WHITE PAPER

HITRUST Preparedness Guide

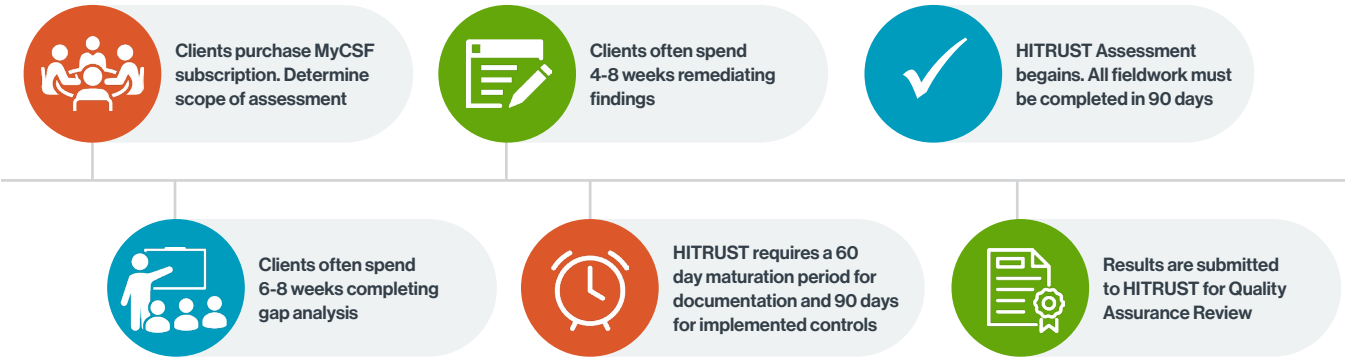
CALFIRE

Introduction

Navigating the path to HITRUST Certification can feel like a daunting task. For organizations striving to demonstrate robust security, compliance, and privacy practices, achieving HITRUST Certification sets a gold standard. The HITRUST CSF provides a comprehensive and flexible framework that streamlines regulatory compliance and strengthens your organization's risk management practices. It combines the best aspects of major frameworks into one certifiable standard, empowering organizations across industries to protect sensitive information while gaining a competitive edge in the marketplace.

This guide is designed to simplify the journey by providing actionable insights, timelines, and recommendations. Whether you're a small business or a large enterprise, Coalfire®'s HITRUST Advisory team is here to guide you every step of the way. From scoping and gap analysis to remediation and assessment, we help organizations achieve and maintain certification with confidence. Let's break down the process and ensure you're prepared to meet HITRUST's rigorous requirements.

The Typical HITRUST Timeline



The journey to HITRUST Certification follows a structured timeline with key milestones. It begins by contracting with HITRUST to gain access to the MyCSF platform. Once your MyCSF object is set up, the next step is scoping, where your organization identifies the systems, processes, and data that fall within the certification boundary.

After scoping, organizations perform a gap analysis to identify areas where their current security controls fall short of HITRUST standards. Following this, a remediation phase addresses any gaps identified, ensuring all necessary policies, processes, and controls are in place. HITRUST requires a maturation period to validate that documentation has been in place for at least 60 days, and that implemented controls have been operational for a minimum of 90 days.

When the maturation period concludes, the formal assessment begins. This involves a rigorous review of all controls and supporting evidence, and all fieldwork must be completed within 90 days. After the assessment, results are submitted to HITRUST for a Quality Assurance Review, which ensures the final report meets their stringent requirements. From start to finish, this structured process provides a pathway to achieving HITRUST Certification efficiently and effectively.

Coalfire's HITRUST Advisory: Industry Insights

Achieving HITRUST certification is a critical milestone in demonstrating your organization's commitment to security and compliance. Along the way, organizations often encounter challenges that can complicate the process. Coalfire's actionable insights highlight key areas of focus to help you navigate the HITRUST journey efficiently and effectively.

Insight 1: Scope the MyCSF Object Accurately

Why it Matters:

Properly scoping the MyCSF object is essential to identifying the applicable HITRUST controls for your organization. This ensures your assessment addresses the right requirements without unnecessary complexity.

The Challenge:

The HITRUST CSF draws from nearly 2,000 requirements, tailored to your organization's characteristics via the MyCSF scoping tool. Missteps during this process can result in excessive controls or missed requirements, leading to wasted effort or critical gaps.

How We Help:

- Leverage Coalfire's expertise to guide you through the MyCSF scoping process.
- Our advisors will help ensure the scope aligns with your operational environment and stakeholder expectations, setting the foundation for a successful assessment.

