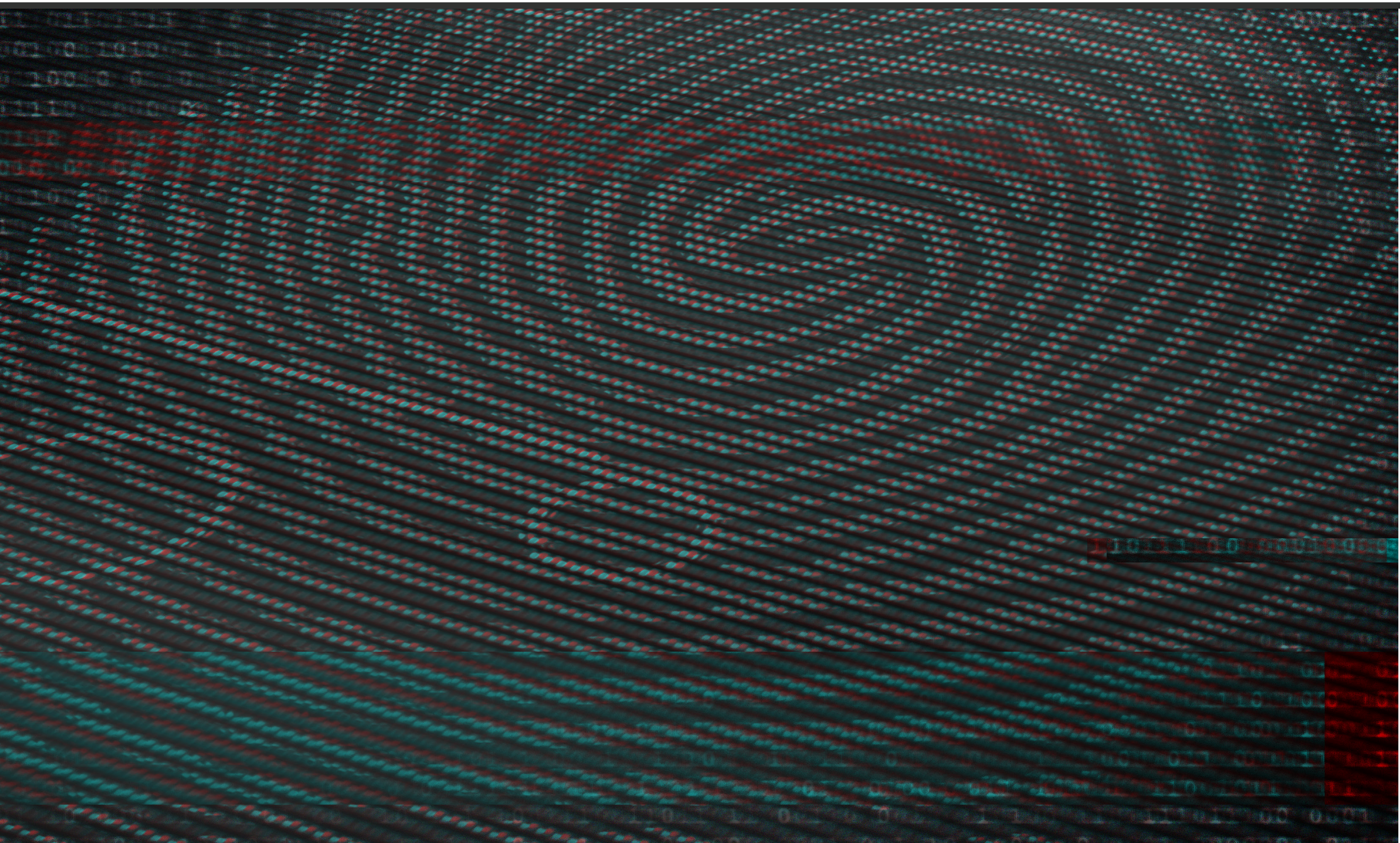
How to become HITRUST CSF-certified

TAKING CONTROL OF YOUR DATA COMPLIANCE



ePHI, a goldmine for hackers

Hackers learn as they go, changing their techniques, tactics, and procedures to achieve the greatest gain for the least effort. And with the rise of electronic health records (EHR) and healthcare marketplaces, hackers have discovered an ocean of data that is more valuable than the data held by retailers and financial organizations.

