HITRUST

Risk Analysis Guide for HITRUST Organizations & Assessors

A guide for self and third-party assessors on the application of HITRUST's approach to risk analysis

February 2016

Contents

Preface

The HITRUST Common Security Framework™ (CSF) and CSF Assurance Program™ provide a consistent, managed methodology for the assessment and certification of healthcare entities and the sharing of compliance and risk information amongst these entities and their key stakeholders. However, to provide the level of consistency and repeatability needed for an industry-accepted framework, both organizations receiving assessments and the assessors conducting the assessments (either self- or third-party) must fully understand the methodology in order to apply it appropriately.

This risk analysis guide for HITRUST organizations and assessors:

- Provides introductory information on risk management frameworks (RMFs) and the HITRUST RMF,
- Briefly describes CSF assessments and the CSF control structure,
- Presents the HITRUST maturity model used to evaluate control effectiveness along with several explanatory examples,
- Discusses the use of HITRUST's illustrative procedures in conjunction with general criteria for each maturity level, and
- Provides an appendix on risk treatments, which includes some of HITRUST's views on transference, avoidance, mitigation and acceptance with explanatory examples, including corrective action plan (CAP) prioritization and alternate control risk analysis.

Users of this guide are expected to have a basic level of knowledge about information security and privacy, risk management and risk analysis commensurate with holders of the International Information Systems Security Certification Consortium (ISC)²™ Health Care Information Privacy and Security Practitioner (HCISPP℠) certification or the HITRUST Certified CSF Practitioner (CCSFP™) credential. Alternatively, readers should review the following documentation prior to using this guide:

- HITRUST RMF Whitepaper
- HITRUST CSF Assessment Methodology
- HITRUST CSF Assurance Program Requirements

Readers may also benefit from reviewing other CSF assessment-related information:

- Comparing the CSF, ISO/IEC 27001 and NIST SP 800-53
- HITRUST MyCSF™ datasheets

Introduction

The Health Insurance Portability and Accountability Act (HIPAA) Final Omnibus Rule requires covered entities and their business associates (BAs) to implement "reasonable and appropriate safeguards" to provide "adequate protection'" for sensitive health information. But what constitutes reasonable, appropriate or adequate? Or stated another way, how can an organization select and implement a specific set of controls to manage information security and privacy-related risk at an acceptable level?

The textbook answer is through a comprehensive risk analysis that (1) includes threat and vulnerability assessments, information asset valuation, and the selection of a comprehensive set of information security and privacy controls that address the enumerated threat-vulnerability pairs (a process sometimes referred to as threat modeling), (2) is cost-effective, and (3) manages risk at a level deemed acceptable by the organization.

In practice, this process is virtually impossible for most—if not all—organizations from a quantitative viewpoint. For example, 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 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 threat actor's objectives. As a result, it is similarly difficult to develop a valid business case for a specific risk response or treatment based on a return on investment. Organizations could take a semi- or quasi-quantitative approach or even a purely qualitative approach; however, it would still be difficult for an organization—especially one in healthcare—to develop a valid business case, particularly for a comprehensive set of risk responses.

An alternative approach is to rely on another organization that does have the resources to develop such a set of controls that addresses similar threats to similar information and technologies used by their own organization. This is the approach employed by the intelligence community (IC), defense department and civilian agencies of the federal government with their respective information security control frameworks, which are currently in the process of being consolidated into a single framework for all federal agencies. It is also the approach used by HITRUST with the CSF, the most widely adopted security framework in the U.S. healthcare industry.

The security control frameworks noted above are also part of a broader risk management framework. For the IC, it was embodied in Director of Central Intelligence Directive (DCID 6/3). For the Department of Defense (DoD), it was the control catalog contained in DoD Instruction (DoDI) 8500.2 combined with other documentation such as the Defense Information Assurance Certification and Accreditation Process (DIACAP) outlined in DoDI 8510.01. For federal civilian agencies, it continues to be the control catalog contained in NIST SP 800-53 r4 and the many publications that make up the NIST Risk Management Framework. And for government healthcare entities, it includes other NIST resources such as NIST SP 800-66 r1, which provides information on how NIST controls support the HIPAA Security Rule, and the NIST HIPAA Security Rule (HSR) Toolkit.

The risk management framework for the broader U.S. healthcare industry consists of the HITRUST CSF combined with CSF Assurance Program-related documents and tools, such as the HITRUST CSF Assurance Program requirements, HITRUST CSF Assessor requirements, HITRUST CSF assessment methodology, and HITRUST's comprehensive online tool, MyCSF.

HITRUST Risk Management Framework (RMF)

Organizations can use targeted risk assessments, in which the scope is narrowly defined, to produce answers to specific questions … or to inform specific decisions[,] … have maximum flexibility on how risk assessments are conducted, … [and] are encouraged to use [NIST] guidance in a manner that most effectively and cost-effectively provides the information necessary to senior leaders/executives to facilitate informed decisions. (NIST SP 800-30 r1)

The HITRUST RMF is a custom framework built around a basic four-step risk management process model designed to meet the specific needs of the healthcare industry.

Step 1—Identify Risks and Define Protection Requirements

The objective of this step is to determine the risks to information and information assets that are specific to the organization. Risks can be identified through the analysis of regulations and legislative requirements, breach data for similar organizations in the industry, as well as an analysis of current architectures, technologies, market trends and related threats. The end result of this analysis should be a prioritized list of high-risk areas and an overall control strategy to minimize the risk to the organization from its use of PHI and other sensitive or business critical information in terms of overall impact to the organization.

The HITRUST RMF, through the CSF, rationalizes relevant regulations and standards into a single overarching control framework to help healthcare organizations meet healthcare clinical and business objectives and satisfy multiple regulatory and other compliance requirements.

Step 2—Specify Controls

The next step 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, detailed and prescriptive set of control recommendations that are customized for the healthcare organization. A control-based risk management framework will provide a comprehensive control catalog as well as specific criteria for the selection of a baseline set of controls, which is performed in this step.

HITRUST built the CSF to accommodate multiple control baselines, and controls are assigned to specific baselines using three risk factors: organizational type and size (e.g., a physician practice with fewer than 60,000 visits per year), system requirements (e.g., the system stores ePHI, is accessible from the Internet, and processes fewer than 6,750 transactions per day), and regulatory requirements (e.g., subject to FTC Red Flags Rule and PCI-DSS compliance). The result is a healthcare industry-specific baseline, which can be further tailored to an organization's specific clinical, business and compliance requirements.

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. A risk management framework will provide guidance and tools for the implementation of the framework, including the controls specified earlier in step 2.

HITRUST trains third party consulting and assessment firms in the CSF and CSF Assurance Program methodologies and tools so that they may offer CSF implementation support, as recommended by OCR, to healthcare provider organizations that lack the capability to implement and assess information security and privacy controls.

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. The end result of these assessment and reporting activities is a risk model that assesses internal controls and those of business associates based on the risk factors identified in Step 2. It should also provide common, easy-to-use tools that address requirements and risk without being burdensome, support third party review and validation, and provide common reports on risk and compliance.

An integral component of the HITRUST RMF is the HITRUST risk assessment methodology, which is built around the concept of residual risk: the risk that remains after controls have been fully implemented. Thus, excessive residual risk occurs when one or more controls are not fully implemented, and it is this risk, i.e., risk that has not been formally accepted by management, which the organization must strive to minimize through avoidance, transference or mitigation.

Figure 1. Risk Management Lifecycle

More detailed information on the HITRUST RMF, such as on the detailed risk factors and how they are used to select an initial set of baseline controls, can be found in the HITRUST RMF Whitepaper.

HITRUST CSF Assessments

Approach

A CSF assessment provides organizations with a means to assess and communicate their current state of security and compliance with external entities along with a CAP to address any identified gaps. An organization can, using the services of a CSF Assessor or performing a self-assessment, conduct an assessment against the CSF and have the results reported by HITRUST under the CSF Assurance Program. Although HITRUST organizations must implement all the CSF controls that apply based on their risk factors to manage risk to an acceptable level, the assessed entity is not required by HITRUST to demonstrate compliance with all of them to obtain certification against the framework. Instead, a CSF Baseline assessment provides stakeholders with a snapshot into the current state of security and compliance of the assessed entity for a specific set of controls, which were selected based on an analysis of healthcare data breaches and the need for minimal but complete coverage of the HIPAA Security Rule implementation specifications. A comprehensive mapping of the CSF to the HIPAA Security Rule can be downloaded from the HITRUST Website.

The level of assurance the assessed entity and/or the relying entity on behalf of the assessed entity has chosen determines the assessment strategy: self-assessment or third party. As suggested by the name, a third party on-site assessment provides a higher level of assurance since it includes independent testing of the security controls, providing a more complete picture of security and compliance to both the assessed entity and the relying entity.

Baseline

As stated previously, a CSF Baseline Assessment is conducted by the assessed entity (self-assessment) or on behalf of the assessed entity (third party assessment) against the controls required for certification and grouped according to specific areas of concern, e.g., an organization's risk management program, access control and physical and environmental security. This is the most cost-effective and efficient assessment for providing necessary assurances to business partners, patients and their families, regulators and other interested stakeholders.

Comprehensive

The CSF Comprehensive Assessment is conducted against all the CSF controls that are in scope for the organization based on their risk factors. This assessment provides a more comprehensive picture of the organization's control environment and, when conducted by a HITRUST CSF Assessor organization, the highest level of assurance.

Refer to the HITRUST CSF Assurance Program Requirements document for additional information on the various types of assessments available.

Additional information on the HITRUST assessment process can be found in the HITRUST CSF Assessment Methodology.

HITRUST CSF Control Structure

The CSF is architected on the ISO/IEC 27001:2005 control clauses but includes additional domains for the information security risk management program and another devoted to privacy practices. The CSF also merges several ISO clauses in the area of development and support processes into a single control on change management. This provides 14 security control categories or domains, 46 control objectives, and 149 controls.

The security and privacy control domains include:

0. Information Security Management Program
1. Access Control
2. Human Resources Security
3. Risk Management
4. Security Policy
5. Organization of Information Security
6. Compliance
7. Asset Management
8. Physical and Environmental Security
9. Communications and Operations Management
10. Information Systems Acquisition, Development and Maintenance
11. Information Security Incident Management
12. Business Continuity Management
13. Privacy Practices

The privacy domain is currently used to support the Texas Covered Entity Privacy and Security Certification Program but will eventually be used as part of a broader CSF privacy certification of the requirements outlined in the HIPAA Privacy Rule.

As indicated, each control domain consists of one or more control objectives, which is a group of controls that have a common purpose. For example, in CSF domain, 01.Access Control, the CSF control objective 01.01, Business Requirement for Access Control, is "to control access to information, information assets, and business processes based on business and security requirements."

A control consists of a control specification and supporting implementation requirements that may address policies, procedures, guidelines, practices or organizational structures, which can be of an administrative, managerial, technical, operational, or physical nature (depending on how one classifies controls). For example, the control specification for CSF domain 01, CSF control objective 01.01, CSF control 01.a, Access Control Policy, is "an access control policy shall be established, documented, and reviewed based on business and security requirements for access."

A control may have up to three levels of implementation requirements, which include requirements integrated from multiple applicable legislative and regulatory sources and best practice frameworks such as HIPAA, TX Health Safety Code, PCI-DSS, and NIST. The selection of these implementation levels is based on specific organizational, system and regulatory risk factors as mentioned earlier in Step 2 of the HITRUST RMF.

HITRUST CSF Control Maturity Model

Evaluating Effectiveness

Controls are often evaluated based on whether or not they are in place or implemented. This results in a very binary, compliance-oriented approach to an assessment, which does little to provide adequate assurances regarding information security and privacy risk to the organization. Models in which partial implementation is noted are arguably more useful, but they also fail to provide an adequate view of organizational risk.

