SecurityScorecard

# COMPLIANCE OFFICER ACTION PLAN

## Creating an Innovative Security Program

# Introduction

**How can highly regulated companies stay innovative in their security and risk programs if they need to invest significant energy toward the deluge of audits, regulator exams and control assessments?**

Cybersecurity attack techniques and threat actors move faster than regulations and industry standards can be updated. Therefore, organizations need an innovative, proactive approach to security, risk, and compliance that moves at the pace of the adversary. Simultaneously, companies need to meet new business challenges, expand their digital footprints in response to customer expectations, and “check the boxes” required by strict compliance mandates. A look at these highly regulated industries explains the reason for the rigid compliance mandates. Whether critical infrastructure, government, financial services, or healthcare; they all collect, transmit, store, and process extremely sensitive data, making them prime targets for malicious actors.

# Creative Security and Compliance Programs Focus on Risk

**Compliance "boxes" exist to make sure risk managers consider everything that could go wrong. The compliance box is a safe place for many financial organizations and others in highly-regulated industries. Organizations worry about regulators and audit teams finding noncompliance issues against the required framework or control set. While audit teams can be more focused on processes that enable compliance, regulators look for organizations to proactively address emerging risks and concerns.**

Thinking "outside the compliance box" takes extra effort. Organizations need to invest in creative people with frontline cybersecurity teams and control methods experience. They need people who understand how to take a risk-based approach that prioritizes allocating scarce resources to the highest-impact risk areas. To uncover key risks, these teams must find the 'needle in the haystack' amongst the constant stream of risk intelligence, while consuming hundreds of findings across their selfassessments, audits, security incidents, and regulator issuances—while also looking at future threat trends.

Finally, connecting with industry peers to share best practices and threat events is critical to uncovering new risks. Regardless of industry, companies that want to prevent incidents in their environments benefit from sharing intelligence with risk peers. Threat actors constantly leverage new techniques to skirt corporate security walls. A unique attack against one industry member is likely to hit others.

For example, a CISO at Interpublic Group spear-headed the first media- and advertising-industry CISO intel sharing forum, which approached and resolved common vendor and industry problems. The group generated better overall results than any single firm alone could have managed. Across industries, most competitors do not allow their teams to talk to each other, but are comfortable with their risk teams sharing cybersecurity risk information when looking to fight against the same fraudsters and attackers.

Fundamentally, organizations in highly-regulated industries want to drive smart spending on targeted investments in high-risk areas that effectively manage cyber and technology risk aligned to critical business assets. The objective of the compliance boxes is preventing significant negative events from impacting the company. Taking a risk-driven approach that sees the big picture, and allocates limited resources to the most prescient risks, can both minimize risk to the company and win the confidence of regulators and customers.

# Security Innovation in Highly-regulated Industries

**An 'innovative' security solution closely aligns with the changing business and technology trends that companies are embracing in this accelerated digital era. Innovation requires making decisions based on capabilities—not just packaging new trends.**

## LEVERAGE ARTIFICIAL INTELLIGENCE (AI) AND MACHINE LEARNING (ML)

While AI and ML promise to process data and apply analytics at a much more rapid pace than human teams can, organizations must be able to measure their effectiveness. As an example, improved automation and data analytics applied to security and infrastructure protection will likely find more attacks, reduce false alerts, and perform faster detect-and-respond functions. But to do it right, organizations need data science experts to vet these solutions.

**Key considerations include:**

- How to view/control your data that the solution uses
- Whether the solutions send your data outside the organization
- How the vendor protects this data
- Relevant security and performance metrics to prove AI's value to the program
- Peer reviews of the solution
- Staff and time required to maintain the solution
- Solution's ability to integrate into enterprise workflow
- Solution's integrations with GRC and other tools and applications
- Where the solution gets the data signals it uses

Security and risk leaders should take the lead in establishing what the organization requires and how AI can assist in that. Companies should also set reasonable expectations for what AI can realistically provide, and select projects based on areas where AI can have the greatest impact.

## PARTNER WITH SECURITY COMPANY START-UPS

Partnering with start-ups and early-stage security companies can provide insight into the most innovative solutions and talent in the industry, enabling a creative approach to solve the biggest or newest risk challenges. Quite a few of the largest retail and investment banks in the country have dedicated resources assigned to evaluating, piloting, and potentially investing in innovative security solutions. Providing feedback on an early-growth company's roadmap can help address a current gap within the organization and build the ecosystem. Many security leaders complain that getting an established vendor to innovate is like getting an oil tanker to turn. Early-stage and start-up cybersecurity firms provide program and technology agility.