Insight 2: Define Clear Boundaries for the Implemented System

Why it Matters:

Defining the assessment boundary is critical to determining which systems, processes, and technologies will be evaluated for compliance. This clarity ensures a focused and efficient assessment.

The Challenge:

Ambiguity in defining the boundaries of the implemented system can lead to unnecessary inclusion of unrelated components or the exclusion of critical systems, undermining the assessment's value.

How We Help:

- Coalfire assists in developing precise assessment boundaries by reviewing system diagrams, data flows, and security controls.
- We ensure all in-scope systems are accurately identified and documented to streamline the assessment process.

Insight 3: Understand HITRUST Scoring Differences Across Assessment Types

Why it Matters:

HITRUST scoring criteria vary based on the type of assessment—e1, i1, or r2. Each assessment type has specific expectations for the maturity levels being evaluated.

The Challenge:

Organizations unfamiliar with HITRUST scoring may misalign their efforts, particularly when transitioning between assessment types. For example, the e1 and i1 assessments primarily focus on implementation maturity, while the r2 includes all five levels: Policy, Procedure, Implementation, Measured, and Managed.

How We Help:

- Coalfire provides tailored guidance on HITRUST scoring for your specific assessment type, helping your organization understand the criteria and set realistic expectations.
- Our advisors assist in aligning your internal scoring with HITRUST's rubric to minimize surprises during the validated assessment.

Insight 4: Gain Clarity on HITRUST Requirements and Testing Expectations

Why it Matters:

Misunderstanding how HITRUST requirements apply or will be tested during the assessment can lead to failed controls and wasted effort.

The Challenge:

HITRUST requirements often include specific definitions and expectations that can be difficult to interpret. Organizations without HITRUST experience may struggle to apply these requirements correctly or prepare for assessor testing.

How We Help:

- As one of the longest-standing HITRUST External Assessor firms, Coalfire has extensive experience helping organizations interpret and implement HITRUST requirements.
- We use our deep knowledge of HITRUST assessments to clarify expectations, identify potential challenges, and ensure your controls meet compliance standards.

Insight 5: Build a Sustainable Compliance Strategy with Regular Assessments

Why it Matters:

HITRUST compliance is an ongoing journey, not a one-time event. Regular reviews and gap analyses are essential for maintaining readiness and adapting to changing requirements.

The Challenge:

Without a proactive strategy, organizations risk falling behind on HITRUST requirements, leading to increased gaps and misaligned compliance efforts.

How We Help:

- Many organizations partner with Coalfire for annual HITRUST risk assessments and management reviews to stay aligned with the latest requirements.
- We also support biannual gap analyses, helping organizations address deficiencies and prepare for validated assessments according to their HITRUST validation schedule.

HITRUST Readiness Checklist

Understanding your organization's readiness for HITRUST Certification begins with evaluating basics from each of the 19 HITRUST domains. These domains cover a wide range of controls, from access management and incident response to physical security and risk assessment. To simplify this process, we've included a checklist to help you assess your preparedness and identify potential gaps. For your validated assessment, you will be required to show supporting evidence including policies, procedures and proof of implementation for each requirement, unless you and your external assessor determine the control to be out of scope, or the responsibility of a third party.

Instructions for Scoring the Checklist

- **Review Each Domain:** Carefully evaluate the HITRUST expectations and additional considerations provided for each domain to understand their relevance to your organization.
- **Answer the Questions:** For each row in the checklist, respond with "Yes" if your organization meets all of the expectation or "No" if it does not
- **Calculate Your Score:** Tally the total number of "Yes" responses across all domains.
- **Determine Your Readiness Level:** Compare your total score to the chart on page 12 to assess your organization's readiness for HITRUST certification.

If you need assistance or have questions about interpreting the expectations, contact your Coalfire HITRUST expert.

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
Information Protection Program • Policies and procedures that sufficiently address all information protection requirements. • An Information Security Management Program (ISMP) is formally documented, including objectives, roles, and frameworks covering all HITRUST domains. • Terms and conditions for employment, including acceptable use, are distributed to all personnel, with documented acceptance.	**Information Security Policy Development** • Does your organization have a clear, documented information security policy that explains its purpose, who's responsible, and includes management's commitment to security? **Policy Communication and Updates** • Has your information security policy been approved, made easy to access, shared with all relevant people, and is there a process in place to regularly review and update it as needed?	

