Guide

How to Automate Financial Institution Data Compliance

QOHASH

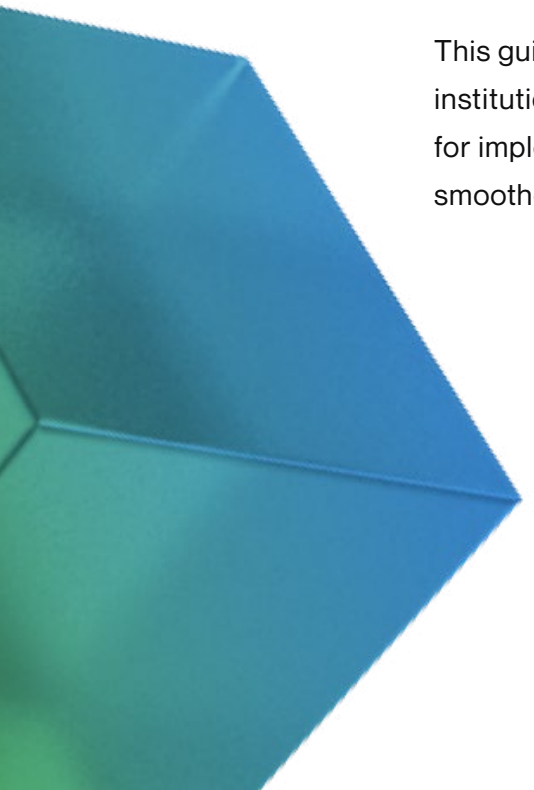
Compliance is a serious business for financial institutions, and fraught with danger in the age of work-from-home and increased cybersecurity threat.

A host of data compliance regulations face the typical financial institution. These include the Gramm-Leach-Bliley Act (GLBA), Sarbanes-Oxley (SOX), California Consumer Protection Act (CCPA), General Data Protection Regulation (GDPR) and industry-led regulations such as the Payment Card Industry Data Security Standard (PCI-DSS), among others. New regulations are on the way, too, such as California's CPRA data privacy rules that come into effect in 2023.

At the same time, CIOs and security professionals are increasingly nervous about their organization's data security stance, which can lead to compliance violations. A new study by IDG Research Services found that roughly 78 percent of senior IT and security leaders believe their organization lacks sufficient protection against cyberattacks, and 55 percent said they lacked confidence in their data management strategy.

Automation can help. With more robust data management and security automation, financial institutions can speed up threat detection and protect against compliance violations, improve incident response, increase compliance visibility, and help standardize compliance processes.

This guide will look at four of the biggest data compliance challenges that financial institutions face, outline the processes that should be automated, define the steps for implementing data compliance automation, and suggest six best practices for a smoother compliance automation rollout.



Four Data Compliance Risks Top the List

Financial institutions face a laundry list of compliance obligations when it comes to business data. Meeting these obligations is far from assured in the age of cloud services, employees working from home and rapid digital change, however.

While there are many compliance risks that financial institutions must protect against, four core risks stand out. These four are the data risks that absolutely require attention and systems for minimizing compliance issues.

Risk #1: Incomplete Data Classification

Financial data compliance starts with proper classification. Automated compliance procedures and appropriate access restrictions are only possible if data that falls under regulatory jurisdiction is correctly identified and tagged. Without robust and complete data classification, financial firms cannot track and control regulated data, enable quarantining, apply legal hold or archive according to regulatory mandates.

Despite the importance of data classification, a recent study found that more than 52 percent of data within the typical organization goes unclassified.

This is because much of the sensitive data employees require for their work is performed outside of strictly controlled services such as databases or SaaS applications. Knowledge workers spend a lot of time downloading, manipulating and uploading unstructured data between applications. This browser swivelling creates inadvertent but dangerous compliance and security risks to an organization.

Financial firms usually have a classification procedure in place for obviously regulated data such as bank account information and personally identifiable information (PII), but there's often room for regulated data leakage if these classification procedures do not encompass all data within the organization and classify it in real-time.

Risk #2: Shadow IT

While the term sounds shady, most shadow IT within an organization occurs because well-intentioned employees augment IT systems or create workarounds as a means to drive efficiency and get more done. A spreadsheet might be uploaded to Google Drive for easier access while working from home, or a personal mobile device might be used for capturing information during a client meeting.