Financial and information technology auditors address this issue by evaluating something referred to as control effectiveness, which has two components: design effectiveness and operational effectiveness. The first, design effectiveness, refers to how well a control is designed to address a specific control objective, i.e., the risk it was designed to control. The second, operational effectiveness, addresses whether or not controls consistently operate over time as designed, i.e., if they continue to effectively address the risks they were designed to control.

HITRUST takes this concept of effectiveness and applies it through the lens of process maturity; however, rather than evaluate the maturity of a specific process, assessors evaluate the effectiveness of a control's implementation through the achievement of specific maturity levels in the model, which describe important aspects of an organization's control implementation.

Maturity Approach

HITRUST's approach is based on a control maturity model described in NIST Interagency Report (IR) 7358, Program Review of Information Security Management Assistance (PRISMA), which provides five levels roughly similar to the Carnegie Melon Software Engineering Institute's (CM-SEI's) Capability Maturity Model Integrated (CMMI) process improvement model. But HITRUST modified the PRISMA model to be more intuitive and measurable. Like the PRISMA model, the HITRUST model's first three levels provide rough equivalence with traditional compliance-based assessments. First, control requirements must be clearly understood at all levels of the organization through documented policies or standards that are communicated with all stakeholders. Second, procedures must be in place to support the actual implementation of required controls. And third, the controls must be fully implemented and tested as required to ensure they operate as intended. These three levels essentially address the concept of design effectiveness. HITRUST then modified the PRISMA model to specifically incorporate the concept of "you can't manage what you don't measure." The model's last two levels address the concept of operational effectiveness.

In the initial maturity level, Policy, the assessor examines the existence of current, documented information security policies or standards in the organization's information security program to determine if they fully address the control's implementation specifications. For example, if a particular requirement statement has multiple actions associated with it, does a corporate policy or standard address all five elements, either directly in the policy or indirectly by reference to an external standard? And does the policy apply to all organizational units and systems within scope of the assessment?

The second maturity level, Procedures, reviews the existence of documented procedures or processes developed from the policies or standards to determine if they reasonably apply to the organizational units and systems within scope of the assessment. For example, are there one or more written procedures that address the implementation of all elements in a particular requirement statement?

The third maturity level, Implemented, reviews the implementation of the policies and procedures to ensure the control's implementation specifications are applied to all the organizational units and systems within scope of the assessment. For example, are all elements of a particular requirement statement addressed by the implementation for all corporate shared services?

The fourth maturity level, Measured, reviews the testing or measurement (metrics) of the specification's implementation to determine if they continue to remain effective. This idea of monitoring is not new, as the American Institute of Certified Public Accountants (AICPA) lists monitoring, i.e., the process of assessing performance over time, as one of five interrelated components of internal control. However, the concept of continuous monitoring, upon which this level is based, is relatively new. The National Institute of Standards and Technology (NIST) equates continuous monitoring with maintaining ongoing awareness to support organizational risk decisions. The terms "continuous" and "ongoing" in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. Thus, testing of the control to support an annual assessment or audit will likely not satisfy this requirement for many if not most controls. Instead, an organization must periodically (and possibly aperiodically) measure and track this information over time. For example, an organization may use a management console to track antivirus software implementation status in near real-time and produce metrics of the percentage of end-user devices that have the latest software and signature updates.

The highest maturity level, Managed, reviews the organization's management of its control implementations based on these metrics. For example, if common or special variations are discovered through testing or measurement of a control's effectiveness such as the antivirus deployment described earlier, can the organization demonstrate it has a management process for this metric and, when general or special variations occur, can it show it has performed a root cause analysis and taken corrective action based on the results?

The following table provides a bulleted list of general requirements for an organization to fully achieve each of the five HITRUST maturity levels:

Table 1. Maturity Level Requirements

Maturity Level	Requirements
Policy	• Formal, up-to-date documented policies or standards stated as "shall" or "will" statements exist and are readily available to employees, • Policies or standards establish a continuing cycle of assessing risk and implementation and uses monitoring for program effectiveness, • Policies or standards are written to cover all facilities and operations and/or systems within scope of the assessment, • Policies or standards are approved by key affected parties, • Policies or standards delineate the information security management structure, clearly assign Information security responsibilities, and lay the foundation necessary to reliably measure progress and compliance, and • Policies or standards identify specific penalties and disciplinary actions to be used if the policy is not followed.
Procedures	• Formal, up-to-date, documented procedures are provided to implement the security controls identified by the defined policies, • Procedures clarify where the procedure is to be performed, how the procedure is to be performed, when the procedure is to be performed, who is to perform the procedure, and on what the procedure is to be performed, • Procedures clearly define Information security responsibilities and expected behaviors for (1) asset owners and users, (2) information resources management and information technology personnel, (3) management, and (4) Information security administrators, • Procedures contain appropriate individuals to be contacted for further information, guidance, and compliance, and • Procedures document the implementation of and the rigor in which the control is applied. • Procedures are communicated to individuals who are required to follow them,
Implemented	• Information security procedures and controls are implemented in a consistent manner everywhere that the procedure applies and are reinforced through training, • Ad hoc approaches that tend to be applied on an individual or case-by-case basis are discouraged, and • Initial testing is performed to ensure controls are operating as intended.

Maturity Level	Requirements
Measured	• Tests are routinely conducted to evaluate the adequacy and effectiveness of all implementations, • Tests ensure that all policies, procedures, and controls are acting as intended and that they ensure the appropriate information security level, • Self-assessments, a type of test that can be performed by organization staff, by contractors, or others engaged by management, are routinely conducted to evaluate the adequacy and effectiveness of all implementations, • Independent audits are an important check on organization performance, but are not to be viewed as a substitute for evaluations initiated by organizational management, • Information gleaned from records of potential and actual Information security incidents and from security alerts, such as those issued by software vendors, are considered measurements. Such information can identify specific vulnerabilities and provide insights into the latest threats and resulting risk, • Evaluation requirements, including requirements regarding the type and frequency of testing, are documented, approved, and effectively implemented, • The frequency and rigor with which individual controls are tested depend on the risks that will be posed if the controls are not operating effectively, • Threats are continually re-evaluated, • Costs and benefits of information security are measured as precisely as practicable, and • Status metrics for the information security program as well as individual information security investment performance measures are established.
Managed	• Effective corrective actions are taken to address identified weaknesses, including those identified as a result of potential or actual information security incidents or through information security alerts issued by US-CERT, vendors, and other trusted sources, • Policies, procedures, implementations, and tests are continually reviewed and improvements are made, • Information security is integrated into capital project/budget planning processes, • An active enterprise-wide information security program achieves cost-effective information security, • Security vulnerabilities are understood and managed, • Controls are adapted to emerging threats and the changing information security environment, • Decision-making is based on cost, risk, and mission impact, • Additional or more cost-effective information security alternatives are identified as the need arises, and • Status metrics for the information security program as well as individual information security investment performance measures are met.

By understanding these general requirements, self- and third party assessors are better prepared to assess the maturity (effectiveness) of requirements derived from a CSF control's implementation specifications.

Adapting Implementation Specifications for Assessment

Since the CSF is based on ISO/IEC 27001:2005, the CSF control implementation specifications consist of various policy, process and other requirement statements. Therefore, the language had to be modified slightly to ensure it lent itself to PRISMA's approach for the evaluation of control effectiveness.

For this reason, CSF assessments are based on the evaluation of requirements statements derived from the implementation specifications in the CSF rather than on the actual language contained in the CSF. The intent is to focus on actionable requirements rather than on any policy or process requirements contained in the specifications. For example, CSF control 01.a, Access Control Policy, states "the organization shall develop, disseminate, and review and update the access control policy and procedures annually." Rather than associate this requirement statement with 01.a, it's addressed by the general policy development and review requirements specified in 04.a, Information Security Policy Document, and 04.b, Review of the Information Security Policy. By addressing policy and process requirements in this way, the assessment can focus on more actionable requirements.

The implementation specifications for CSF control 01.a, level 1 can be used to further illustrate the approach:

Access control rules shall account for and reflect the organization's policies for information dissemination and authorization, and these rules shall be supported by formal procedures and clearly defined responsibilities. Access control rules and rights for each user or group of users shall be clearly stated in an access control policy. Access controls are both logical and physical and these shall be considered together. Users and service providers shall be given a clear statement of the business requirements to be met by access controls.

Specifically the policy shall take account of the following:

i. *security requirements of individual business applications;*
ii. *policies for information dissemination and authorization (e.g., need-to-know, need to share, and least privilege principles; security levels; and classification of information.)*
iii. *relevant legislation and any contractual obligations regarding protection of access to data or services;*
iv. *standard user access profiles for common job roles in the organization;*
v. *requirements for formal authorization of access requests;*
vi. *requirements for emergency access;*
vii. *requirements for periodic review of access controls; and*
viii. *removal of access rights.*

The organization shall develop, disseminate and review and update the access control policy and procedures annually.

HITRUST generated seven actionable requirements from this language (i.e., statements that do not specifically address policy or procedural requirements):

1. Access control rules and rights for each user or group of users are based on clearly defined requirements for information dissemination and authorization (e.g., need-to-know, need-to-share, least privilege, security levels and information classification).
2. Access control rules and rights for each user or group of users are clearly defined.
3. Users and service providers are given a clear statement of the business requirements (e.g., relevant legislation and any contractual obligations) to be met by access controls (i.e., to protect access to data or services).
4. The security requirements of individual business applications are defined.
5. The organization uses standard user access profiles for common job roles.
6. Requirements for formal authorization of access requests, emergency access, and the removal of access are defined.
7. The organization develops, disseminates, reviews and updates the access control program annually.

These seven requirements were then condensed into the following three requirement statements for use in the MyCSF assessment and reporting tool to support a Baseline or Comprehensive Assessment.

1. Access control rules and rights for each user or group of users for each application are clearly defined in standard user access profiles (e.g., roles) based on need-to-know, need-to-share, least privilege and other relevant requirements.
2. Users and service providers are given a clear statement of the business requirements for controls needed to protect access to data or services.
3. The access authorization process addresses requests for access, changes to access, removal of access, and emergency access.

During an assessment, the self- or third party assessor evaluates each of these three requirement statements based on general guidelines/criteria, which are essentially derived from the requirements outlined in the previous table, and specific assessment procedures for each of the five maturity levels.

Evaluating Requirements Statements

The following table provides a minimum generic set of criteria (questions) based on the general requirements for full compliance, which assessors should consider when evaluating a requirements statement at each level of the model, as they provide the necessary context for scoring against the specific evaluation criteria contained in HITRUST's illustrative procedures, which are discussed at more length in the next section.

Table 2. Generic Evaluation Criteria by Maturity Level

Level	Generic Evaluation Criteria
1 – Policy	• Do formal, up-to-date policies or standards exist that contain "shall" or "will" statements for each element of the requirement statement? • Do the policies and standards that exist for each element of the requirement statement cover all major facilities and operations for the organizations and/or systems/assets in scope for the assessment? • Are the policies and standards that exist for each element of the requirement statement approved by management and communicated to the workforce?
2 – Procedures	• Do formal, up-to-date, documented procedures exist for the implementation of each element of the requirement statement? • Do the procedures clarify where the procedure is to be performed, how the procedure is to be performed, when the procedure is to be performed, who is to perform the procedure, and on what the procedure is to be performed? • Do the procedures address each element of the requirement statement across all applicable facilities, operations and/or systems/assets in scope? • Are procedures for the implementation of each element of the requirements statement communicated to the individuals who are required to follow them?
3 – Implemented	• Is each element of the requirements statement implemented in a consistent manner everywhere that the policy and procedure applies? • Are ad hoc approaches that tend to be applied on an individual or on a case-by-case basis discouraged?
4 – Measured	• Are self-assessments, audits and/or tests routinely performed and/or metrics collected to evaluate the adequacy and effectiveness of the implementation of each element of the requirements statement? • Are evaluation requirements, including requirements regarding the type and frequency of self-assessments, audits, tests, and/or metrics collection documented, approved and effectively implemented? • Does the frequency and rigor with which each element of the requirements statement is evaluated depend on the risks that will be posed if the implementation is not operating effectively?
5 – Managed	• Are effective corrective actions taken to address identified weaknesses in the elements of the requirements statement, including those identified as a result of potential or actual information security incidents or through information security alerts? • Do decisions around corrective actions consider cost, risk and mission impact? • Are threats impacting the requirements periodically re-evaluated and the requirements adapted as needed?

