

TECHNICAL VALIDATION

Coalfire Compliance Essentials

Reducing Costs and Efforts in Executing Compliance Workflows

By Alex Arcilla, Senior Analyst, Validation Services
Enterprise Strategy Group

April 2024

Contents

Introduction	3
Background	3
Coalfire Compliance Essentials	4
Enterprise Strategy Group Technical Validation	5
Decrease Time and Effort in Executing Compliance Workflows	5
Maintain and Monitor Compliance in Real Time	8
Manage Compliance Risk	10
Conclusion	12

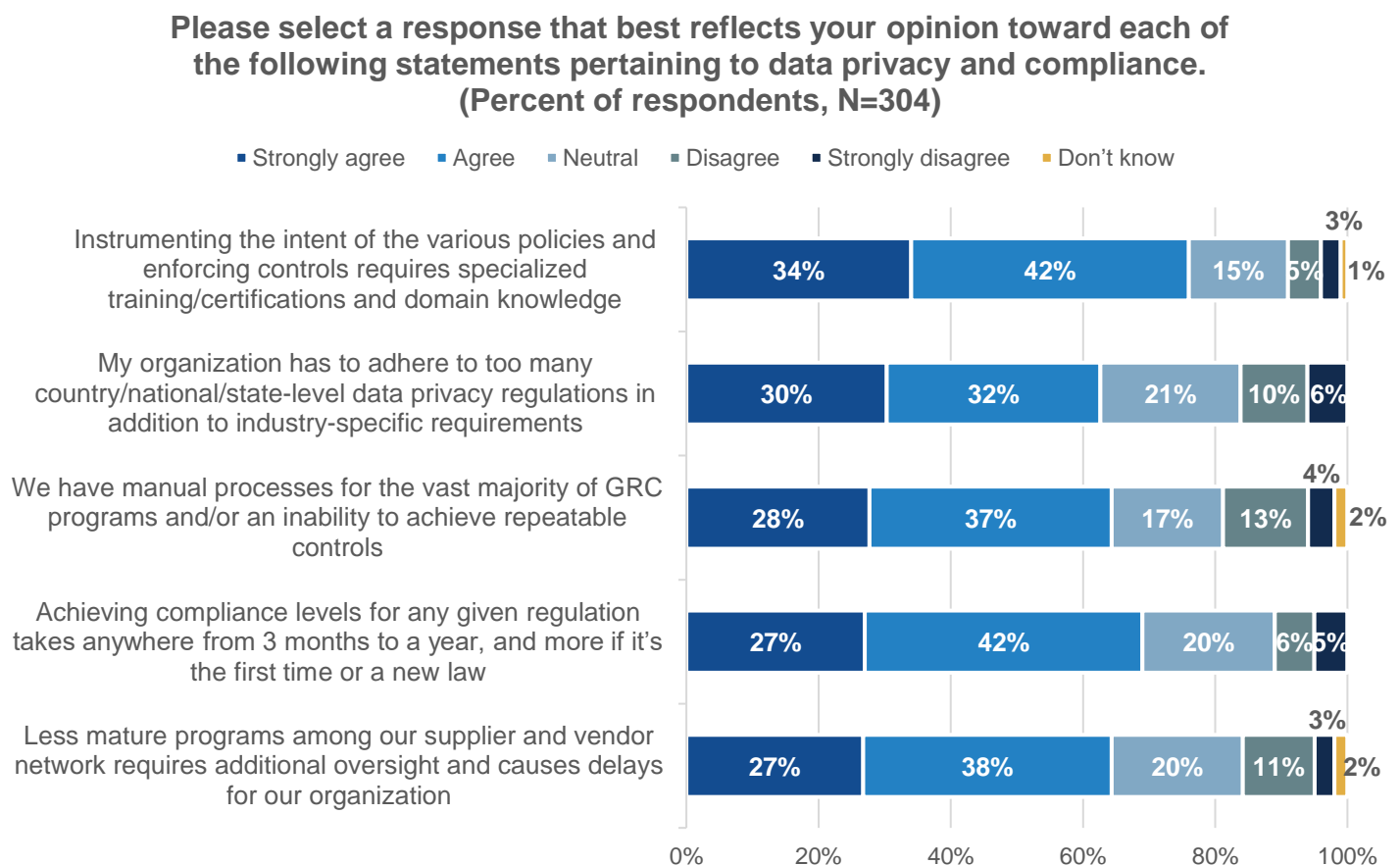
Introduction

This Technical Validation from TechTarget's Enterprise Strategy Group documents our evaluation of Coalfire Compliance Essentials. We reviewed how this platform can simplify how organizations coordinate and complete the required governance, risk, and compliance (GRC) activities more efficiently, thus bolstering data security and privacy. We also examined how Coalfire Compliance Essentials can help organizations to better maintain compliance simultaneously with multiple information security, data privacy, and compliance regulations, subsequently leading to improved data security, decreased business risk, and, ultimately, compliance.

