SPOTLIGHT ON DIGITAL ASSETS

Building a Compliance Program with California's Digital Financial Assets Law

A Spotlight on California's Digital Financial Assets Law: Operational, Strategic, and Market Implications

Effective July 1, 2026

StratisAdvisory

RISK | STRATEGY | CYBER | COMPLIANCE MANAGEMENT

Redefining Digital Finance in California

Digital assets continue to reshape certain parts of global finance and regulatory oversight. For years, California stayed on the sidelines without a digital asset-specific regulations. Starting on July 1, 2026, California's Digital Financial Assets Law (DFAL) becomes effective and requires licensing for certain digital asset companies.

Key Milestones

October 13, 2023

DFAL was enacted through the Assembly Bill (AB) 39 and Senate Bill (SB) 401. AB 39 introduced the licensing backbone while SB 401 added the stablecoin and transaction rules.

July 1, 2026

Licensing requirements become operative on this date. Firms must apply for and obtain DFAL license from Department of Financial Protection and Innovation (DFPI).

The implementation date was already an extension from the July 2025 original date. DFPI is expected to begin examinations, enforcement, and rulemaking.

Regulatory Authority

DFPI
DEPARTMENT OF FINANCIAL PROTECTION & INNOVATION

DFAL licenses are issued and overseen by DFPI. It is the state agency that is responsible or has the authority to grant and revoke licenses, conduct examinations of licenses firms, enforce compliance, and issue guidance to clarify statutory obligations of companies.

DFAL is more than just a state law. It is a geopolitical signal, declaring digital assets must be safe, transparent, and resilient. This will be a new passport to global credibility as it sets regulatory alignment to licensing, consumer protection, cybersecurity and resilience, and risk oversight.

Alignment Activities

Licensing

Mandates exchanges, custodial wallets, and digital asset businesses to obtain DFAL license through DFPI.

Consumer Protection

Companies must provide disclosures, safeguard customer assets, and handle complaints in a transparent manner.

Cybersecurity and Resilience

Operational standards are required such as cybersecurity controls, incident response mechanism, and vendor oversight.

Risk Oversight

Embed risk oversight into overall licensing and supervision of digital asset business.

Exploring the Market and Operational Impact to FinTechs

DFAL is a strategic framework that established to encourage tech and digital asset firms manage risk, innovate responsibly while making sure consumers are protected. While compliance systems will change, firms that meet the DFAL standards will benefit from improved consumer trust and credibility. The following is a more structured view into the elements that companies must consider when complying with the law.

Market Impact

California will now have a dedicated licensing and supervisory framework for digital financial assets businesses with explicit consumer protection and cybersecurity expectations. This positions the state to influence other states to adopt similar frameworks.

Consumer Protection

DFAL requires FinTechs to provide mandatory disclosures and risk statements clearly defining the nature of digital asset activities. The law aims to reduce misleading marketing practices by enforcing transparency around fees, and product claims.

Cybersecurity Trends

DFAL embeds cybersecurity into compliance expectations, making resilience a licensing condition. Zero-trust architectures are becoming standard for digital asset platforms, ensuring strict access controls and continuous verification of customers.

