ProSight™

Regulatory Updates

for 2026 Affecting Policies and Procedures

What financial services organizations need to know—and do now—to stay compliant and competitive in a rapidly evolving regulatory landscape.

Now that we are in 2026, many of the regulatory developments introduced throughout 2025 are beginning to take shape and influence how financial services organizations operate. From regulatory localization and evolving AI legislation to heightened cybersecurity expectations and a shift toward risk-based examinations, the landscape is actively changing. Institutions must move beyond awareness and focus on execution—reviewing, updating, and strengthening their policies and procedures to align with new requirements and supervisory priorities. Without a clear, proactive plan, organizations risk falling out of compliance and exposing both their business and their customers to unnecessary risk.



ProSight Financial Association provides the resources you need to navigate new regulations and emerging trends.

Regulatory Updates
for 2026 Affecting Policies and Procedures

Over the course of 2025, we saw many regulatory updates that will impact financial services organizations' policies and procedures in 2026. Businesses should be aware of these changes to understand what will affect them and when the changes take place so they can create action plans to address them before they become effective. Without having a solid plan in place, financial services organizations can risk operating out of compliance, putting their company and their customers at risk.

Below is a list of the top changes coming to the financial services industry that organizations should be aware of with advice on how policy management programs should be updated:

Regulatory Localization:

National regulators in the financial services industry are increasingly reshaping rulebooks to align with domestic economic priorities, rather than solely adhering to longstanding international standards. In recent years, policymakers have shifted toward "localization", where regulation is anchored in national goals of growth, innovation, and competitiveness rather than one-size-fits-all global frameworks. This trend reflects a broader strategic realignment: regulators want to support home-grown fintech ecosystems, attract investment, and enhance economic autonomy, even if that leads to a patchwork of divergent rules across borders.

One example of this is includes congress passing the Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act) in 2025. This law aims to bring clarity and certainty to how stablecoins — digital assets designed to maintain a stable value — are regulated in the U.S., with the goal of encouraging innovation and keeping activity "on shore". The GENIUS Act becomes effective on the earlier of the following two dates:

- January 18, 2027 (which is 18 months after enactment); or
- 120 days after the "primary federal payment stablecoin regulators" issue final implementing regulations, which federal agencies are required to complete within one year of enactment which would be around July 18, 2026.

As new technologies and capabilities are created in the financial services industry, organizations will have to pay attention to how congress and state legislatures approach them and adhere to any guidelines and reporting requirements they issue for them and update their policies and procedures to be compliant with that new guidance.

Stay Ahead. Act with Confidence.
Contact Us Today!

National and State Level Artificial Intelligence Legislation:

AI continues to be a massive discussion point among national and state legislative bodies. Many states have already passed or are in the process of passing their own rules and laws that focus on ensuring AI data is secure, non-discriminatory, and is used to protect and serve consumers without directly or indirectly exploiting them.

On a national level, legislation has been slower, but many discussions are being had on country-wide guidelines on how to properly utilize AI in business. The current focus is to ensure AI can be utilized safely and as a result, the Unleashing AI Innovation in Financial Services Act was proposed in 2025. The bill is designed to enable and accelerate the safe use of AI technologies within the U.S. financial services sector by allowing businesses to create formal regulatory test environments or "sandboxes" (also referred to as AI Innovation Labs) that are hosted by many of the major federal financial regulatory bodies including:

- Federal Reserve
- FDIC
- OCC
- SEC

The purpose of the bill is to provide a controlled framework where financial services organizations that are regulated by any of the above entities can test and experiment with AI systems ranging from AI-driven credit scoring, automated investment advice, fraud detection, risk analytics, or customer support tools without the immediate risk of enforcement actions under existing regulations while innovations are evaluated. This allows organizations to build solutions with regulatory approval given from the beginning as opposed to building and implementing a solution and having it fail an examination and being assessed enforcement actions.

If this bill gets passed, financial services organizations should create policies and procedures for building new AI solutions and working with the appropriate regulators to adhere to their requirements so they're building helpful, compliant resources for their stakeholders.



Cybersecurity and Consumer Protection:

There are many benefits AI can provide in the financial services industry, but there are also many risks it presents. Cybercriminals are using AI to automate and scale credential harvesting and identity attacks, making them far more effective than traditional malware. These attacks can bypass basic defenses by using massive datasets to generate highly convincing phishing messages. AI tools also accelerate brute-force and hybrid identity exploits at cloud and on-premises systems. Banks and other institutions that hold high-value accounts and sensitive customer data need to implement strong identity protection and verification tools that flag suspicious activity and notify customers immediately if someone is trying to access their accounts.

