DATA SECURITY
CREATIVE
COUNCIL

Workshop #2:

Navigating Compliance in a Shifting Regulatory Landscape

Data Security Creative Council
Workshop #2

Navigating Compliance in a Shifting Regulatory Landscape

The data compliance landscape presents a significant challenge, particularly for smaller and medium-sized organizations striving to keep pace with evolving laws and regulations. This paper is derived from the Data Security Creative Council (DSCC) workshop that brings together leading experts in data and security to discuss these challenges and share their insights on navigating the complex world of data management, privacy, security, and compliance. The workshop fostered in-depth discussions centered around crucial problem statements, focusing on understanding compliance mandates, the obstacles in proving compliance, the tools and processes employed in managing audits, quantifying compliance-related risks, and identifying improvements for day-to-day job duties.

Central to the workshop's discussions was recognizing the substantial obstacles that organizations must overcome to maintain data compliance. These include staying informed about the rapidly changing regulatory landscape, proving compliance amidst diverse and often conflicting mandates, managing audits effectively with the right tools and processes, quantifying compliance-related risks accurately, and seeking operational improvements to ease day-to-day compliance burdens.

This paper captures the collective wisdom and actionable advice from the experts in the DSCC workshop. It aims to provide a comprehensive guide for organizations striving to navigate the shifting sands of data compliance, highlighting the nuanced discussions around the identified problem statements and offering insights into developing effective strategies within the constraints of operational realities.

DATA SECURITY CREATIVE COUNCIL

Contributing Members

The contributions of esteemed professionals enriched the dialogue, each an authority in their respective domains.

Ray Stirbei, CISO at Signet Jewelers, emphasizes the global scale of compliance challenges. With a focus on EU/UK GDPR, US State, Canada, and Israel regulations, he showcases the breadth of legal landscapes his organization navigates. His contributions shed light on the complexities of adhering to multiple international compliance mandates, illustrating the intricate balance required to operate successfully across diverse legal jurisdictions.

Mahesh Ayyala, CISO and Chief Data Protection Officer at Hidden Road Inc., details the extensive range of compliance frameworks his organization adheres to, including GDPR (EU), NIST, SGP Risk Framework (Data), UK GDPR, EU DORA, EU NIS 2, and NYC DFS. He articulates the challenges of vague and high-level regulatory directives and the need for specialized tools.

Jeff Farinich, SVP CISO at New American Funding, specializes in financial compliance across multiple states. His extensive experience managing compliance in a complex regulatory environment provides critical insights into the financial sector's unique challenges.

Sonali Bhagwat, Sr. Director of Data Governance at Adobe, is an expert in risk quantification and data protection. Her expertise in establishing robust governance frameworks helps organizations navigate the intricacies of data compliance and risk management.

Ilan Dar, CISO and SVP of Technology at AutoFi, is renowned for his insights into notification requirements and geographic regulatory variances. His experience underscores the importance of understanding the nuances of compliance across different jurisdictions.

Karen Lopez, Data Evangelist at InfoAdvisors, focuses on anti-spam and anti-telemarketing regulations. Her role as a compliance officer has equipped her with practical knowledge of the challenges organizations face in adhering to these specific regulatory demands.

Current Compliance Landscape and Geographic Regulatory Challenges

The compliance realm is governed by well-known regulations, such as the California Consumer Privacy Act (CCPA) and the General Data Protection Regulation (GDPR), alongside emerging frameworks that continually reshape the compliance landscape. **Ray Stirbei** of Signet Jewelers notes:

"Navigating through a spectrum of regulations from the EU/UK GDPR to US and Canadian laws requires a dynamic approach to compliance, given the distinct nuances each brings."

This environment is further complicated by specific mandates like the IRS Taxpayer First Act and the FTC Safeguards Rule, which introduce stringent requirements for digital communication and consumer information security. Financial service providers, in particular, are challenged by regulations like the New York State Department of Financial Services (NYSDFS) cybersecurity rules, demanding robust data protection mechanisms.

As businesses expand across multiple geographies, they face diverse regulatory standards that significantly impact their compliance strategies. **Ilan Dar** of AutoFi highlighted the challenges posed by state-level consumer privacy regulations, where the requirements for consent record storage can vary dramatically from one jurisdiction to another, leading to operational and compliance headaches.

The influence of cross-jurisdictional regulations on data management practices is profound. **Mahesh Ayyala** from Hidden Road Inc. elaborated on the difficulties of adhering to frameworks like the GDPR, NIST, and upcoming regulations like EU DORA and EU NIS 2. These dictate the protection and privacy measures necessary and how data is stored, accessed, and transferred across international borders, requiring a detailed and structured approach to compliance management.