Data stolen from stores and banks has a limited life span; the fraud detection capabilities of these organizations can typically identify fraudulent activity when it occurs - rendering the value of stolen data essentially worthless. Even if the exposed business doesn't catch the breach, the consumer will notice when their credit card is declined at the gas station or their monthly bill shows purchases of luxury goods in Romania. As soon as the fraud is exposed, the data is null and void.

But the theft of health records can go unnoticed indefinitely. The Excellus breach exposed as many as 10 million records over a period of at least 22 months, and was only discovered when the company ran an assessment on its networks after reports of breaches at similar healthcare organizations emerged.

PHI can be used to commit insurance fraud, make purchases of prescription drugs, and commit other illegal acts that can deliver a greater financial reward than the relatively limited returns on stolen credit card numbers. In addition to a victim's social security number, PHI records provide a nearly complete snapshot of the individual – opening the door for potential identity theft.

Considering that several recent large-scale PHI data thefts have been attributed to state-sponsored hacking teams , the possibility that enemy states are seeking to combine PHI with security clearances for the purposes of espionage is not a stretch.

Of course, HIPAA regulations are intended to help healthcare organizations follow best practices for the management of sensitive information. Yet the breaches roll on as organizations confuse meeting compliance requirements with achieving true security while overlooking the fact that their security is only as strong as the security of the least secure of the business associates connected to their networks.

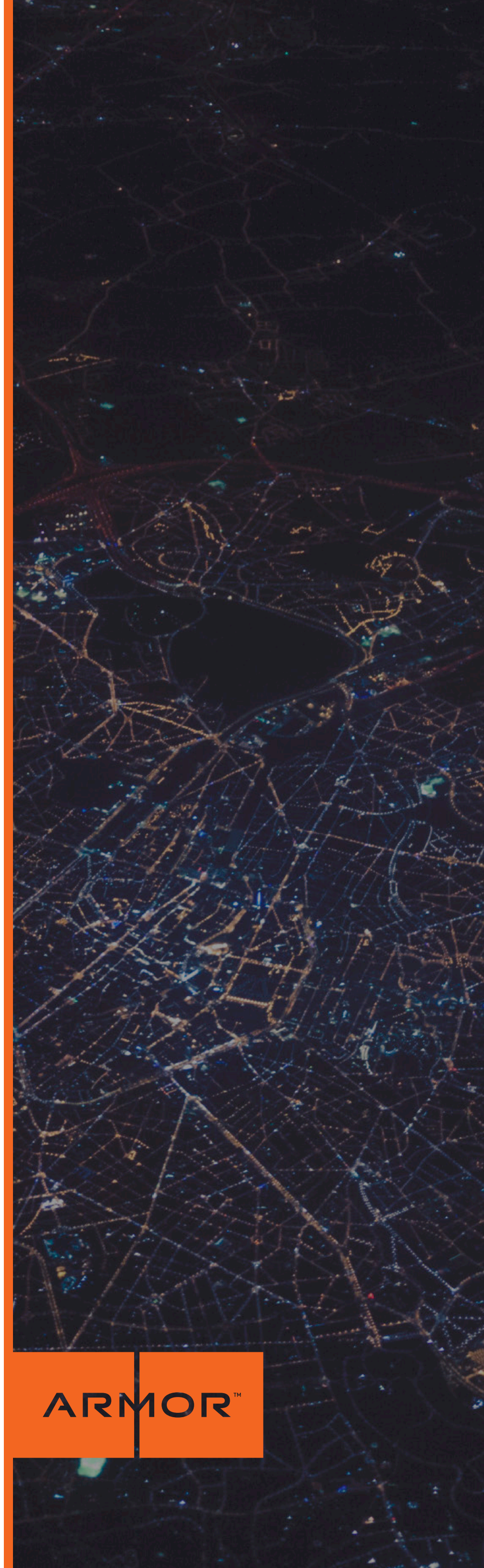
A crowded outlook

The majority or breaches happen in the supply chain. However, evaluating the security of business associates' networks is difficult; a healthcare organization may have many associates and vendors, each with a different set of security tools and processes in place.

While many healthcare organizations have general associate and vendor management practices, they are often not specific enough to meet the requirements necessary for an organization to declare itself "HIPPA Compliant."

To vet their associates, healthcare organizations are forced to patch together risk assessment programs from a sea of requirements, such as NIST, ISO 27001/27002, SSAE16, PCI DSS, and other standards. Industry best practices are part of the mix as well. Each risk assessment program must be updated each time a standard is updated, and each business associate must be assessed annually. These efforts are time-consuming, costly and difficult.

