CEP Magazine - December 2022

Sandeep Bhide (sandeep.bhide@processunity.com) is Vice President of Product Management at ProcessUnity in Concord, Massachusetts, USA.

How you can remain compliant in a fast-paced regulatory environment

By Sandeep Bhide

A well-conceived and well-executed third-party risk management (TPRM)-related regulatory compliance program establishes a common language for you and your third parties to discuss security improvements. Regulations regarding third parties and cybersecurity continue to evolve, regardless of your work sector.

New regulations continue to increase the stakes for an organization's management of risks posed by third parties. For example, the United Kingdom Prudential Regulatory Authority has set new guidelines on outsourcing and TPRM that standardize how financial institutions should manage their vendor risk.[1] These rules redefine materiality and have set new standards to improve how organizations protect themselves against risky vendors.

The European Union's Digital Operational Resilience Act (DORA) may also impact United States regulations.[2] It establishes security requirements for financial companies' network and information systems and third-party technology vendors. Regardless of where you do business, it has now become imperative to monitor your vendors for information and communications technology-related disruptions and threats.

As for new cybersecurity regulations, the White House's January 2022 *Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems* focuses on transitioning to a zero-trust architecture.[3] Although currently only mandatory for government systems, it's only a matter of time before private businesses are held accountable for it. The executive order raises the bar for organizations everywhere to reevaluate and improve upon their current security.

Organizations must also pay attention to existing privacy laws and regulations, such as the Health Insurance Portability and Accountability Act (HIPAA), General Data Protection Regulation (GDPR), and California Consumer Privacy Act (CCPA), along with upcoming environmental, social, and governance reporting mandates.[4] With companies beholden to so many regulations, it's no wonder leadership is turning to TPRM teams for clarity on compliance throughout the extended enterprise.

TPRM teams rely on a third-party risk platform for automated assessment and auditing processes to manage their compliance. Automation and standardization help them meet constant compliance needs while adjusting to a fast-paced regulatory environment. Without this assistance, it's easy for organizations to suffer one or more pitfalls of a noncompliant vendor: financial penalties, regulatory sanctions, and reputational damage.

Challenges to maintaining compliance

Regulatory compliance would be easy if regulations were static. In reality, regulations often change rapidly in response to global events, and the ways that organizations need to protect their data does as well. According to Gartner, approximately five billion people will have access to privacy rights by the end of 2023.[5] And by 2025, 80% of enterprises will have web, cloud, and private applications unified under a single vendor's platform.

To prepare for this future of hyper-interconnectivity, organizations need to baseline their third-party compliance now—especially when it comes to cybersecurity.

That's often easier said than done. Companies face three main challenges when complying with internal and external regulations.

1. Lack of transparency with third parties

Since 2019, software publishers have ranked as the highest risk for third-party breaches because hackers exploit software vulnerabilities and rewrite and repurpose the code.[6] First-party companies and organizations often skip securing their software and services, wrongly assuming both are trustworthy. Organizations often find out too late when a third party is out of compliance due to a lack of transparency in the relationship. This anecdote outlines why you should take a "never trust, always verify" approach to your third parties.

You can't assume your third parties are as concerned with regulatory compliance as you are. In fact, as regulations change, you need assurances that third parties will make the necessary changes to comply.

This is one reason third parties need to be continuously monitored throughout the relationship, with ongoing assessments to validate their compliance. Your organization needs to be aware of changes to regulations to know when to trigger a reassessment of your vendors. Regulations like GDPR and HIPAA pose steep penalties for organizations that work with noncompliant third parties.[7]

2. Redundant control management

Cybersecurity regulations are constantly changing, which means organizations must frequently update their cybersecurity control libraries to meet the latest standards. Many organizations don't do this efficiently—they have multiple redundant controls across several regulations and standards that could be consolidated. As a result, their process for updating controls with regulatory changes is inefficient, making it more difficult to keep up with changes.

Outdated controls could potentially fail a cybersecurity audit or slow down the certification path. A consolidated control library with an accurate mapping to authoritative sources and evidence-collection questionnaires enables an organization to evaluate compliance across every applicable regulation and standard while streamlining the process of evaluating third parties against relevant controls.

3. Lack of cybersecurity and TPRM integration

In many organizations, procurement and cybersecurity stakeholders work in silos, despite the overlap in their security and compliance objectives. There is a huge opportunity for both stakeholders to work in harmony to link the internal cybersecurity performance management program with the external TPRM program. This fusion helps reduce redundancy, achieve efficiency, and improve cycle times while maintaining regulatory compliance.