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
• An organizational chart is established, reviewed annually, and documented. • Disciplinary and sanctioning procedures are established, and actions are documented. • Independent audits are conducted annually, with corrective actions for critical findings formally documented and tracked to completion.		
Endpoint Protection • Policies and procedures that sufficiently address all endpoint protection requirements. • Real-time or near real-time alerting and scanning for malicious software on all endpoints. • Auto-updating of endpoint protection software, ensuring distribution of the latest updates. • Filtering and blocking of spam and malicious code on all endpoints. • A centrally managed endpoint protection solution is in place. • Protection against mobile code is implemented. • Host-based firewalls are configured for all endpoints.	**Mobile Code Protection and Security** • Does your organization regularly update mobile code protection tools like anti-virus and anti-spyware on all devices, and have you set up firewalls to block all unnecessary traffic? **Endpoint and Firewall Configuration** • Are all your endpoint devices set up with firewalls that block all traffic by default, only allowing trusted services and ports, and is this configuration reviewed regularly for updates and improvements?	
Portable Media Security • Policies and procedures that sufficiently address all portable media security requirements. • Usage and transportation of removable media are logged. • User access to removable media is limited, or all usage is blocked via technical configurations. • Vulnerabilities associated with removable media are identified and assessed.	**Policy on Writable Removable Media** • Does your organization have and enforce a policy that restricts the use of writable, removable media on organizational systems to authorized and monitored devices only? **Controls for Personally Owned Media** • Are controls in place to prevent or restrict the use of personally owned, removable media on organizational systems unless explicitly authorized?	

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
• Removable media is encrypted to ensure data protection. • Proper handling and sanitation procedures for removable media are in place. • Non-digital media (e.g., paper records, faxes) are protected and controlled.		
Mobile Device Security • Policies and procedures that sufficiently address all mobile device security requirements. • Logging and alerting on unauthorized connection attempts from unknown devices. • Proper encryption is enforced on all mobile devices. • Annual training covers the risks of working remotely, and all users attest to understanding their responsibilities. • Technical configurations prevent jailbreaking or the installation of unauthorized applications. • A centralized device management tool ensures all devices are secured, encrypted, enrolled, and up-to-date.	Do you make sure that all mobile devices and platforms handling sensitive information are identified and encrypted to keep the data safe?	
Wireless Security • Policies and procedures that sufficiently address all wireless security requirements. • Quarterly scanning for unauthorized wireless access points. • Proper key management and password protection for wireless access points. • Perimeter firewalls configured to control traffic from wireless access points. • Encryption in transit for wireless access points.	Do you make sure that all wireless access is explicitly approved, and that devices and access points use strong encryption, like WPA2 or better, for authentication and data transmission?	

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
• Physical placement of wireless access points is secure and out of reach of unauthorized personnel. • Formal authorization and approval processes for wireless access points.		
Configuration Management • Policies and procedures that sufficiently address all configuration management requirements. • Change documentation includes testing, QA, development, and approval processes. • Segregation of duties (SOD) between development, testing, authorization, and implementation. • Physical and logical separation of development, testing, and production environments. • Requirements for backout/rollback procedures in place. • Emergency change processes are in place and logged. • System patching includes approval processes and controlled rollout. • Blacklisting/whitelisting tools are implemented to prevent unauthorized changes. • Formal documentation of baseline configurations exists. • A configuration management process ensures all software is current and up-to-date. • Annual technical compliance checks (e.g., penetration testing) and corrective actions are completed	**Vendor-Supplied Software** • Do you ensure that vendor-supplied software used in your systems is kept up to date and supported by the supplier? **Web Browser Security** • Are you using the latest versions of web browsers on your systems to take advantage of modern security features? **Baseline Configuration and Security** • Do you maintain a current baseline configuration for your systems and set security parameters to prevent misuse? **Change Management** • Are all changes to your system-like updates to applications, databases, or configurations—documented, tested, and approved before implementation (except for automated security patches)?	
Vulnerability Management • Policies and procedures that sufficiently address all vulnerability management requirements. • Comprehensive asset inventory that includes all in-scope assets.	**IT Asset Inventory Review** • Do you regularly review your organization's IT asset inventory at least once a year to make sure it's complete and accurate?	