Background

According to a research survey by Enterprise Strategy Group, 62% of respondents agree that they need to adhere to too many data privacy regulations in addition to industry-specific requirements.¹ Indeed, the number of data security, privacy, and compliance regulations and requirements that exist—whether issued by U.S. or international governments, standards bodies, or industry-specific committees—can be overwhelming. Yet, when it comes to current GRC programs, 65% stated that they have manual processes in place and/or an inability to achieve repeatable controls (see Figure 1).

Figure 1. Current Opinions Toward Data Privacy and Compliance



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

¹ Source: Enterprise Strategy Group Research Report, [The State of Data Privacy and Compliance](#), March 2022. All Enterprise Strategy Group research references and charts in this Technical Validation have been taken from this research report, unless otherwise noted.

Compliance with data security and privacy regulations and requirements is unavoidable. Not only does compliance ensure that an organization maintains an acceptable data security and risk posture, but it also assures potential partners or customers that they can do business safely and reliably with that organization.

While a number of GRC solutions are available for supporting organizations' compliance efforts, utilizing those tools can be difficult due to the complexity of the regulations and the need to coordinate multiple activities in order to maintain compliance across all regulations, especially when preparing for periodic and overlapping audits and assessments.

Simply put, tracking and coordinating multiple tasks when maintaining compliance across a growing number of regulations is difficult to achieve. To achieve compliance, organizations would ideally employ a solution that combines expert assessment services that establish compliance against desired regulatory frameworks with a platform that supports ongoing compliance by keeping track of tasks to complete in preparation for audits and certifications.

Coalfire Compliance Essentials

Coalfire Compliance Essentials is a SaaS-based compliance management and automation platform designed to reduce business risk and minimize costs associated with maintaining compliance across multiple regulatory frameworks. As part of Coalfire's solution for achieving compliance, the platform can help organizations reduce the manual and repetitive efforts typically associated with compliance tasks, as well as provide real-time visibility into ongoing compliance efforts (see Figure 2).

To ensure that organizations are up to date in their compliance activities and tasks, Coalfire Compliance Essentials can continuously assess compliance against multiple regulatory frameworks. The platform can then flag tasks to be completed prior to upcoming audits. By tracking this activity (over 365 days), organizations can be proactive, subsequently increasing the success of passing formal audits and assessments. Organizations no longer have to scramble to complete these tasks at the last minute, as the platform details the tasks to complete according to predetermined timelines. Also, since similar tasks can exist across multiple regulatory frameworks, Coalfire Compliance Essentials tracks these action items so that organizations can minimize duplicate efforts and their associated costs.

When business needs dictate (such as entering new markets or geographies), organizations can add additional data security, privacy, and regulatory frameworks to Compliance Essentials. Once input into the platform, organizations can begin tracking the tasks required for meeting new frameworks, without the need to develop the expertise in-house. Organizations can then enter new markets and verticals requiring compliance to specific frameworks more quickly.

Ensuring compliance against multiple frameworks is also supported by Coalfire's experience in delivering compliance advisory and assessment services. Because the expertise is built into the platform, Coalfire Compliance Essentials can identify gaps between the current status of compliance and existing frameworks. The platform also provides recommendations and guidance on how an organization can show compliance with specific aspects of regulatory frameworks, such as identifying what evidence should be provided. To prepare for formal audits, the platform can conduct internal assessments to reveal any compliance gaps.

Figure 2. Coalfire Compliance Essentials

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

With Coalfire Compliance Essentials, organizations can:

- Decrease costs by automating a number of the tasks associated with monitoring and maintaining compliance against multiple frameworks.
- Reduce both data security and business risk by continuously tracking how well organizations are complying with the latest version of regulations.
- Accelerate entry into new markets and geographies by ensuring that organizations can quickly and completely adhere to required frameworks.

