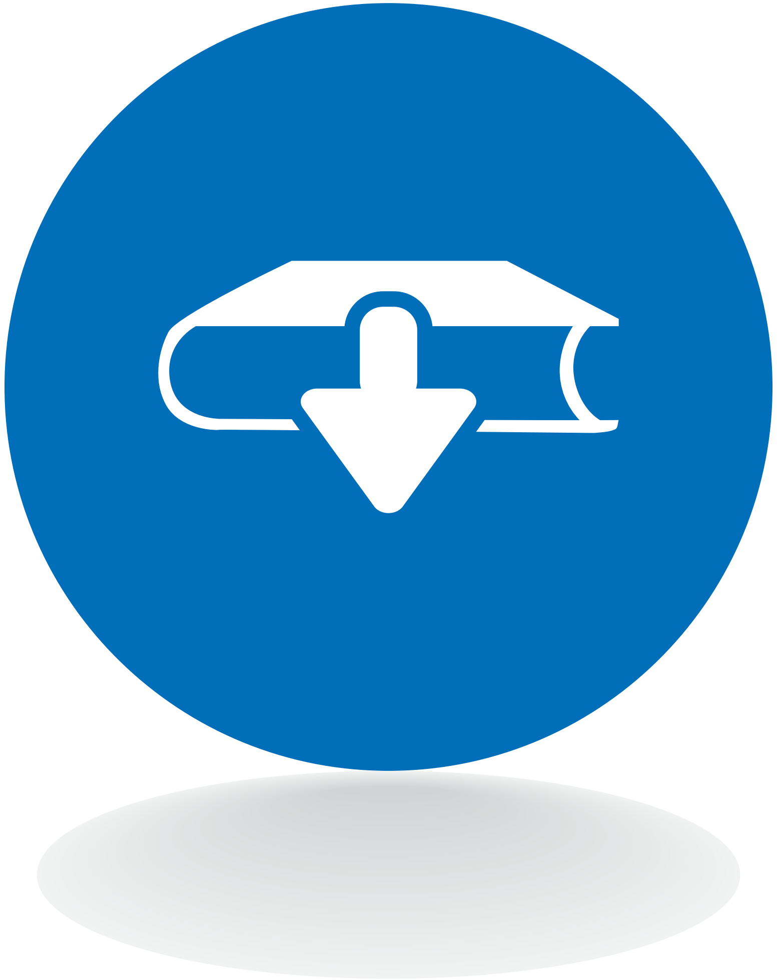
MetricStream
PERFORM WITH INTEGRITY™

JULY **2019**



THE GRC EBOOK

Curated Insights, Case Studies, and Whitepapers on Risk, Compliance, Cybersecurity and Audit.

Table of Contents

Riding the Wave of Disruption

Key Risk Considerations for Fintechs and Banks

Around the world, fintech companies are challenging the very fundamentals of the banking and financial services industry through a combination of innovative business models and disruptive technology. Today, they are one of the fastest growing markets, notching a record $111.8 billion in global investments in 2018, up 120% from 2017, according to KPMG.

Supporting the surge in growth are a number of fintech-friendly government policies and initiatives like the UK's Open Banking reforms and the EU's PSD2, as well as the US OCC's[1] proposed special purpose national bank charter and India's Aadhaar Stack. Many countries have also set up regulatory sandboxes that allow fintech firms to test their products at a lower cost before obtaining full regulatory approval.

Another factor driving the rapid adoption of fintech is the changing customer mindscape. Today's customers are demanding faster and better financial services, better digital banking experiences, personalized interactions, intuitive interfaces, and empowered decision-making—all of which fintech companies have the agility and innovative capabilities to meet.

Fintech firms are also rapidly finding powerful allies in the financial might and infrastructural prowess of technology industry bigwigs like Apple, Amazon, Facebook, Google, and Microsoft who are increasingly looking to expand and diversify their business interests.

Even established banks are beginning to recognize the potential of acquiring or collaborating with fintech companies to thrive in a digital banking era. In the US last year, Goldman Sachs acquired Clarity Money, a personal finance startup, to bolster the finance giant's Marcus online lending business, while in Asia, Standard Chartered has teamed up with Ant Financial to launch one of the first blockchain-based cross-digital wallet remittance services.