The HITRUST control maturity model also incorporates the following 5-point compliance scale which is used to rate each level in the model: Non-Compliant (NC), Somewhat Compliant (SC), Partially Compliant (PC), Mostly Compliant (MC) and Fully Compliant (FC).

Table 3. Score Descriptions

Maturity Level	Requirements
Non-Compliant (NC)	Very few if any of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 0% (point estimate) or 0% to 12% (interval estimate).
Somewhat Compliant (SC)	Some of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 25% (point estimate) or 13% to 37% (interval estimate).
Partially Compliant (PC)	About half of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 50% (point estimate) or 38% to 62% (interval estimate).
Mostly Compliant (MC)	Many but not all of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 75% (point estimate) or 63% to 87% (interval estimate).
Fully Compliant (FC)	Most if not all of the elements in the requirement statement exist for the maturity level evaluated (policy, procedure, implemented, measured or managed). Rough numeric equivalent of 100% (point estimate) or 88% to 100% (interval estimate).

The ranges for the interval estimates are meant to be guidance; assessor judgment should always be applied when determining the level of compliance with a specific requirement. The non-compliant and fully compliant ratings are relatively straight forward, but let's look at some examples of how the other three 'partial ratings' may be determined.

Suppose an organization has specified all the elements of a requirement statement in policy, but the policy only applies to three of the four business units within scope of the assessment. The organization would be mostly compliant (MC) for level 1, Policy. Now suppose that organization had processes supporting implementation of all the elements of the requirement statement across all four business units but only used/implemented the processes of these elements in three of the four business units covered by the policy. The organization would be fully compliant (FC) for level 2, Procedures, and mostly compliant (MC) for level 3, implementation.

For further illustration, let's examine one element, encryption, from a specific requirement statement for mobile computing devices, which was derived from CSF control 01.x, Mobile Computing and Communications:

Mobile computing devices are protected at all times by access controls, encryption, virus protections, host-based firewalls, secure configuration, and physical protections.

The assessor has determined that the academic hospital in this scenario requires by policy, signed by executive management, that all portable computing devices, whether a laptop or a smartphone, be encrypted if the device is used to access covered information. The organization gets credit for full compliance with the policy maturity requirements. The organization has formal written procedures in place to ensure Windows-based laptops and all smartphones are encrypted according to the policy requirements, but has yet to establish procedures for the encryption of a limited number of Mac laptops due to resistance from the research community. As it can demonstrate all Windows-based laptops and smartphones were encrypted when the capability was rolled out earlier in the year, the hospital scores mostly compliant for procedures and implementation. The management console used by end-user devices and the mobile device management console for smartphones both have the capability to report on the encryption status for these devices, but the reports are seldom run. Since manager bonuses are tied to meeting operational service levels, executive leadership lost interest once the encryption project was completed for Windows-based devices, which accounts for 95% of the total environment. The organization gets a somewhat compliant score for measured and noncompliance for managed, as the organization does not use this information to evaluate and manage the effectiveness of the encryption implementation.

Based on the facts presented, the scoring might look as follows for this requirement statement:

Table 4. Scoring Example

Level (Points)	NC	SC	PC	MC	FC
Policy (25)					X
Procedures (25)				X	
Implemented (25)				X	
Measured (15)		X			
Managed (10)	X				

The compliance scale is evenly weighted (0, 25, 50, 75, 100), but the PRISMA scores for each level are weighted differently (25, 25, 25, 15, 10). Essentially, the last two levels (measured and managed) are combined (for a total of 25 points) to address the concept of "one can't manage what one can't measure" and still account for the fact that not all organizations actively manage their controls even while measuring their effectiveness. For example, an organization may perform a root cause analysis after every security incident, but fail to take appropriate measures based on the results.

In this example, the academic hospital would score the following for the encryption component of the requirement: (1.0)(25) + (.75)(25) + (.75)(25) + (.25)(15) + (0.0)(10) = 66.25.

Although this example focused on a specific element of the requirement statement, a self- or third party assessor would likely not determine the state of compliance for any level of the model until all elements of the requirement were evaluated and could be aggregated to support a single score.

By way of another example using the first level, Policy, assume that requirements for access controls, encryption, virus protections, secure configuration and physical protections are fully addressed by organizational policy. However, host-based firewalls are not. For this level, the state of compliance can be evaluated as (1+1+1+1+1+0) / 6 = 5/6 = 0.83, which is closest to Mostly Compliant, or MC. This exercise would then be repeated for the remaining four levels, after which an overall score for the requirement statement could be computed in the same manner as the encryption element described earlier.

Once all the elements of all the requirement statements are evaluated against HITRUST's PRISMA-based maturity model, the scores can be aggregated across all the requirement statements for a particular control or across multiple controls in a domain. These estimates can also be used to support reporting against specific controls or domains for one or more organizations, type(s) of business units across multiple organizations, one or more information systems, or type(s) of information systems. Estimates can also be used to generate one or more Scorecards, such as for HIPAA or cybersecurity.

Although the intent is for assessors to understand and apply these concepts to the scoring of each maturity level based on specific illustrative procedures for each requirement, HITRUST recognizes that third party and self-assessors have various levels and types of experience upon which to base decisions. To help assessors score control maturity in a consistent and repeatable way, HITRUST has developed the following rubric for each maturity level.

Table 5. Scoring Rubric

Rating (Score)	Policy	Procedure	Implemented	Measured	Managed
NC (0%)	None of the CSF requirements	None of the CSF requirements	None of the CSF requirements	No measure or metric in place	No management action taken
SC (25%)	Some CSF requirements AND ad hoc	Some CSF requirements are supported by ad hoc procedures	Some CSF requirements AND partial scope	Operational OR independent measure	Measure or metric AND management actions are sometimes taken on an ad hoc basis
PC (50%)	All CSF requirements AND ad hoc	All CSF requirements are supported by ad hoc procedures	Some CSF requirements AND full scope	Operational AND independent measure	Measure or metric AND management actions are sometimes taken AND a formal action management process exists
MC (75%)	Some CSF requirements are written/ signed AND the remainder ad hoc	Some CSF requirements are supported by written and/or automated procedures, AND the remaining CSF requirements are addressed by ad hoc procedures.	All CSF requirements and partial scope	Operational OR independent METRIC	Metric only AND corrective actions are always taken AND on an ad hoc basis
FC (100%)	All CSF requirements and written/signed	ALL CSF requirements are supported by written procedures and/or are automated	All CSF requirements AND full scope	Operational metric AND independent measure or metric	Metric only AND corrective actions always taken AND a formal remediation management process exists

Definitions and examples of key terms are provided in the following table.

Table 6. Rubric Definitions

Term	Definition	Example (based on patch management)
Operational	Influenced by the person or entity responsible for the requirement/control being evaluated.	The patch manager and any separate IT business unit that reports to the same manager, which could include functions like desktop engineering or field support (depending on the organization).
Independent	Not influenced by the person or entity that is responsible for the requirement/control being evaluated.	Internal audit, quality assurance group, or separate IT business unit that does not report to the same manager as the patch manager, which might include IT risk management or the CISO (depending on the organization).
Measure	A qualitative or quantitative assessment of the performance or quality of a requirement.	The percentage of end user devices with current patch levels.
Metric	A measure, tracked over time, with specific performance or quality targets.	The percentage of currently patched end user devices tracked weekly against a target objective of 99% of all end user devices.

We can now rescore our previous portable device encryption example using the rubric.

- **Policy:** All the requirements for the encryption of portable devices are formally stated in a signed policy, which results in a score of 100%.
- **Procedure:** Although the organization's formal written procedures address all the CSF policy elements, the procedures do not address encryption of Mac laptops owned by the research community. This does not satisfy the generic evaluation criteria for fully compliant procedures, which states they must address each element of the requirement statement across all applicable facilities, operations and/or systems/assets in scope. This results in an MC rating, or a score of 75%.
- **Implemented:** Since all the requirements are addressed by the implementation but not across the entire scope, i.e., the research community, the organization receives 75% for implementation.
- **Measured:** The organization has the capability to run routine reports but does so on an ad hoc basis. These reports satisfy the requirements for a measure (as opposed to a metric). The reports are run by the organizational element that manages laptop encryption, so the measure is operational. Subsequently, an operational measure receives 25% for this level.
- **Managed:** No action is being taken due to a lack of interest due to other priorities, so the organization receives 0% for this level.

We stress again that the generic evaluation criteria must be considered when using the rubric to help score the requirement statements for each level of the maturity model.

Now let's consider two specific cases in which a particular technology is not implemented and illustrate how requirements associated with the technologies would be evaluated.

Suppose an organization prohibits the use of wireless access points in its environment. One might assume the assessor would indicate any CSF control requirements associated with this technology are not applicable and move on; however, this can't be done when the vulnerabilities associated with a technology like wireless could be introduced without the knowledge of the organization. As such, the self- or third party assessor should ask the following types of questions to evaluate the effectiveness of controls intended to ensure wireless access points are not procured or installed in violation of policy:

1. **Policy:** Does the organization have a policy that states wireless access points are not allowed in any part of the environment within scope of the assessment?
2. **Procedure:** Does the organization have processes in place to ensure that wireless access points are not procured or installed in any part of the environment within scope of the assessment, e.g., rogue wireless detection?
3. **Implemented:** Does the organization check for wireless access points in all parts of the environment in scope for the assessment? Have these checks been accomplished at a frequency and manner (periodic and aperiodic/ randomly) as required by policy?
4. **Measured:** Does the organization track the results via some type of metric?
5. **Managed:** Does the organization have a process in place to report the metric to management and take corrective action? In documented instances in which wireless access points have been detected, did the organization follow the process and take appropriate corrective action?

The percentage of compliance for each level (scoring) would be based on how completely the elements of the organization's policy statement prohibiting wireless were addressed for all organizational units and systems in scope for the assessment. And again, the results of this evaluation would then be applied to any CSF assessment requirement statement associated with the security of wireless access points (if their implementation had been allowed).

Let's look at another example. CSF control 01.b, User Registration states: "User identities are verified in person before a designated individual or office to receive a hardware token." How should an assessor evaluate this requirement if the organization does not use hardware tokens?

Unlike our wireless access point example, CSF control requirements associated with the use of this technology would truly be 'not applicable' or 'N/A' for this organization. The reason is this control addresses a risk that does not exist and will likely not exist given the very slim (virtually zero) likelihood the organization or individual (either well-meaning or malicious) would implement a rogue hardware token infrastructure. Basically there's no need to have a policy restricting the use of hardware tokens or procedures in place to ensure hardware tokens aren't utilized. Scores for related-requirement statements would not be calculated and subsequently not included in the scoring of any control, group of controls or domain.

Converting Maturity Scores to the Rating Scale

As currently used in the HITRUST CSF Assurance Program, the PRISMA-based maturity scores are converted to a 15-level maturity rating for CSF certification:

Table 7. Score to Rating Conversion

Maturity Level	1-	1	1+	2-	2	2+	3-	3	3+	4-	4	4+	5-	5	5+
Cutoff PRISMA Score	<10	<19	<27	<36	<45	<53	<62	<71	<79	<83	<87	<90	<94	<98	<100

However, one should note that the aggregated scores simply provide likelihood estimators for the probability that one or more controls might fail to operate as intended. When used for CSF validation and certification, these aggregated scores provide guidelines for HITRUST's quality assurance evaluation of the self- or third party assessment and the evidence obtained to support the scores. However, other factors such as a significant deficiency in the implementation of one or more controls could prevent an organization from becoming CSF Certified even though they score a "3" or better in every assessment domain.