Managing third-party data processors introduces additional layers of complexity, as organizations must ensure these entities adhere to diverse regulatory standards. This challenge is accentuated by the rapid evolution of regulations and the necessity for businesses to stay informed and adaptable. **Karen Lopez** of InfoAdvisors reflects on this:

"Legislation like CCPA, which may suddenly extend its scope, requires us to be vigilant and proactive in our compliance strategies."

Moreover, the need for common frameworks further complicates the compliance landscape. **Jeff Farinich** of New American Funding illustrates this with the example of the NYDFS 23NYCRR500, a New York State Department of Financial Services regulation that mandates financial service providers implement a robust cybersecurity program to protect consumer data privacy alongside many other state-specific requirements. Organizations must navigate different state financial regulations, each with rules and enforcement mechanisms.

Companies must tailor their compliance programs to each jurisdiction's specific legal obligations, navigating the maze of local, state, national, and international regulations. This dynamic interplay of regulations underscores the critical need for organizations to develop informed, flexible, and robust compliance strategies to manage the current landscape's complexities effectively. The variances in regulations exacerbate the challenges of proving compliance, necessitating that organizations interpret and apply these diverse regulations accurately and effectively, often under tight scrutiny and with significant legal and financial implications at stake.

Tools and Processes for Compliance Management

Effective compliance management is predicated on utilizing robust tools and processes to streamline audits and enhance overall compliance efforts. Organizations leverage various methods to manage compliance and audit requirements, each with advantages and challenges.

Ilan Dar from AutoFi shared that their audit workflow is supported by third-party purpose-built tools, complemented by a mix of AWS & G-Suite for Identity and Access Management (IAM) and data visibility & encryption. This mix signifies a trend towards integrating specialized software with cloud-native services to ensure comprehensive coverage of compliance needs. However, Ilan also noted the challenges of proving compliance, particularly regarding third-party risk management (TPRM), highlighting the need for tools to manage and monitor these relationships effectively.

On the other hand, **Jeff Farinich** of New American Funding pointed to the limitations of legacy Governance, Risk, and Compliance (GRC) tools, which often fail to meet the nuanced requirements of specific regulations like NYDFS or FTC Safeguards. His organization's shift towards a next-generation GRC tool underscores the industry's move towards solutions that offer continuous control monitoring and can adapt to the varied data collection methods and standards imposed by different regulators.

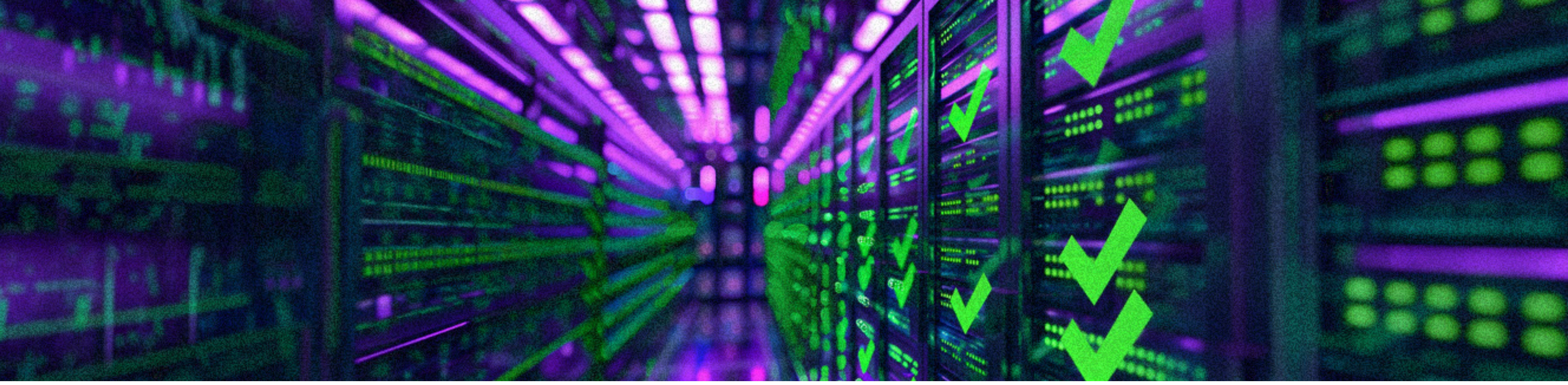
Karen Lopez emphasized the need for tools to address the data literacy gaps within organizations. Many need help with the basics of data management, such as fulfilling Subject Data Requests. This lack of data literacy and the resultant compliance exhaustion underscore the necessity for intuitive, comprehensive tools to alleviate these burdens.

