COSMOS
Navigate the Compliance Universe

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.