## PERSONALIZATION

With start-ups, CISOs can influence the product's roadmap by advocating for features that suit their organization's unique security needs. Start-ups lack the bureaucracy of established vendors, giving CISOs the opportunity to have their voices heard by forging relationships with senior management. This relationship helps smooth out the inevitable bumps in the road. Established vendors often lack this personalized experience because they manage a multitude of customer requirements on their roadmaps.

## INFLUENCE

Less obviously, the features co-created with the early-stage cybersecurity firms can influence the entire industry, possibly changing the industry approach in the start-up's area. Partnering can enable CISOs to deliver business value faster and remain ahead of the curve. For example, one CISO indicated that they could deliver their services more quickly and, in some cases, had also removed a lot of cost from how their team delivers security to their organization. Reviewing innovative security solutions can keep an organization's security program ahead of the curve by giving an early look at the industry's responses to newly identified problems.

## AGILITY

Organizations can move faster and have greater flexibility with early stage cybersecurity firms. Without the red tape, early-stage firms can move more quickly to pivot their technology. From inception to prototype, they are unencumbered by legacy technical debt, allowing them to act more rapidly. Thus, the CISO can shape the solution's roadmap to meet their needs and have it done more rapidly.

## CREATING AN EFFECTIVE PARTNERSHIP

CISOs need to create a plan if they want to work with start-ups and early-stage cybersecurity firms. The plan should include:

- Providing strategic focus areas
- Prioritizing the security team's review of emerging technology
- Formally assigning this responsibility to a team member
- Establishing an innovation fund that bypasses organizational inertia to drive proofs of concept and solution testing in the environment

# Establishing an Integrated, Innovative Security and Compliance Program

**Every organization should be looking to establish a security compliance program as innovative as the organization's business goals. In a digitally transformed world, being forward thinking in business requires a similar future-forward focus on mitigating security and compliance risk. To do this, senior leadership, risk management, and security leaders must work as a team.**

## GAINING CONTINUOUS VISIBILITY

Continuous risk intelligence monitoring is key. Risk teams in the first or second line of defense need to identify the right risk indicators (KRI's) by tracking what is most critical. This can be done by having a continually refreshed set of KRI's and Key Performance Indicators (KPIs) with thresholds to call out when high risk patterns appear. Leveraging data analytics and other automated tools helps support the business by identifying pertinent risk triggers. With predictive analytics, organizations can align their security and compliance postures more effectively and take a future-focused risk management approach that ultimately reduces audit and regulatory findings, as well as security incidents.

## LEVERAGING COLLABORATION TOOLS

Feeding issues into a central risk management platform is critical to giving teams the integrated and accurate view of risk intelligence they need to make the right decisions. With a centralized risk management platform enabling more cohesive collaboration, organizations can realize the unified vision. They need a single, authoritative source of risk documentation–past, present, and predicted-future–to see patterns as they emerge. Past findings need to be applied to current-state processes and operations. All of this needs to be aligned with predictive risk triggers so that organizations can continuously iterate based on data.

## FOCUSING ON GOVERNANCE

Many organizations use customized frameworks to manage their security controls. Staff typically only review these controls frameworks quarterly or annually, viewing them as a checkmark for the compliance box. Ideally, they should switch to a governance process that lets them perform continuous monitoring of controls. Creativity and innovation require evaluation and response to emerging risk patterns. A governance-focused security and compliance program shifts from following possibly outdated compliance requirements, to proactively managing emerging risks shown to have a high impact on the success of the security program.


## About SecurityScorecard

Funded by world-class investors including Evolution Equity Partners, Silver Lake Waterman, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings with more than 12 million companies continuously rated.

**Founded in 2013** by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 30,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight. SecurityScorecard is the first cybersecurity ratings company to offer digital forensics and incident response services, providing a 360-degree approach to security prevention and response for its worldwide customer and partner base.

SecurityScorecard continues to make the world a safer place by transforming the way companies understand, improve and communicate cybersecurity risk to their boards, employees and vendors. Every organization has the universal right to their trusted and transparent **Instant SecurityScorecard** rating. For more information, visit **securityscorecard.com** or connect with us on **LinkedIn**.

SecurityScorecard

**SecurityScorecard.com**
info@securityscorecard.com
United States: (800) 682-1701
International: +1(646) 809-2166