Sonali Bhagwat of Adobe explained how comprehensive policy frameworks and regular Business Impact Analysis (BIAs) underpin their compliance strategy. She highlighted using internally built tools alongside Data Security Posture Management (DSPM) systems and data catalogs integrated with custom-built retention and classification solutions. Utilizing OneTrust as part of their toolkit signifies a strategic approach to managing data privacy and security across the organization. This blend of clear policies, regular assessments, and a mix of bespoke and off-the-shelf tools illustrates a sophisticated approach to navigating the complexities of compliance, balancing manual oversight with automated processes to optimize the audit and compliance workflow.

Karen Lopez on the challenges of compliance and data literacy:

"Many of my clients are totally unprepared for Subject Data Requests and panic when they get one. They have legal staff that aren't data literate, so they get what I'm seeing as problematic advice. The Venn diagram of literacy involves legal/compliance literacy, data literacy, security literacy, and technology literacy. Very few people have enough understanding of two overlaps, let alone all of them."

The effectiveness of current tools and processes in aiding compliance is thus a critical consideration for organizations. As they navigate the evolving landscape of data regulations, the demand for tools that can provide clarity, automate processes, and offer visibility into data and third-party relationships becomes increasingly paramount. The right mix of technology and process management, tailored to an organization's specific needs and challenges, is essential for maintaining robust compliance in today's complex regulatory environment.



Quantifying Compliance-Related Risks

Quantifying compliance-related risks is essential for organizations to understand the potential financial, operational, and reputational implications of failing to adhere to regulations. Effective risk quantification highlights areas of vulnerability and helps prioritize mitigation strategies, ensuring that resources are allocated efficiently.

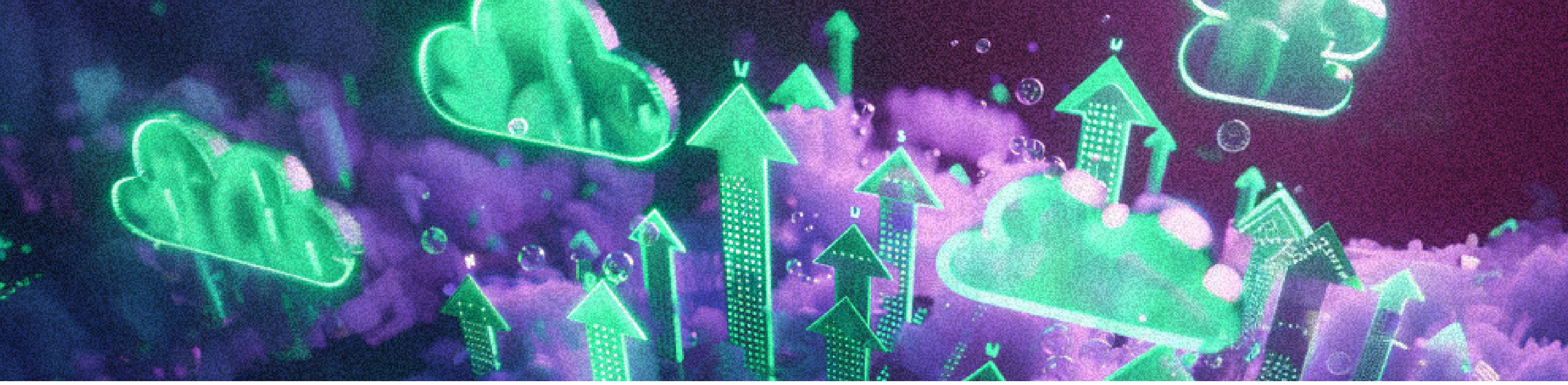
Financial Risk Quantification: Organizations often begin assessing the financial risks associated with non-compliance, including hefty fines, penalties, and legal costs. Jeff Farinich of New American Funding utilizes a cost-of-risk quantification (CRQ) approach, showing per-record cost liability to communicate potential financial exposure to the board and secure a budget for compliance measures. This method provides a clear monetary value to risk, making the implications of non-compliance tangible for decision-makers.

Operational Risk Assessment: Operational risks involve disruptions to business processes resulting from failing to comply with necessary regulations. Mahesh Ayyala from Hidden Road Inc. discusses leveraging third-party tools that use industry data to simulate compliance failure scenarios. These tools help understand the impact of compliance lapses on business operations, allowing companies to prepare better and implement effective controls.

Reputational Risk Measurement: Noncompliance's reputational damage can be severe and long-lasting. Sonali Bhagwat of Adobe points out the need for tools that quantify the direct costs of non-compliance and highlight potential reputational risks. She envisions dashboards that identify data and risk hotspots, providing executives with a visual representation of areas that could impact the company's reputation and require immediate attention.

