It's Time to Automate

21st Century Business Requires a 21st Century GRC Management Tool

HARLAND CLARKE®

It's a fact: despite all the evidence that automated tools increase the efficiency and effectiveness of most business processes, many financial institutions waste significant time and money using manual processes for governance, risk and compliance (GRC) management. More importantly, using these outdated techniques in an increasingly complex environment puts financial institutions at greater risk of having data compromised, failing to address reported incidents in a timely fashion, and being penalized for noncompliance.

It's time to replace spreadsheets and manual processes with an automated solution.

Outdated manual processes put financial institutions at greater risk of having data compromised, failing to address reported incidents in a timely fashion and being penalized for noncompliance.

Manual processes cultivate a silo-based approach to compliance, risk management and IT security, with individual groups or departments focused on specific risks or guidelines.

This structure — or lack thereof — usually involves hundreds or thousands of documents and spreadsheets scattered in multiple network folders in various shared drives with different permission levels, with distinct processes and tools based on department, business unit or geography.

Today this approach no longer works. Regulatory requirements, operational risks and cyber-threats are now entwined and more complex. Dividing these disciplines:

- Prevents financial institutions from creating a common framework to manage compliance
- Hinders management's ability to develop a unified risk appetite
- Limits the ability to report on cross-functional issues
- Requires more time to accumulate data across various business functions, resulting in isolated business decisions made by each function, instead of enterprise-wide
- Prevents auditors from establishing a universal view of the institution

Automated GRC platforms, on the other hand, facilitate a unified approach by:

- Integrating operational, vendor and security risk assessments with appropriate compliance activities, giving you a holistic view into all risk and compliance activities
- Systematizing processes to eliminate redundancies and decrease risk of human error
- Importing relevant data from multiple sources
- Enhancing process maturity by establishing standard, repeatable procedures
- Providing management with visibility into the overall risk posture to identify trends before they become issues
- Organizing, storing and managing records across processes in a single location
- Increasing communication and collaboration between departments and business lines
- Giving users the ability to create reports that highlight relevant information, as needed
- Decreasing audit preparation and execution time

This paper outlines six key areas in which financial institutions must consider replacing outdated manual processes with a comprehensive software solution.

If you are responsible for any of the following tasks or processes, you likely spend a significant portion of your day locating documents, comparing multiple versions of those documents and updating spreadsheets to track risks and compliance efforts. Your financial institution may be putting itself at risk of fines, data breaches and negative publicity.

IT Risk Management

IT threats are ubiquitous. The hacker industry grows every day and everyone is a potential target. At the same time, organizations expose themselves to more IT risk by expanding their infrastructure: More assets mean more potential vulnerabilities.

The job of hackers is made easier by attempts to manage, identify, assess and analyze risks using 30-year-old technology like spreadsheets and network folders. A financial institution using manual processes to manage IT risks likely:

- Analyzes data on a case-by-case basis using multiple risk assessment tools based on organizational silos
- Uses email as the primary method to follow-up with internal stakeholders in an effort to resolve a risk
- Tracks assets via unstructured methods on spreadsheets resulting in duplication and redundancy

Compare the manual approach to one utilizing an automated platform for the management, measurement and reporting of IT risk. GRC software can make IT policy and risk management more effective by providing financial institutions the ability to:

- Correlate scan data from multiple configuration, web application, and vulnerability scanners to identify trends and achieve a holistic risk profile
- Perform rapid analysis on large data sets to prioritize and track their risk profile
- Integrate scan data with the National Vulnerability Database to gain a comprehensive threat picture
- Analyze incidents to spot trends (i.e., an abnormal number of successful phishing scams) and use this information to increase security and/or training
- Allow visibility into employee remediation efforts, length of time and systems impacted, along with trends over time with intuitive reporting capabilities
- Associate vulnerabilities directly to their assets and devices
- Leverage existing IT investments to optimize data from third-party security vendors to holistically expose threats and obtain a true view of their vulnerabilities
- Automatically flag duplicate records and identify known issues
- Take action on threats by assigning remediation tasks to the proper personnel

A common issue in most financial institutions is what happens when an associate loses a laptop. Without an automated solution, there's little way to verify whether the laptop was encrypted, had any vulnerabilities patched, and what information is stored on the device. The right GRC solution, on the other hand, gives you the ability to pull up all that information as soon as you become aware that the device is missing and assess the risk.

Operational Risk Management

How does an organization effectively manage operational risk in a volatile environment? First, risks must be uncovered and identified, then prioritized. They should be tied to the institution's strategic objectives, mapped to business processes and compliance mandates, and linked to key performance indicators. In some situations, a process needs to be established to manage operational risk. In addition, regulators, auditors, and boards of directors are increasingly pressuring financial institutions to improve their risk reporting.

Using a manual process to analyze and manage operational risks increases the chances of disruptive incidents occurring because risks and incidents are documented in an unstructured manner. This makes it difficult to establish accountability for remediation or mitigation of risks.

Automating the investigation process, on the other hand, helps financial institutions relate incidents to internal and third-party policies, risks, and business continuity plans. This allows users to proactively close the incident in a timely fashion, thus minimizing the effects of the incident.