Aligning the TPRM and cybersecurity performance management programs can help create holistic insights about compliance levels and the organization's risks, helping the business achieve better outcomes with greater process efficiency.

How to achieve compliance in three steps

Companies need to be proactive in keeping up with internal and external compliance. The three steps below can help you approach compliance holistically to keep up with shifting regulations.

Step 1: Continuously monitor your vendors

Compliance requirements are different for every organization. Aside from keeping tabs on the legislation that directly applies to your organization, you should stay on top of the regulatory landscape to be aware of changes to regulations that involve your third parties.

Develop transparency with your third parties to understand their compliance efforts. Before they are onboarded, third parties must demonstrate compliance with regulations that apply to your organization. Before entering the relationship, you should understand any prior noncompliance incidents the third party has encountered.

When new regulations are released, you should distribute targeted questionnaires to the relevant third parties to ensure that they meet the required changes. Periodic, ongoing risk-based assessments, centrally managed on a unified platform, will enable you to keep tabs on their compliance throughout the relationship.

Step 2: Align TPRM and cybersecurity

Bridging the gap between TPRM and cybersecurity performance drives efficiency in your compliance efforts by reducing the overlap between the two disparate efforts. TPRM should work with cybersecurity to ensure that all new and existing vendors align with the organization’s security baseline and compliance goals.

TPRM should communicate with cybersecurity to understand the organization’s cybersecurity objectives and verify that all third parties support them, too. Working with TPRM, cybersecurity can validate the effectiveness of third-party controls and compliance. And TPRM can help communicate to third parties any upcoming and necessary changes to external controls for a proactive approach to cybersecurity compliance.

Step 3: Consolidate your cybersecurity control library

Your cybersecurity control library helps you maintain compliance. Most organizations’ control libraries are informed by various applicable regulations and standards. Unless managed carefully, inefficiencies invariably creep in, resulting in duplicative controls assessments.

Quickly growing companies rarely have the people power required to meet the entire scope of their business needs. With an automated tool, however, consolidating your control library enables you to reduce the time and cost of regulatory compliance by mapping and maintaining linkages between threats, risks, issues, and incidents.

Takeaways

- Regulations continue to evolve, and companies are finding it challenging to keep up with third-party vendor compliance.
- Europe and the United States have pending cybersecurity regulations that could impact companies of all sizes.
- The risk of noncompliance is significant—cyberattacks, breaches, government penalties, class-action lawsuits, reputational damage, and more.

- Integrating cybersecurity and third-party risk management (TPRM) compliance activities under a streamlined platform can help eliminate redundant workflows.
- A good TPRM platform can help you be continuously compliant as regulations evolve.

[1] ProcessUnity, "Are You Ready for the PRA's New Guidelines on Outsourcing and Third-Party Risk Management?" *Process Unity* (blog), accessed August 18, 2022, https://www.processunity.com/prepare-for-pra-outsourcing-tprm/.
[2] European Council, "Digital Finance: Provisional Agreement Reached on DORA," *European Council*, news release, May 11, 2022, https://www.consilium.europa.eu/en/press/press-releases/2022/05/11/digital-finance-provisional-agreement-reached-on-dora/.
[3] President Joseph R. Biden Jr., "Memorandum on Improving the Cybersecurity of National Security, Department of Defense, and Intelligence Community Systems," Presidential Actions, The White House, January 19, 2022, https://www.whitehouse.gov/briefing-room/presidential-actions/2022/01/19/memorandum-on-improving-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/.
[4] ProcessUnity, "ESG Reporting Mandates to Know for Third-Party Risk Management," *Process Unity* (blog), accessed August 18, 2022, https://www.processunity.com/esg-reporting-mandates-third-party-risk-management/.
[5] Gartner, "Gartner Unveils the Top Eight Cybersecurity Predictions for 2022-23," news release, June 21, 2022, https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio.
[6] Black Kite, 2022 *Third-Party Breach Report*, January 20, 2022. https://blackkite.com/whitepaper/2022-third-party-breach-report/.
[7] Elliot Dinkin, "Recent Fines Illustrate the Importance of Third-Party Vendor HIPAA Compliance," *Corporate Compliance Insights*, September 4, 2019, https://www.corporatecomplianceinsights.com/third-party-hipaa-compliance/.