COALFIRE

CASE STUDY

Blend minimizes business disruption and lowers total cost of compliance with Coalfire's coordinated assessment

AT A GLANCE

A leader in the financial services space, Blend was looking for a way to manage compliance by coordinating efforts that would reduce the total time associated with independent audits of its program – while maintaining high-quality audits.

"To improve efficiency, we challenged our security compliance team to coordinate their efforts and reduce time spent on recertification from six months to three months. The results have been game-changing for our business."

– GREG JANOWIAK,
SECURITY POLICY LEAD, BLEND

CHALLENGE

Traditionally, organizations manage their governance, risk, and compliance initiatives via decentralized methods, where each assessment is contracted separately across multiple vendors despite many of the same internal teams facilitating the audits. Many organizations, however, are finding that as their volume of compliance requirements expands and becomes intertwined, there is justification to pursue integrated approaches that permit the collection of evidence to be completed once and used for several purposes, assuming the audit periods for these external reviews can be aligned.

Blend strives to remain on the bleeding edge of what is considered the benchmark for current-state security compliance among its direct as-a-service competitors. As part of this focus, Blend realized the opportunity to consolidate its compliance across PCI DSS, ISO 27001, and SOC 2 tasking through a strategy that coordinated evidence collection, combined on-site walkthroughs, and minimized the number of requests to its engineers in an effort to alleviate the negative disruptions to ordinary business activities commonly associated with third-party audits.

When describing the before-state of Blend's audit operations, Greg Janowiak, the company's security policy lead, explained, "We were duplicating work during process walkthroughs and evidence collection phases. To make matters worse, reports tended to turn up informational observations that were light on deep process improvements."

Blend explored the consolidation of its audits to achieve better security compliance outcomes and decided it needed the expertise of a partner with experience performing audits for multiple frameworks. The company had strict requirements on this partner's accreditations to ensure that each reporting activity would be performed within the bounds of varying governing body rules.

"At Blend, we're never content to let the status quo dictate how we operate," said Janowiak. We realized that going through three separate audits was no longer scalable. To get the best possible information from each assessment without completing multiple engagements, we decided to partner with Coalfire and utilize their coordinated assessment service," said Janowiak. "We respected the fact that Coalfire has cloud and enterprise expertise and is accredited to perform more than 40 compliance frameworks, including PCI DSS, SOC, ISO, FedRAMP, HIPAA, and HITRUST, and is the largest vendor of this combination of compliance audits globally."

APPROACH

Coalfire assigned a program executive to oversee the complex integrated audit and a project manager to coordinate teams, align timelines, and ensure smooth coordination across Blend's control owners when interfacing with the auditors.

"We had the ability to manage the logistics on the Blend side but did not have the same visibility into the auditors' requests," said Janowiak. "Our Coalfire project manager ensured all parties were communicating proactively, requests for information were fulfilled on a timely basis, and that escalations to potential project issues were emphasized during regular health checks."

In addition to the program executive and project manager, Coalfire utilized their powerful project and collaboration platform, CoalfireOne℠, to coordinate the request for information across all three in-scope frameworks. "We uploaded evidence once to CoalfireOne, and the technology automatically mapped the submission to all requirements across the audit criteria being assessed, eliminating the need to manually tie out artifacts," said Janowiak. "CoalfireOne gave us real-time status dashboards, control assignments, requirements mapping, and fluid channels for communicating directly with the Coalfire auditors."

After evidence was received, Coalfire's audit teams came on-site to the Blend offices to complete a single, combined walkthrough. "Meetings with key stakeholders occurred concurrently," said Janowiak. "This approach allowed both teams to dive much deeper into key processes and provided the audit team with a comprehensive understanding of our program operations."

RESULTS

Through the utilization of Coalfire's coordinated assessment and the technology advantages provided by CoalfireOne, Blend reduced its audit cycle from an average of six months annually to only three months. "Not only did we benefit from time and cost savings using the coordinated assessment approach, but [we also] received insightful recommendations that provided valuable improvements over checkbox activities for our program," said Janowiak.

"Blend is a success story that demonstrates the value of using an effective information security management system (ISMS) to expand the audit criteria context beyond ISO 27001 as a response to the needs of internal interested parties and the requirements expected by its external customers," said David Forman, managing principal of ISO assurance at Coalfire.

COALFIRE

About Coalfire

Coalfire is the trusted 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 nearly 20 years and has offices throughout the United States and Europe. For more information, visit **Coalfire.com.**

CS_Blend_040320