Opportunities Galore. But What about the Risks?

The changes ushered in by the fintech revolution—including paradigm shifts in banking models, as well as customer interactions and operational technologies—warrant a serious rethink of the underlying risks and possible points of failure.

Fintech companies derive much of their competitive edge from their ability to anticipate and respond swiftly to latent trends and customer demands—particularly those around simplicity, personalization, transparency, and continuous innovation. Their secret sauce? Data. In an increasingly digital landscape, fintechs have increasing volumes of information available to them for predictive analysis and response. Adding to their advantage are open banking reforms which require larger banks to permit customers to share their own transaction data with authorized third parties, including fintechs.

However, the more one's access to data, the greater one's liability—not just for fintech companies, but also for the banks sharing that data with them. A single data breach, as we saw at Equifax, can have an exponential impact on company financials and regulatory compliance, as well as reputation, trust, and credibility.

[1] PSD2 - Second Payment Services Directive; OCC – Office of the Comptroller of the Currency

Consequently, some of the largest financial services institutions globally are investing in GRC tools that enable them to structure their data landscape, and then align it to global information security regulations like GDPR[2], as well as key business risks. The idea is to build an integrated risk model that maps IT risks, controls, and compliance requirements to the larger operational risk framework. Through this tightly mapped structure, stakeholders can proactively understand how a data security risk can impact the business, and what kind of mitigation measures need to be implemented.

Ultimately, fintech companies and banks have a responsibility as data custodians i.e. keepers of information who ensure that the data in their hands is used appropriately and in accordance with privacy standards and accessibility permissions. Cambridge Analytica's unauthorized harvesting and use of personal data was a harsh reminder of just how harmful ineffective data governance can be, and why it's so important for organizations to take their role as data custodians seriously.

Many leading financial services companies are now leveraging GRC technology to build and maintain a robust data governance program across their operational infrastructure. Their aim is to ensure that while access to data is regulated, business lines can still leverage this data to drive competitive advantages.

Banks are also adopting IT vendor governance solutions to manage the risks of collaborating with fintech companies. By streamlining and standardizing vendor due diligence, risk assessments, and continuous monitoring processes, banks gain better visibility into the data security risks associated with fintech partners which, in turn, enables them to make better-informed decisions.

Risk Velocity and Regulatory Shifts

One of the advantages of fintech companies is their ability to pivot around changing market and customer needs very quickly. This agility, however, increases the velocity of emerging risks i.e. the speed at which a risk materializes. Smaller fintech firms may find it easier to deal with these dynamic risks, but for larger and more traditional banks, the velocity of an emerging risk is compounded by its impact and influence on the organization's existing risk universe, including risk appetites and risk measures.

To deal with these challenges, some global banks are integrating their complex, multi-faceted risk universe in a centralized framework. They are also aligning their risk events and losses to risk assessments and control evaluations. This data model helps them ensure that as a risk profile evolves, the changes are quickly captured. Meanwhile the underlying analytical capabilities enable stakeholders to identify both the direct and indirect impact of the risk.

[2] GDPR – General Data Protection Regulation

Regulatory change is another critical source of risk triggered by an increasingly dynamic financial services market. Striving to keep up with emerging fintech innovations and the resulting risks, regulators are rapidly issuing new policy guidelines, or making changes to existing compliance requirements. China, for instance, is considering a ban on cryptocurrency mining, while the US recently warned cryptocurrency exchange operators about the repercussions of not complying with regulations around the prevention of money laundering and terrorism financing.

All these developments require both fintechs and banks to stay vigilant and to implement robust regulatory compliance management systems that can automatically track regulatory changes, measure their impact on the business, and then initiate responsive action. One of the largest global banks, for instance, is using a compliance management solution to identify and respond to regulatory changes in over 67 markets.

Interestingly, regulators too are depending on compliance and risk data to drive regulatory changes in their jurisdictions. As an example, the banking regulator for one of the leading economies in South East Asia, is leveraging a risk reporting and analytics capability to aggregate risk event information from over 200 of their regulated entities, based on which the organization can determine its regulatory direction.

A New Normal

The fintech revolution will continue to reshape the global banking and financial services landscape in the years to come. Everyone—especially the end customer and even traditional banks—stand to benefit from the resulting innovation and continuous improvement, as long as risk awareness and compliance remain key priorities.