Enterprise Strategy Group Technical Validation

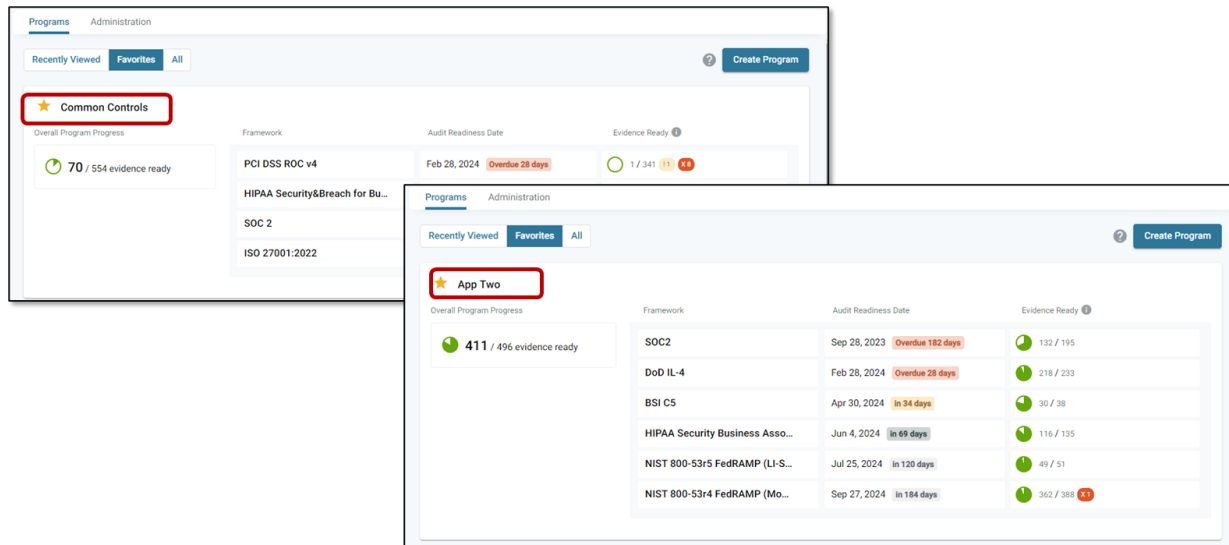
Enterprise Strategy Group validated how Coalfire Compliance Essentials helps organizations simplify compliance against multiple regulations and standards, continuously. We specifically reviewed how this platform coordinates compliance tasks and activities while removing duplicative effort, how it maintains and monitors compliance to ensure ongoing adherence, and how it manages ongoing risk.

Decrease Time and Effort in Executing Compliance Workflows

To do business in today's environment, organizations can expect to comply with multiple regulatory frameworks. Yet, managing compliance can easily become a complex web of tasks to coordinate throughout the year, especially when preparing for external audits. Coalfire Compliance Essentials can reduce the time and effort typically spent on compliance activities.

Enterprise Strategy Group Testing

Enterprise Strategy Group first navigated to the dashboard in the Continuous Compliance Module (see Figure 3). We first noted how compliance activities are grouped by programs, enabling organizations to track and monitor compliance against multiple frameworks. Programs (noted by the red boxes) can categorize frameworks according to which ones apply to a specific or business unit. A program can also group multiple versions of the framework, should different groups within an organization differ as to which version they are compliant against.

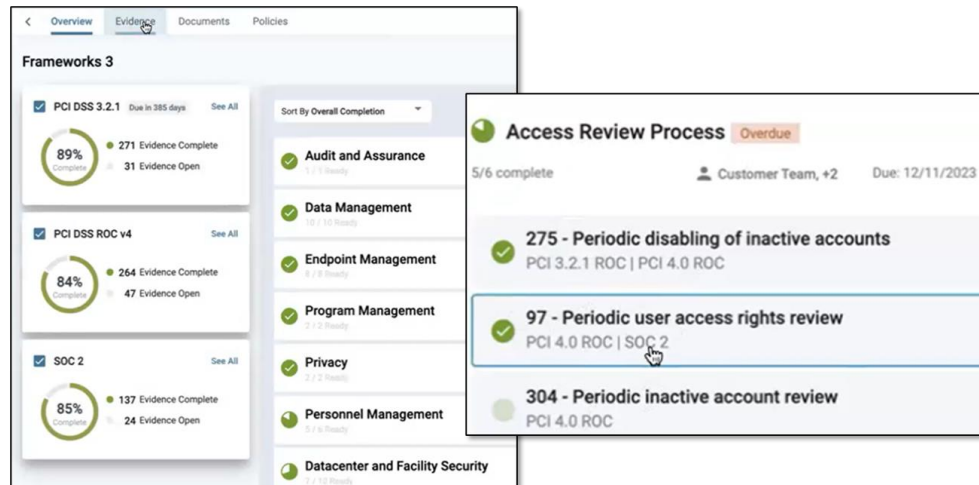
Figure 3. Programs for Tracking Compliance Status