> While many healthcare organizations have general associate and vendor management practices, they are often not specific enough to meet the requirements necessary for an organization to declare itself "HIPAA Compliant."



Simplifying compliance

To resolve these challenges, the Health Information Trust Alliance, a non-profit organization, collaborated with leaders in healthcare and information security to develop the HITRUST Common Security Framework (CSF). CSF is a certifiable security framework that scales according to the type, size, and regulatory requirements of an organization and its systems. HITRUST CSF enables healthcare organizations to tailor their security control baselines to fit their specific needs.

The usefulness of HITRUST CSF is evidenced by its widespread adoption. According HITRUST, more than 84 percent of hospitals and healthcare organizations use CSF to strengthen the security of their PHI and PII creation, access, storage, and exchange, and an increasing number of large organizations, including Anthem, Highmark, as well as United Health Group, already require their vendors to possess or be in the process of acquiring CSF certifications.

Even if its business associates do not currently require CSF certification, a vendor still benefits from possessing this certification. A CSF certification can dramatically reduce the security review cycle and gives compliance and security officers at purchasing organizations a higher level of comfort about entering into a relationship with a vendor.

80% of all healthcare data will pass through the cloud at some point in its lifetime by the year 2020.

The future for business associates and healthcare partners is clear: businesses that want to work with major healthcare organizations and in certain geographies need to start their CSF certifications without delay.

HITRUST MyCSF™

A Scalable Security Framework

HITRUST CSF addresses the requirements of existing standards and regulations, including:

HIPAA COMPLIANCE

COBIT® 5

PCI DSS COMPLIANT

NIST

ISO

FEDERAL TRADE COMMISSION

From framework to a compliance platform

Because many organizations deal with multiple types of regulated data including PHI, Cardholder data and PII, they need overlapping controls to manage HIPAA, PCI, and other requirements. MyCSF, the online tool used in the certification process, simplifies the management of multiple standards and regulations, so while the framework was originally conceived as a security framework for HIPAA, it is now used to assess the maturity of business associates' security systems across a spectrum of regulatory requirements.

An important distinction to understand is that organizations are not eligible to become CSF-certified—rather, specific systems within an organization are certified. Some healthcare organizations require their business associates to certify just a few systems while others require many systems to be certified.

Flexible and scalable

CSF can produce a control to meet any organization's regulatory requirements. Sixty-four control categories are required for CSF certification, but more can be produced if an organization needs them. For example, an organization that only handles PHI in lightly-regulated Wyoming may certify its systems using the base level of 64 categories, while an organization handling PHI and PII in heavily-regulated Massachusetts will need additional controls in order to certify its systems.

HITRUST MyCSF™

MyCSF, the online tool used in the certification process, simplifies the management of multiple standards and regulations, so while the framework was originally conceived as a security framework for HIPAA, it is now used to assess the maturity of business associates' security systems across a spectrum of regulatory requirements.

Understanding CSF scores

CSF certifications are performed by certified assessors who produce reports detailing the maturity of specific systems within an organization. An organization may, for instance, certify only its EMR systems or only its radiology department.

Unlike HIPAA compliance, which is determined by a vendor's self-assessments or PCI, which is based on a pass/fail system, CSF certifications require a passing score of at least 3 on a scale of 1-5 in each control category.

An organization that fails to receive a score of 3 in a category can still become certified, and as long as a vendor meets a particular measurable level, healthcare organizations will be willing to conduct business with it. In the meantime, HITRUST will work with the vendor to develop one or more corrective action plans to improve the score, following up within a specified timeframe to see if the changes have been made.

Proof must be provided in the form of evidence from an external assessor; if that proof is not supplied, HITRUST will pull the certification.

CSF Maturity Levels*

CSF is built around five maturity levels, based on the PRISMA model from the National Institutes of Standards and Technology. The first three levels focus on design effectiveness and the final two levels focus on operational effectiveness.

