How to Innovate Governance, Risk and Compliance Efforts with Transformative Technology

By Kevin Malicki

HARLAND CLARKE®

Between the changing political landscape, new or changing banking regulations, and ongoing program management — who can stay on top of institutional compliance? More so, if ongoing maintenance is a challenge, much needed innovation takes a backseat, leaving financial institutions with outdated practices plus multiple documents and processes in play.

The solution to both problems — how to streamline ongoing maintenance while up leveling risk management efforts — is surprisingly simple All it takes is technology and a handful of key best practices to truly transform your institution's governance, risk, and compliance efforts into something manageable, comprehensive, strategic, and most importantly effective.

5 Best Practices to Innovate and Simplify Governance, Risk, and Compliance

1 Take an Enterprise View

The concept of governance, risk, and compliance (GRC) management is nothing new. Ever since banking regulations started, banks needed to comply in order to continue doing business. Over time, GRC management has grown to include multiple aspects of a financial institution's business, including:

- Compliance
- Risk
- Business continuity
- Audit
- Third-party risk management
- Incident Management
- Operational Risk

Typically, all of these components are managed separately across different teams. To garner insight into multiple areas of compliance practices, financial institutions will often use a hybrid of technologies: a mix of spreadsheets, emails, documents, and shared drives and files.

While this approach is one way of getting the work done, it's imperative to instead take an enterprise view of compliance and risk management. Otherwise, risks can pop up in the gaps in between these silos of the business. For this reason, many documents across many technologies may not be enough to prevent these "risks found in the gaps." Nor is it very efficient.

Potential GRC Risk:

A financial institution is unprepared to handle an unforeseen weather emergency. When weather hits, account holders are unable to access their money in branch or via mobile banking.

Likely, this institution didn't have an enterprise view to see these risks ahead of time. Additionally, controls likely failed, for example senior management didn't have an inclement weather policy.

When looking at it end-to-end, from a truly enterprise level view, senior management would've been able to see the lack of weather policy and take measures to put a plan in place. When controls fail, visibility is the stop gap, but this can only happen when a full view is available to the institution.

2 Leverage Data Effectively

Even with an enterprise level view, you'll need data to support conclusions. If you're not leveraging data effectively, it's hard to interpret risks and could result in missed opportunities. Having multiple documents and technologies in place creates headaches when it comes to analyzing data, but having such data is critical to innovating GRC efforts in the modern age — the data doesn't lie, and it also tells the story.

There are two ways to ensure your institution is fully utilizing its data: having a proper technology solution in place that can pull data and having a proper technology for reporting and analysis of said data. Ideally, you'd get one technology for both the pulling and reporting. Having strong data governance oversight will also help with the credibility of the data.

Potential GRC Risk:

Because data is so critical to financial institutions, extreme measures should be taken to secure it. An example of risk in this area is a financial institution solely relying on a software security solution for protecting data.

Exclusively trusting your software technology security solution is not enough in an era where hackers go to extreme measures and are very persistent. Instead, information security teams must continually search for vulnerabilities and test controls.

Ways to properly manage risk in this area include: consistently inventorying all software and solutions, conducting vulnerability scans, and testing controls. These initiatives will help in preventing a breach that could increase reputational risks down the road.

3 Foster Greater Internal Collaboration

Fostering cross-department collaboration can be tricky even for non-financial institutions, but it's important to governance, risk, and compliance. Institutions placing an emphasis on breaking down organizational silos will see the benefits reflected in a better risk management and compliance program overall.

Greater internal collaboration significantly improves:

- Engagement of multiple areas for risk assessments
- Incident management
- Fraud prevention and control
- Policy review

Potential GRC Risk:

For example, a financial institution develops a new policy and it's going to impact IT, training, HR, and legal. All of these areas need to look at the document *and* they all have edits. How does an institution bring all the feedback in, manage it and then disperse out again until a final version is agreed upon?

If it sounds complicated, that's because it is.

Many financial institutions today don't have a transformative technology solution to track all of these reviews, so they're doing it through an email platform — where multiple versions of documents go back and forth between departments of the organization. To cut down on the "back and forth," an institution should invest in a specific GRC solution.

This makes the process easier to manage rather than doing it manually, in addition to creating efficiencies, reducing time, increasing collaboration and providing a central repository to archive versions.

4 Properly Map Risks with Controls

The best defense against gaps in your governance, risk, and compliance program comes down to a simple process: properly mapping every risk with a control.

The problem is that it's easy to identify risk, but not always so easy to identify the proper control to go along with it. Still, every risk *needs* a control, and every control needs to be tested. If not, you have a gap and may need to assess if you want to accept the risk or not.

Once a risk is mapped, assigned a control, and then the control is tested, it's important to see if there is any residual risk leftover afterward.

Potential GRC Risk:

Fraud is an issue every financial institution faces. For example, each institution must hire individuals who have access to account holders' most sensitive information. This is a huge risk, but one that is unavoidable, because banks still need in-branch employees. While chances of identity theft are low, it's important to ensure these employees can't access and steal information.

Below is an example of how to map risks with controls >>>

Risk:

Individuals (such as tellers, lending officers, etc.) have access to sensitive information such as account and social security numbers.

Controls:

- Properly identify individuals who handle sensitive data, and make sure there are no reputational risks
- Conduct background checks on all new employees
- Ensure employees do not have exposure to an excess of information either through security or facility protocols
- Develop dual control policies and procedures
- Create separation of control procedures
- Ensure email and other technologies aren't vulnerable to data theft
- Do not allow smartphones/camera technology on the floor

Ideally, an institution would conduct this exercise for every risk they identified in their business.

5 Integrate Technology for Ease and Innovation

Technology is the best way to implement and simplify the best practices outlined above. In addition to making daily management of GRC easier, technology can truly innovate two other areas of institutional compliance: third-party risk management and process automation.

Specific to third-party risk management, which is a large part of what banks are required to do from a regulatory standpoint, institutions have to obtain sources of evidence to demonstrate they are properly managing the partner or vendor. Technology systems can be set up automatically to ask for certain documents the institution maintains on an annual basis, such as:

- SOC1
- Review of contract
- On-site review of vendor
- Complaint management
- Vendor risk assessment

Many banks are allocating significant resources to vendor management without realizing technology automates many of these processes.

Conclusion

The bigger the financial institution, the bigger the business. The bigger the business, the more third-party vendors and partners, and thus more regulatory scrutiny. For this reason, it's imperative institutions implement a technology platform to break down organizational silos and provide greater visibility into the business.

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

Kevin Malicki joined Harland Clarke in 2017 as Director of Product Management for Governance, Risk and Compliance (GRC). He brings 20 years of banking experience, including senior level positions at SunTrust Bank and Fidelity Southern Bank, driving risk management activities.