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

By grouping frameworks into “Programs,” we could see how this can help organizations eliminate duplicative effort when completing compliance tasks across multiple frameworks that are tracked separately across business units or product lines (e.g., when providing evidence of compliance).

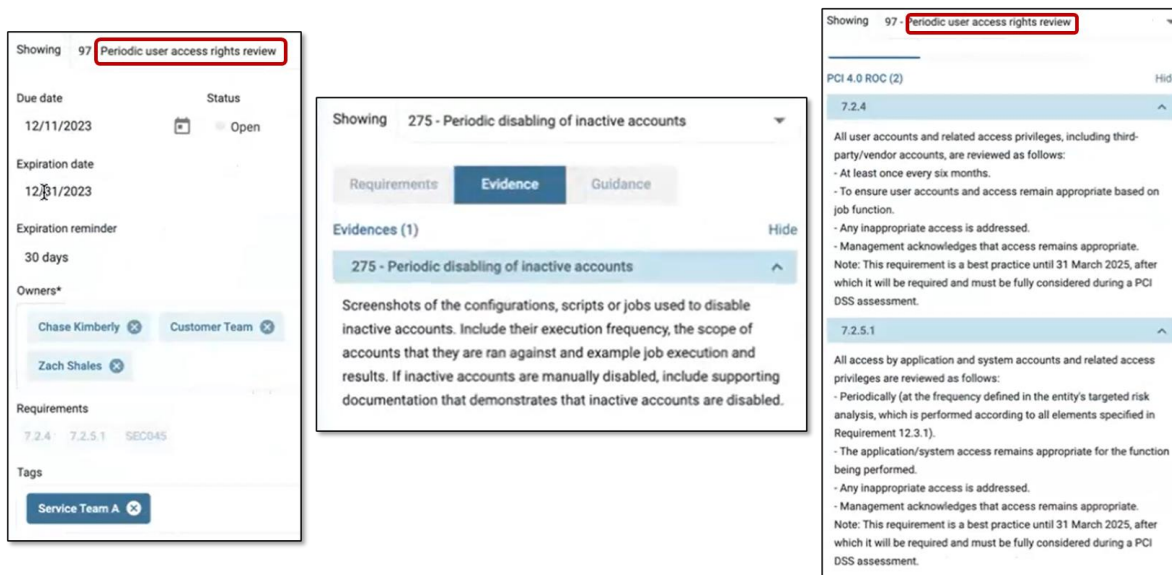
Enterprise Strategy Group then navigated to a Program that was tracking compliance status against multiple versions of the PCI DSS standard, as shown in Figure 4. (Other programs can easily focus on versions of the other 60-plus regulatory frameworks that Coalfire Compliance Essentials supports.) The platform assigned a completion percentage to each framework, indicating those tasks that had been completed to meet compliance.

The view of current compliance status was broken down into specific categories of the framework, such as “Audit and Assurance,” “Endpoint Management,” and “Privacy.” Enterprise Strategy Group clicked on the **Access Review Process** category to view evidence required to show compliance, as well as the frameworks in which the evidence could also be applied. We noted that the need to upload frameworks into a GRC solution and configure with the evidence needed to pass an internal assessment or external audit was eliminated. The platform already mapped the categories of evidence requests to ensure compliance, eliminating any chance that required evidence was overlooked.

Figure 4. Compliance Status for One Framework in a Program

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Enterprise Strategy Group then viewed the specific details associated with an evidence request under the Access Review Process category named **Periodic user access rights review** (see Figure 5).