Beyond basic risk assessments, some organizations adopt more sophisticated models, such as the Factor Analysis of Information Risk (FAIR) model, which Mahesh Ayyala mentions. These models provide a more detailed analysis of compliance risks by quantifying the probability and impact of potential security incidents, facilitating more nuanced risk management strategies.

Quantifying compliance-related risks requires a multi-faceted approach incorporating financial calculations, operational impact assessments, reputational considerations, and advanced risk modeling. By combining these methods, organizations can gauge the severity of compliance risks and prioritize their compliance efforts effectively, ensuring that they address the most critical areas first. This strategic approach to risk quantification is crucial for maintaining robust compliance and safeguarding the organization against the myriad risks associated with regulatory infractions.



Improving Compliance Efficiency

Improving the efficiency of compliance activities is critical for organizations looking to streamline their operations and reduce the burden on compliance officers and data security professionals. This section explores potential tools, processes, and regulatory enhancements that could significantly improve day-to-day compliance activities.

Enhancing Tool Capabilities: More sophisticated compliance tools that automate routine tasks are paramount. Ilan Dar of AutoFi suggests implementing a tool that automatically alerts him when there is a deviation from stated data policies. Such automation would reduce manual monitoring efforts and ensure faster response times to potential compliance issues, enhancing overall compliance efficiency.

Streamlining Processes: Karen Lopez of InfoAdvisors highlights the potential for improvement by integrating tools across multiple expertise areas, such as legal, data management, and security. She suggests employing AI technology that could automatically flag non-compliance in communications and operations. This type of integration could significantly aid compliance officers who manage complex data landscapes, ensuring they don’t miss critical compliance requirements due to oversight or lack of expertise in one area.

Regulatory Simplification: Simplifying regulations could significantly enhance compliance efficiency. Compliance professionals must navigate a labyrinth of overlapping and sometimes conflicting regulations. Simplifying these regulations or creating more unified standards could reduce complexity and make it easier for organizations to comply without extensive cross-referencing and consultation with legal experts.

Improving Training and Support: Compliance efficiency could be improved by offering more targeted training and support for compliance officers and data security professionals. Tailored training programs that focus on specific industry or jurisdiction compliance challenges can more efficiently equip professionals with the necessary skills than generic programs.

Developing Collaborative Platforms: Encouraging the development of collaborative platforms where compliance professionals can share insights and best practices could lead to improvements in compliance procedures across the board. Such platforms could facilitate better understanding and quicker adoption of new regulations and compliance strategies, benefiting individual professionals and their organizations.

Enhancing day-to-day compliance activities involves a multifaceted approach that includes upgrading technological tools, streamlining processes, simplifying regulatory requirements, improving training, and fostering collaboration. By focusing on these areas, organizations can increase compliance efficiency, reduce non-compliance risk, and enable compliance personnel to focus more on strategic initiatives rather than routine tasks.

Synthesizing Insights for Strategic Compliance

This white paper, derived from the **Data Security Creative Council (DSCC)** workshop, encapsulates the collective insights of leading experts in data and security. Throughout the discussions, participants focused on crucial problem statements, addressing data compliance's complexities and evolving nature, particularly for smaller and medium-sized organizations. The workshop emphasized understanding compliance mandates, overcoming obstacles in proving compliance, enhancing tools and processes for managing audits, quantifying compliance-related risks, and identifying ways to improve day-to-day compliance activities.

Central to the discussions was the acknowledgment of the significant hurdles that organizations must overcome to maintain robust compliance. These include staying informed about rapidly changing regulations, managing audits effectively, quantifying risks accurately, and implementing operational improvements to streamline compliance processes.

Moving forward, there is a clear need for ongoing research, policy development, and practice improvements in compliance management. Future efforts should develop more intuitive and comprehensive tools to automate compliance processes, enhance data visibility, and support compliance officers in their day-to-day operations. Additionally, fostering a deeper understanding of the nuances of various compliance mandates across different jurisdictions will be crucial.

For those looking to dive deeper into the complexities of data compliance or to engage further with leading experts in the field, we invite you to explore more resources or request an invitation to participate in the **DSCC**. Whether you're seeking guidance on specific compliance challenges or wish to contribute to ongoing discussions with your insights, the **DSCC** is an invaluable resource.

Visit Dasera's Data Security Creative Council page for more information about past workshops, upcoming events and how you can join this dynamic community. Join us in shaping the future of data security and compliance by sharing your experiences and learning from seasoned professionals in the field.

Interested in the latest in data security and governance?

For insights from the Data Security Creative Council Workshop, details about our founding members, or to join our dynamic community of data and security professionals, click here. Don't miss out on our upcoming content, webinars, workshops, and events designed to keep you at the forefront of data security innovation.