General definitions for each of the 15 maturity ratings are provided in the table below:

Table 8. Rating Descriptions

Maturity Level	Rating Description
Level 1-	Few if any of the control specifications included in the assessment scope are defined in a policy or standard and may not be implemented as required by the HITRUST CSF.
Level 1	Many of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.
Level 1+	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard but may not be implemented as required by the CSF.
Level 2-	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard but few if any of the requirements are supported with organizational procedures or implemented as required by the CSF.
Level 2	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard, many of the requirements are supported with organizational procedures, but few if any are implemented as required by the CSF.
Level 2+	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, but few if any are implemented as required by the CSF.
Level 3-	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and some are implemented as required by the CSF.
Level 3	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard and supported with organizational procedures, and many are implemented as required by the CSF.

Maturity Level	Rating Description
Level 3+	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard, supported with organizational procedures, and implemented as required by the CSF.
Level 4-	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes and implemented, and some of these control specifications are routinely measured to ensure they function as intended and as required by the HITRUST CSF.
Level 4	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes and implemented, and many of these control specifications are routinely measured to ensure they function as intended and as required by the HITRUST CSF.
Level 4+	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured to ensure they function as intended and as required by the HITRUST CSF.
Level 5-	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured, and some are actively managed to ensure they continue to function as intended and as required by the HITRUST CSF.
Level 5	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, and routinely measured, and many are actively managed to ensure they continue to function as intended and as required by the HITRUST CSF.
Level 5+	Most, if not all, of the control specifications included in the assessment scope are defined in a policy or standard, supported by organizational processes, implemented, routinely measured, and actively managed to ensure they continue to function as intended and as required by the HITRUST CSF.

In our previous example on mobile device encryption, a score of 66.25 for the encryption component of the requirement statement would result in a maturity rating of a "3," which by definition would indicate that most if not all of the organizational units and systems within scope of the assessment are required to have encrypted mobile devices according to a policy or standard and have formal processes supporting their encryption, and many if not most of the devices are encrypted as required.

HITRUST Illustrative Procedures

MyCSF provides illustrative procedures for each control requirement contained in a Baseline or, when completed, Comprehensive Assessment. These procedures provide additional context for evaluation of these requirements and should be leveraged by self- and third party assessors to help ensure consistency and repeatability of their control assessments.

Let's look at the procedures associated with the following level 1 requirement statement for CSF control 09.n, Security of Network Services:

Agreed services provided by a network service provider/manager are formally managed and monitored to ensure they are provided securely.

The illustrative procedures associated with this requirement statement are as follows:

1. **Policy:** Review relevant policies or standards on contracting and/or network services and determine if formal management and monitoring of agreed in-house or contracted outsourced network services is required. Verify that the policy requires specific security arrangements for particular services to be included in a network services agreement, including security features, service levels, and management requirements. The policy or standard should also require the agreements address the right to audit. If policies or standards do not address this requirement, determine who is responsible for managing network service providers and determine if the management, monitoring and documentation requirements are understood. Evidence of ad hoc or informal policy may also be provided by reviewing any written procedures or examining documentation associated with formal or ad hoc processes to determine if the requirements are addressed consistently by the entity.

2. **Procedure:** Determine if formal or informal written procedures for the management of network services address both internal sources (i.e., by a network services manager) or external sources (i.e., by an outsourced network services provider). Verify the procedures address development and implementation of a network services agreement, including specific requirements for documenting the security of those services and carrying out the terms of the agreement, e.g., monitoring to ensure the network service provider implements the measures. Interview key personnel responsible for developing and implementing/managing the network services agreements and ask them if the procedures address the requirements. Ask them to describe the procedures and compare their description(s) to written procedures, if they exist, to determine if they are consistent.

3. **Implemented:** Inquire of management if internal and external/outsourced network services are managed and monitored according to a network services agreement. Ask management if the agreements provide the right to audit. Interview key personnel involved in the development and management of these network services agreements and verify they are followed consistently. Obtain a list of network service providers, including any internal network services provided locally or as an enterprise service, and compare the list to a list of network services agreements. Verify that each provider, including any internally provided services, has a network services agreement. Examine a representative sample of network services agreements and ensure they address the policy requirements for security, including the right to audit. If the original dates of the agreements can be determined, verify the network service agreements sampled were established prior to implementing/using the services. Ask if any of the service providers, including those provided by an internal network services manager, have been audited. Review documentation substantiating the audits. Review documentation substantiating the monitoring of these network services, including any actions taken to actively manage any security-relevant issues with the provided services.

4. **Measured:** Examine metric(s) or other measure(s) that evaluate(s) the organization's compliance with the policy on contracting and/or network services to determine if the requirements are addressed by the metric. For example, the metric could indicate the number of network services that do not have a policy-compliant network services agreement as a percentage of all network services received. Non-compliance with the policy requirements could be part of a broader metric that considers all deviations from network services requirements regardless of type if non-compliance with the requirements for network services agreements can be ascertained. Note a measure could include regular or "ad hoc" reports or audits of contractual agreements or network services if they consider the policy requirements for network services agreements. If a metric or measure adequately evaluates the policy requirements for network services agreements, determine if the measure is tracked over time and if performance goals have been established.

5. **Managed:** Determine if the individual or office that receives the measure or metric is able to correct issues with network services agreements without the need to routinely escalate the issues to the next level of management. Note the ability to escalate issues must also exist if the root cause of a specific incident cannot be addressed by the individual or office receiving and reviewing the metric or measurement. Examine related records to determine if deviations/incidents occurred and if appropriate action was taken to identify, investigate, correct and follow-up on deviations/incidents. If written records do not exist, interview personnel who receive and review the metric(s) to determine if ad hoc processes for investigation and resolution exist, and whether deviations/incidents were corrected if they occurred.

Self- and third party assessors would use these procedures along with the more general criteria (questions) and the scoring rubric provided for the maturity levels earlier in this document to evaluate the level of compliance with each level for this requirement statement. For example, when reviewing the access control policy to evaluate compliance with level 1, Policy, does it provide language addressing defined requirements for standard access control profiles based on need-to-know, need-to-share, and least privilege, at a minimum? Does this particular policy cover all the

organizational units and systems/assets in scope for the assessment? And has this particular policy been approved by management in accordance with organizational policy requirements and adequately communicated to the workforce?

Assessors should also note the general criteria and illustrative procedures, while intended to ensure a minimal level of rigor, consistency and repeatability, are indeed illustrative and subsequently the minimum. Self- and third party assessors should use these criteria and procedures as the basis for more detailed assessment work plans (also known as test and evaluation plans), which must also accompany any assessment submitted to HITRUST for quality assurance review in support of validation or certification.

Readers should note that the wireless scenario presented earlier indicates self- and third party assessors cannot rely solely on illustrative procedures for the development of their work plans, which third party assessors are required to submit to HITRUST as part of the validation and certification quality assurance process. An assessor would necessarily document alternate testing in the work plan similar to the language provided in the wireless scenario.

However, although requirement statements marked as N/A would not be evaluated (scored) during an assessment, self- and third party assessors must provide the rationale for marking the requirement N/A in the requirement's comment field in the appropriate tab within the MyCSF tool.

Final Thoughts

If properly followed, HITRUST's RMF provides the structure and rigor needed to ensure consistent and repeatable assessments that provide reliable assurances to organizational and external stakeholders. However, the rigor of these structured assessments may be somewhat new to many healthcare and assessor organizations.

Self- and third party assessors cannot rely solely on past experience with PCI, AICPA or other security and privacy assessment methodologies to provide a HITRUST CSF assessment. HITRUST organizations and assessors should ensure they understand the HITRUST RMF, CSF Assurance Program requirements, and the CSF assessment process outlined in the CSF Assessment Methodology. Only then can one thoroughly understand how to evaluate CSF controls using the HITRUST maturity model, evaluation and scoring approach, and the use of general criteria and specific illustrative procedures to build out the work plans needed to conduct a successful CSF assessment.

About HITRUST

In 2008, representatives from across the healthcare industry came together in support of HITRUST to develop the Common Security Framework (CSF™). Many of the leading, most experienced and knowledgeable organizations in healthcare worked in conjunction with top professional services and technology firms to develop a single framework that leverages the best of existing standards and is tailored for the specific needs of the industry. The CSF is now the de facto information security standard in healthcare with over 70% of hospitals and large insurers (> 500,000 members) utilizing the framework in various ways. By adopting and implementing the CSF, organizations have a common security baseline they can use to communicate the status of their security controls to key stakeholders, including regulators, auditors, business partners and customers.

HITRUST exists to ensure that information security becomes a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. Security is critical to the adoption, utilization and confidence in systems and electronic exchanges of protected health information (PHI). This, in turn, is critical to realizing the related promise of quality improvement and cost containment in America's healthcare system.

In addition, HITRUST developed the CSF Assurance Program™ to set the bar for the minimum healthcare and information security expertise required of CSF Assessors and provide a standard methodology for the evaluation and scoring of information security controls by assessor organizations. By utilizing a common set of controls mapped to multiple legislative and regulatory requirements and industry standards and best practice frameworks, the program improves efficiencies and reduces the number and associated costs of security and privacy risk assessments.

Figure 3. One program for multiple assurances between covered entities and their business associates

Unlike other programs in healthcare and in other industries, the oversight, vetting and governance provided by HITRUST affords greater assurances and security across the industry. HITRUST CSF Assessor organizations must meet specific requirements for their assessment methods and tools, as well as the experience and qualifications of their personnel. (See the HITRUST CSF Assessor Requirements document for more information on program requirements.) This ensures the results are consistent and repeatable regardless of the CSF Assessor selected by an organization, which provides high levels of assurance when exchanging risk information with regulators and business partners.

HITRUST has a broad cross-section of Assessor organizations participating in the CSF Assurance Program focused on various types and sizes of healthcare entities. (See a current list of HITRUST CSF Assessor organizations.) With more added every year, these organizations range from small professional services companies to large audit and consulting

organizations targeting different healthcare segments and sizes of covered entities. The number and quality of these organizations help ensure covered entities receive the most comprehensive, consistent and repeatable information protection risk assessments in the industry.

HITRUST is the only information protection standards body that is (1) devoted to healthcare and (2) has provided standards-based certification to the industry since 2009. More healthcare organizations use the CSF than any other framework in the industry, whether as a reference for industry best practices or a standard by which to measure their organizational information security programs. No other organization can claim this level of experience with healthcare information protection assessment and certification.

HITRUST is also helping the industry drive adoption of sound risk management practices through awareness, education, advocacy and other outreach activities, such as the aforementioned development of a healthcare-specific credential for information protection professionals, a cybersecurity incident response coordination center for the sharing of real-time threat intelligence and remediation strategies, and tools such as MyCSF™, a fully integrated, optimized, and powerful tool that marries CSF content and methodologies with the technology and capabilities of a governance, risk and compliance (GRC) tool.

Appendix A: Risk Treatments

HITRUST recognizes that, although the intent of CSF certification is to ensure compliance with a risk-based standard, not all organizations handle information security-related risks in the same manner. Organizations may wish to transfer risk by adding cyber insurance to deal with anticipated costs due to the higher likelihood of a compromise should a control requirement not yet be fully implemented. In some cases, organizations can avoid risk, e.g., by using hardware tokens in lieu of passwords, and the associated control requirements may simply not be applicable. In others, control requirements may not or cannot be implemented for various reasons, and alternate (compensating) controls may be specified to mitigate the risk. And in some others, an organization may wish to accept risk.

Transference

Transference of information security and privacy-related risk is normally accomplished through some type of cyber or data breach insurance. Transference can be accomplished through appropriate contract language when outsourcing IT services by reducing exposure. While not all risk can be transferred, it's possible to reduce some of the risk through indemnification. HITRUST addresses this type of insurance in several controls.

Let's look at a typical transference requirement. Consider an organization that needs to know how to interpret the following requirement statement for CSF Control 01.y, Teleworking: "Additional insurance to address the risks of teleworking is provided."