Figure 5. How Compliance Status Is Displayed for Supported Frameworks

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

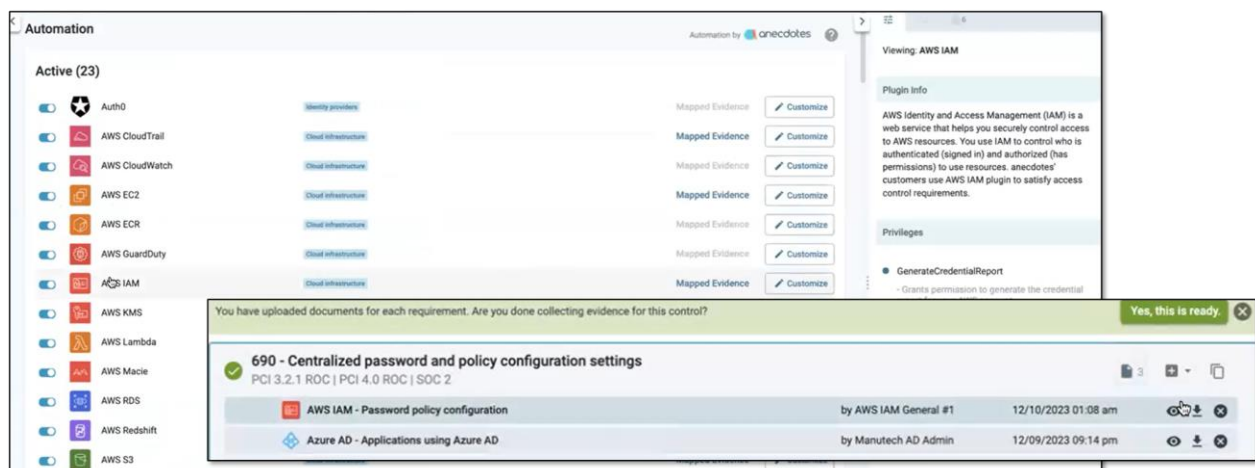
Details such as owners and due dates were displayed, providing clear timelines for completion. In addition, we saw how the platform could educate organizations on how evidence should be collected and presented, as well as how the evidence applied to multiple frameworks.

Enterprise Strategy Group saw how using this platform can help make compliance workflows more efficient. One alternative would be managing and tracking compliance-related tasks manually via spreadsheets, which has typically proven to be inefficient and unreliable. On the other hand, an off-the-shelf solution could be used. Yet,

organizations would need to input the frameworks they need to satisfy and, more importantly, know the frameworks well enough to enter the level of detail to track—specifically, how to present evidence. However, such expertise may not exist within the organization.

To further increase efficiency of gathering evidence, Enterprise Strategy group then observed how Coalfire Compliance Essentials can import evidence from cloud-based services. We navigated to the Automation page to see the public cloud services connected to the platform (see Figure 6). For frameworks that require evidence from these services, we saw how the platform could pull and map evidence for support frameworks. In Figure 6, the platform pulled evidence from both AWS Identity and Access Management (IAM) and Azure Active Directory (AD) for a specific requirement.

Figure 6. Automated Compliance Assessment



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

Tracking tasks to complete in compliance workflows can be complicated and time-consuming. Organizations find that they must adhere to multiple standards and regulations in order to conduct their business. And the reality is that these tasks are typically not completed in a systematic and timely way, increasing the risk of overlooking tasks or not fully satisfying requirements, especially when formal audits are to be conducted.

Enterprise Strategy Group validated that Coalfire Compliance Essentials can increase the efficiency of compliance workflows. We saw how the platform can provide a clear roadmap of tasks to be completed in order to achieve compliance against multiple frameworks simultaneously. We also saw how organizations can use the platform to coordinate and schedule tasks, as well as present evidence in preparation for audits, preventing any “last-minute” activity from occurring.

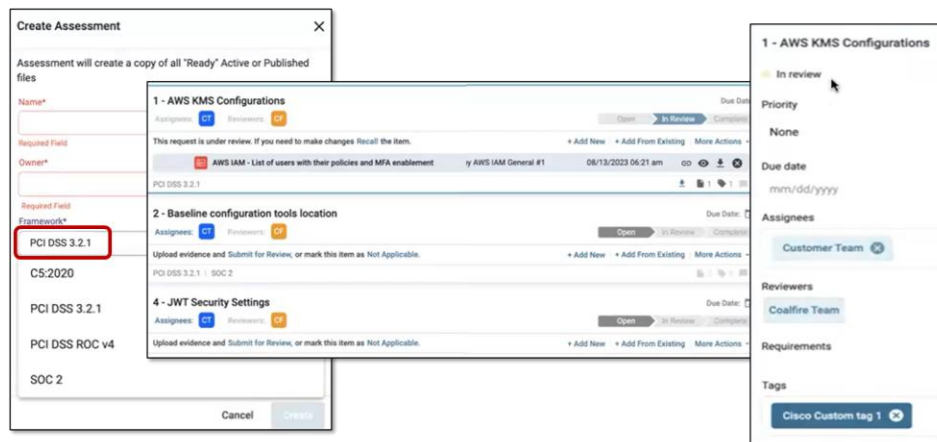
Maintain and Monitor Compliance in Real Time

By providing continuous visibility into the level of compliance against active frameworks, organizations can prevent “last-minute” efforts to gather evidence and complete tasks prior to formal audits.