Moving the Needle on Compliance Risk Management in Financial Services

The years that followed the financial crisis were marked by a globally coordinated effort to implement stricter regulatory measures aimed at guarding the financial system against future shocks. Basel III, for instance, introduced tighter capital requirements, widened risk coverage, and stipulated leverage ratios to protect against excessive borrowing, among other requirements.

Today, however, there appears to be a gradual shift away from global regulation, as each geography implements laws or standards that are specific to their own markets, needs, and concerns. The US, for instance, is in the thick of a deregulatory drive, but in regions like Europe, regulators show no signs of slowing down with new directives like MiFID II and PSD2[1].

As regulatory agendas continue to diverge, global banks and financial services institutions face the two-fold challenge of not only juggling multiple international compliance requirements that often vary from one jurisdiction to the next, but also conforming to local regulations governing business models and operations.

Meeting the demands of this complex regulatory environment calls for a renewed approach to compliance -- one that focuses on analyzing the business impact of regulations, identifying and prioritizing the underlying compliance risks, applying mitigating controls, and monitoring the entire system consistently.

Compliance Risk Management Matters

Over the last decade, compliance risk—i.e. the potential for material loss and legal penalties arising from violations of, or non-conformance to, industry regulations, laws, and codes of conduct—has become a key concern, driven largely by a wave of record-high regulatory fines. Yet, compliance risk is more than just a regulatory issue. It's also a business one with the potential to damage organizational reputations, diminish customer trust, and limit market opportunities.

Despite these consequences, many financial institutions are lagging in their compliance risk management efforts. McKinsey research finds that most senior managers feel more comfortable with their credit-risk management than with their control of compliance risk. The reasons for this are many -- best practices for compliance risk are still emerging, few agree on the most effective organizational approach, and business ownership of the risk is weak.

Some banks, however, are changing the tide. A top Canadian bank, for instance, has found a way to strengthen the effectiveness and efficiency of their compliance risk management program. Ad hoc and siloed risk assessments have given way to standardized and integrated processes that offer stakeholders a holistic view of compliance risks across the organization. A strong foundational framework maps compliance risks to regulations, controls, processes, and internal organizations, enabling the bank to easily understand the business impact of a compliance risk. Legacy tools and manual processes have been replaced with automated workflows, while advanced analytics accelerate decision-making by drawing out meaningful insights from compliance risk data. All these changes have strengthened the bank's credibility with senior stakeholders and regulators.

[1] MiFID II - Markets in Financial Instruments Directive; PSD2 - Second Payment Services Directive

What Makes a Robust Compliance Risk Management Program?

Compliance risk management can turn into a strong driver of integrity and performance if it has the right ingredients in place. Here are a few aspects to consider:

1 Assess and Prioritize Risks

A systematic assessment of compliance risks across the enterprise enables financial institutions to clearly understand their risk exposure, including the likelihood that a particular compliance risk will occur, the reasons for its occurrence, and the extent of its impact. Risk computations also make it easier for organizations to rank and prioritize compliance risks, link them to the appropriate risk owners, choose the right approach to mitigation, and allocate resources efficiently.

A well-defined risk assessment methodology helps stakeholders understand the impact of compliance risk not just at a financial level, but also at a reputational, legal, and business impact level. Having both qualitative and quantitative risk measures in place goes a long way towards providing a nuanced picture of risk. Also of significant value is an integrated compliance data model which can provide a contextual view of risk i.e. in terms of its link with other risks, as well as controls, regulations, policies, departments, and objectives.

2 Determine the Right Controls

Once compliance risks have been assessed and ranked, the appropriate controls can be chosen to prevent or detect the risks. These controls, in turn, need to be evaluated periodically based on their design and operating effectiveness. Higher risk controls require more comprehensive and frequent evaluations, while lower risk controls may not require as much focus.

Compliance software tools can help accelerate control assessments by streamlining and automating the process. Some tools offer predefined criteria and checklists to simplify assessments, along with mechanisms to score, tabulate, and report results. Any potential risk issues or exceptions that are found can be documented in the compliance tool, post which a systematic mechanism of issue investigation and remediation can be initiated and tracked up to closure.

