirements. It does so by providing some initial tailoring of the CSF to a common class of healthcare organizations that present a similar level of risk through the application of key organizational, system and regulatory risk factors. These factors, which were developed through industry working groups, representing a variety of healthcare sectors, allow large, highly complex healthcare insurers as well as smaller, resource-constrained providers to adopt an approach to security that may be further tailored to their individual risk and compliance needs.

As HITRUST continually strives to maintain the framework's relevance to the healthcare industry, the CSF is updated no less than annually to address changes in the authoritative sources that the CSF harmonizes and integrates as well as changes in the healthcare threat environment. The ongoing enhancements and maintenance of the CSF continues to ensure the framework provides value to healthcare organizations, sparing them from much of the complexity and expense of addressing its requirements for due care and due diligence on their own.

As part of the ongoing maintenance of the CSF, HITRUST chartered an industry working group consisting of representatives from multiple healthcare organizations to review the current risk factors, which have been used since the CSF's inception, and make recommendations for change if necessary to ensure their continued relevance in the ever changing healthcare environment. Upon review, the working group recommended specific changes to the organizational risk factors for volume of business, the most notable of which were recommendations for a vertical-independent factor for individual health record count.

Today, the CSF is the most widely adopted information security and compliance risk management framework in the healthcare industry. Through annual updates and significant community engagement, the CSF has evolved to effectively align the requirements and controls of over 15 standards, regulations, and best practice frameworks. Organizations are also proactively seeking Certification and Validation of their CSF-based information protection programs through the CSF Assurance Program due to the value it provides, especially with regard to third party assurances for regulators and other external stakeholders.

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net