Enterprise Strategy Group Testing

Enterprise Strategy Group first created an internal assessment to check compliance status against the PCI DSS v3.2.1 framework (see Figure 7). Once running the assessment, we could review open items and upload or provide evidence requested. After submitting the assessment, the review was performed by Coalfire's in-house experts, and after the assessment was completed, the platform returned open items to address (e.g., noncompliance of specific requirements). Open items were determined by what the framework defines as activities to complete throughout the year before a formal audit is conducted.

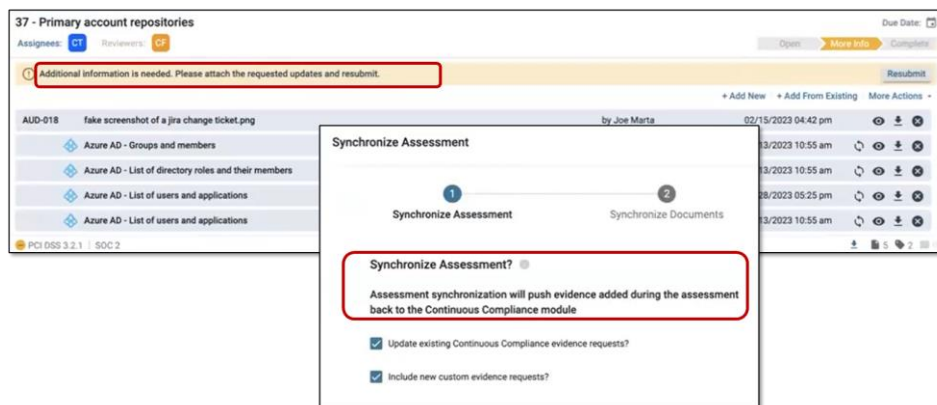
Figure 7. Performing Internal Assessments



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Once the internal assessment was complete, Enterprise Strategy Group viewed evidence requests to be completed (see Figure 8). Requests were listed according to specific requirements within specific frameworks that were not satisfied due to insufficient evidence.

Figure 8. Monitoring Ongoing Actions to Complete



Source: Enterprise Strategy Group, a division of TechTarget, Inc.

By performing these assessments, we noted how they could help organizations maintain compliance between formal audits and across multiple frameworks, as opposed to waiting until a formal audit is scheduled. Highlighting evidence requests to complete provided opportunities to upload additional information should organizations want another review.

We also reviewed how the platform could synchronize internal assessments so that the latest evidence and reviews were uploaded into the Continuous Compliance module. At this point, organizations had the latest evidence to be used for upcoming audits.

Another way that organizations can manage and monitor ongoing compliance is by tracking issues manually inputted (e.g., related to evidence preparation, upcoming audits, or internal assessments) so that organizations can follow those actions through to completion (see Figure 9).

Figure 9. Ongoing Monitoring of Issues and Tasks To Be Resolved

The screenshot displays two overlapping tables from the Coalfire Compliance Essentials interface. The top table, titled 'Issues', lists various compliance issues with columns for ID, Name, Status, Framework(s), Requirements, Priority, Due Date, Assignees, Reviewers, Last Updated, and Created From. The bottom table, titled 'Periodic Compliance Task', lists scheduled tasks with columns for ID, Name, Status, Framework(s), Requirements, Priority, Due Date, Assignees, Reviewers, and Last Updated.