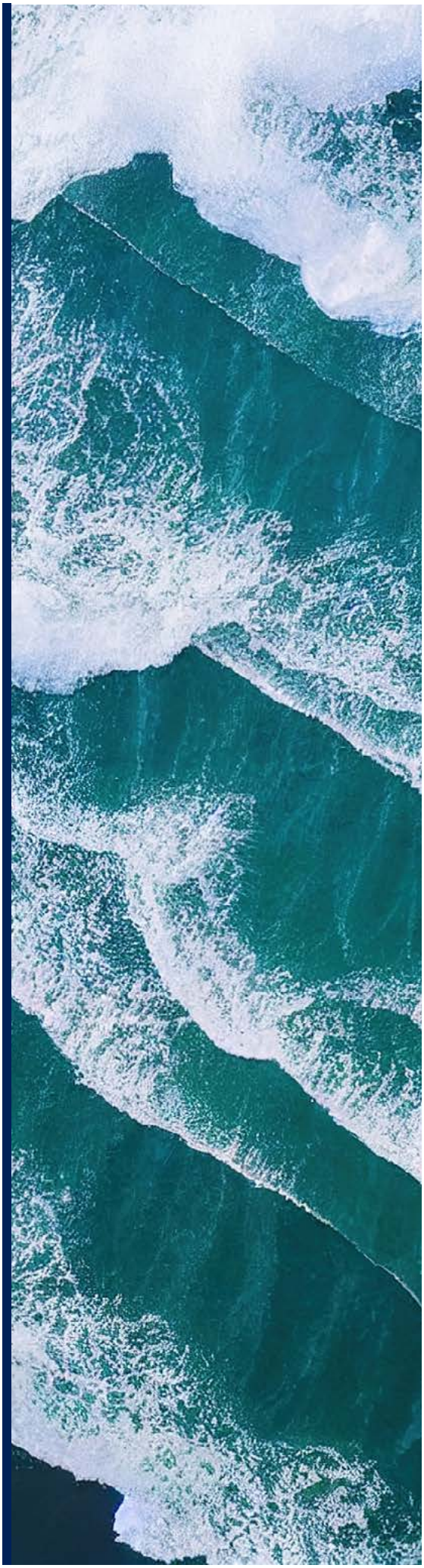
In addition to direct attacks on customers, there are more ways cybercriminals can exploit gaps in security of third-party vendors. Financial services are deeply interconnected with cloud platforms, API ecosystems, and other third-party services that are necessary for business. Weaknesses in a vendor's software supply chains can provide attackers indirect access to critical infrastructure. Even if a financial institution's own defenses are strong, a partner's compromised service could expose customer data, trigger breaches, or interrupt cloud-based operations.

To combat these risks, congress has recently extended the Cybersecurity Information Sharing Act (CISA) through September of 2026. CISA provides a network for both public and private companies to share cybersecurity threats and information with one another. It is unclear if CISA will be extended past the new sunset deadline, so companies should be working to find an alternative cybersecurity threat community or developing their own resources to monitor threats that directly impact them and their customers. Whatever strategy they take, they should ensure all of their cybersecurity policies and procedures reflect the most recent trends to ensure they keep themselves and their customers safe.

Risk-Based Examinations:

Of the many regulatory shifts that took place in 2025, one of the big ones included regulators shifting away from compliance-based examinations to risk-based examinations. Adhering to compliance standards is still critically important for financial services organizations, but the level of compliance requirements businesses have when it comes to collecting and reporting data has gone down greatly.

In 2026 and beyond, the focus regulators will have is more on how well organizations are identifying and managing risks. Regulators will want to see the methodology businesses have when assessing what types of risks they face and how they will address and mitigate them. They want to ensure businesses understand the biggest internal and external forces that could put their organization and their customers at risk and that there are plans in place to mitigate those risks or avoid unnecessary risks. Financial services organizations will have to create policies and procedures on how to properly document their enterprise risk appetite strategies and their business unit risk assessments, along with plans on how they will monitor risks throughout the year and how they will adjust if there are gaps in their strategy.



Enhance Your Policy Management in 2026 with ProSight:

ProSight Financial Association empowers financial services leaders to strengthen and advance our industry. Formed through the merger of BAI and RMA—trusted organizations with rich histories and deep expertise in risk, fraud, compliance, and retail and commercial banking— we provide connections, training, insights, tools, and analytics to help you act with confidence.

Our solution is an end-to-end solution that helps financial services organizations make informed decisions when creating, updating, communicating, and tracking their organizational policies and procedures. The ProSight Policy Manager includes many features to help automate workflows and better manage policies and procedures including:

- Industry-specific regulatory resources including: regulatory alerts (CFPB changes, FDIC updates, NCUA rules, etc.), policy considerations, policy templates, and regulation overviews
- Powerful communication tools that help you communicate policies and procedure effectively, including a centralized repository, full text search, acknowledgement tracking, quizzes, and more
- Focused processes to help compliance professionals make timely updates and collect acknowledgements by utilizing managerial and user dashboards, report subscriptions, and automated reminder emails
- Easy setup and administration to ensure your organization can quickly start managing policies and procedures effectively through bulk data importing, a human resources information system (HRIS), and configurable and reusable workflows.



Enhance Your Policy and Procedure Management with ProSight

ProSight Financial Association empowers financial services leaders to strengthen and advance our industry. Formed through the merger of BAI and RMA—trusted organizations with rich histories and deep expertise in risk, fraud, compliance, and retail and commercial banking—we provide connections, training, insights, tools, and analytics to help you act with confidence.

The ProSight Policy Manager helps financial services organizations make informed decisions when creating, updating, communicating, and tracking their organizational policies and procedures.

To learn more about the ProSight Policy Manager and how it can help your organization align and manage policies and procedures in 2026 and beyond, contact us to learn more or schedule a demo today!