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
• Annual review and reconciliation of the asset inventory. • Assets are classified by criticality and ownership is assigned. • Proper lifecycle management processes for assets, including usage, transfer, and disposal. • Input validation is performed for all applications. • Regular vulnerability scanning conducted. • Vulnerabilities are remediated based on their criticality in a timely manner. • Systems are auto-updated to ensure they run the latest versions of software.	**Automated Software Updates** • Do you use automated tools to keep your systems up to date with the latest security patches, and manually install updates for systems that can't automate this process? **Vulnerability Scanning** • Do you scan your information systems at least once a year to proactively identify and address any technical vulnerabilities? **Asset Inventory and Documentation** • Do you maintain an inventory of all your organization's assets, including sensitive information (e.g., PII) and devices, and document the importance of each asset, whether they are connected to your network?	
Network Protection • Policies and procedures that sufficiently address all network protection requirements. • Inbound and outbound rules are configured with a "deny all" approach. • Cloud security groups restrict access appropriately. • Network segregation implemented to reduce risks. • Network diagrams are formally documented and updated at least every 6 months. • IPS/IDS systems are implemented and configured. • Encryption in transit across all network connections. • Agreements with network service providers are in place and reviewed annually. • Web application firewalls (WAF) in place where applicable.	**Blocking Malicious Addresses** • Do you prevent your systems from accessing known malicious websites and domains, using methods like browser settings, DNS filtering, or subscription services, unless there's a clear business need and you understand and accept the risks? **Network Security and Segregation** • Do you use firewalls or secure gateways to control traffic and prevent unauthorized access between your internal network, external networks, and any demilitarized zones (DMZ), and ensure wireless networks are segregated from sensitive internal systems?	

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
Transmission Protection • Policies and procedures that sufficiently address all transmission protection requirements. • Encryption in transit protocols (TLS, IPsec VPN, SSH, HTTPS, SFTP) are established and in use, ensuring no deprecated protocols. • Protection of encryption keys from unauthorized access, destruction, or loss. • Email filtering and blocking mechanisms in place. • SPF, DKIM, and DMARC protocols implemented for email security.	**Email Authentication and Protection** • Has your organization set up SPF, DKIM, and DMARC to help prevent email spoofing and ensure that only legitimate emails from your organization are delivered? **Email Filtering Solution** • Do you use an email filtering solution to block suspicious emails and unnecessary file types before they even reach your employees' inboxes?	
Password Management • Policies and procedures that sufficiently address all password management requirements. • Password configurations are applied consistently and configured with complexity for all access points. • Passwords are securely stored and transmitted via encryption methods. • A list of compromised passwords is maintained and updated every 6 months. • Users are trained annually in secure password management and acknowledge these guidelines. • Password resets are tracked and logged, including user verification, random password generator, secure transmission, confirmation of receipt, and successful reset.	**Changing Default Passwords** • Does your organization change all default passwords on devices like routers, firewalls, and applications to strong, unique passwords before connecting them to the network? **Password Policy and Enforcement** • Do you have a documented password policy for your systems, and is it enforced through technical controls to ensure strong passwords are always used?	
Access Control • Policies and procedures that address all access control requirements.	**Account and Privilege Review** • Does your organization review all accounts (user, privileged, system, etc.) and their associated privileges at least once a year to ensure they're up to date?	

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
• Proper onboarding process with access approvals for new hires. • Timely removal of access when no longer needed, with proper logging. • Multi-factor authentication (MFA) implemented for access control. • Privilege access controls and approval process for high-level permissions. • Limiting privileged access accounts to the minimum number of users. • Unique identification for each user account. • Quarterly reviews of user access for all accounts. • 60-day access reviews for privileged accounts. • Proper password management and restrictions applied to service, group, and default accounts. • Session time-out configurations that sever connections after 15 minutes of inactivity, requiring re-authentication.	**Account Lockout Policy** • Do you have a documented policy for locking accounts after several failed login attempts, and is it enforced through technical controls? **Multi-Factor Authentication for Privileged Accounts** • Does your organization require multi-factor authentication (MFA) for accessing privileged accounts, both locally and over the network? **Access Reviews for Changes in Responsibility** • When there's a change in an employee's role or status, do you ensure their access to systems and equipment is reviewed, updated, or revoked as needed? **Separation of Admin and Non-Admin Accounts** • Do system administrators use separate accounts for administrative tasks and non-privileged activities (like browsing the web or checking email)? **MFA for Remote Access to Non-Privileged Accounts** • Do you require multi-factor authentication for accessing non-privileged accounts from remote networks, including VPNs and web applications? **Session Time-Out Enforcement** • Are both BYOD and company-owned devices set to automatically time out after a period of inactivity, as enforced by technical controls? **Accountability of User IDs** • Is each user ID in your system assigned to a specific person to maintain accountability for their actions?	
Audit, Logging and Monitoring • Policies and procedures that sufficiently address all audit logging and monitoring requirements.	**Audit Log Retention and Access** • Does your organization have a clear policy for how long audit logs are kept, and are these logs protected from unauthorized access?.	