Many large banks, like the Canadian one mentioned earlier, are beginning to rationalize their compliance controls, thus minimizing redundancies in control testing, while also saving on the time and effort involved in compliance. Fewer and better controls improve not only risk mitigation, but also compliance monitoring and testing.

Meanwhile, some financial institutions are looking at the use of robotic process automation (RPA) in control assessments. RPA tools have the potential to minimize manual intervention, thus freeing up time for compliance managers to focus on more strategic, high-priority, and value-adding tasks.

3 Report Findings Early and Often

Compliance managers are almost always under pressure from senior stakeholders to report on the status of compliance risks and controls in as close to real time a manner as possible. Meeting these expectations can be extremely difficult given the number of departments and processes that a compliance program covers. Reporting becomes even more complex in organizations that operate across multiple countries.

Advanced reporting tools can be useful in these situations. Graphical dashboards, for instance, offer compliance managers comprehensive visibility into the compliance risk management process with aggregate reports, as well as individual status trackers. Viewers can browse both historical and real-time data on risk, including an analysis of control and risk assessment results.

These insights enable compliance managers to stay in constant touch with the ground reality and progress on their compliance risk management program. Automated alerts for events such as exceptions and failures help eliminate any surprises, and make the compliance process predictable.

Many financial institutions are also exploring the use of advanced analytics and machine learning in detecting and predicting compliance risks. With faster, better, and more in-depth risk insights, decision-makers can swiftly identify potential compliance blind spots, and address them before they snowball into bigger issues.

Looking Ahead

In an era of rapidly changing and diverging regulatory landscapes, a solid compliance risk management program is key to reducing the likelihood of compliance failures. But the program must become an integral part of day-to-day business operations, as well as a priority for the senior management and board. Sustained collaboration across the three lines of defense, coupled with well-designed and well-implemented compliance risk management processes and tools, will be integral in building financial institutions that are able to thrive in a complex, highly regulated world.

10 Insights from Non-financial Companies about Operational Risk and Resiliency

Financial services firms have put a lot of focus on operational risk over the past couple of decades – and more recently, on operational resiliency. However, some operationally complex industries have been formally managing operational risk and resiliency for decades, and so have a significant amount of experience to share about these disciplines.

At a recent MetricStream breakfast in London, risk executives – both speakers and audience members – came together to talk about the potential lessons that financial institutions could learn from organizations in other industries. Below are 10 important insights the gathering discussed during the event:

1. There is no “one size fits all” approach to managing either non-financial risks or operational resiliency.

Every organization is different, and so every op risk or resiliency framework will be as unique as the organization’s operating strategy. Certainly, standards and regulatory guidance are available as a place to start from. However, fleshing out any risk framework begins with understanding the risks the firm faces, the appetite it has to take risk, and how the organization’s strategy should align with its risk framework and appetite. If another part of the organization is charged with looking at strategy and strategic risk, it’s important to have an open dialogue with them. Also, boards, audit committees, and senior managers might have different perspectives on the impact that risks can have and the levels of resiliency required. These differing perspectives contribute to the uniqueness of the organization’s operational risk and resiliency picture

2. In making decisions around operational risks and resiliency issues, executives need to become more comfortable with ambiguity.

Operational risks cannot be measured with the same level of precision that financial risks – such as credit risk and market risk – are able to be. While this has long been viewed as a challenge within the discipline, financial firms should embrace this ambiguity, and learn to think about operational risk and resiliency differently. It’s important to understand that quantitative indicators can be helpful, but they are only indicative and not exact depictions of reality. Think about the risk framework and risk reporting as prioritization tools. They can help executives understand the relative impact a risk might have, the accountability within the organization for the risks, why the level of risk has changed, and what the new, emerging risks are. Avoid talking about financial risk and operational risk side-by-side, to side-step the common error of perceiving op risk and financial risk data as the same kind of information.

3. An operational risk framework shouldn’t be comprehensive, static.

Today’s world moves faster than ever before – technology, regulation, and other important aspects of a firm’s ecosystem are evolving at accelerating rates. Gone are the days when frameworks had to be considered comprehensive – today new risks are emerging all the time. As a result, operational risk management and resiliency teams need to be nimble, and so do their frameworks. The framework should be a set of guidelines – it does not codify a decision-making process, or provide “the answer.” It should be constantly updated and refined.