Even though the intentions behind shadow IT often are benign, the effects are not. Unauthorized software and systems pose a significant risk for compliance violation because data accessed or stored in these systems falls outside a financial institution's watch. Further, shadow IT is not vetted for appropriate security controls. These systems might be secure, but they also might not.

Typically, financial institutions enforce strict policies against the use of unauthorized devices and software applications. Nevertheless, these technologies find their way into corporate organizations, introducing compliance and security risk.

Risk #3: Poor Digital Hygiene

A related but distinct compliance risk for financial institutions is sloppy digital habits among employees.

In the normal course of business, employees typically create or come in contact with sensitive corporate data, some of it regulated. While the majority of this data stays within secure IT systems, sometimes employees might save data in inappropriate places or sidestep specified security protocols through carelessness or expediency. A cell in a spreadsheet is copied outside company systems, for instance, or a file is moved to a local hard drive and then not deleted afterwards. Maybe an employee keeps a local copy of a regulated document they've created before uploading it to a company account.

There's wide scope through poor digital hygiene for employees to create a data compliance violation unintentionally, especially with the vast majority of employees working from home for the first time as a result of the Covid-19 coronavirus pandemic. The work-from-home trend might keep employees safe, but it does the opposite for data compliance.

Risk #4: Unauthorized Data Sharing

Finally, a fourth significant data compliance risk for financial institutions is unauthorized sharing of regulated data.

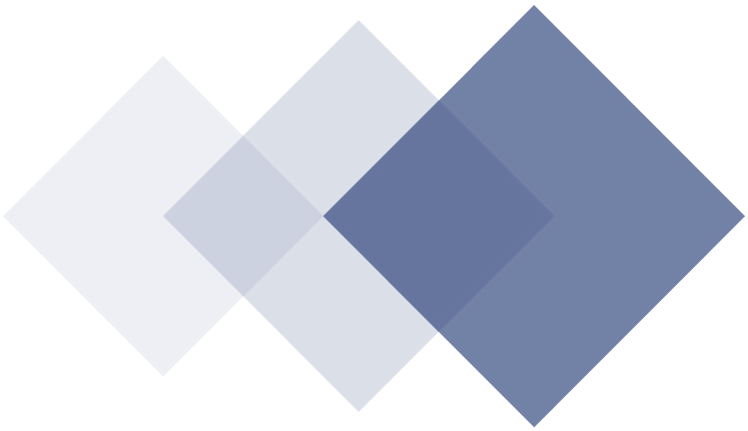
Regulated data can escape a company in many ways. Employees can share it unintentionally through email forwards or data buried in conversation threads. APIs can expose regulated data to partner organizations or the public at large. Authorized third-parties can be granted access to more data than they should, or employee devices can contain software that exposes regulated data to other users or systems.

There's a number of ways that access to a financial institution's regulated data can migrate outside the list of authorized users. Unfortunately, it takes only one such exposure to create a compliance violation.

What to Automate For Compliance

There are several areas where automation can help financial institutions with data compliance. Chief among those are automations for data discovery, classification, monitoring, threat detection and cybersecurity processes.

Let's look at each of these major areas where financial institutions should be applying compliance automation today.



Data Discovery Automation

Untracked data represents the greatest threat to compliance. If a financial institution does not have complete visibility into its data universe, including real-time awareness of where data is created and stored, maintaining compliance becomes nearly impossible. Yet, 55 percent of all data within the typical company is “dark data” that is unknown or untracked.

To eliminate dark data, financial institutions should have data discovery automation in place that automatically finds and catalogues all data within the organization. This automation should extend beyond just corporate data centers and company-owned devices, too. Since employees increasingly work from home and use personal devices, a complete data discovery solution should extend to personal devices where employees perform work, as well as public cloud drives where corporate data might end up.

Data Classification Automation

Compliance rules and safeguards required vary according to data type. European customer data might fall under GDPR regulations and a handful of others, while credit card data interacts with PCI-DCS and other financial compliance requirements. Accurately classifying and tagging data therefore is essential for meeting compliance and security demands. The volume of data within the typical organization today makes this a problem, however; more than half of all data within the typical organization is unclassified or untagged, as noted earlier.