Using the right software can also provide an audit trail detailing who, what, when, where and how in order to satisfy regulators and outside investigators. These complex requirements are difficult if not impossible to fulfill using manual processes.

In addition, automation allows financial institutions the ability to more proactively monitor risks in an attempt to avoid incidents altogether through:

- The ability to mimic, streamline and systematize business processes
- Comprehensive risk registers
- Risk-scoring systems using common industry-standard scoring methods
- Automated assignment of tasks with corresponding due dates to direct identified risks to specific users for additional analysis
- Project schedules for risk tasks, tracking progress and holding stakeholders accountable
- Built-in mechanisms for tracking various exceptions throughout the organization
- Links to specific assets and third parties
- Assessments to gather, organize and report on critical risk-related information
- Anonymous portals that empower employees to report violations while protecting their privacy

Vendor Risk Management

Third parties are extensions of your organization and their actions can have a direct impact on compliance efforts and brand reputation. Regulators are increasing their focus on potential third-party risks. To comply, financial institutions must identify third-party risks, verify that business partners and their employees are compliant, monitor for changes that might create new risks, and manage the investigation and remediation of incidents. This requires financial institutions to survey, assess, and follow-up with dozens, hundreds or even thousands of third parties, and take action against those not in compliance.

An automated system can help you identify, classify, monitor, and recommend risk mitigation to support business operations and regulatory requirements.

This is an arduous task if conducted manually. A manual process of inputting data, assigning risk levels, and following up requires multiple employees dedicating numerous hours. A manual process also makes it difficult to ensure harmony between an organization's policies, regulatory requirements and those of the vendor or supplier.

On the other hand, an automated system can help financial institutions identify, classify, monitor, and recommend risk mitigation to support business operations and regulatory requirements. The right software solution allows organizations to better manage vendor risk by:

- Creating dynamic assessments using prebuilt questions based on standards and regulations to obtain relevant vendor information
- Grouping third parties by role or type to segment the survey types or frequency for different vendor sets
- Automatically generating a score to determine the risk profile of a third party across different risk categories
- Automating periodic reviews of high-risk vendors to maintain ongoing compliance

Audit Management

Preparing for a regulatory audit can be daunting. Responding to 10 or 20 every year can be extremely burdensome. Undertaking the process manually usually means having data and information required by auditors stored in separate systems and even different geographic locations. This makes it difficult to compile into one comprehensive report, which increases the chances of fines and future scrutiny.

Relying on manual processes to manage audit tasks usually leads to repetitiveness. There is often a great deal of overlap between different audits, and those in charge of audit preparation frequently ask the same people for the same information multiple times a year while themselves digging through the same documentation to prepare similar audit reports.

Automate this process and you can easily replicate these tasks. This can reduce the time and resources required from hundreds of hours over several weeks to an individual or two getting it done in a few days.

A lack of automated audit tasks also makes it difficult to prove to auditors that employees have been notified of policies and understand their role in complying. If done via email, this task lacks an efficient method of tracking and confirming the receipt and understanding of policies. An automated solution can easily streamline this process.

An automated audit solution can also streamline the effort of identifying auditable entities and conducting audit tasks. It makes communicating audit findings more efficient by centralizing all audit activities into one accessible platform. Users can provide auditors with permission-based access to just the pertinent documents housed in an automated tool instead of sending them on a search for documents hidden on your network or forcing internal staff to spend hours compiling documentation.

A software solution can also help internal audit teams document and track phases of the audit cycle: audit planning, audit risk assessment, audit project management, time and expense management, issue tracking, audit paperwork management, audit evidence management, and reporting. This is accomplished through:

- A central repository for collecting and sharing information
- An automated workflow engine that generates audit and remediation tasks and allows for the viewing and sharing of audit performance, findings and history
- The ability to track audit requests, internal controls and all communications between team members and external auditors
- The mapping of policies to regulations, laws, standards and risks, and mapping risks to controls
- The ability to track inactivity in the audit process, pending risk remediation activities, and finalized audit findings and observations

A lack of automated audit tasks makes it difficult to prove to auditors that employees have been notified of policies and understand their role in complying.

Proactive compliance requires a minimal amount of effort and resources to meet obligations. And it allows financial institutions to self-police and remediate issues before auditors show up onsite.

Business Continuity Management and Planning

From hurricanes to security breaches, if disaster strikes, financial institutions of all sizes need to ensure their essential business functions remain available. Business continuity management and planning involves coordinating, facilitating and executing activities to identify and mitigate operational risks resulting from a potential disruptive event.

This can be one of the least prioritized tasks in the overall risk management and compliance process because audits and fines occur more frequently than earthquakes and epidemics. But if your financial institution is using manual processes for business continuity and disaster recovery, here's the hypothetical scenario of what could happen when a crisis hits:

- Somebody will have to locate the disaster plans, which are probably stored on shared drives and individual computers. This will prove fruitless if your facility can't access its computer network.
- There will probably be multiple versions of the plans because the approval and updating process took place via email. So good luck finding the most recent version.
- Provided somebody locates the most up-to-date plan, it likely hasn't been tested against disaster scenarios to determine outcomes. It's anybody's guess which sections of the plan should be prioritized in a given situation. The tasks of informing suppliers and ensuring compliance in the midst of the crisis have not been assigned.

