Guidepost

LINES OF AUTHORITY: THE CRITICAL NEED FOR ROLE CLARITY IN INFORMATION SECURITY COMPLIANCE

Clearly defined roles and responsibilities are an essential component of an effective compliance program. Failure to adequately assign responsibility can lead to gaps in compliance coverage and a lack of accountability.

In a recent NAVEX survey 76% of the respondents indicated that the compliance function in their infosec compliance group is not an independent Compliance department reporting to the chief executive officer or board of directors (for instance, it reports up through IT/data security/data privacy, Legal or Human Resources).

When compliance for a particular function (like InfoSec) sits outside of the Compliance department and hierarchy, the function becomes siloed from the rest of the organization and Compliance is shielded from any subject matter expertise related to that function. This set-up results in – at best – operational inefficiencies and inconsistent treatment between functions within the same organization.

In its worst iteration, when compliance is not embedded in the larger Compliance function, the siloed function (e.g., InfoSec) feels empowered to make its own compliance-related decisions outside of the risk appetite and processes already established by Compliance. This arrangement can lead to inconsistencies in the organization's approach to compliance, variations in decisions that may impact the organization's risk profile or risk appetite, and reputational damage and monetary penalties for non-compliant violations.

It is in this context that nearly a third of the respondents in the NAVEX survey said their firm had suffered a data privacy or cybersecurity breach within the past three years. The prevalence of data breaches, and the legal and regulatory consequences that flow from them, makes clear that organizations should not wait to evaluate their InfoSec compliance programs and reporting lines. Where compliance functions or subject matter expertise are siloed and exclusively housed in the InfoSec , organizations should strongly consider restructuring to bring those roles within the Compliance department.

Ultimately – in order to leverage efficiencies and derive benefits from consistency – InfoSec matters should be treated

the same as all other compliance matters, including assigning appropriate roles and responsibilities throughout the first and second lines of defense, including InfoSec topics in Internal Audit plans, and inclusion in risk assessments.

Moreover, clarifying roles and responsibilities helps ensure compliance with relevant regulatory requirements and ensures that assets are adequately protected. This minimizes duplication of tasks across the organization and provides a baseline for appropriate resource allocation.

As data privacy and cybersecurity continue to become more and more critical in daily business operations – and more highly regulated – increased emphasis must be placed on Information Security compliance. Clarifying compliance roles related to InfoSec compliance, as well as adjusting organizational structures to ensure InfoSec is handled within a larger Compliance function, are paramount to ensure ongoing compliance within an ever-evolving landscape.

ALLISON SPAGNOLO CIPP

Chief Privacy Officer, Senior Managing Director

Allison Spagnolo, a managing director in the Financial Crime Consulting practice, has worked on numerous engagements involving government contracting and financial institution matters. This includes reviewing anti-money laundering and sanctions issues for global banks and multi-national companies, as well as advising on financial crime compliance issues specific to cryptocurrency exchanges and Fintech companies. She has traveled extensively in Europe and Asia for the purpose of leading and conducting on-site inspections and reviews related to monitorships and other compliance matters.