Automated data classification makes it possible for an organization to identify the correct compliance and security processes to put in place for a given piece of data. Financial institutions should have automation in place that can identify data based on defined rule sets for each set of regulations and level of sensitivity, then accurately apply tags to data so other automated systems can process and restrict it appropriately.

Data Monitoring Automation

Data within financial institutions is created, accessed and shared on a daily basis. Maintaining compliance and effective cybersecurity requires monitoring this data and having visibility into how it is used and where it goes. IDG has found that 73 percent of companies currently are pursuing data visibility and identification projects given the critical importance of monitoring corporate data.

Manually monitoring data flows and the corporate data landscape is no longer functionally possible given the large volumes involved. Financial institutions must therefore have automated monitoring in place that tracks corporate data in real-time. As with automated discovery, data monitoring automation should extend into employee devices and public cloud drives as well as corporate-owned resources.

Threat Detection Automation

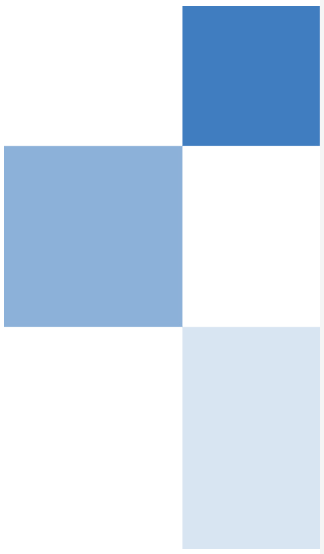
Looking for compliance and security threats is both time-consuming and highly technical. Although all financial institutions have cybersecurity professionals that hunt for threats and some manner of threat detection automation in place, roughly 44 percent of security alerts still go uninvestigated as a result of the overwhelming data volume that security professionals face. Increasingly sophisticated cyberattacks also make manual threat detection a challenge even if infinite data security staffing were possible.

Financial institutions should therefore augment existing cybersecurity threat hunting systems with intelligent, automated threat detection. This automated threat detection should not only flag potential threats, but also take advantage of adaptive risk scoring, compare employee and system behavior with baselines, prioritize threats so security analysts can triage the most pressing concerns, and apply behavior assessment for spotting potential compliance and data security issues before they actually occur.

Cybersecurity Process Automation

Enforcing correct data compliance processes and appropriate cybersecurity requires a multitude of systems and manual tasks such as applying correct access controls, remotely wiping decommissioned devices, segmenting networks, anonymizing data and maintaining encryption keys. These processes and systems can suffer from human error, and IDG has found that cybersecurity hiring is flat even as security professional responsibilities are on the rise. Financial institutions must do more with less.

Cybersecurity process automation both cuts down on the chance for human error and lessens the burden on already overworked cybersecurity staff. Financial institutions should automate each aspect of their compliance and cybersecurity processes so the role of data compliance officers and cybersecurity professionals is wholly oversight instead of manual application of security practices. While some security processes might partially remain manual, firms should gradually move away from these manual processes until all aspects of compliance and cybersecurity are automatically applied through automation.



Setting Up Your Data Classification Scheme

Data classification is a foundation for proper compliance and security processes, and it is essential for data automation. The good news is that establishing a robust classification system is not hard.

You can get help with the data classification planning process by downloading our free ebook, How to Identify and Classify Sensitive Data. The guide outlines the advantages of data classification, the method for developing a classification scheme, and the process for actually putting that classification scheme into practice.

Steps for Implementing Data Automation

The process of rolling out data compliance automation varies, and it often is company and solution specific. But the overall automation implementation journey can be broadly broken down into six key steps. These steps provide an overall framework for implementing data compliant automation at financial institutions.

Step 1: Define Your Automation Plan

The first step is determining the full scope of expected data within the organization, who owns and accesses it, and which data regulations apply to the organization. This usually will require input from stakeholders throughout the company. As part of this plan, you should also define the various objectives and data sensitivity categories for each group of data, categorize data according to data type, and define classification levels for use later in the automation process.

During the planning process, you also should define and select the various technologies that will be used for data compliance automation. The needed tools largely will flow from your list of objectives and security requirements, but it should include a comprehensive data discovery and monitoring solution, an automated data classification engine, a real-time threat detection solution based in the cloud, and an automated security provisioning system.