In general, the organization should ensure it adequately addresses—through inclusion or exclusion—any risk associated with teleworking, not just theft of data or equipment. For example, the policy should address costs associated with a data breach caused by teleworking. It would also need to address costs associated with the unauthorized or unintended modification or destruction (loss) of data due to a compromise of the teleworker's location or equipment.

Thus, a self- or third party assessor should simply determine if the assessed organization's cyber insurance policy addresses teleworking (to whatever extent the insurance company provides). If the policy doesn't mention teleworking or—more telling—specifically excludes teleworking from the policy, then this could be considered a control deficiency. (Note, insurance for non-cyber risks such as injuries at the teleworking site are probably beyond the scope of the control.)

Avoidance

Organizations can avoid risk by not taking a particular action that entails some type of risk. For example, an organization can avoid the risk of a Tsunami destroying its data center by placing it in Dallas, TX, rather than Honolulu, HI. It can also avoid risk by not implementing specific technologies, such as by prohibiting the implementation and use of wireless access points. However, this does not mean that organizations do not need to implement additional controls to ensure the risks remain avoided. For example, organizations need to prohibit the implementation and use of wireless access points in policy and require specific controls to ensure these access points are not implemented or used, e.g., by requiring rogue access point detection on a recurring if not continuous basis.

Assessors should ensure these additional requirements are adequately addressed in their assessment work plans.

Mitigation

After controls are specified by an organization to ensure risk is controlled to a level formally deemed acceptable by executive leadership, the most common way of dealing with deficiencies observed with the implementation and management of those controls is to remediate them. This subsequently reduces risk to an acceptable level, a process referred to as mitigation.

Corrective Actions Plans

An essential component of risk analysis is the selection of a risk treatment for identified deficiencies and the management of any actions needed to correct those deficiencies selected for remediation.

HITRUST requires assessed entities to prepare CAPs for identified deficiencies. Subsequently self- or third party assessors, as applicable, must describe the specific measures intended to remediate (correct) deficiencies identified during an assessment for validation or certification. HITRUST understands that most organizations have more vulnerabilities than they have resources to address, so organizations should prioritize corrective actions based on the sensitivity and criticality of the information systems or assets affected, the direct effect the vulnerability has on the overall security posture of the information systems or assets, and the requirements for CSF certification.

CAP Requirements

A complete CAP should include, at a minimum, a control gap identifier, description of the control gap, CSF control mapping, point of contact, resources required (dollars, time, and/or personnel), scheduled completion date, corrective actions, how the weakness was identified (assessment, CSF Assessor, date), date identified, and current status. Note, third party assessors must review the CAP to evaluate the effectiveness of the remediation strategy, provide recommendations or feedback as needed, and document any findings for submission to HITRUST.

Non-contextual Impact and Relative Risk

Although HITRUST organizations and CSF Assessors typically have no problem with identifying the corrective actions needed to address specific deficiencies, some have difficulty rating the risks associated with these deficiencies and subsequently prioritizing the work. To help with CAP prioritization, HITRUST provides non-contextual impact ratings for each CSF control on the following page, which allows the computation of relative risk for each deficiency identified in an assessment. The ratings are non-contextual in that they assume the probable impact should the control fail, assuming all other controls are in place.

Impact is described using five rating levels (codes): Very Low (1), Low (2), Moderate (3), High (4) and Very High (5). For the purpose of computing risk, ratings may be assigned specific values such as those prescribed by NIST SP 800-30 r1, Guide for Conducting Risk Assessments: Very Low (1) = 0, Low (2) = 2, Moderate (3) = 5, High (4) = 8, and Very High (5) = 10. HITRUST uses a similar approach and computes impact (I) as a function of the impact rating (IR):

Impact = I = (IR - 1) x (25),

which equates to Very Low (1) = 0, Low (2) = 25, Moderate (3) = 50, High (4) = 75, and Very High (5) = 100. When converted to a 10 point scale and rounded up, the values are identical to the NIST model.

The following table provides the HITRUST impact codes for all 135 CSF controls:

Table 9. Impact Codes

Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code
0.a	3	01.o	3	02.e	5	05.e	3	06.i	4	08.i	4	09.k	3	09.z	5	10.i	4
01.a	5	01.p	3	02.f	5	05.f	4	06.j	3	08.j	4	09.l	3	09.aa	3	10.j	4
01.b	5	01.q	5	02.g	5	05.g	4	07.a	4	08.k	5	09.m	4	09.ab	3	10.k	4
01.c	5	01.r	4	02.h	5	05.h	5	07.b	3	08.l	5	09.n	4	09.ac	3	10.l	3
01.d	5	01.s	4	02.i	5	05.i	4	07.c	5	08.m	5	09.o	3	09.ad	3	10.m	3
01.e	5	01.t	3	03.a	3	05.j	5	07.d	4	09.a	5	09.p	5	09.ae	3	11.a	3
01.f	5	01.u	3	03.b	3	05.k	5	07.e	5	09.b	4	09.q	4	09.af	3	11.b	4
01.g	4	01.v	3	03.c	3	06.a	4	08.a	5	09.c	5	09.r	4	10.a	4	11.c	3
01.h	3	01.w	3	03.d	3	06.b	4	08.b	5	09.d	4	09.s	5	10.b	4	11.d	3
01.i	4	01.x	5	04.a	3	06.c	3	08.c	5	09.e	4	09.t	3	10.c	4	11.e	3
01.j	5	01.y	5	04.b	3	06.d	3	08.d	4	09.f	4	09.u	3	10.d	3	12.a	3
01.k	4	02.a	4	05.a	4	06.e	5	08.e	5	09.g	4	09.v	4	10.e	4	12.b	3
01.l	4	02.b	5	05.b	5	06.f	4	08.f	4	09.h	3	09.w	4	10.f	3	12.c	3
01.m	3	02.c	5	05.c	3	06.g	4	08.g	4	09.i	4	09.x	4	10.g	3	12.d	3
01.n	4	02.d	4	05.d	3	06.h	4	08.h	3	09.j	4	09.y	4	10.h	4	12.e	3

The numbers are intended to provide a starting point for assignment of relative risk to CAPs based on relative maturity of the controls as determined by a HITRUST CSF assessment. For internal remediation planning purposes, organizations may adjust the impact ratings/codes based on the status of other controls in the environment or the sensitivity and/or criticality of the information assets in scope. However, these non-contextual impact ratings/codes may not be adjusted for validation and certification reporting to ensure consistency across the industry.

Note, the formula for computing risk using the HITRUST CSF control maturity score from MyCSF may be written as

$$\mathbf{R = L \times I = [(100 - MS) / 100] \times [(IR - 1) \times 25],}$$

where, R = risk, L = likelihood, I = impact, MS = HITRUST CSF control maturity score, and IR = impact rating.

Suppose an organization obtains a maturity score of 75 for CSF control 01.a. Since this is a very high impact control, the risk would be computed as [(100 - 75) / 100] x [(5 - 1) x 25) = .25 x 100 = 25, which is a moderate risk, as shown below.

HITRUST recognizes two types of risk scales, a traditional bell-shaped model and a left-skewed bell-shaped "academic" model. Although the traditional model is best used for communicating risk to external stakeholders, the academic model provides a very intuitive approach to understanding risk when presented as risk grades, similar to the model used by the federal government to report security compliance for federal agencies.

The following table provides the intervals for both models:

Table 10. Risk Scales

Risk Level	Range (Traditional Model)	Range (Academic Model)
Very High (Severe)	96-100	41-100
High	80-95	31-40
Moderate	21-79	21-30
Low	5-20	11-20
Very Low (Minimal)	0-4	0-10

Risk grades would be computed from the academic risk scores by subtracting them from 100 and using a traditional academic grading scale: A (90-100), B (80-89), C (70-79), D (60-69) and F (0-59). The grades basically let management know how well they are managing residual risk due to "immature" controls in the environment. Full implementation of a control, i.e., full credit for the policy, procedures and implementation maturity levels, would generally provide an overall "C" for the organization, which would be considered average for the industry. Organizations can receive a higher grade (an "A" or "B") through continuous monitoring (measurement) and active management of control effectiveness.

Prioritization

HITRUST also provides implementation dependencies amongst CSF controls based on priority codes for the federal controls contained in NIST SP 800-53 r4. The priority codes indicate relative order of priority (sequencing) for implementation, which helps provide a more structured, phased approach by ensuring controls upon which other controls depend are implemented first.

Priority code sequencing, consistent with NIST SP 800-53 r4, is as follows:

- P1 – First (Control contains significant number of foundational requirements)
- P2 – Next (Control contains requirements that depend on the successful implementation of one or more foundational control requirements)
- P3 – Last (Control contains requirements that generally depend on the successful implementation of one or more priority 2 requirements)

The following table provides the HITRUST priority codes for all 135 CSF controls:

Table 11. Priority Codes

Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code	Ctrl	Code
0.a	P1	01.o	P1	02.e	P1	05.e	P2	06.i	P1	08.i	P1	09.k	P1	09.z	P2	10.i	P2
01.a	P1	01.p	P2	02.f	P3	05.f	P3	06.j	P1	08.j	P1	09.l	P1	09.aa	P1	10.j	P2
01.b	P1	01.q	P1	02.g	P2	05.g	P3	07.a	P1	08.k	P1	09.m	P1	09.ab	P2	10.k	P1
01.c	P1	01.r	P1	02.h	P2	05.h	P3	07.b	P1	08.l	P1	09.n	P1	09.ac	P1	10.l	P2
01.d	P1	01.s	P1	02.i	P2	05.i	P1	07.c	P1	08.m	P1	09.o	P1	09.ad	P1	10.m	P1
01.e	P1	01.t	P3	03.a	P1	05.j	P1	07.d	P1	09.a	P1	09.p	P1	09.ae	P2	11.a	P1
01.f	P1	01.u	P2	03.b	P1	05.k	P1	07.e	P1	09.b	P1	09.q	P1	09.af	P1	11.b	P1
01.g	P2	01.v	P1	03.c	P1	06.a	P1	08.a	P1	09.c	P1	09.r	P2	10.a	P1	11.c	P1
01.h	P1	01.w	P1	03.d	P1	06.b	P1	08.b	P1	09.d	P1	09.s	P1	10.b	P1	11.d	P1
01.i	P1	01.x	P1	04.a	P1	06.c	P2	08.c	P1	09.e	P1	09.t	P2	10.c	P1	11.e	P1
01.j	P1	01.y	P1	04.b	P1	06.d	P2	08.d	P1	09.f	P1	09.u	P1	10.d	P1	12.a	P1
01.k	P1	02.a	P1	05.a	P1	06.e	P1	08.e	P1	09.g	P2	09.v	P1	10.e	P2	12.b	P1
01.l	P1	02.b	P1	05.b	P1	06.f	P1	08.f	P1	09.h	P1	09.w	P1	10.f	P1	12.c	P2
01.m	P1	02.c	P1	05.c	P1	06.g	P3	08.g	P2	09.i	P3	09.x	P1	10.g	P1	12.d	P1
01.n	P1	02.d	P1	05.d	P3	06.h	P3	08.h	P1	09.j	P1	09.y	P2	10.h	P1	12.e	P3

Whether or not these priority codes will be useful to an organization will depend on the specific deficiencies requiring CAPs. Self- and third party assessors must also fully understand the requirements in order to understand their dependencies.

An organization should understand that CAP prioritization will depend on other factors unique to the organization, which cannot be addressed by an RMF like HITRUST or NIST. Examples include available operational and capital budget, budget planning processes, architecture and infrastructure constraints, and even organizational culture and politics.

HITRUST generally requires CAPs for all CSF requirements that score a 3 or below and for any requirement that is not fully implemented (i.e., not fully compliant for maturity level 3, Implemented).

To illustrate how risk and priority codes can be applied to CAP prioritization, consider a scenario in which an organization has an immature business continuity program and received the following HITRUST maturity scores for controls 12.a thru 12.e.

