

## **OVERVIEW**

Fintech and Financial Services customers face several challenges, from constantly evolving regulatory requirements to the need for active management of security and compliance in a highly dynamic threat landscape. Digital Edge's NY DFS 500 Financial Services Security and Compliance Framework and consulting offer includes our DFS Reference Architecture which specifically guides customers in their AWS deployments and addressing the new requirements that have become a part of the NYS DFS 500 Law.

How can I comply with DFS running my infrastructure in AWS?

What DFS 500 Controls can be covered by AWS services?

How to automate validation of controls and their effectiveness?

How to implement AWS technology to address security and compliance risks instead of responding to them?

How to configure visibility of my compliance program and assurance of the compliance status of my cloud environments?

Digital Edge's deep knowledge and experience supports customers in fintech, financial services and highly regulated industries. Our expertise covers off on the legal aspects for cybersecurity laws and regulations, and our staff includes cybersecurity lawyers and auditors. With in-house legal and auditing staff, Digital Edge can save our clients time by quickly identifying a control standard to implement a control framework. With DFS Financial Services Security and Compliance Framework, customers can establish continuous compliance through the use of cloud-native tools, market-leading products, and Digital Edge DFS compliance framework to ensure current and ongoing compliance through visibility and active management of security and compliance risks.

## **BENEFITS**

- Implementing Digital Edge DFS compliance framework allows financial companies to avoid risks including service disruption, fees, fines, lawsuits, and reputational damage.
- Using Digital Edge's compliance service gives clients opportunity to consolidate AWS operation, cybersecurity, compliance under one integrated service allowing cost optimization, simplifying vendor management, enabling profitable operation in highly regulated industry.

## **HOW IT WORKS**

Digital Edge has decades of experience working with financial services organizations, particularly in helping them leverage new technologies such as AWS. Digital Edge has developed a unique understanding of New York State Department of Financial Services requirements and how to build and operate systems automating large aspect of the compliance with DFS 500 using AWS tools and services. Our techniques and solutions in coordination with our own legal staff will ensure the compliance, collect require artifacts, install necessary guardrails and alert to maintain the compliance regime. Digital Edge will begin with an assessment of the current landscape and approach to cyber security and security controls within your organization and alignment of them with DFS 500 regulation.

Digital Edge will conduct an assessment of environment, business services, and AWS services in use, engaging your architects, engineers and security specialists. This will provide a view of the of cloud security controls, their implementation and effectiveness.

When the assessment is complete, the Digital Edge team will produce a gap analysis showing what recommended technology should be implemented and what aspects for DFS 500 requirements can be automated. Digital Edge's DFS Financial Services Security and Compliance Framework has strong methodology of mapping DFS requirements to AWS tools and services allowing us to quickly establish referring architectures achieving confidence in compliance with NYS DFS 500.

Each assessment will be reviewed by Digital Edge's cybersecurity lawyer.

Digital Edge will provide referred architecture and multiple suggestions for implementation of native AWS tools and services to support compliance program with NYS DFS 500 and automate as many controls as possible, promoting a "secure by default" approach and vastly reducing the overhead associated with maintaining and evolving the control framework over time.

The engagement will conclude with training and handover to ensure the relevant client teams are empowered for the future, enabling you to own and evolve the framework as your cloud estate grows and changes over time.

## **KEY STEPS**

### **Assess**

Digital Edge works with your security and technology teams to understand your security and controls landscape.

### **Control cross-reference**

We will review existing control catalog and mapping to referring DFS Compliance Framework and Reference Architecture. (See DFS Security Controls Mapping)

Control framework implementation. Review Reference Architecture and current client's technology needs. Implementation required services.

Working with your technology teams, Digital Edge advise on deployment of the DFS Financial Services Security and Compliance framework, and best practices defined in Reference Architecture across your AWS estate to enable strict security, compliance, and risk-management controls.

### **Reviewing and adjusting Policies and Procedures documentation.**

DFS 500 requires extensive set of documentation including Policies and Procedures. One of the serious violations from our previous experience is using Policies and Procedures documentation without adjusting them to current technology and cybersecurity state. Polices and Procedures cannot be written by compliance specialists only and must include unique knowledge of AWS specifics. Digital Edge legal and compliance team working together with security and DevOps engineers will produce high quality documentation. Our policy writing methodology was tested by many audits and legal reviews.

### **Continues monitoring and enforcement**

DFS Financial Services Security and Compliance Framework and Reference Architecture implements means for security monitoring and detection of risk escalation events, cybersecurity threats and incidents. Digital Edge will educate your organization on responding and escalation of such events. Digital Edge may perform continues monitoring of your infrastructure and perform incident response as per below:

Digital Edge will be available work with your organization to determine the appropriate course of action to take when any cybersecurity incident or high-risk event occurs.

### **Customization**

If required, Digital Edge will build custom controls and any other customizations specific to your needs.

### **Deployment to development teams**

Digital Edge will work with your development teams to help them leverage the framework and the reference architecture to enable "secure by default" techniques in your Continuous Integration and Development (CICE) and DevOps activities.

### **Operational handover and practices**

Digital Edge legal team will consult your operations team on required processes and standard operating procedures (SOPs) that needed to be implemented outside of AWS to ensure continues compliance with non-technological requirements of NYS DFS 500.

### **CUSTOMER CONTRIBUTION**

Existing policies and procedures: Digital Edge will review any existing cybersecurity management systems, policies, standard operating procedures, and any other related documentation to consult on the gaps in the compliance with NYS DFS 500.

Systems access: Digital Edge will require read-only access to relevant systems.

Security and risk teams: Digital Edge collaborates with your teams to determine the appropriate controls for your organization.

Technology teams: Digital Edge works with your technology teams to hand over the knowledge of how to operate and extend the system.

## ABOUT THIS CONSULTANT

Digital Edge helps customers to promote the protection of customer's information as well as the information technology systems of regulated entities. We assist fintechs, financial service and highly regulated companies to assess their specific risk profile and *design a program that addresses its risks in a robust and secure fashion which has given us the tagline CONFIDENCE SECURED.*

Digital Edge helps companies adopt new technologies and techniques to make their business more agile, improve customer experience, and ultimately drive efficiency and growth. Digital Edge plays an active role in enabling customers at all stages of their cloud journey.

Digital Edge is an AWS Level 1 MSSP Partner in Security. As an AWS Partner We have significant experience working with fintech and financial Services firm, from the early stages of design and architecture through to build, migration, and management of applications on AWS, Digital Edge help customers maximize the benefits of AWS.

Digital Edge has delivered projects across almost every industry sector, but its true superpower is experience in accelerating cloud adoption within regulated industries, in particular in the financial services and fintech sector. Digital Edge has a deep understanding of the issues faced by businesses in this industry, the necessary focus on risk and regulation, and concerns around security and cyber controls that can quickly become a roadblock to innovation and delivery.

### **Overall Value Proposition: Confidence Secured**

Digital Edge provides an integrated approach to data governance, risk and compliance in public clouds. We secure client confidence by providing a comprehensive legal and technology approach to addressing information protection and compliance in highly regulated industries.

As an AWS MSSP with a Level 1 competency we are uniquely prepared to manage the complex workloads of Fintechs, ensuring operational efficiencies cost optimization and continuous monitoring while ensuring your Cloud infrastructure is fully compliant.

## DFS Security Control Matrix

See DFS-Security-Controls-Mapping.xlsx

## Architecture Diagram:

