SECURITY COMPASS WHITEPAPER 2017

Make NY DFS Cybersecurity Regulation Compliance Easy with Security Compass

Security Compass

New Standards for Application Security

Cybersecurity Regulation 23 NYCRR Part 500 introduces unprecedented levels of cybersecurity requirements to financial institutions in New York State. Dark Reading called this, “One of the harshest cybersecurity regulations to hit companies in the US.” These are some of the major rules affecting Application Security:

Section 500.05: Risk Assessment and Continuous Monitoring

> The cybersecurity program for each Covered Entity shall include monitoring and testing, developed in accordance with the Covered Entity’s Risk Assessment, designed to assess the effectiveness of the Covered Entity’s cybersecurity program. The monitoring and testing shall include continuous monitoring or periodic Penetration Testing and vulnerability assessments. Absent effective continuous monitoring, or other systems to detect, on an ongoing basis, changes in Information Systems that may create or indicate vulnerabilities, Covered Entities shall conduct:
>
> (a) Annual Penetration Testing of the Covered Entity’s Information Systems determined each given year based on relevant identified risks in accordance with the Risk Assessment; and
>
> (b) Bi-annual vulnerability assessments, including any systematic scans or reviews of Information Systems reasonably designed to identify publicly known cybersecurity vulnerabilities in the Covered Entity’s Information Systems based on the Risk Assessment.

Section 500.08: Secure Application Development and Auditing

(a) Each Covered Entity's cybersecurity program shall include written procedures, guidelines and standards designed to ensure the use of secure development practices for in-house developed applications utilized by the Covered Entity, and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the Covered Entity within the context of the Covered Entity's technology environment.

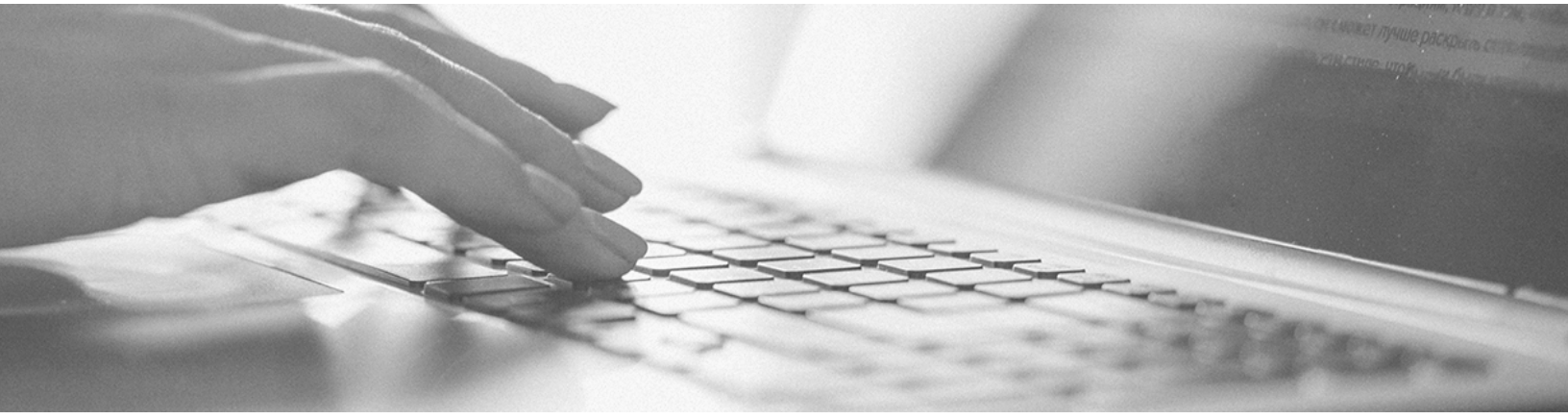
(b) All such procedures, guidelines and standards shall be periodically reviewed, assessed and updated as necessary by the CISO (or a qualified designee) of the Covered Entity.

Section 500.14: Cybersecurity Awareness Training

As part of its cybersecurity program, each Covered Entity shall: Provide for regular cybersecurity awareness training for all personnel that is updated to reflect risks identified by the Covered Entity in its Risk Assessment.

Financial institutions will be challenged to enforce these new policies and provide auditable evidence that they are following a secure development process.

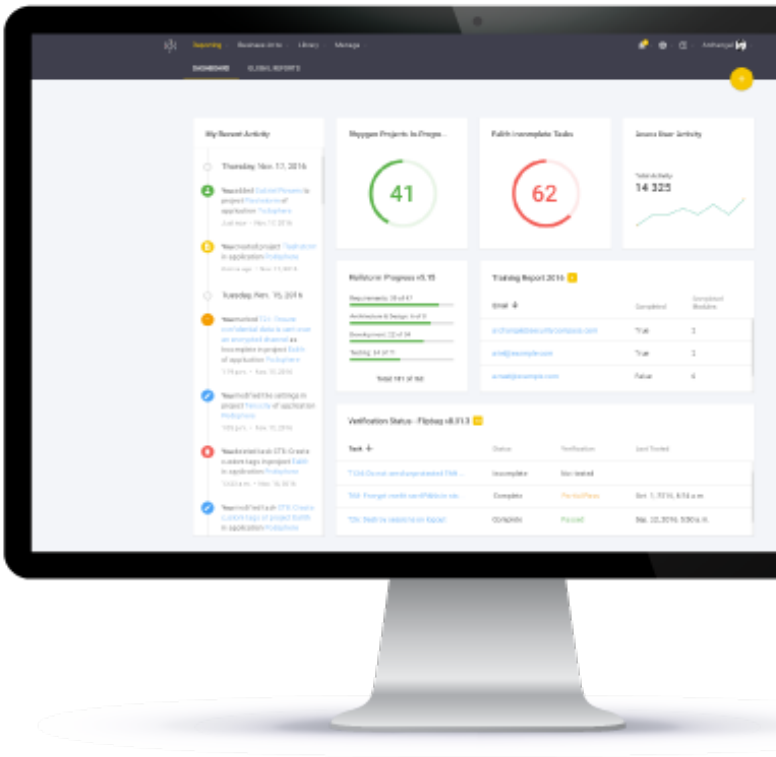
How can they achieve this?



SD ELEMENTS

A Scalable and Auditable Solution

With SD Elements, the leading Policy-to-Execution platform, organizations can manage a robust, scalable, secure SDLC program with auditable reports. SD Elements provides several capabilities to build security into the SDLC with auditable evidence and can provide output to third party developers to ensure they too are building secure applications.



Track flaws, reviews, and compliance through one platform

Best-practice organizations create a single, central repository for information about software weaknesses, as well as proposed, accepted and rejected mitigations. SD Elements both streamlines compliance and maximizes the effectiveness of security assessments by consolidating the results of multiple testing methods in one place.

Automate and audit compliance workflows

SD Elements automates workflows, reduces communication overhead, and delivers a secure audit trail for compliance processes, creating a robust policy management framework to document and communicate security policy. It can also integrate with other key systems to share critical information, like application security scores, listings of all discovered flaws, and flaw status information.

Move past the limits of security testing tools

Many organizations rely on security testing tools like Static Analysis Security Testing (SAST), Dynamic Analysis Security Testing (DAST), and Interactive Application Security Testing (IAST). However, these tools are insufficient to show that a company has followed a holistic secure development program and, on their own, will be unlikely to satisfy sophisticated auditors. SD Elements helps developers build in security requirements while they code and leaves a record that CISOs can depend upon when audited.

Keep nonpublic data safe, whether in internal or third-party applications

The new NY DFS regulations require an organization to protect nonpublic information generated both internally and by a contractor or vendor. SD Elements helps ensure that the cryptography used by an application remains intact and is implemented correctly, and helps organizations work towards a program that holds third-party software to the same security standards as internally developed software.

Achieve continuous compliance monitoring

Compliance isn't an end goal, but rather part of an organization's overall security framework to better protect its systems and data, and this means continuous and ongoing compliance. SD Elements enables continuous compliance monitoring with security testing that integrates with the secure SDLC, regular discovery scans of web applications (internal and acquired), virtual patching for web application firewalls based on the security intelligence from application assessments, and auditing and protection during actual cybersecurity events that take aim at common vulnerabilities.

SecurityCompass

A Software Security Solution

In addition to its SD Elements platform, Security Compass offers training and advisory services that will help financial institutions meet compliance with sections 500.05 and 500.14 of the law.

Application Security Training

Security Compass's training courses and services can help organizations provide regular cyber security awareness training for all required personnel. Our training is designed to meet the agile needs of today's modern organizations through adaptive courseware that is tailored to what a student needs to know. We provides an industry first in (ISC)² accredited courses with Software Security Practitioner (SSP) Suites, as well as instructor-led training that combines classic classroom training with SSP Suites, building security conscious staff across an enterprise. Our training platform also integrates into SD Elements to provide just-in-time training for developers.

Penetration Testing Services

Security compass offers a variety of industry leading penetration testing services, including testing for web, desktop, and mobile applications, network and wireless testing, social engineering testing, and more. With nearly a 15 years in the application security industry, our advisors are prepared to offer expert solutions to complex security challenges.

Contact us to speak with one of our representatives about how Security Compass can make compliance easier for your organization.

About Security Compass

Security Compass is a leader in helping customers proactively manage cybersecurity risk, without slowing down business. Offering SD Elements, Just-in-Time Training, and Enterprise Delivery Services, as well as Verification Services, we help your organization efficiently deliver technology that's secure by design. At the core of our solution is our policy-to-execution software platform, SD Elements, which translates policies into actionable tasks for technical teams. Security Compass services some of the world's largest enterprises, as well as 4 of the largest tech companies in the world. We're headquartered in Toronto with global offices in the United States and India. Follow Security Compass on Twitter @securitycompass or visit https://www.securitycompass.com/