4. Risk assessment is more helpfully thought of as a spectrum

Certainly, there are times when risk should be thought of as binary – for example, when life could be at risk, or when certain ethical or regulatory standards are involved. However, the rest of the time, it’s much more useful to think about risk and resilience as being a spectrum, which organizations can dial up and down. Operational risk teams should look at operational risk and resiliency reporting they produce for the business, senior management, and the board and consider how the reporting reflects and supports the way the organization should be making strategic and tactical decisions. For example, does the reporting box executives into binary thinking about risk, or does it provoke a more nuanced exploration of non-financial risks?

5. It’s enriching to consider an operational risk from different perspectives.

It can be very easy for a group to consider a risk from a limited number of perspectives – it is a natural human response to want to be in agreement with others. To bring a diversity of perspectives into a room, think about assigning individuals the task of considering a risk from other perspectives, such as those of a customer, or a third party vendor. Encourage the individuals to share these alternative perspectives so that the whole group can gain a fuller understanding of the potential impact of a risk, and what important elements of an operational resiliency approach might be.

6. The risk framework must have buy-in from the whole organization.

The risk framework should align the board and senior executives behind it. Much is said about the importance of the “tone at the top” for achieving engagement from the whole organization. It’s all true. However, the framework must also have acceptance all the way down to the front line, customer-facing employees, and the tone from the top will only help to a point. Operational risk teams should be sure the right policies, processes, tools, and training are in place to align the whole organization with the cultural values the risk framework represents.

7. There are upsides to managing risk and resiliency well – this could unleash value for the organization.

Risk management as a discipline can often seem to focus exclusively on the “what not to do” things – how not to buy a company, how not to do a process. It’s important when talking about risk and resiliency to discuss the upsides these disciplines can create as well. Questions to ask include: What are we trying to achieve as an organization – what are our goals? How does the way we take risk reflect our strategic priorities as a business? What does managing risk and resiliency well enable the company to do? What value does it help generate? Applying these questions could help the organization see operational risk and resiliency in a new light.

8. It’s important to be mindful of replicating bias.

Organizations tend to create frameworks that reflect previous experience and actions – this is human nature. However, taking this approach – either consciously or unconsciously – can result in bias. A real-world, high-tech example of this concept is the Amazon automated CV processing gender bias incident. Amazon wanted to automate the initial stage of processing CVs for many of the roles it hires for, and so it created an artificial intelligence program that would sift through CVs. It trained the tool by feeding it past CVs as well as previous decisions about whether to take the candidate forward. When the project was done, Amazon discovered that the tool was making gender-biased decisions about candidates – because the information that had been fed into it was biased. The AI program simply magnified the level of bias that human beings were making to begin with.Organizations can be unintentionally biased in their decision-making, including decisions about risk and resiliency, and this can be hard-wired into the organization by the risk framework. Operational risk teams should be asking themselves what unintentional biases their risk framework and resiliency programs are amplifying, before they emerge as loss events.

9. Cultures where it’s OK to deliver difficult news are more risk aware and resilient.

Open and honest discussion about risks and resiliency requires individuals to be able to be candid in their views with others, particularly those in positions of authority. Organizations that “shoot the messenger,” for example, are unlikely to be places where individuals feel comfortable flagging risks or pointing out resiliency issues. Within the firm’s culture, having the ability to challenge is essential – intelligence about risk and resilience needs to flow up and down the organization fluidly. Overall, of course, the nature of the culture that a firm has is extremely important. Within financial services, accountability for culture is now being hardwired into the industry in the UK through the Senior Managers & Certification Regime (SM&CR). This is already in force for banks and has a December implementation deadline for other types of financial services firms. Other countries are considering implementing a similar regulatory approach. With individual executives now formally accountable for certain risks, a failure to be open to “bad news” that might alert an executive to potential risk could eventually have career-ending consequences.

10. Ultimately, the risk framework is about what you do with it.

It may sound cliché, but an operational risk framework really should be an ongoing journey. What it should not be is a manual that gathers dust on the shelf. The framework should come alive through the sharing of risk intelligence and having lively discussions around that intelligence. So, the operational risk team should consider carefully how it brings the risk framework to life within the organization today, to support everyone on that journey. Better risk management processes, enhanced reporting, improved communications and other steps can all contribute to a vibrant, successful culture and risk framework.

