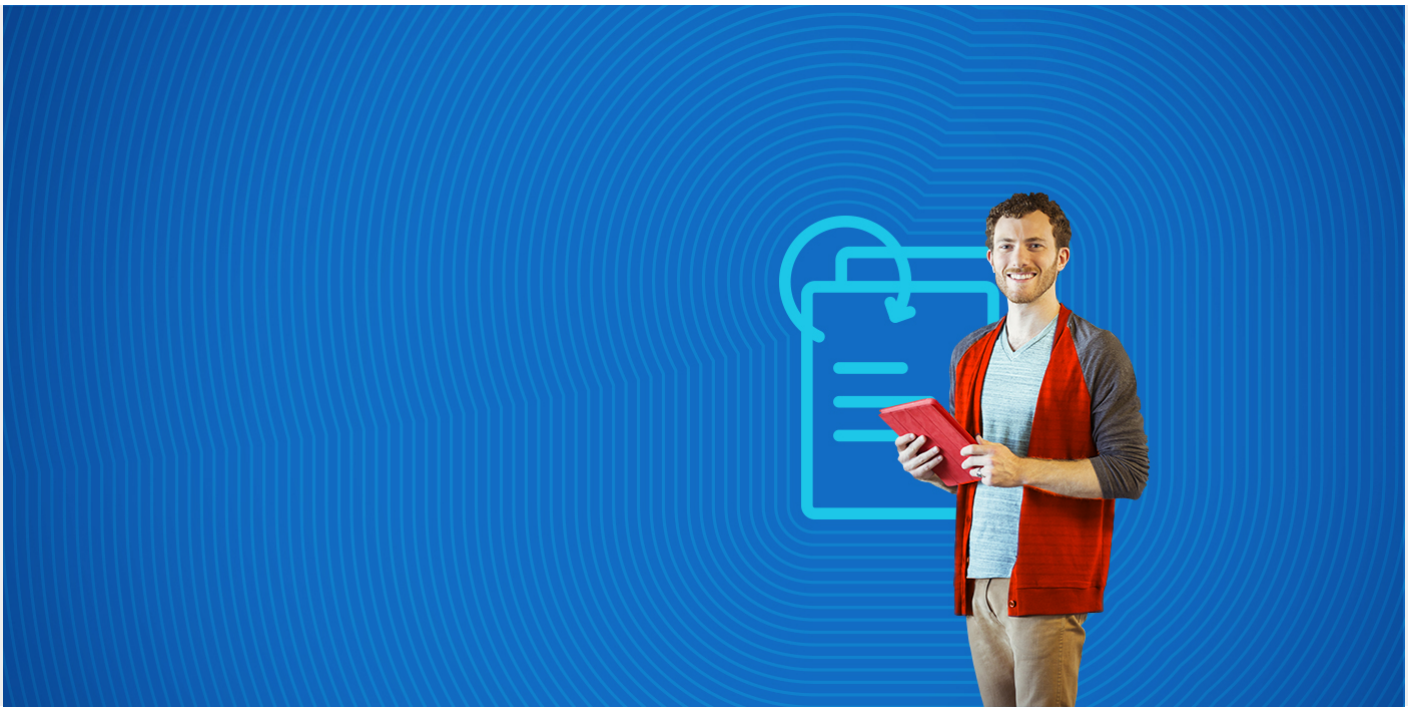
IT SECURITY & COMPLIANCE INTRODUCTION



New to IT Security & Compliance? Start here!

The “digitization of everything” trend is forever changing our lives. The growth of mobile devices along with their increasing capabilities result in people having instant access to information on-the-go. They can conduct business wherever they are at any time, often blurring the line between work and leisure. Because of the always-on, always accessible nature of the digital economy, your customers expect a consistently excellent user experience regardless of whether they are at home or at work.

But keeping organizations secure in this increasingly digital world has never been tougher. The fast-paced demands of users put even more pressure on enterprises to prevent and stop threats and data breaches, meet regulatory compliance requirements, and govern their operations more efficiently.

What’s the best way for your organization to address this challenge? By developing processes to meet new digital requirements for security and compliance and automating those processes as effectively as possible. Automation should integrate the objectives and activities of Security and Operations teams and enable them to protect the enterprise while providing the performance and availability required for businesses to remain competitive.

Organizations who rely on manual administration of security and compliance find it impossible to scale, which in turn limits their ability to keep up with business opportunities and challenges in the growing digital economy. Plus, manual administration is also particularly subject to human error, which makes it dangerous. Delays in responding to security threats and compliance issues can lead

to breaches, failed audits, financial loss, and damage to a company's reputation and other serious business consequences.

In this guide, you'll learn about the security compliance audit process, security risk management, and how to deal with persistent threats in the digital economy. The guide will also describe how best-practice processes and automation can help organizations meet the challenges of today and the future while also increasing collaboration between Security and Operations. This unifying strategy can enable these teams to improve uptime, customer satisfaction, and security.

Having an effective strategy is critical to success. This guide will help you understand the risks that must be mitigated or eliminated. You'll also learn important considerations for developing a plan that focuses on integrating the roles of people, processes, and technology to address the increasing challenges related to security and compliance in the digital economy. As Figure 1 indicates, vulnerabilities and exposures to threats are increasing rapidly. Organizations must prioritize efforts and focus on the most critical vulnerabilities.



The role of Operations in maintaining security, compliance and control

Keep in mind that maintaining a secure environment is more than just the Security team's concern. Operations teams play a critical role as well, however they may not appreciate how important they are in the process. The Security team identifies the risks, but Operations must implement the changes to remediate those risks.

Officially the charter of the Security team is to keep the organization secure while the Operations team works on supporting the business demand for high availability to avoid risking performance or reliability on production systems.

This situation creates a **gap** between Security and Operations known as the SecOps Gap: Two groups driven by competing priorities which ultimately result in long lag times to close security vulnerabilities, business-system downtime, excessive labor costs and challenges in meeting regulatory requirements.

Many attacks can be prevented by closing this gap. More than 80 percent of attacks target known vulnerabilities and 99 percent of exploits were compromised over a year after the CVE was published. According to Rob Joyce, Chief of NSA's Tailored Access Operations, "There're so many more vectors that are easier, less risky and quite often more productive than going down that route. This includes, of course, known vulnerabilities for which a patch is available but the owner hasn't installed it."

Closing the SecOps Gap protects company assets and reduces costs

The misalignment between Security and Operations goes beyond poor communication paths and conflicting objectives. A Forbes Insights survey commissioned by BMC reported that Operations and Security teams have only a general or little understanding of each other's requirements. So they are not even speaking the same language or providing one another with what they need to be successful. Some examples include – Security runs a scan and delivers it to Operations and it is sorted by IP address. If the Operations team does not use IP address as a reference point, they have to sort through the data line by line trying to figure out what it means. Going in the other direction, Operations provides their plans to remediate vulnerabilities to Security based on server group. Unless Security knows which servers are in the group and what role those servers play it does not help in giving them a view into the security posture of the organization.

Breaches occur even when vulnerabilities and their remediation have been identified, but not yet implemented, due to a lack of coordination between the teams. Half of the organizations that experienced a breach in the last year also reported a **loss of data**, which can result in failing to meet compliance requirements, fines, and impact the business by having to deal with this loss. It can also cause customer dissatisfaction that leads to litigation.

Providing a secure environment involves a clear focus on people, processes, and technology to address vulnerability remediation and compliance. This guide, which offers a comprehensive overview of security and compliance, helps explain how best practices and automation can enable organizations to optimize their resources, increase efficiency, reduce costs and improve the quality of service while meeting security and compliance objectives.