Had an organization used a GRC platform to build and maintain business continuity and disaster recovery plans, it would have:

- Centralized its plans and key contacts into a single accessible repository
- Conducted business impact analysis to determine the effects of business continuity
- Simulated various situations to test its plans
- Created reports to gather valuable insight about the execution of its plans
- Established workflows to allow collaboration between stakeholders to ensure the plans receive all required approvals prior to publishing
- Mapped the plans to risks, controls, processes, and vendors

Corporate Compliance and Oversight

Compliance typically occurs in one of two manners:

- Reactive, distracting the financial institution from its core business with last-minute fire drills and attempts to avoid heavy fines.
- Proactive, allowing financial institutions on top of regulatory changes to self-police and remediate issues before auditors show up onsite. This will require a minimal amount of effort and resources to meet obligations.

Reactive compliance occurs for a number of reasons, all of which can be attributed to reliance on manual compliance processes. It happens because rules and policies aren't always followed.

Without visibility, compliance documents can stagnate for years without being reviewed and updated, even as regulatory requirements and industry standards change.

Being proactive requires staffers to know and understand policies and procedures, and having people in authority know when regulations aren't being adhered to. For most financial institutions, failing to comply usually isn't a matter of defiance. Most often, rules aren't followed because somebody didn't understand a rule, or didn't know it even existed, and no one was tracking operations enough to know regulations and procedures weren't being followed.

Simply having policies written down is not enough to satisfy auditors. Internal policies must correspond with regulatory controls. Furthermore, auditors want to see evidence that the organization is actually following the rules in its everyday operations.

Manual processes also hinder the ability for financial institutions to conduct gap analysis — a proactive compliance activity — between their current processes and what is required by regulatory requirements and industry standards. For some companies, gap analysis occurs when auditors discover noncompliance within operations, causing them to reactively comply.

The trouble with relying on manual processes is that policies are contained in multiple authority documents spread out across an organization. Tucked away in binders on an office shelf, in network folders or on individual hard drives, these policies can be buried and overlooked. Without visibility, compliance documents can stagnate for years without being reviewed and updated, while regulatory requirements and industry standards change.

In addition, authority documents don't have associated controls to easily translate policies into action. Personnel have little to no awareness of policies that impact their business function, and it becomes cumbersome to measure how well they understand and adhere to those policies.

An automated GRC process, on the other hand, is designed to prevent compliance oversights. A robust GRC solution provides the advantages of:

- A comprehensive compliance content library that includes rules, regulations, and best practices
- Authority documents that are mapped to internal controls, allowing the ability to de-duplicate compliance efforts and eliminate redundant requirements
- A centralized repository for all existing policies as well as results from previous audits that users can reference for future gap analysis
- A configurable workflow that facilitates collaboration between stakeholders to ensure the proper people are notified and reminded to perform periodic policy review and approval
- Awareness events to socialize policies within or outside the organization and track acknowledgment to ensure receipt and understanding by all
- The ability to report on and receive notifications as the content library is regularly updated with changing rules and regulations
- Being able to easily launch educational campaigns to introduce new policies and track understanding and awareness

It's Time to Automate

Software and other advanced technology has removed the tediousness and minimized the amount of human error from a multitude of jobs. A new generation of software has done the same for the complex task of managing risk and complying with multiple regulations. Compliance, risk management and security needs that exist today may broaden tomorrow, and concerns you don't have today may manifest in a few months or years. In this complex world, you can't settle for just any GRC tool. You need one that:

- Won't take months to implement and configure
- Can scale as your company grows and expands
- Can be changed without a single line of programming code
- Can conform to your processes rather than your having to adapt your business to the software

Harland Clarke's GRC Spotlight, powered by LockPath®, was created by industry experts who recognized the need for easy-to-use software that is flexible and scalable to serve ever-changing and expanding financial institutions.

Our goal is to implement GRC Spotlight within 30 days. Plus, GRC Spotlight is easily configurable so it can be adapted to changes in operations, regulations or security needs. In fact, while most GRC platforms require additional programming and code writing to configure, GRC Spotlight requires just a mouse and keyboard.

If you're frustrated by the slow implementation of your current GRC software, still trying to retrofit your existing technology to meet new standards, or just throwing in the towel and hoping spreadsheets and other manual tools can do the job, contact **Harland Clarke.**

About Harland Clarke

Harland Clarke is a leading provider of best-in-class integrated payment solutions, marketing services, and retail products. It provides integrated solutions for financial institutions; investment firms; business-to-business clients; individual consumers; and small, medium and large businesses serving multiple industries. Harland Clarke's clients range in size from major financial institutions and corporate brands to small businesses and individual consumers. Harland Clarke provides products and services to nearly 15,000 financial and commercial clients. harlandclarke.com

Call 1.800.351.3843
Visit harlandclarke.com/GRC
Email contactHC@harlandclarke.com