In summary, according to non-financial services organizations, a robust approach to operational risk and resiliency requires transparency, nimbleness, and imagination – among other qualities. To learn more about how MetricStream can support your organization on its operational risk and resiliency journey, please contact us at info@metricstream.com.

NORTH AMERICAN TRANSPORT GIANT STRENGTHENS CYBERSECURITY WITH IMPROVED RISK TRANSPARENCY AND RESPONSE

For one of North America's largest transport companies, the opportunity to continue serving millions of customers depends, to a large extent, on the organization's ability to manage and mitigate cyber threats. Earlier, cybersecurity was just one part of the company's larger technology and IT security program. But as the focus on cyber steadily increased, stakeholders set out to establish a dedicated cybersecurity governance, risk management, and compliance initiative.

Focused Approach to GRC

After several years of working with internal experts to manage cybersecurity requirements, the organization approached MetricStream for an integrated GRC solution. They wanted a single, unified platform that would enable them to simultaneously manage all their IT risks and IT compliance requirements.

Increased Focus on IT and Cyber Risks

Today, the MetricStream solution for IT risk management has given the organization a centralized and flexible system to manage and track various IT risks, including cybersecurity risks. It also supports a consistent risk and control vocabulary which simplifies risk communication and reporting.

Built on a common GRC platform, the solution enables a standardized, streamlined process for IT risk documentation, risk assessments, control management, issue detection, and resolution. The solution has also helped the company build clear risk governance structures with well-defined roles and risk owners across the three lines of defense.

Advanced business intelligence reports and dashboards provide an in-depth, near real-time view of IT and cybersecurity risks aligned to business risks, thus enabling senior stakeholders and board members to make faster and better-informed decisions.

In addition to the IT risk management solution, a separate exceptions management solution has been built by MetricStream to help the company raise exceptions as part of their risk assessments. Users can add a monetary value to each risk exception to understand its business impact on the company.

Challenge

- Absence of a baseline security guide to track and monitor cybersecurity risks
- Insufficient focus on IT risks

Solution

- IT risk management
- IT compliance management

Value Delivered

- Optimized overall cybersecurity investment
- Standardized classification of systems as per GRC cybersecurity definitions
- Simplified the risk taxonomy across the enterprise
- Improved visibility into top risks across the three lines of defense
- Helped link cybersecurity risks to business risks for faster decision making

Federated IT Compliance

Using the MetricStream solution for IT compliance management has made it easier for the company to handle and track compliance with various IT and cybersecurity regulations and standards. The solution supports the process of scheduling assessments, automating them, and performing control tests based on specific company procedures.

It also enables a federated approach to IT compliance management through which the company can link IT compliance controls and assessment activities according to specific regulatory requirements. Alerts, notifications, and updates on IT regulatory content, as well as actionable insights from various online sources, are delivered on an automated basis.

The solution provides comprehensive visibility into the IT compliance process through a built-in reporting and dashboard engine.

In addition to a range of standard reports, MetricStream has built a detailed "security book" report for the company which offers a complete snapshot of the cyber-risk posture of each business asset.

Extending the Maturity of GRC

The company now plans to continue their GRC journey with MetricStream by extending their GRC platform to include new solutions for third-party management, as well as policy and document management. The former will enable the company to efficiently identify, assess, mitigate, and monitor IT vendor risks, while also managing vendor compliance. The latter will help the company map their policies to regulations, risks, and controls, thus making it easier for users to identify and close compliance gaps or deficiencies proactively.

MULTINATIONAL OIL AND GAS COMPANY FORTIFIES INTERNAL CONTROL SYSTEMS WITH EFFICIENT, RISK-BASED AUDITS

As the third line of defense in one of the largest oil and gas companies in the world, the internal audit organization has a challenging responsibility -- to ensure that controls across multiple global locations are sufficient and working as expected, while also calling out potential risks and areas of opportunity that could impact business performance.

In the past, these requirements were managed in a largely ad hoc and siloed manner. Each stage of the audit was enabled by a different tool providing different workflows and capabilities. Without a unifying framework to connect these systems, the organization faced several issues related to audit productivity and transparency.

Looking for a solution, they found one in MetricStream's integrated audit management system which facilitates a cohesive, collaborative, and streamlined approach to internal auditing.