- 12.a, Including Info. Security in the Business Continuity Mgmt. Process: 50
- 12.b, Business Continuity and Risk Assessment: 75
- 12.c, Developing and Implementing Continuity Plans Including Info. Security: 50
- 12.d, Business Continuity Planning Framework: 50
- 12.e, Testing, Maintaining, Reassessing Business Continuity Plans: 38

CAPs would likely be required to address deficiencies with one or more requirement statements for controls 12.a, 12.c, 12.d and 12.e; however, for the sake of simplicity, we'll assume we're dealing with one requirement specification for each control.

Risk and priority information for these four controls are provided in the next table.

Table 12. CAP Prioritization Example

CSF Control	Maturity Score (MS)	Impact Rating (IR)	Raw Risk Score (R)	Priority Code	Assigned Priority
12.a	50	3	25	P1	2
12.c	50	3	25	P2	3
12.d	38	3	31	P1	1
12.e	50	3	25	P3	4

The highest risk gap has a priority code of 1, so this CAP is assigned the highest priority. The three remaining controls have similar excessive residual risk, and so they may be ordered according to their priority codes: 12.a (P1), 12.c (P2) and 12.e (P3).

Alternate Controls

Compensating Controls

Information protection cannot be a "one size fits all" approach for many reasons. For example, organizations more often as not have different information systems (or different implementations of similar systems), different business and compliance requirements, different cultures, and different risk appetites. Even the HITRUST CSF cannot account for all these differences through the tailoring of controls based on specific organizational, system and regulatory risk factors.

So for whatever reason an organization cannot implement a required control, one or more compensating controls should be selected to address the risks posed by the threats the originally specified control was meant to address. But while compensating controls are well-known and extensively employed by such compliance frameworks such as PCI-DSS, the term compensating control has often been used to describe everything from a legitimate work-around to a mere shortcut to compliance that fails to address the intended risk.

As a result, organizations should be able to demonstrate the validity of a compensating control by way of a legitimate risk analysis that shows the control has the same level of rigor and addresses a similar type and level of risk as the original. In addition, the compensating control must be something other than what may be required by other, existing controls.

HITRUST Approach

HITRUST also provides for the selection of compensating controls based on a standardized risk analysis, which is used to justify an exception to one or more HITRUST CSF control requirements applicable to a specific organization or gain HITRUST approval for its broader application across the industry. HITRUST refers to compensating controls submitted to and approved by the HITRUST Alternate Controls Committee, which may be used by any organization seeking validation or certification against the CSF, as "alternate controls."

While any risk analysis has its limitations based on the specific methods, tools and data used, the methodology should be sufficiently robust to meet the needs of the decision maker, i.e., the information provided should be of sufficient quality to make a reasonably good decision. So while NIST allows "maximum flexibility" in how targeted assessments are conducted, the healthcare industry must have a minimum standard of care for the evaluation of alternative controls to ensure organizations have a common understanding of the risks mitigated or—more importantly—not mitigated by the controls selected.

Risk may be computed in several ways, but perhaps the simplest form is some function of the likelihood a threat will successfully exploit a vulnerability and the damage that would likely result from the compromise, which are typically of the confidentiality, integrity or availability of information.

Risk = Fn (Likelihood of Occurrence, Expected Impact).

The likelihood a threat will materialize depends on several factors: threat source (which also considers the capabilities and motivation of the source if a human actor), threat event, and the vulnerability (or vulnerabilities) being exploited.

Risk = Fn ([Threat Source, Threat Event, Vulnerability], Impact).

In terms of conditional probability, risk may then be written as

Risk = P (Successful Exploit | Threat Event Occurs) x Impact.

Controls may reduce the likelihood a threat source will successfully exploit a vulnerability or they may reduce the likely impact should the threat event occur. We address the former here.

For the purposes of evaluating controls that address a specific threat, we can assume:

1. The impact from a successful exploit is identical regardless of the control that failed, and
2. The threat event has actually occurred, e.g., an external attacker sends an email with embedded malware or an insider has attempted to guess another user's password.

The analysis of alternative controls can then focus on the probability of a successful exploit of a particular vulnerability given a particular control is employed, assuming of course the controls are similar in the way they address the risk (e.g., both are preventative controls). In other words, we want to determine if

$$\mathbf{P(\text{Successful Exploit of Control}_A) \approx P(\text{Successful Exploit of Control}_{CSF}),}$$

which implies we need simply to know how well each control or set of controls address(es) the threat and any 'unintended consequences.'

The rubric used by the HITRUST Alternate Controls Committee to evaluate the sufficiency of a risk analysis is as follows:

- Threats appropriately identified & described?
- Alternate control adequately specified?
- Risk analysis adequate (reasonable, correct/accurate)?
- Additional controls adequately specified if equivalent risk not addressed?
- Additional risk issues ("unintended consequences") identified & described?
- Compensating controls adequately specified for additional risk issues?
- All risks addressed satisfactory (rough equivalency)?
- Unmitigated risks (low only) formally identified and accepted by management?

Analysis Requirements/Flow

Accordingly, all alternate control risk analyses submitted to HITRUST must comprehensively address the elements identified in the following flow chart:

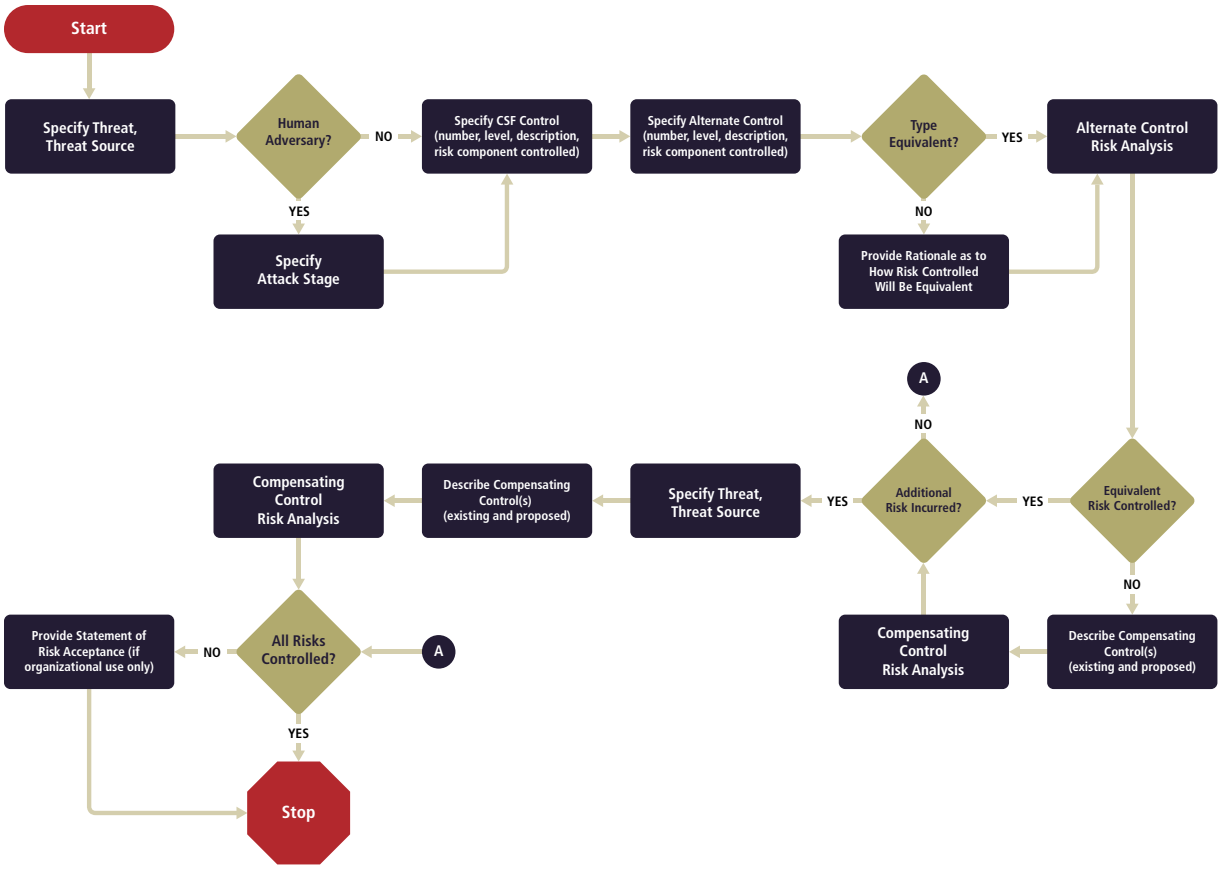

Figure 4. Alternate Control Risk Analysis Flow

To illustrate the risk analysis required to support an alternate control submission to HITRUST, consider the following example in which an organization needs to extend the expiration of user passwords beyond the 90-day requirement specified in CSF control 01.d, User Password Management. The analysis provides justification for extending the expiration period to one year based on how passwords are generated and provides a brief recommendation on how to address the "unintended consequences" associated with stale passwords.

Threat Addressed: User passwords are susceptible to guessing or online cracking methods.

Threat Source (Human Actor or Natural Event): Human Actor

If Human Actor is Adversarial, Specify the Attack Methodology Stage (Reconnaissance, Penetrate, Entrench, Pivot, Disrupt, or Counter Defense): Penetration

CSF Control Reference(s): 01.d, User Password Management

CSF Control Specification(s):

"vii. Passwords shall be changed at least every 90 days…

…

"ix. Passwords shall require at least eight (8) characters which are:

"1. Easy to remember;

"2. Not based on anything somebody else could easily guess or obtain using person related information …

"3. Not vulnerable to dictionary attack …

"4. Free of consecutive identical characters; and

"5. A combination of alphabetic, upper and lower case characters, numbers and special characters (combination of any three [3] of the above four [4] listed is acceptable)."

"x. Passwords shall be prohibited from being reused for at least six (6) generations; and

"xi. At least four (4) characters are changed when new passwords are created.

Issues with CSF Control Specification(s):

Users have expressed dissatisfaction with frequent changing of their password, which is often difficult to remember from one change to the next. As a result, passwords are often written down or constructed so they are easily remembered but relatively weak from one change to the next, e.g., L0v{1234, L0v{5678, L0v{2345, L0v{6789, L0v{3456 and L0v{7890.

Proposed Alternate Control Specification(s):

"vii. Passwords shall be changed at least annually …

…

"ix. Passwords shall require at least six (6) randomly-generated characters from a 95-character key space (i.e., a combination of alphabetic, upper and lower case characters, numbers and special characters) OR passwords shall require at least thirteen (13) user-chosen characters which are:

"1. Easy to remember;

"2. Not based on anything somebody else could easily guess or obtain using person related information …

"3. Not vulnerable to dictionary attack …

"4. Free of consecutive identical characters; and

"5. Derived from a 95-character key space."

Comparative Analysis (Address how the CSF control specification addresses the threat and then provide a similar explanation of how the proposed alternate control specification addresses the threat):

Although techniques such as selecting a dictionary word and padding either side, especially if complex, does help (see the article, "Why Steve Gibson's Password Padding Works for Humans"), the relative weakness of user versus randomly chosen passwords is well known. This is why other estimates of entropy such as guess entropy and min-entropy exist, albeit they aren't easily determined.

The analysis takes a conservative approach by using standard entropy rather than other forms of entropy such as guess entropy or min-entropy. The table below, obtained online from "How Big is Your Haystack?" provides the following values for a 95-character key space (spaces or blanks allowed).