Operational Impact

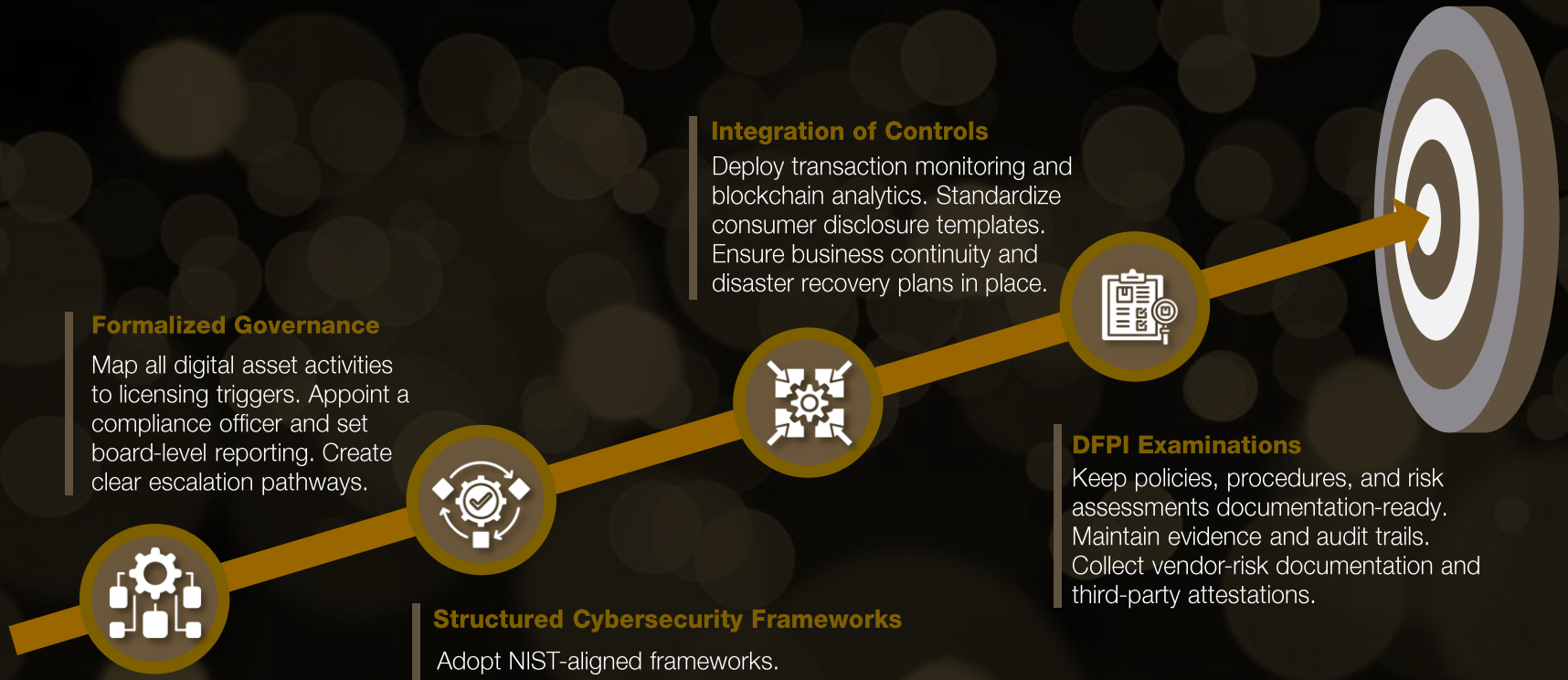
DFAL requires implementation of strengthened cybersecurity controls such as incident response planning, penetration testing, and secure key management. Vendor risk oversight will also be critical as well as documentation governance structures and audit trails.

Innovation Implications

Regulatory clarity under DFAL may accelerate institutional adoption of digital assets. Tokenization projects, stablecoin issuers, and DeFi protocols will need to adapt their models to fit licensing requirements, potentially reshaping product design.

Framing a Compliance Program

Building a DFAL-ready compliance program means starting with a clear gap assessment and governance framework. It is important to put emphasis on embedding cybersecurity resilience into daily operations and strengthening consumer protection through transparent disclosures and secure custody practices. DFAL overhauls compliance as gateway to innovation, resilience, and shapes California's evolving digital assets and finance ecosystem.



Formalized Governance

Map all digital asset activities to licensing triggers. Appoint a compliance officer and set board-level reporting. Create clear escalation pathways.

Structured Cybersecurity Frameworks

Adopt NIST-aligned frameworks. Strengthen identity and access management (IAM). Use secure custody. Implement continuous monitoring and threat-intelligence feeds.

Integration of Controls

Deploy transaction monitoring and blockchain analytics. Standardize consumer disclosure templates. Ensure business continuity and disaster recovery plans in place.

DFPI Examinations

Keep policies, procedures, and risk assessments documentation-ready. Maintain evidence and audit trails. Collect vendor-risk documentation and third-party attestations.

Discover what Stratis Advisory can do for you

Cybersecurity Risk Assessment

Beyond Service and Organization Controls (SOC) audit(s), penetration testing, and PCI Security Standard assessments, dedicated risk assessments help you understand the inherent risks in information technology systems, processes, and programs. Stratis can execute your cybersecurity risk assessment to identify broader risk identification and control mitigation across key information systems.

AML Independent Review

Whether operating as a regulated financial institution or through various bank, payment, or lending partnership models, typically an annual review of your AML and sanctions programs is a requirement. As Stratis serves a portfolio of global regulated and unregulated companies, Stratis can help you with performing your required AML and sanctions review on a scale and risk-appropriate basis to satisfy your statutory requirement, but also any requirement(s) from your banking partner.

Token Due Diligence Listing and Monitoring

Transactions with virtual currency or digital assets pose risks such as regulatory uncertainties, fraud, and technological vulnerabilities. Stratis can assist you by providing comprehensive token due diligence reviews to further understand a token's functionality, identify legal and regulatory risks, and whether a token may be classified as a security under the Howey Test.

Stratis Advisory | 1.415.352.1060 | www.stratisadvisory.com | info@stratisadvisory.com