DATASHEET

Radar® Compliance

Radar® Compliance: A Configurable Assessment Engine

Operationalize Compliance, Risk, and Cyber Notification Obligations

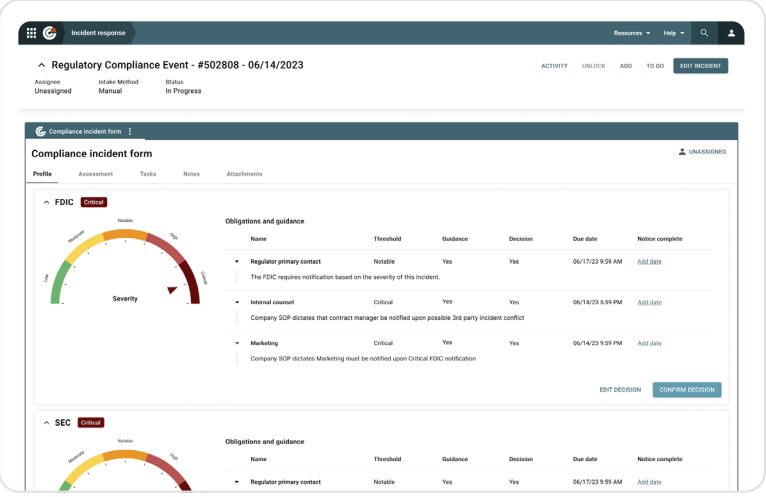
Incident notification obligations are becoming more strict and punitive—and at the same time less well-defined. Additionally, regulators are insisting on clearly documented evidence that a "materiality" risk assessment was performed as part of the notification obligation decisioning process.

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

The Solution

Radar® Compliance is a configurable rules and assessment engine. Built on the Radar platform—in existence for the past 10 years and enabling the market leading privacy incident management solution, Radar® Privacy—the solution offers organizations the ability to define their own notification triggers and obligations to stakeholders, from federal regulators to the board of directors.

Highly configurable, Radar® Compliance is able to address a wide variety of incidents, including but not limited to cyber events, health and welfare, operational interruptions, and internal compliance. When an incident involves personal information (PI), Radar® Privacy can be available within the context of the incident as well to further streamline the incident workflow process.



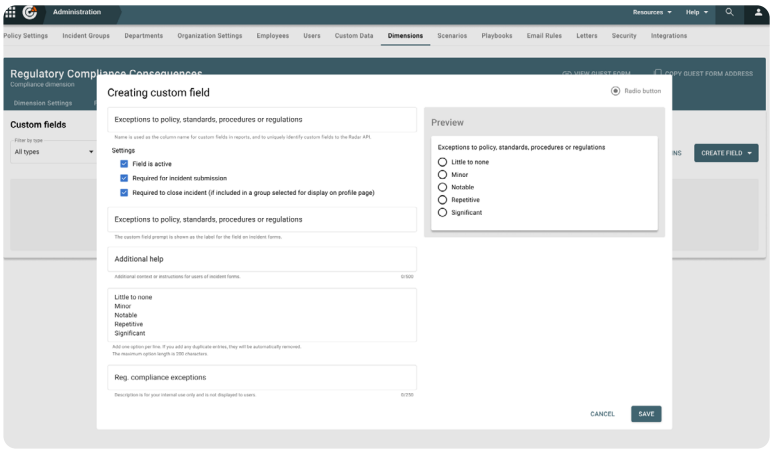
While many organizations may already have a clearly defined risk matrix, they often lack the ability to consistently and transparently operationalize incident assessment against their own predetermined notification triggers. The configurable workflow offered by Radar® Compliance operationalizes Compliance, 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 company-wide streamlined 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 incident notification obligations to each and every stakeholder but, critically, also meet the regulatory need for defensible and consistent documentation.

Key Solution Features

Drive cross-departmental efficiency by replacing current processes that rely on a combination of office tools, such as email, spreadsheets, and shared document systems, while ensuring risk mitigation and compliance at all organizational levels. Key benefits of Radar® Compliance include:

- **Consistent and defensible incident risk assessment** 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.
- **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.
- **Elimination of over and under incident reporting**, potentially reducing fines leveraged by regulatory bodies.
- **Increased controls** that simplify record keeping and create streamlined, documentable processes.
- **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.



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**.

The CISO **needs a solution that will allow the InfoSec team, in collaboration with IT and Compliance, to internally establish clear, transparent, and consistent processes regarding cyber incident notification decisioning**, both to internal and external stakeholders, such as the Board of Directors and regulators. It is critical that the Infosec team be able to **demonstrate to regulators that they have a controls process** in place for documenting Cyber events, as well as transparency around the criteria used to determine whether or not to notify regulators of the event.

Radar® Compliance addresses the need for a 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 and Compliance teams to establish a controls process that enables incident response consistency 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 time lines and content.**

Use Case: *Internal Stakeholder Incident Communication*

A financial institution is struggling to document, track, and determine notification requirements for fraud events. Specifically, they are looking for **a solution that would allow them to not only track the fraud event itself, but also the monetary impact of the event, and whether or not a Suspicious Activity Report (SAR) is required**, according to the Bank Secrecy Act (BSA). Additionally, **when a SAR is required, they want to ensure that their Legal team, their insurance company, as well as other internal stakeholders, such as the board of directors, are notified** of the fraud event.

Radar® Compliance offers a configurable rules and assessment engine and workflow solution that not only allows for the **consistent documentation and tracking of fraud events**, but additionally solves for the challenge of **evaluating whether or not a SAR is required**, and therefore an internal notification to their Legal team as well.

With Radar® Compliance, the **Compliance team has increased productivity and reduced risk to the organization** thanks to the solution's streamlined incident and event intake form, configurable notification triggers, and risk-mitigating controls process. **Fraud events are now easily documentable, trackable, and reportable** to both internal stakeholders, like the Legal team and board of directors, as well as to regulators, such as the Financial Crimes Enforcement Network (FinCEN).

Ready to learn more?

Watch the Radar® Compliance video.

INFO@RADARFIRST.COM | 1.844.737.3778

Watch Now >

RadarFirst

Learn more at radarfirst.com

RadarFirst's award-winning incident management solutions are trusted by organizations to reduce risk and simplify obligation decisioning as mandated by privacy, cyber, and compliance laws. With patented Radar® technology, organizations can define, streamline, and scale decision-making against time bound regulatory requirements supported by consistent, objective processes with defensible, documented outcomes.