A Look Back

Before MetricStream, the audit organization had a well-defined global internal audit program. However, they also had three different systems to manage their audit processes. The lack of integration between these systems resulted in inconsistencies between audit teams, as well as duplication of work, limited visibility into audit progress, and process inefficiencies.

Adding to these challenges was the sheer scope of the audit program. Audit teams often had to juggle assignments across multiple onshore and offshore locations throughout the world. In total, there were 1,000 auditable entities and more than 20 global audit divisions that had to be managed.

To bring some measure of efficiency to this effort, the organization decided to implement an integrated internal audit management system. Their objective was to manage the entire audit lifecycle from a single platform instead of several, disintegrated tools. The system they chose would have to improve visibility into global audit operations, while enhancing collaboration across audit teams. It would also need to enable a risk-based approach to auditing, and in the long run, evolve beyond current audit needs, to meet future requirements.

After evaluating various technology providers, the organization decided to implement the MetricStream solution for audit management which, they believed, would address their specific requirements —particularly the need for a unified, consistent, and efficient approach to internal auditing.

Structured, Standardized Auditing

Today, the MetricStream solution acts as the backbone of the organization's internal audit function, providing a single, integrated foundation on which to manage global audit operations. The solution facilitates a systematic, structured approach to audit processes, thereby minimizing duplication of effort and data. It also simplifies information-sharing between audit teams and auditees.

With well-defined workflows, as well as automatic notifications and alerts, the internal audit team can perform their activities and tasks in a streamlined, collaborative manner – including audit planning and scheduling, risk assessments, workpaper management, time management, audit reporting, recommendations management, and follow-ups.

Challenge

- Multiple audit tools with no integration between them
- Lack of standardization and consistency in audit processes
- Limited visibility into audit plans, status, or progress at an enterprise level

Solution

- Audit management

Value Delivered

- Replaced three siloed audit systems with a single, unified solution
- Streamlined audits for improved consistency and efficiency
- Enabled focused, risk-based audit planning along with optimal resource allocation
- Accelerated field audits with offline auditing capabilities
- Delivered real-time insights into audit issues and processes for informed decision-making

Targeted, Risk-Based Audit Planning and Execution

Considering the number of audits that need to be conducted for 1,000+ auditable entities, the organization has to ensure that they're focusing on the highest areas of risk first. Using the solution, audit teams can view all the risks associated with each auditable entity. They can then develop targeted audit plans and schedules that prioritize audit resources towards key risk areas, thereby improving overall audit effectiveness.

Optimal Audit Resource Allocation

Given that the organization's auditors often have to travel for onsite audits, their schedules and tasks need to be planned and prepared much in advance—sometimes even a year ahead—to ensure appropriate allocation of resources.

Earlier, this was difficult to achieve because the audit organization didn't have sufficient visibility into their global pool of teams and resources. However, with the MetricStream solution, the organization can now plan their resources better, managing 200+ auditors across various regions.

Budgets and teams are optimally allocated for each auditable entity, following which detailed tasks are scheduled and assigned. Thus, the solution increases overall audit productivity. It also enables audit managers to continuously monitor the status of each audit.

Swift, Efficient Audit Fieldwork

Due to both onshore and offshore auditing requirements, auditors often end up working in remote locations with limited or no connectivity to the corporate network. Many times, they have to respond to data requirements at an offsite contractor or vendor location, as well as airports or airplanes. In such situations, they need access to relevant documentation – which the MetricStream solution provides.

Using the solution's offline briefcase capability, auditors can easily perform their tasks offline, while also accessing the required forms, workpapers, and documents. The data entered into their systems can be synched with the main database later. This approach has given them the flexibility to record audit evidence accurately and quickly wherever they are, while preventing data loss. Additional solution capabilities such as mass reassignment and approval of workpapers have further accelerated audit task performance.

Complete Audit Transparency

Through the solution's real-time audit status reports and dashboards, audit managers can closely monitor the progress of audit projects across the organization, while gaining a consolidated view of the global audit program.

The solution delivers 400+ reports with deep insights into various audit stages and activities, as well as issues and risks at multiple levels of the organization. This comprehensive information enables the audit organization to plan effective and timely recommendations ahead of time which can then be communicated to the senior management and board.