Step 2: Inventory Data Resources

With a plan in place, next build an accurate inventory of the financial institution's data universe by scanning all corporate resources, devices employees use for working with data, and any public cloud drives that may contain corporate data.

You'll want to use an automated data discovery solution for uncovering the full scope and location of all corporate data. Make sure you select a solution that maintains employee privacy through anonymization, and communicate this to employees so they sign off on having their personal devices scanned. You can lessen resistance to this scanning by tying data discovery to your company's work-from-home policy.

Set up your data discovery solution so it scans continuously after the initial scan, providing ongoing data discovery as new data is created.

Step 3: Tag Data According to Classification

Once the full data landscape is known, tag each piece of corporate data according to the classification schema established during the planning phase. Each piece of data likely will have more than one tag, and tags will correspond to compliance requirements, sensitivity level and security needs. With these tags, automation can act upon the data intelligently and apply the appropriate governance and security frameworks.

An automated classification engine is essential for tagging the large volume of data within the organization. The process for tagging should start with setting up the classification rules, running an automated classification process, then refining the automated classification and correcting initial misclassifications through manual review.

As with data discovery, tagging should happen continuously after the initial categorization effort so new data is automatically tagged as well.

Step 4: Set Up Real-Time Data Monitoring

The next step is putting a data monitoring and threat detection system in place for ensuring ongoing compliance and security. This could be a single all-in-one monitoring and detection system or multiple, overlapping monitoring solutions.

Whatever security stack is chosen, make sure it scans continuously so your organization can monitor data flows and risky behavior in real-time. It should be cloud-based so it covers the entire data landscape, and it should have the capacity for monitoring, not just corporate-owned resources but also devices and cloud services employees use during the normal course of business.

The right solution will provide an ongoing high-level snapshot of data, but also allow for drilling down to specific data elements. It should include automated flagging based on rules set by the compliance and security teams, adaptive risk scoring for spotting issues before they arise, and both accumulation and exfiltration indicators.

Step 5: Apply Automated Security Controls

With all data now tagged, next set up and apply automated access and security controls for each data category. The tagging done earlier in the process will serve to guide and trigger the appropriate automated compliance and security processes for each piece of data.

The nature and scope of security controls will vary according to each financial institution, but the crucial element is making sure that all compliance and security processes are automated and do not require manual intervention. Financial institutions will want to monitor these processes and refine them over time, but all processes should occur automatically without manual intervention so data compliance is maintained regardless of staff workloads or human error.

Step 6: Test and Refine the Automation System

The final step in automating data compliance often gets minimized, but it is one of the most important. Once automation is in place, financial institutions should rigorously test each step in the process against defined objectives, ensuring automation performs as expected. Even if the right planning and implementation have occurred, there will be a few kinks in the system that must be corrected before it performs as expected.

This process of testing and refinement should be ongoing, too. As part of the automation rollout, establish a periodic review process for updating compliance rules based on changing regulations, adapting security controls for the latest threats, and evolving data compliance automation based on changing corporate needs. This should include periodically reviewing all steps in the automation process to ensure that the system continues to perform according to compliance and security objectives.

Best Practices for Data Automation

All financial institutions have some form of data compliance automation in place. Not all automation efforts are equally successful, however.

With that in mind, here are six best practices for ensuring your organization's compliance automation efforts hit the mark. These best practices should be factored in during the automation planning process mentioned earlier in this guide.

Best Practice #1: Make Infrastructure Automation the Priority

While low-level data automation is important, a financial institution will make the biggest impact if it starts with building out infrastructure automation for a more adaptive, responsive IT backend. When infrastructure is automated, businesses lay the foundation for the depth of automation that is part and parcel of digital transformation.

This is more possible, and more necessary, as businesses move toward running largely or wholly on cloud services. Cloud-based services are inherently well-positioned for infrastructure automation.

Best Practice #2: Lean on Automated Detectors

Compliance and security analysts typically are overloaded with responsibilities. That's why roughly 44 percent of security alerts go uninvestigated, as noted earlier.

Shift as much of the work as possible from compliance and security professionals to automated detectors, whether these detectors are rule-based or AI-driven. Offloading workloads to detectors is essential for handling the scale of data that must be identified and addressed for compliance.