Table 13. Time to Crack Passwords of Specific Key Lengths

Size	Entropy	Search Space Size	Online Attack	Offline Fast Attack	Massive Cracking Array
4	26.3	8.23×10^{7}	22.87 hours	0.000823 secs	0.000000823 sec
5	32.9	7.82×10^{9}	2.9 months	0.0782 secs	0.0000782 sec
6	39.5	7.43×10^{11}	23.62 years	07.43 secs	0.00743 sec
7	46.1	7.06×10^{13}	22,440 yrs	11.76 mins	0.706 sec
8	52.7	6.70×10^{15}	2,130,000 yrs	18.62 hrs	1.12 mins
9	~60	6.37×10^{17}	203,000,000 yrs	2.43 mos	1.77 hrs
10	65.9	6.05×10^{19}	6,330,000,000 yrs	6.33 yrs	2.31 days

The table only provides estimates based on maximum entropy of the key space and doesn't consider the techniques used by cracking tools to reduce the key space when passwords are user-chosen. (One would need to use entropy values to support a true comparison.)

What the data suggests is the existing password requirements address protection against online attacks (1000 guesses per second), which essentially sets the standard for password expiration. As seen from the table, a random 5-character password using a 95-character key-space provides 32.9 bits of entropy and usable life of 2.9 months (as opposed to less than one second for an offline attack). As seen in Appendix A of NIST SP 800-63-1, Electronic Authentication Guideline, a user-generated 10-character complex password yields a similar amount of entropy (32 bits).

According to the CMS IS ARS Moderate-level Baseline, a user selected 8-character, complex password with 30 bits of entropy provides a useful life of 60 days. It seems reasonable that a decision was made at CMS to "round down" because the full 2.9 months would be needed by the hacker/cracker if the right password was the very last one guessed, which is arguably unlikely. Regardless, the CSF requirement allows for 3 months as opposed to 2 months for a standard user. The CSF requires account lockouts after a few failed login attempts, which supports the reasonableness of the CSF's 90-day requirement. (However, a privileged user is required to change their password every 2 months, consistent with CMS requirements.)

To determine the entropy required for a useful life of 1 year given a randomly chosen password, one must compute the exact theoretical length of the password required, which is somewhere between 5 and 6 according to the table above.

$$\textbf{Time to Crack} = \textbf{(Search Space Size) / (Guessing Rate)}$$

$$= \textbf{(Key Space)}^{\textbf{(Key Length)}} \textbf{ / (Guessing Rate), or } T = S^L / R.$$

(The search space size determination assumes the user would only use the minimum number of characters required, otherwise one would need to take into consideration the total search space sizes of 8-digit, 9-digit, 10 digit … M digit passwords, where M is the maximum key size allowed by the system.)

Since T = 1 year, S = 94 characters, and R = 1000 passwords/second, the

$$1 \text{ year} = 94^L \text{ passwords/ (1000 passwords/second)}$$

$$31{,}536{,}000 \text{ seconds} = 94^L \text{ seconds / } 1000$$

$$94^L = 31{,}536{,}000{,}000$$

$$\text{Log } 94^L = \text{Log } 31{,}536{,}000{,}000$$

$$L \text{ Log } 94 = \text{Log } 31{,}536{,}000{,}000$$

$$L = \text{Log } 31{,}536{,}000{,}000 / \text{Log } 94 = 10.4988 / 1.9731 = 5.3210.$$

Given a theoretical password length of 5.3210, we may compute entropy as follows:

$$\text{Entropy} = H = \log_2 (SL) = \log_2 (945.32) = 34.8770.$$

The table in Appendix A of NIST SP 800-63-1 suggests a user selected, 13-character complex password will likely provide a password life of 1-year. (And a quick calculation shows that a 12-digit password only provides about 6 months of password life.)

Once again, this analysis does not consider offline attacks, which have a minimum rate of 100 billion guesses (passwords) per second. Defense against an offline attack would require an entropy of 61.4, which suggests a random 10-character password or a user selected 40-character complex password to obtain a useful life of one year.

Additional Control Requirements:

The assumption that expiration can be based on the online guessing rate is based on another assumption around the protections afforded the hash table. Organizations must ensure that, should the password hash table be exported, the table's encryption must be able to resist a local brute force attack for at least a year. Hashed passwords should be provided similarly strong encryption during transmission.

One might consider leveraging adaptive (risk-based) authentication methods to address some of the additional risks associated with an extended password expiration requirement. Risk-based authentication may be necessary given that changing passwords periodically mitigates the risk of "password leakage" where another user, malicious or not, becomes aware of the actual password. Fingerprinting user devices, registering IP addresses, and presenting challenge/response questions in abnormal or high-risk scenarios should provide sufficient mitigation for the threat of password leakage.

Acceptance

Since controls are specified a priori based on an organization's specific risk factors and there are often multiple remediation activities going on at any one time, there may be cases in which an organization may wish to simply accept a limited amount of risk rather than plan for the remediation of one or more control deficiencies.

Consistent with NIST SP 800-30 r1, HITRUST allows organizations to accept rather than mitigate control gaps when the control has an average score of 3 or better, as—given the correlation between maturity and risk—the risk associated with such a control may be considered relatively low.

When an organization chooses to accept risk, the analysis submitted in MyCSF to support the selection must show the residual risk for all the requirement statements supporting the control evaluation is less than 20 using the risk formula presented earlier. To illustrate, let's look at a control that has an impact rating of moderate.

CSF control 0.a, ISMP, level 1 has four requirement statements:

1. The information protection program is approved by executive management.
2. The information protection program addresses all the HITRUST Control Objectives and the rationale for the exclusion of any CSF control domains.
3. The information protection program is reviewed and updated when there are significant changes in the environment but no less than annually.
4. The organization shall formally establish, implement, operate, monitor and improve the ISMP.

Let's assume the organization wants a HITRUST certification, but does not wish to manage its risk program to the HITRUST framework as it previously made a sizable investment working with a high-end consulting firm. It also runs a GRC platform against this proprietary framework, which was formally approved by executive management just one year ago. Let's now assume there are some gaps between the program and the CSF control objectives (which are with the non-required controls, so the gaps aren't readily apparent in the assessment report) and the organization only reviews its information protection program every three years in concert with its strategic planning process, which also acts as formal re-approval of the information protection program. We can assume that any new requirements will be identified and incorporated into the program during this three-year review. So let's say the organization scores as follows:

1. FC, FC, FC, FC, FC, which yields a score of 100.
2. PC, PC, PC, NC, NC, which yields a score of 38.
3. SC, SC, SC, SC, SC, which yields a score of 25.
4. FC, FC, FC, FC, FC, which yields a score of 100.

Assuming the scenario supports the results, this provides an average maturity score of 66 for the control. This results in possible CAPs for two gaps in this control's requirements:

1. (Requirement #2) The organization's information protection program does not address all the HITRUST Control Objectives and the rationale for their exclusion.
2. (Requirement #3) The organization reviews and updates its information protection program every three years rather than annually.

Now let's say the organization approves a CAP for the first issue and will do a gap analysis between its framework and the CSF, add some controls, and perhaps exclude some others based on a specific rationale (which we'll assume is acceptable to HITRUST). It also decides it does not want to do annual reviews of its information protection program and will continue to tie it into its strategic planning process every three years. The organization wishes to accept the risk for this control requirement based on a valid risk analysis that shows the operational benefits of incorporating the review in its organizational strategic planning process outweigh the risks from specific threats stemming from a "stale" program. It can accept the risk because the risk score for the overall control is L x I = [(100-66)/100] x [(3-1)x25) = 17, which implies the risk is low. Note, organizations may adjust the impact rating up or down one level when used for risk acceptance based on a valid rationale, which must be provided in the risk analysis submitted in MyCSF. Risk acceptance is tentative for the purposes of validation or certification until approved by HITRUST during its quality review.

The scores will look like this when the CAP is completed:

1. FC, FC, FC, FC, FC, or 100.
2. FC, FC, FC, SC, SC, or 81.
3. SC, SC, SC, SC, SC, or 25.
4. FC, FC, FC, FC, FC, or 100.

This results in an aggregated maturity score of 77, which is equivalent to a "3+" maturity rating. However, a formal risk acceptance for this requirement is still needed since requirement #3 is not fully implemented (i.e., fully compliant for level 3, Implemented).

Appendix B: Frequently Asked Questions

Where can I find NIST publications like NIST SP 800-66 r1?

NIST has a Web site with links to all the 800-series publications.

More Info: http://csrc.nist.gov/publications/PubsSPs.html

Where can I find HITRUST publications like the HITRUST CSF and HITRUST Assessment Methodology documents?

Documents can be downloaded from the HITRUST Website.

More Info: http://hitrustalliance.net

Are NIST SP 800-series documents intended for all healthcare organizations?

No, you'll find in the introduction of most NIST SP 800-series publications (e.g., NIST SP 800-66 r1, p.1) that they're primarily written as guidance for federal agencies; however, they may also be used by non-federal organizations on a strictly voluntary basis. Not all guidance may be applicable to a particular non-federal healthcare entity or the healthcare industry as whole.

What is the NIST HSR Toolkit?

The NIST HIPAA Security Toolkit Application is intended to help organizations better understand the requirements of the HIPAA Security Rule, implement those requirements, and assess those implementations in their operational environment. Target users include, but are not limited to, HIPAA covered entities, business associates, and other organizations such as those providing HIPAA Security Rule implementation, assessment, and compliance services. Target user organizations can range in size from large nationwide health plans with vast information technology (IT) resources to small healthcare providers with limited access to IT expertise.

More Info: http://scap.nist.gov/hipaa/

What is the OCR Audit Protocol?

The OCR HIPAA Audit program analyzes processes, controls and policies of selected covered entities pursuant to the HITECH Act audit mandate. OCR established a comprehensive audit protocol that contains the requirements to be assessed through these performance audits. The entire audit protocol is organized around modules, representing separate elements of privacy, security, and breach notification. The combination of these multiple requirements may vary based on the type of covered entity selected for review.

The protocol covers Security Rule requirements for administrative, physical, and technical safeguards as well as Privacy Rule requirements for (1) notice of privacy practices for PHI, (2) rights to request privacy protection for PHI, (3) access of individuals to PHI, (4) administrative requirements, (5) uses and disclosures of PHI, (6) amendment of PHI, and (7) accounting of disclosures. The protocol also covers requirements for the Breach Notification Rule.

More Info: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

What's the difference between the NIST HSR Toolkit and the OCR Audit Protocol?

The NIST HSR Toolkit provides a way to assess an organization's compliance with the HIPAA Security Rule implementation specifications. The OCR Audit Protocol provides a set of audit procedures for a large subset of the Rule's specifications, which are of particular interest to OCR, but does not go into the same level of detail that the Toolkit is capable of providing.

What is 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.

More Info: http://www.hitrustalliance.net/mycsf/

What assessments are available in MyCSF for validation or certification?

There are two types of assessments available in MyCSF for this purpose:

- **Baseline Assessment –** The baseline assessment efficiently measures an organization against a streamlined set of requirements from the controls required for CSF certification, which are identified and selected based upon risk. A HIPAA scorecard, which reports an organization's compliance with HIPAA requirements only, is also available once a baseline assessment is complete.
- **Comprehensive Assessment –** The comprehensive assessment efficiently measures an organization against a streamlined set of requirements from all 135 controls of the CSF. Scorecards for any of the other CSF authoritative sources will be available once a comprehensive assessment is complete.

More Info: http://www.hitrustalliance.net/mycsf/

What's the difference between the NIST HSR Toolkit and the assessments available in MyCSF?

The NIST HSR Toolkit assessment is most similar to the MyCSF Comprehensive Assessment. However, the Toolkit is only scalable to "standard-" and "enterprise"-level organizations and does not support tailoring based on other risk factors. Only simple "Yes/No" responses with the ability to provide comments are available. The Toolkit does not provide a control maturity or effectiveness rating that would provide a repeatable, consistent likelihood estimator.

What's the difference between the OCR Audit Protocol and the assessments available in MyCSF?

The OCR Audit Protocol is most similar to the illustrative procedures contained in the MyCSF Baseline Assessment. However, the Protocol is primarily a compliance tool as it does not provide a control maturity or effectiveness rating that would provide a repeatable, consistent likelihood estimator. The Protocol is not designed to be scalable or tailorable to the organization.

Is there a difference between a risk assessment and a risk analysis?