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
• User actions are logged with detailed time/event information. • Audit logging is configured to alert on all critical functions and events. • Regular reviews of audit logs and event alerts, with formal documentation of review activities. • Audit logging criteria and strategy formally documented and reviewed annually. • Segregation of duties to prevent modification of logs by system administrators. • Time synchronization from at least two sources to ensure log accuracy.	**Audit Log Details** • Do your audit logs include key details like a unique user ID, data subject ID (if applicable), the function performed, and the date and time of the event?	
Education, Training and Awareness • Policies and procedures that address all training requirements. • Formalized training program in place and implemented. • Training completion is logged and tracked. • Annual training cadence enforced across the organization. • Role-based specific training is delivered to employees. • Initial training for new hires is required before accessing in-scope systems. • All users acknowledge that their actions are monitored, and violations may lead to disciplinary actions. • All users acknowledge and accept company policies/ procedures through formal acknowledgment. • Users trained on the prohibition of installing unauthorized software, with technical controls in place to prevent this.	**Phishing Awareness Training** • As part of your onboarding, does your organization provide dedicated training on recognizing and reporting phishing attempts, and track completion of this training? **Software Installation and Security Training** • Are users trained on the prohibition of installing unauthorized software, including data from external networks, and informed about security measures like disabling auto-run features to prevent unauthorized file execution?	

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
• Specialized training programs exist for incident management, development, executive leadership, and remote work.		
Third Party Assurance • Policies and procedures that address all third-party assurance requirements. • Clear distinction between critical and non-critical vendors. • Review of attestation reports from critical vendors. • Vendor risk questionnaires required for critical vendors without an attestation. • Formal collection and archiving of executed agreements with vendors. • Due diligence is performed during vendor onboarding with formal documentation. • Annual vendor reviews that assess potential risks to the ongoing relationship. • Vendor access is limited to appropriate personnel, with access removal when no longer needed. • All relevant agreements (BAAs, SLAs, MSAs, IEAs) in place with vendors, including services rendered and indemnity clauses. • Restriction and limitation of customer access as appropriate.	Does your organization ensure that access granted to external parties is limited to only what's necessary, given for the shortest time possible, and revoked as soon as it's no longer needed?	
Incident Management • Policies and procedures that sufficiently address all incident management requirements. • Incident identification and classification process in place. • Defined incident response procedures for various incident types.	Does your organization have a clear incident handling process in place that includes detecting, analyzing, containing, and recovering from security incidents, along with defined roles, procedures, and communication plans, and ties into your vulnerability management program?	

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
• Incident tracking and documentation system for incidents. • Root cause analysis and system impact analysis for each incident. • Defined escalation procedures for incidents and lessons learned. • Tracking and implementing changes to remediate incidents. • Disciplinary actions for incidents resulting in unauthorized disclosures or breaches. • Breach notification procedures defined and communicated. • Incident reporting mechanisms are available and accessible. • Employee training on general incident response procedures, including insider threat topics. • Specialized training for incident response personnel, including participation in an annual test.		
Business Continuity and Disaster Recovery • Policies and procedures to address all BCDR requirements. • Update the BCDR plan annually. • Conduct BCDR testing, Business Impact Analysis and backup restoration at least annually. • Configure and maintain backup strategies (incremental and full backups). • Implement offsite backup rotation and/or replication.	**Backup Storage and Security** • Does your organization store backup copies of data in a secure remote location, ensuring they're far enough from the primary site to protect against potential damage, and have physical and environmental controls in place? **Backup and Restoration Testing** • Are backup copies made regularly according to a set policy, tested at proper intervals, and are restoration procedures also tested to ensure they work when needed?	