Best Practice #3: Automate Everything

The entire process should be automated and only require oversight.

Don't settle for partial automation, which is a pre-digital transformation methodology. Everything from alert collection, prioritization, task delegation and processes can and should be automated. Even areas such as compliance checks, vulnerability management and orchestration should happen automatically.

Best Practice #4: Iterate Continuously

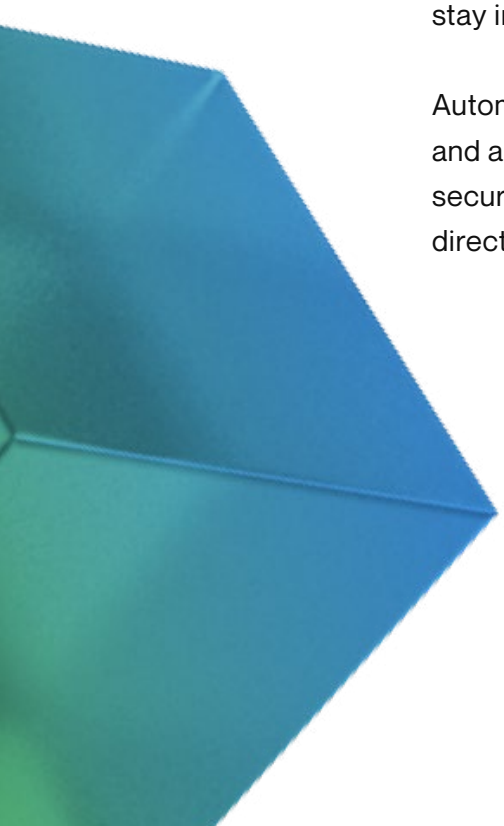
Compliance regulations change, business needs evolve, and new security threats emerge. Data compliance automation is not one-and-done.

Automation that stays relevant and meets current needs requires a continuous process of review and adjustment. So financial institutions should build their compliance automation around an agile methodology of constant iteration and adaptation. Include periodic review of the whole automation system as part of the compliance automation project.

Best Practice #5: Always Stay Involved

While data compliance should be automated end-to-end and require no manual intervention, it still is critically important that compliance and security personnel stay involved through ongoing monitoring of the automated systems.

Automation solutions have come a long way, but they are not yet fully self-correcting and automatically adaptive. With widespread automation, the role of compliance and security personnel shifts to overseeing the processes instead of handling the work directly. Automation still requires human oversight, though.



Best Practice #6: Tightly Restrict Automated System Access

The power of automation is a double-edged sword. While it reduces workloads and enables much greater levels of data protection, in the wrong hands it also opens the door for catastrophic data leaks and huge process challenges.

Access to a firm's automated systems should be tightly controlled and limited to the handful of compliance and security professionals who are trained on and responsible for the automated systems. All key stakeholders within an organization should have input into the automation put in place, but access to the actual systems should be far more limited.

Make Data Compliance Automatic

A recent study by the Ponemon Institute found that only 23 percent of businesses rely on automation extensively for data security and compliance. With the vast array of compliance requirements that the financial industry faces, and increasing privacy regulation in general, financial institutions cannot be among the three-quarters of businesses that forgo robust data automation.

The good news is that data compliance automation is easier than ever, and numerous solutions exist today that facilitate the process. Some are even tailored specifically to financial institution compliance needs.

If a financial institution still relies on manual compliance processes, or has worryingly brittle compliance protection, now is a good time for putting more robust automation in place.

Make all your sensitive data secure

Identifying and classifying data is not instant. But at the same time, it is easier than many businesses realize. All it takes is awareness of a company's data landscape, a little structured planning, and the right automation technology in place. With a little work and the right data classification system, even businesses with small cybersecurity departments can ensure that sensitive data remains safe.

Qohash is a leader in data discovery and classification security software. It blends innovative and easy to understand security technologies, allowing businesses to gain visibility on sensitive data. Founded in 2018 with solutions available in the U.S. and Canada, Qohash provides customers with solutions tailored to meet today's hybrid and remote work environments in the financial services sector.

To learn more about Qohash Solutions, schedule a demo. Write us at info@qohash.com