DATASHEET

Post-HITRUST CSF certification services

Optimize your certification for maximum benefit

As one of the original HITRUST CSF Assessor firms, Coalfire provides guidance and insights gleaned from years of interaction with HITRUST and organizations that have undergone HITRUST CSF certification. Many organizations are often unaware of the ancillary benefits that certification offers – from managing third-party risk and tackling continuous monitoring challenges to using the framework to meet regulatory requirements or as an enterprise risk solution. Our post-certification services help you fully understand how to optimize the framework and maximize your investment.

INTERIM AND CONTINUOUS MONITORING ASSESSMENTS

HITRUST CSF certification is valid for two years with the following expectations:

- The effective operation of controls is continuously monitored.
- Your organization does not report any data breaches to federal or state agencies.
- There are no significant changes in your business or security policies and practices.
- Progress is made on corrective action plans (CAPs) identified in the assessment.
- An assessor firm completes an interim assessment in the year following certification.

Many organizations invest heavily in the HITRUST CSF certification process, but a few months later, they can lapse into a comfortable state where security procedures and compliance requirements are not continuously monitored. This leaves them open to risks and unprepared for future threats. Our continuous monitoring program helps you develop a culture and strategy to continually review compliance status to meet industry and regulatory demands while maintaining secure systems. Both the interim and continuous monitoring assessments address a subset of requirements that were reviewed during the validated assessment for certification.

BRIDGE ASSESSMENTS

The HITRUST CSF is updated annually to address advancements in technology, emerging threats, and changes to the security landscape.

That means the HITRUST CSF may have undergone up to two version updates by the time you need to conduct your next full validated assessment. Our bridge assessment identifies changes in requirements between the version used in your last validated assessment against those in the current version.

This assessment identifies gaps in policy and process documentation before your next validated assessment. We evaluate documentation for additional controls and score them against the HITRUST maturity model. We then help remediate documentation issues, bring you into compliance with changed and/or additional requirements, and may provide additional guidance for implementing new requirements.

HIPAA SECURITY RISK ANALYSIS AND HITRUST CSF CERTIFICATION

To ensure certification covers the risk analysis requirement mandated by HIPAA, Meaningful Use, MACRA, and other regulations, you need to assess your environment to determine the location of sensitive information and examine the risks to that information by identifying key threats and vulnerabilities. You also must review the security controls and resulting likelihood, impact, and final risk rating determinations in accordance with the OCR risk analysis guidelines, the NIST framework, and other relevant regulations.

To obtain HITRUST CSF certification, you must:

- Identify and implement a tailored control overlay from the HITRUST CSF based on specific organizational, system, and regulatory risk factors to protect the confidentiality, integrity, and availability of protected health information (PHI).
- Perform a controls assessment and gap analysis.
- Address any excessive residual risk due to the identified gaps in implementation.

You should consult with your assessor firm and legal counsel to determine if using the HITRUST CSF sufficiently addresses the performance of risk analysis to meet the HIPAA Security Rule requirements.

THIRD-PARTY RISK MANAGEMENT

Creating a program to oversee your third-party relationships can help you avoid damages to your bottom line and reputation. By leveraging the HITRUST CSF Assurance Program's integrity, transparency, and consistency to enhance and streamline third-party risk management processes, you can reduce efforts associated with vetting, onboarding, and continuous monitoring of third-party risk. HITRUST CSF assessment reports offer a comprehensive, consistent, and standardized approach for evaluating the effectiveness of your vendors' privacy and security controls, while helping vendors reduce efforts by having a single assessment that multiple customers can leverage. Our practitioners design and implement programs to manage risk and establish organizational approaches and governance models. We help you identify, understand, and manage third-party risk throughout the risk management lifecycle.

ENTERPRISE RISK MANAGEMENT

The combination of HITRUST CSF certification and the NIST Cybersecurity Framework (CsF) subcategories is becoming a standard reporting approach for boards of directors. The HITRUST CSF Assurance Program and assessment scorecard for the NIST CsF offers an effective and efficient means of assuring management, business partners, and regulators of compliance with the NIST CsF's objectives. We can help you obtain a HITRUST CSF certification of your cybersecurity program's implementation against the NIST CsF by submitting an assessment through the current HITRUST CSF assurance program.

CERTIFICATION MARKETING SUPPORT SERVICES

HITRUST CSF certification meets customer demands for a more mature security posture and demonstrates the highest levels of data protection. Using certification as a competitive differentiator can also increase revenue. We can assist you with developing marketing materials (e.g., press releases, sales collateral, webinars, and tradeshow activities) that promote your HITRUST CSF certification to your customers and prospects.

DS_Post-HITRUST_082818

OPTIMIZE HITRUST CSF CERTIFICATION FOR SUCCESS.

Learn more about Coalfire's post-HITRUST CSF certification services.

Coalfire.com | 877.224.8077

COALFIRE

About Coalfire

Coalfire is the cybersecurity advisor that helps private and public sector organizations avert threats, close gaps, and effectively manage risk. By providing independent and tailored advice, assessments, technical testing, and cyber engineering services, we help clients develop scalable programs that improve their security posture, achieve their business objectives, and fuel their continued success. Coalfire has been a cybersecurity thought leader for more than 17 years and has offices throughout the United States and Europe. **Coalfire.com**