ID	Name	Status	Framework(s)	Requirements	Priority	Due Date	Assignees	Reviewers	Last Updated	Created From
1	Example audit issue	Open			Low	11/04/2023	Customer Team	Coalfire Team	02/27/2024 08:04 am	Zachary Shales
2	Audit Issue 2	Open			Low	11/06/2023	Bret Peresch	Chase Kimberly	03/21/2024 11:32 am	Zachary Shales
3	Testing to test	Open			Low		Zachary Shales	Zach Shales	02/13/2024 09:27 am	Zachary Shales
4	Added to evidence	Open	CS Customized	CS107	Low	12/01/2023	Admin User	Admin User	03/14/2024 09:42 am	Pablo Casale
5	NCF-1	Open			Low	12/13/2024	Joe Marks	Chase Kimberly, Joe Marks	03/21/2024 11:00 am	Zachary Shales
6	Test test	Open			Low		Dixon Wright	Zachary Shales	03/25/2024 01:02 pm	Zachary Shales
7	Firewall Review - Semi Annually	Open			Low	06/06/2024	Bret Peresch	Zach Shales	01/12/2024 10:40 am	Zachary Shales
8	Gap 1	Open			Low	03/16/2024	Customer Team	Michael Twardowski, Customer Team	02/13/2024 09:27 am	Zachary Shales
9	New linked gap	Open			Low		Customer Team	Coalfire Team	02/13/2024 09:27 am	Zachary Shales

ID	Name	Status	Framework(s)	Requirements	Priority	Due Date	Assignees	Reviewers	Last Updated
1	Quarterly Access Review	Open			High	07/01/2024	Zach Shales, Zachary Shales	Zach Shales (zshales@manuscriptdemo...)	02/20/2024 03:05 pm
2	Quarterly Internal Vuln Scans	Open			High	03/03/2024	Zachary Shales	Dixon Wright	03/21/2024 11:32 am
3	Semi-annual Pen Test	Open			High	06/02/2024	Chase Kimberly	Zachary Shales	03/21/2024 11:32 am
4	Security Awareness	Complete	SOC 2	SEC001	High	12/06/2024	Dixon Wright	Luke Singer	03/25/2024 01:07 pm

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Why This Matters

To ensure compliance throughout the year, organizations should review current compliance status internally and ensure that they will be prepared for formal audits. Yet, self-directed assessments across multiple frameworks are too complex to complete and manage, especially if in-house expertise on how to comply with these frameworks does not exist.

Enterprise Strategy Group validated that Coalfire Compliance Essentials can enable organizations to be proactive in maintaining compliance by performing internal assessments with the support of Coalfire's advisory services. We observed how an organization can submit an assessment request prior to external audits to highlight evidence requests and action items to be completed. Not only does the assessment gauge current compliance status, but it also prompts end users to be proactive in completing compliance-related tasks.

Manage Compliance Risk

Managing compliance effectively translates directly into reducing business risk. By recording and tracking the possible risks of noncompliance, along with the potential business impact, organizations can mitigate risks more effectively.

Enterprise Strategy Group Testing

Enterprise Strategy Group navigated to the Risk Register to highlight issues raised by the organization itself that, if not resolved, can negatively affect the business (see Figure 10). Risks were classified according to likelihood of occurrence, revenue impact, and control effectiveness (i.e., how much impact can be achieved and the corresponding reduction in risk). We also noted how end users could specify the affected frameworks and relevant requirements. By tracking risks, we saw how organizations can continuously assess overall risk and prioritize those issues to resolve that present the greatest risk. Organizations could see the consequences of not being complaint and, therefore, know the value of mitigating any identified risks.

Figure 10. Assessing Ongoing Risk Due to Noncompliance

The screenshot displays the 'All Risks Register' interface. The main table lists several risks, including 'Application 6 - Breach scenario', 'Clean and Clear Desk', 'Disc Encryption on Laptops', 'End Point patching', and 'Example 99'. A modal window is open, showing three scales: Likelihood, Impact, and Control Effectiveness. Each scale has a table of values and descriptions.

Likelihood			
Value	Label	Score	Description
Highest	Very High	8	Likely to happen more frequently than monthly
High	High	5	Likely to happen monthly
Medium	Moderate	3	Likely to happen every 6 months
Low	Low	2	Likely to happen once a year
Lowest	Very Low	1	Likely to happen every few years

Impact			
Value	Label	Score	Description
Highest	Very High	8	> \$10M
High	High	5	< \$5M
Medium	Moderate	3	< \$1M
Low	Low	2	< \$100K
Lowest	Very Low	1	< \$50K

Control Effectiveness			
Value	Label	Score	Description
Highest	Effective	50%	This control can be expected to reduce the risk by 50%
High	Largely effective	30%	This control can be expected to reduce the risk by 30%
Medium	Partially effective	20%	This control can be expected to reduce the risk by 20%
Low	Largely ineffective	10%	This control can be expected to reduce the risk by 10%
Lowest	Ineffective	0%	This control is not expected to make a material difference in reducing risk

Source: Enterprise Strategy Group, a division of TechTarget, Inc.

