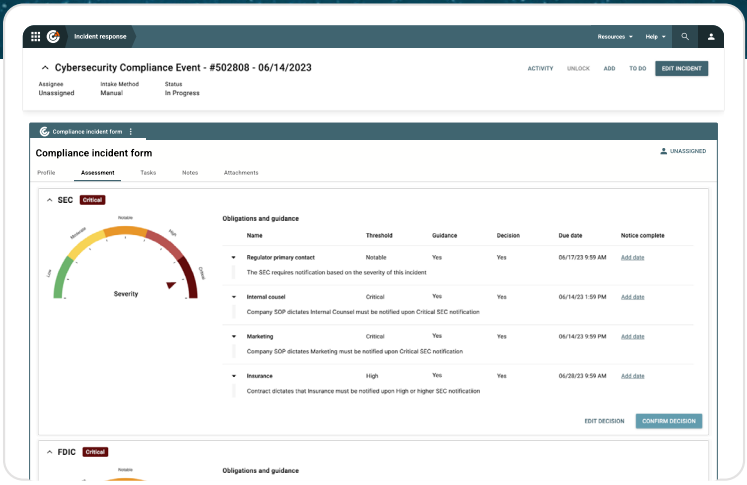
DATASHEET

Radar® Compliance

Radar® Compliance

Operationalize Cyber Event Notification Obligations



Cyber event notification obligations are becoming more strict and punitive—and at the same time less well-defined. Additionally, regulators are insisting on clearly documented evidence that a consistent and transparent risk assessment was performed as part of the notification obligation decisioning process.

Organizations need a flexible, scalable, and configurable notification management solution to ensure compliance—and risk mitigation—in today's complicated cyber regulatory landscape.

Radar® Compliance is a configurable rules and assessment engine purpose built for cybersecurity, InfoSec, legal, and compliance teams. Built on the Radar® platform—which has also enabled the market leading privacy incident management solution, Radar® Privacy, for over 10 years—the solution offers organizations the ability to define their own cybersecurity notification triggers and obligations to all internal and external stakeholders, from federal regulators to the board of directors.

Key Solution Features

Inconsistent processes prone to human error are a thing of the past. Increase controls and mitigate organizational risk with Radar® Compliance.

Key benefits of Radar® Compliance include:

- **Intelligent notification decision support** eliminates subjectivity inherent in manual approaches to assessing an incident against a risk matrix. Ad hoc notification decisions will be a thing of the past.
- **Cross-functional communication** solution that allows cybersecurity to collaborate across IT, privacy, compliance, and legal teams to mobilize a cross functional response team to swiftly contain and stabilize the breach.
- **Proof of compliance,** i.e. audit trails, provide a transparent process to internal and external stakeholders; the solution offers the inherent traceability and defensibility that every organization subject to a regulator needs.
- **Increased controls** that simplify record keeping and create streamlined, documentable processes.
- **Elimination of over and under incident reporting**, potentially reducing fines leveraged by regulatory bodies.
- **Reduction of fines** and decreased instances of enforcement actions leveraged due to poor controls.
- **Customizable to fit a company's unique culture of compliance and risk** via the ability to create rules based on a business case unique to the organization, and specific to their definition of material harm.

© Copyright RADAR, LLC. All Rights Reserved. 0624

Use Case: Cyber Event Documentation and Notification

An energy utilities company is challenged by the fact that recent regulations and laws concerning cybersecurity are not only stricter and riskier than privacy laws, but are also less well-defined. While they have determined a risk matrix, with the significant help of outside counsel, they are still relying on manual processes, such as spreadsheets and email, for their incident management.

The CISO is becoming increasingly concerned about the risk inherent in manual processes prone to human error and subjectivity, particularly as the SEC has made it clear that transparent, consistent, and documented processes are as critical, if not more so, than the notification obligation decision itself.

Radar® Compliance addresses the need for a demonstrable controls process around cyber event notification triggers via a configurable workflow solution that allows the company to verify, against their own determined criteria and risk matrix—and in a consistent and standardized manner—whether or not there is a need to notify internal and/or external stakeholders of an event.

This documentation and evaluation process reduces risk of a missed obligation, regulatory sanctions, and/or being out of compliance with board of director mandates by mobilizing the InfoSec, cybersecurity, IT, legal, and compliance teams to establish a controls process that enables consistency by using the same set of notification triggers for each cyber-related event.

And, when multiple regulators are involved, **Radar® Compliance can be used to prioritize notification timelines and content.** And, when an incident involves personal information (PI), Radar® Privacy can be available within the context of the event as well to further streamline the incident workflow process.

While many organizations may already have a clearly defined risk matrix, they often lack the ability to consistently and transparently operationalize cyber-based event assessments against their own predetermined notification triggers.

The configurable workflow offered by Radar® Compliance operationalizes security, risk, and cyber requirements with their associated internal and external notification obligations, shortening the time spent getting to a notification decision, freeing up resources for incident investigation, and providing a transparent process to all stakeholders.

The result is a streamlined, company-wide cybersecurity compliance process that enables cross functional collaboration and risk mitigation between IT, InfoSec, cybersecurity, privacy, legal, HR, and compliance teams.

Organizations can be confident that they not only fulfill event notification obligations to each and every stakeholder but, critically, also meet the regulatory need for defensible and consistent documentation.

Ready to learn more? Schedule a demo of Radar® Compliance.

INFO@RADARFIRST.COM | 1.844.737.3778

Schedule a Demo >

RadarFirst

Learn more at radarfirst.com

RadarFirst supports governance, risk, and compliance (GRC) with incident management solutions that automate intelligent decisions and streamline compliance with cybersecurity, privacy, and compliance laws. Our patented assessment automation helps organizations act quickly to comply with obligation requirements and notification deadlines. With RadarFirst, organizations can remain in compliance with new and evolving regulations, scale decision-making, and provide consistent documentation.

© Copyright RADAR, LLC. All Rights Reserved. 0624