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
Risk Management • Policies and procedures to address all risk management requirements. • Identify and prioritize critical information assets essential for business operations. • Assess the impact of threats to critical information assets. • Evaluate the vulnerabilities associated with those identified threats. • Assess the likelihood of identified threats and vulnerabilities. • Determine and address risks through mitigation, acceptance, or corrective action techniques. • Evaluate risks associated with significant changes, software releases, and commercial product purchases. • Conduct and document annual risk assessments.	Does your organization regularly conduct risk assessments that address key information security objectives and review the results annually, while also considering major changes in your environment?	
Physical & Environmental Security • Policies and procedures to address physical and environmental security requirements. • Implement environmental controls such as generators, UPS, HVAC, and fire suppression systems. • Manage physical access with controls and badge logging for facility entry and exit. • Log visitor access to the facility. • Conduct quarterly reviews of physical access permissions. • Utilize active surveillance (e.g., cameras) for facility monitoring. • Track, log, and authorize third-party personnel for maintenance activities.	**Access Control for Sensitive Information** • Is access to areas where sensitive information is processed or stored strictly controlled and limited to authorized personnel only? **Destruction of Sensitive Media** • Does your organization properly destroy media containing sensitive information (e.g., through methods like shredding, degaussing, or incineration) when it is no longer needed for business or legal reasons?	

HITRUST Domain Key Expectations	Additional Considerations	Meets? Y/N
• Ensure secure storage for surplus equipment. • Track and log the disposal and sanitation of equipment.		
Data Protection & Privacy • Policies and procedures to meet data protection requirements. • Classify and label sensitive data (e.g., PII, PHI), and managing its retention, access, and disposal. • Implement non-disclosure agreements (NDAs) with relevant parties. • Encrypt sensitive data at rest, including internal-facing records. • Limit and train users who have access to publicly accessible sites to ensure appropriate content is posted. • Control and approve the use of open-source software within the organization.	Are individuals authorized to post content on publicly accessible systems properly trained to ensure no nonpublic or sensitive information is accidentally shared?	

Total Yes: _____

Determining your readiness level:

15 - 19 Elevated Readiness

Your organization has built a strong foundation for security and compliance with well-documented policies and processes that address risks and drive continuous improvement. With these preparations, you're ready to pursue HITRUST certification. However, even with a high readiness level, Coalfire recommends engaging an advisory subject matter expert (SME) to review your results and provide expert guidance during your validated assessment. This additional oversight can ensure no gaps are overlooked and maximize your chances of success. As a licensed HITRUST Assessor, Coalfire offers comprehensive services to support your certification journey from start to finish. Contact us today to learn how we can help you achieve HITRUST certification with confidence.

11 - 14 Developing Readiness

Your organization has made significant strides in implementing security controls and managing risk, but certain areas may require further documentation or process optimization before pursuing HITRUST certification. Coalfire's readiness assessments and advisory services can help you prioritize improvements, streamline efforts, and refine your compliance program. Our team will work with you to strengthen your documentation, perform gap analyses, and provide tailored recommendations. Whether you need support defining key controls or are preparing for a readiness review, Coalfire has the expertise to help you meet your HITRUST goals.

0 - 10 Foundational Readiness

Every journey toward HITRUST certification begins with a solid foundation, and your organization is taking its first steps. Establishing core processes, documenting policies, and addressing risks is crucial at this stage. Coalfire offers comprehensive services to guide you through this process, from building an initial compliance framework to implementing best practices for risk management. Regardless of where you are on your HITRUST journey, Coalfire's experienced team is ready to help you move forward confidently and efficiently. Start your path to certification with Coalfire today.

Partner with Coalfire for HITRUST Success

Navigating HITRUST certification doesn't have to be daunting. Coalfire's HITRUST advisory services are designed to provide actionable insights, practical solutions, and expert guidance at every stage of the process. Whether you're just starting or refining an existing program, Coalfire helps you stay on track and achieve certification with confidence.

Ready to get started? Contact Coalfire today to take the next step in your HITRUST journey.

About Coalfire

Coalfire®, headquartered in Denver, Colorado, is a global leader in cybersecurity services and solutions. The company offers cutting-edge offensive security, advisory, and compliance services, as well as develops technology platforms that automate defenses against security threats for the world's leading enterprises, cloud providers, and SaaS companies. Coalfire is the foremost provider of FedRAMP assessments and penetration testing services in the United States. For more information, visit **Coalfire.com.**

Copyright © 2024 Coalfire. All rights reserved. The information in this document is subject to change at any time based on revisions to applicable regulations and standards. Any forward-looking statements are not predictions and are subject to change without notice. Coalfire is not responsible for any errors or omissions.