Risks could also be associated with other areas of the platform, such as Assessments, Issue Modules, and Framework Requirements. This would enable organizations to tie risk to specific controls within the platform. As these controls are executed, risk can be continuously assessed.

Why This Matters

Noncompliance can negatively affect the business. Without knowing the business risk imposed by noncompliance, along with the actions to mitigate that risk, organizations cannot prioritize resolution of the issues that present the greatest risk to the business.

Enterprise Strategy Group validated that Coalfire Compliance Essentials can help organizations ensure that all applicable risks are recorded and tracked. To help in prioritizing issues to be resolved, the platform highlights the associated risk in terms of business impact. Organizations can then choose those issues to resolve that will minimize overall negative impact. By tying these risks to other modules in the platform, organizations can continually assess risk as action items are continually resolved.

Conclusion

Risking failure of a compliance audit is something to avoid, as noncompliance results in the inability to conduct business and enter select markets or industry verticals. In fact, 47% of respondents stated that they failed a formal audit two to five times in the past three years. This is no surprise, as organizations need to adhere to multiple regulatory frameworks simultaneously in today's business environment. Ensuring compliance across mandated frameworks can be time-consuming and easily mismanaged, as all associated requirements need to be met satisfactorily.

Coalfire Compliance Essentials has been designed to support organizations in meeting and adhering to multiple frameworks. The platform enables organizations to track and manage evidence requests, issues, and action items related to the frameworks to which organizations must comply simultaneously. By facilitating ongoing compliance on an annual basis, organizations can ensure that they are prepared for formal audits in a timely manner, reducing any "last-minute efforts." Combined with advisory and assessment services, Coalfire Compliance Essentials supports organizations in achieving compliance with more efficiency, while reducing business risk.

Throughout our evaluation, Enterprise Strategy Group validated that Coalfire Compliance Essentials supports organizations in:

- Decreasing time and effort in executing compliance workflows by scheduling and managing tasks and evidence requests across multiple frameworks simultaneously, while removing duplicate work.
- Maintaining and monitoring compliance in real time by enabling continuous visibility into tasks and evidence requests to be completed, as well as providing internal assessment of compliance on an ongoing basis, prior to formal audits.
- Managing compliance risk effectively by tying action items and evidence requests to actual business risk (e.g., lost revenue), should they not be completed, and helping to prioritize those items and requests accordingly.

Meeting regulatory requirements is necessary, but managing compliance workflows does not need to be complicated by using manually driven processes (i.e., spreadsheets) or off-the-shelf solutions requiring in-house expertise of various frameworks. Moreover, adhering to compliance standards is not a "checkbox" item; noncompliance translates directly into business risk. Enterprise Strategy Group validated that Coalfire Compliance Essentials can support your efforts in achieving compliance and suggests taking a closer look.



©TechTarget, Inc. or its subsidiaries. All rights reserved. TechTarget, and the TechTarget logo, are trademarks or registered trademarks of TechTarget, Inc. and are registered in jurisdictions worldwide. Other product and service names and logos, including for Bright TALK, Xtelligent, and the Enterprise Strategy Group might be trademarks of TechTarget or its subsidiaries. All other trademarks, logos and brand names are the property of their respective owners.

Information contained in this publication has been obtained by sources TechTarget considers to be reliable but is not warranted by TechTarget. This publication may contain opinions of TechTarget, which are subject to change. This publication may include forecasts, projections, and other predictive statements that represent TechTarget's assumptions and expectations in light of currently available information. These forecasts are based on industry trends and involve variables and uncertainties. Consequently, TechTarget makes no warranty as to the accuracy of specific forecasts, projections or predictive statements contained herein.

Any reproduction or redistribution of this publication, in whole or in part, whether in hard-copy format, electronically, or otherwise to persons not authorized to receive it, without the express consent of TechTarget, is in violation of U.S. copyright law and will be subject to an action for civil damages and, if applicable, criminal prosecution. Should you have any questions, please contact Client Relations at cr@esg-global.com.

About Enterprise Strategy Group

TechTarget's Enterprise Strategy Group provides focused and actionable market intelligence, demand-side research, analyst advisory services, GTM strategy guidance, solution validations, and custom content supporting enterprise technology buying and selling.

 contact@esg-global.com
 www.esg-global.com