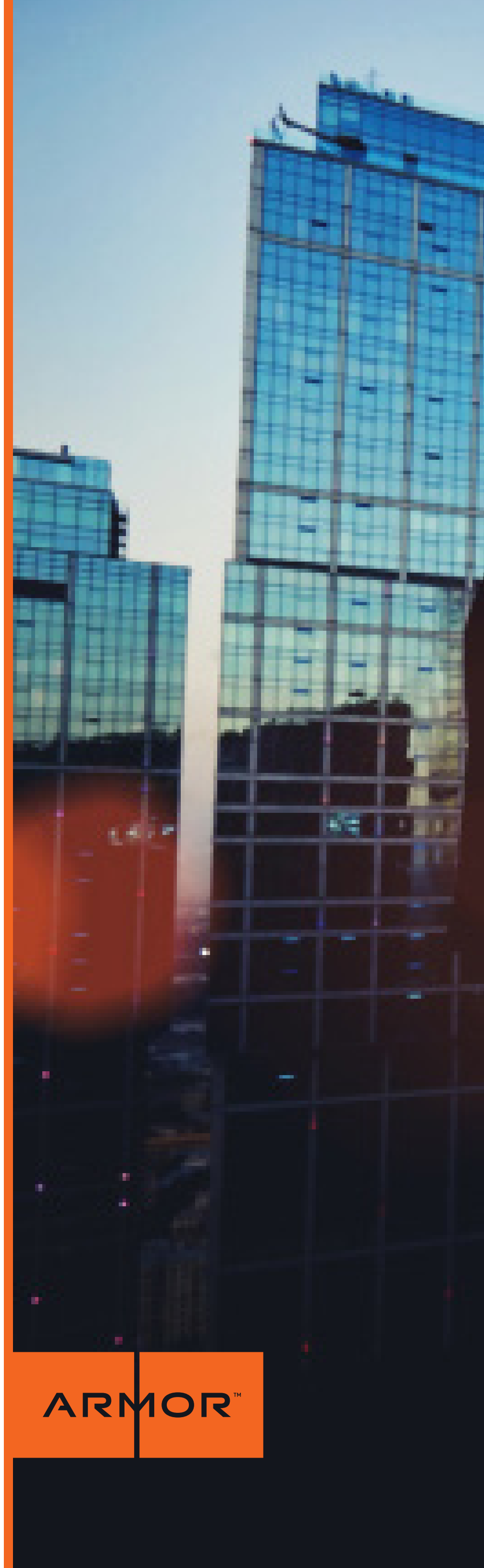
LEVEL 1: POLICY
Control requirements must be documented and shared with all stakeholders

LEVEL 2: PROCEDURES
Procedures must be in place to support the implementation of the controls

LEVEL 3: IMPLEMENTATION
Controls must be fully implemented and tested to ensure they operate as intended

LEVEL 4: MEASUREMENT
The testing and measurement of the implementation is reviewed to check its continued effectiveness

LEVEL 5: MANAGEMENT
The ability of the organization to respond to the results of the earlier levels is analyzed



Preparing for CSF certification

Business associates that wish to work with a healthcare organization must first determine the scope of their certification needs. The systems that need to be certified will depend on the requirements of the healthcare organization, and if there are multiple healthcare organizations in a vendor's trading circle, controls for each set of requirements must be evaluated.

Because the scope will be different for every business, so will the cost. Larger businesses may have to get all of their systems certified, and smaller businesses may need to as well if their systems are all connected. For instance, if a requirement is to certify an EMR system, the scope will depend on how many systems are connected to that EMR system.

Steps to Certification

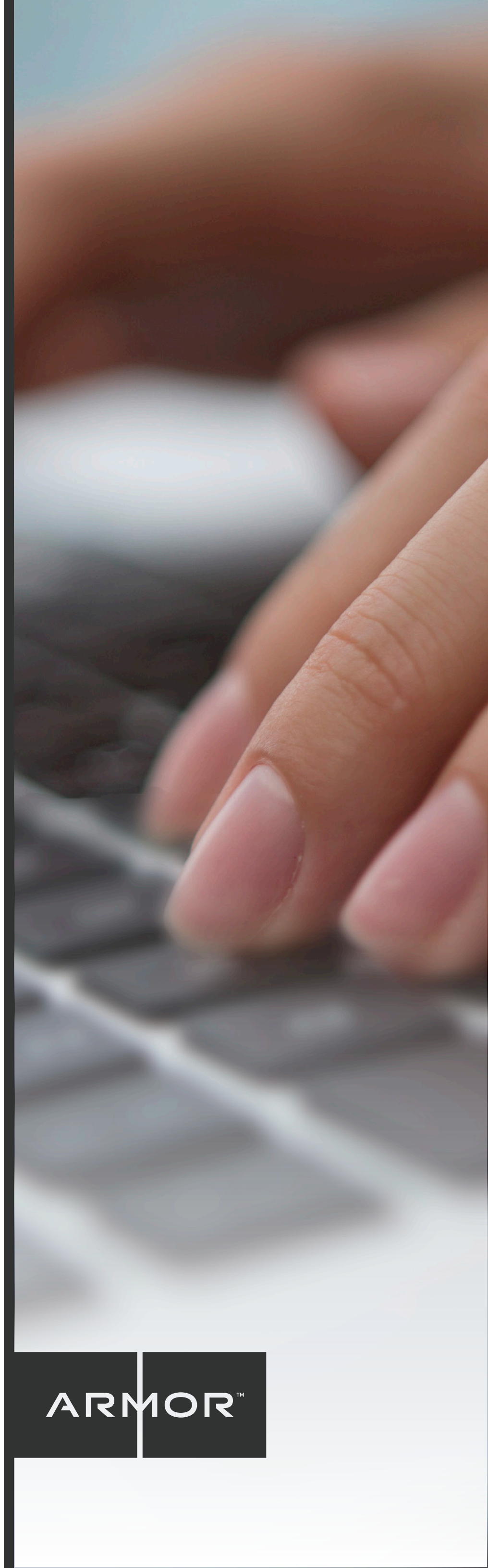
STEP 1	Determine scope
STEP 2	Purchase a subscription to MyCSF tool
STEP 3	Perform a self-assessment
STEP 4	Get an external audit and submit the assessor's work to HITRUST for evaluation
STEP 5	HITRUST will request evidence
STEP 6	HITRUST scores the results
STEP 7	If the score is sufficient, HITRUST will issue the certification

