What's Next:

An update on the NYDFS requirements

Since the release of the New York State Department of Financial Services 23 NYCRR 500 (DFS500), financial services firms have made significant strides to address the regulatory requirements. Although there still remains some compliance concerns, the initially identified key challenges have largely been addressed. Now, Covered Entities are looking ahead to sustainability, consistency, and better oversight of the regulatory environment as a whole.

Common challenges across the financial services industry

Identification of in-scope information systems

The DFS500 requirements are largely centered on the protection of information systems that contain, process, and provide access to nonpublic information. As a result, identifying in-scope information systems has been critical and challenging due to the interconnectedness, number, variety, and residency of constituting components. Some of the larger organizations report identifying hundreds of in-scope information systems each made up of a multitude of components. Furthermore, inclusion of material business information, personally identifiable information, protected health information, and material financial transactions as well as any other specialized systems such as industrial/process control systems, and environmental control systems made identification of in-scope systems a multifaceted activity. Defining "materiality" and applying the definition consistently across has added additional complexity, leading to involvement of a number of different functions, such as Legal, Information Technology, Risk, Compliance, and Finance, in identifying the in-scope information systems, with senior leadership providing the final approval.

Implementation of technical requirements

The other key challenge has been the implementation of technical requirements such as Encryption of Nonpublic Information and Multi-Factor Authentication (MFA). For some, determining system compatibility with selected MFA and encryption solutions has been a challenge due to the sheer number of identified in-scope information systems and for others, it's related to technical feasibility and implementation know-how. To ensure encryption of data-in-transit to external networks, Covered Entities were observed to review and encrypt all potential outbound communication of nonpublic information, such as email communications, transfer to approved third parties, and interfaces of critical applications with external applications. With regards to data-at-rest, encryption at the hardware level, database level, application level, and file level were considered and examined. Due to budget limitations and business justifications for the runtime of critical applications, encrypting data-at-rest proved to be especially challenging. Where infeasible, compensating controls were identified and documented, and long-term project initiatives were added to the roadmaps.

Affiliate concerns

The interconnectedness of in-scope entities with their parent organization and other affiliates, and the identification, management, consumption, and monitoring of services that impact compliance with DFS500 expectations has posed a challenge. Firms are becoming increasingly aware that relevant control, tool, and service ownership that facilitates compliance is distributed throughout the broader organization and that there is no formal structure that governs expectations (SLAs, KPIs) related to these services and tools.

Continuous monitoring and oversight

During evaluation of compliance-supporting functions and tools, Covered Entities stressed that there is a lack of visibility to facilitate a full and continual understanding of compliance with the DFS500 expectations. Executives are seeking dashboards where compliance initiatives are mapped, easily trackable, and associated to risk appetite for each requirement.

Approaches to address the challenges

The path to DFS500 compliance differs for each Covered Entity due to differences in size, business model, structure, and risk tolerances; however, the general approach to tackle key challenges of DFS500 remains consistent: leverage existing processes and tools, develop plans of action to remediate weaknesses, document rationale, and inquire executive input for key decisions and approval.

Leverage existing processes and tools

During varied client engagements, KPMG observed use of existing processes and tools to address key DFS500 compliance challenges, i.e., adapting the existing application risk assessment processes to include the DFS500 requirements: examination of application criticality, measurement of confidentiality, integrity, and availability expectations. These ratings and measurements facilitate logical-driven methodology and workflow for identifying in-scope information systems. Another example is the use of existing controls: mapping the existing organizational and regulatory controls to DFS500 requirements.

Document rationale and provide a plan of action

Covered Entities recognize that, for some areas, they may not be fully compliant at the time of enforcement. In these situations, plans are developed, rationalized, communicated, approved, and maintained. Management of all subsequently created evidence is clearly documented and retained as evidence of decision and proof of action. Although there are set requirements, a key takeaway is that certain requirements may not be feasible to implement due to lack of funding, staff, and/or technical limitations. In instances where there may be constraints preventing a Covered Entity from meeting requirements in expected timeframes, explanatory rationale, in the form of a "plan of action" or "risk acceptance," is documented.

Executive input and approval

KPMG observed that the chief information security officer is not the sole accountable party. Covered Entities have established DFS500 and cybersecurity- focused steering committees as part of a governance body that includes the active participation of the majority of C-level executives. During these meetings, key decisions on DFS500 topics such as definition of materiality and scoping of applications are debated, agreed upon, approved by the members, documented, and communicated.

What’s next?

KPMG is assisting in various initiatives across the DFS500 compliance spectrum, including, but not limited to, DFS500 compliance assessments, gap remediation recommendations, development of strategic roadmap, executive dashboard development, penetration testing, and managed services.

When it comes to implementing our clients’ vision to meet these requirements and enhance compliance posture, the following are the top three areas of concern for the executives.

Moving toward sustainability

As the third certification year approaches, the focus is on moving the DFS500 compliance efforts to a business-as-usual state. Covered Entities are identifying where new processes are needed to mature their cybersecurity program, and which existing processes can be enhanced to provide a stronger security and compliance posture. To complement sustainability, there is an increased focus on identifying the right metrics for both internal and external reporting. Establishing adequate cyber dashboards is becoming a top priority for most organizations. Furthermore, Covered Entities are looking upstream and across all lines of defense to ensure that as processes evolve they remain aligned with DFS500.

Covered Entities are extending and adapting existing Governance Risk and Compliance platforms and programs to facilitate consistent and repeatable performance of required activities to move towards a holistic operational risk management focus and enable the business.

Developing a unified compliance framework

The release of DFS500 has heightened internal attention on effectively and efficiently implementing compliance initiatives to meet regulatory expectations. With the concurrent onset of other prominent regulatory requirements such as the European General Data Protection Regulation and the California Consumer Privacy Act, Covered Entities are seeking to relate the scope of DFS500 activities to meet other, complementary regulatory requirements. By leveraging tools and methodologies to map internal controls and initiatives across all the regulatory requirements and standards, organizations are creating a Unified Compliance Framework (UCF) tailored to their specific needs and regulatory responsibilities. A UCF enables efficient tracking and managing regulatory compliance efforts across all relevant regulations. It maps internal controls to the applicable regulations and organizational requirements, identifies overlap, informs the development of control remediation roadmaps, and provides foundation for the creation of efficient continuous monitoring and sustainability strategies.

Addressing resource needs

DFS500 gave an opportunity to examine whether existing cybersecurity functions have adequate technical and personnel resources to achieve organizational goals and compliance expectations. Covered Entities are assessing their current staffing levels and identifying personnel staffing and knowledge requirements based on peer benchmarking and organizationally defined program requirements. Mechanisms to track skills against targets are being developed. The requirements of DFS500, at times, reveal resource and knowledge gaps that are difficult to fill. Where significant and persistent gaps are identified, Covered Entities are looking to external service providers for security-skilled practitioners to meet their specific cyber security needs.

Contacts

Charles Jacco
Principal,
Cyber Security Services,
Financial Services Industry
Lead
E: cjacco@kpmg.com

Chetan Gavankar
Principal, Cyber Security
Services
E: cgavankar@kpmg.com

Mitushi Pitti
Director, Cyber Security
Services
E: mitushipitti@kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.