According to NIST, the terms are used synonymously. However, the terms can be significantly different in common usage, e.g., technical vulnerability assessments and control effectiveness assessments are sometimes confused with a risk assessment. Also, risk assessments in practice may not always contain all the elements necessary to support a valid risk analysis, e.g., vulnerability assessment, threat assessment, asset valuation and impact assessment, risk evaluation and prioritization, or remediation planning.

Will an assessment using the NIST HSR Toolkit help my organization satisfy the requirements for a risk analysis?

Yes, but not completely. The NIST HSR Toolkit provides a set of questions that map to the HIPAA Security Rule. Although some questions reference a specific NIST SP 800-53 security control, most reference the section in NIST SP 800-66 that addresses that particular implementation specification. The Tool allows organizations to perform a compliance assessment ("Yes/No" responses), but does not provide the estimates of likelihood and impact needed to support a risk analysis. This is left to the organization conducting the assessment.

More Info: http://scap.nist.gov/hipaa/, http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-3_smiller-jsheldondean-swilson_hsr-toolkit-use-case.pdf

Will an assessment using the OCR Audit Protocol help my organization satisfy the requirements for a risk analysis?

No, the OCR Audit Protocol does not address every implementation specification in the HIPAA Security Rule. It will only provide organizations a better chance of "passing" an OCR audit.

More Info: http://www.hhs.gov/ocr/privacy/hipaa/enforcement/audit/protocol.html

Will an assessment using MyCSF help my organization satisfy the requirements for a risk analysis?

Yes, a MyCSF Baseline Assessment will cover every implementation specification in the HIPAA Security Rule. However, a MyCSF Comprehensive Assessment will allow an organization to assess controls that support the primary controls mapped from the Rule to the HITRUST CSF. Both assessments provide likelihood estimators for probability and impact, which support the risk calculations needed to determine a risk strategy and prioritization of risk responses.

More Info: http://www.hitrustalliance.net/mycsf/

What are the key differences between the HITRUST and NIST control frameworks?

Although the HITRUST CSF incorporates a majority of the NIST control requirements, there are marked differences between the two frameworks. NIST is primarily designed for federal agencies and some of the requirements may not be suitable for some healthcare organizations. The CSF is specifically designed to meet the multitude of legislative, regulatory and other requirements relevant to the healthcare industry, whereas NIST—while an excellent framework—is simply one of them. The NIST framework is tailorable in that one of three baselines may be selected based on the highest level of impact from a loss of confidentiality, integrity and availability, whereas the CSF is tailorable based on multiple organizational, system and regulatory risk factors. The CSF scales to the size of organization; NIST does not. However, the NIST HSR Toolkit does scale the NIST controls for standard and enterprise-level organizations. HITRUST also manages additional tailoring through the alternate control approval process whereas NIST allows additional unmanaged tailoring.

Will the results of a PCI assessment address the majority of the requirements needed for a HITRUST CSF assessment?

Although both the PCI-DSS and HITRUST CSF have prescriptive control requirements, PCI-DSS does not cover the same breadth of requirements as the CSF. In addition, PCI's essentially binary approach to assessing controls will not address all the elements of the 5-level HITRUST CSF control maturity model, nor does HITRUST allow the use of compensating controls that are not reviewed and approved by the HITRUST Alternate Controls Committee.

How can I submit a request for an alternate control?

Requests for alternate controls should include a complete risk analysis using the methodology outlined in this document and submitted in a Word document to *ACC@HITRUSTalliance.net*.

Appendix C: Glossary

Adequate Security [OMB Circular A-130, Appendix III]: Security commensurate with the risk and magnitude of harm resulting from the loss, misuse or unauthorized access to or modification of information.

Adversary [DHS Risk Lexicon]: Individual, group, organization or government that conducts or has the intent to conduct detrimental activities.

Alternate Control [HITRUST]: A compensating control that has been submitted and approved for general use by the HITRUST Alternate Controls Committee. See *Compensating Security Control*.

Analysis Approach [HITRUST]: The approach used to define the orientation or starting point of the risk assessment, the level of detail in the assessment, and how risks due to similar threat scenarios are treated.

Aperiodic [Webster]: Occurring without periodicity; of irregular occurrence.

Assessment: See *Security Control Assessment* or *Risk Assessment*.

Assessor [HITRUST]: An individual or organization that conducts control assessments; includes self-assessors or independent assessors (e.g., internal or external auditors or third party assessors); includes HITRUST Certified CSF Assessor Organizations.

Assurance [CNSSI No. 4009]: Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.

Attack [CNSSI No. 4009]: Any kind of malicious activity that attempts to collect, disrupt, deny, degrade or destroy information system resources or the information itself.

Availability [44.U.S.C., Sec. 3542]: Ensuring timely and reliable access to and use of information.

Continuous Monitoring [NIST SP 800-137]: Maintaining ongoing awareness to support organizational risk decisions. See *Information Security Continuous Monitoring*, *Risk Monitoring*, and *Status Monitoring*.

Compensating Security Control [CNSSI No. 4009]: A management, operational, and/or technical control (i.e., safeguard or countermeasure) employed by an organization in lieu of a recommended security control in the low, moderate, or high baselines that provides equivalent or comparable protection for an information system. Synonymous with Alternate Control [HITRUST™].

Confidentiality [44 U.S.C., Sec. 3542]: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

Criticality [NIST SP 800-60]: A measure of the degree to which an organization depends on the information or information system for the success of a mission or of a business function. Criticality is often determined by the impact to the organization due to a loss of integrity or availability.

CSF Assessor Organization [HITRUST]: An independent assessor organization that has undergone a quality assurance review and has been certified by HITRUST that they meet CSF Assurance Program requirements.

Defense-in-Breadth [CNSSI No. 4009]: A planned, systematic set of multidisciplinary activities that seek to identify, manage, and reduce risk of exploitable vulnerabilities at every stage of the system, network, or subcomponent life cycle (system, network, or product design and development; manufacturing; packaging; assembly; system integration; distribution; operations; maintenance; and retirement).

Defense-in-Depth [CNSSI No. 4009]: Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization.

Entropy [NIST SP 800-63-1]: A measure of the amount of uncertainty that an attacker faces to determine the value of a secret. Entropy is usually stated in bits.

HITRUST Organization [HITRUST]: Refers to members of the HITRUST Community, i.e., healthcare organizations (covered entities and their business associates) that have adopted the CSF in some way, either as a simple reference for accepted best practices or those that use it as a compliance standard.

Impact Level [CNSSI No. 4009]: The magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Impact Value [CNSSI No. 1253]: The assessed potential impact resulting from a compromise of the confidentiality, integrity, or availability of an information type, expressed as a value of low, moderate, or high.

Information Security Continuous Monitoring [NIST SP 800-137]: Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Information Security Risk [NIST SP 800-39, p. 1]: The risk associated with the operation and use of information systems that support the missions and business functions of their organizations. See *Risk*.

Information System-Related Security Risk [NIST SP 800-160, adapted]: Risk that arises through the loss of confidentiality, integrity, or availability of information or information systems considering impacts to organizational operations and assets, individuals, and other organizations. A subset of *Information Security Risk*.

Integrity (44 U.S.C., Sec. 3542): Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Likelihood of Occurrence [CNSSI No. 4009, adapted]: A weighted factor based on a subjective analysis of the probability that a given threat is capable of exploiting a given vulnerability or a set of vulnerabilities.

Plan of Action and Milestones [OMB Memorandum 02-01]: A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones. Synonymous with *Corrective Action Plan*.

Quantitative Assessment [DHS Risk Lexicon]: A set of methods, principles, or rules for assessing risks based on the use of numbers where the meanings and proportionality of values are maintained inside and outside the context of the assessment.

Qualitative Assessment [DHS Risk Lexicon]: A set of methods, principles, or rules for assessing risk based on non-numerical categories or levels.

Repeatability [HITRUST]: The ability to repeat an assessment in the future, in a manner that is consistent with, and hence comparable to, prior assessments.

Reproducibility [HITRUST]: The ability of different experts to produce the same results from the same data.

Residual Risk [CNSSI No. 4009]: Portion of risk remaining after security measures have been applied.

Risk Analysis [CNSSI No. 4009, Adapted]: Examination of information to identify the risk to an information asset. Synonymous with risk assessment.

Risk Assessment [NIST SP 800-39, adapted]: The process of identifying, estimating, and prioritizing risks to organizational operations (including mission, functions, image, and 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.

Risk Factor [HITRUST]: A characteristic in a risk model as an input to determining the level of risk in a risk assessment.

Risk Management [CNSSI 4009, adapted]: The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations, and includes: (i) establishing the context for risk-related activities; (ii) assessing risk; (iii) responding to risk once determined; and (iv) monitoring risk over time.

Risk Management Framework [HITRUST]: A common taxonomy and standard set of processes, procedures, activities, and tools that support the identification, assessment, response, control and reporting of risk.

Risk Mitigation [CNSSI No. 4009]: Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process. A subset of Risk Response.

Risk Model [HITRUST]: A key component of a risk assessment methodology—in addition to the assessment approach and analysis approach—that defines key terms and assessable risk factors.

Risk Monitoring [NIST SP 800-39]: Maintaining ongoing awareness of an organization's risk environment, risk management program, and associated activities to support risk decisions.

Risk Response [NIST SP 800-39, adapted]: Accepting, avoiding, mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, or other organizations. Synonymous with Risk Treatment.

Root Cause Analysis [NIST SP 800-39]: A principle-based, systems approach for the identification of underlying causes associated with a particular set of risks.

Scaling [HITRUST]: The act of applying specific considerations related to the size and financial/resource capabilities/constraints of an organization on the applicability and implementation of individual security and privacy controls in the control baseline. A subset of Scoping.

Scoping [NIST SP 800-53, adapted]: The act of applying specific technology-related, infrastructure-related, public access-related, scalability-related, common security control-related, and risk-related considerations on the applicability and implementation of individual security and privacy controls in the control baseline.

Security Control [CNSSI No. 4009, adapted]: The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an organization and/or information system(s) to protect information confidentiality, integrity, and availability.

Security Control Assessment [NIST SP 800-39; CNSSI No. 4009, adapted]: The testing and/or evaluation of the management, operational, and technical security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization.

Security Control Baseline [CNSSI No. 1253, adapted]: A set of information security controls that has been established through information security strategic planning activities intended to be the initial security control set selected for a specific organization and/or system(s).

Semi-Quantitative Assessment [DHS Risk Lexicon]: Use of a set of methods, principles, or rules for assessing risk based on bins, scales, or representative numbers whose values and meanings are not maintained in other contexts. Synonymous with Quasi-Quantitative Assessment.

Status Monitoring [NIST SP 800-137, adapted]: Monitoring information security metrics in accordance with the organization's continuous monitoring strategy.

Tailored Security Control Baseline [NIST SP 800-39]: A set of security controls resulting from the application of tailoring guidance to the security control baseline. See *Tailoring*.

Tailoring [NIST SP 800-53; CNSSI No. 4009]: The process by which a security control baseline is modified based on: (i) the application of scoping guidance; (ii) the specification of compensating security controls, if needed; and (iii) the specification of organization-defined parameters in the security controls via explicit assignment and selection statements.

Threat [CNSSI No. 4009, adapted]: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service.

Threat Assessment [CNSSI No. 4009]: Process of formally evaluating the degree of threat to an information system or enterprise and describing the nature of the threat.

Threat Event [NIST SP 800-30 r1]: An event or situation that has the potential for causing undesirable consequences or impact.

Threat Scenario [NIST SP 800-30 r1]: A set of discrete threat events, associated with a specific threat source or multiple threat sources, partially ordered in time.

Threat Source [CNSSI No. 4009]: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally exploit a vulnerability.

Vulnerability [NIST SP 800-30 r1]: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Vulnerability Assessment [NIST SP 800-30 r1]: Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

HITRUST™

855.HITRUST
(855.448.7878)
www.HITRUSTalliance.net