Scores can be inherited

Even though CSF simplifies the effort of achieving security compliance, getting certified on the framework is still an involved process that many organizations will find daunting. However, businesses that aren't able or willing to enter into the process have another option. CSF scores can be inherited from third parties.

Organizations can partner with a cloud security service provider that is already certified in specific elements of the framework, such as logging or encryption. The service provider can manage these difficult pieces, keeping them up to date for certification purposes so the customer is free to focus on the easier pieces... and on their core business.

To streamline the process further, HITRUST has created a tool called MyCSF, which allows businesses to manage policies, perform assessments and remediation efforts, track compliance, and handle incidents. The tool currently allows an entity to identify controls they believe can be inherited from service providers who have opted into this feature. The provider then validates those controls that can be inherited and the provider's score is then included in the organization's assessment.
This allows for more streamlined assessments for those organizations using HITRUST certified service providers.



Uniting business and security

The adoption of mandatory CSF certification by large organizations and some states is a strong move in a positive direction. HITRUST CSF provides organizations with an additional process through which to manage assessments and consolidate evidence collection. In addition, CSF saves business associates from the pain of completing multiple risk assessments and provides healthcare organizations with a single way to check its business associates' compliance with HIPAA and other regulations.

Although CSF carries many benefits for business associates, becoming certified is not without complications. Many businesses will find the simplest path to CSF is through a security services provider that has already certified its systems. The scores of providers are inheritable, so a business associate that selects a CSF-certified provider can complete its payers' security review cycles as quickly as possible. Since a growing number of large healthcare organizations are making CSF certification a mandatory condition for their business associates, getting certified is now the price of doing business for many companies.

- HITRUST CSF started as a healthcare security framework but is now an overarching framework encompassing many regulatory standards
- HITRUST CSF is becoming a mandatory certification for businesses that wish to trade with large healthcare organizations or in some states
- HITRUST CSF certifies systems, not organizations
- Determining scope is the hardest step
- HITRUST CSF scores can be inherited from a cloud security service provider

Works Cited

- **Brown, Luke. Lessons learned? A look back at five cyber-security trends of 2015.**
  January 13, 2016. http://www.scmagazineuk.com/lessons-learned-a-look-back-at-five-cyber-security-trends-of-2015/article/461033/
  (accessed May 24, 2016).

- **HITRUST ALLIANCE. n.d. https://hitrustalliance.net/**
  (accessed May 24, 2016).

- **Rashid, Fahmida Y. . Why hackers want your health care data most of all. September 14, 2015.**
  http://www.infoworld.com/article/2983634/security/why-hackers-want-your-health-care-data-breaches-most-of-all.html
  (accessed May 24, 2016).

- **Wike, Katie. Prediction: 80% Of Data Will Pass Through The Cloud By 2020. December 2, 2014.**
  http://www.healthitoutcomes.com/doc/prediction-of-data-will-pass-through-the-cloud-by-0001
  (accessed May 23, 2016).

US 2360 Campbell Creek Boulevard, Suite 525, Richardson, Texas 75082 | Phone: +1 877 262 3473
UK 268 Bath Road, Slough, Berkshire SL1 4AX | Phone: +44 800 500 3167