CELENT

the answer company™
THOMSON REUTERS®

ACHIEVING INTEGRATED GRC IN AN INTERCONNECTED DIGITAL AGE

Cubillas Ding and Neil Katkov, PhD
27 March 2018

OLIVER WYMAN

CONTENTS

EXECUTIVE SUMMARY

KEY RESEARCH QUESTIONS

1 *What are the main challenges facing risk and compliance offices today?*

2 *What are the limitations of current approaches to governance, risk and compliance (GRC?)*

3 *What capabilities are needed to support a next-generation, integrated GRC paradigm?*

The environment for financial institutions is rapidly changing and becoming more complex, not only due to the impact of regulation, but also from ongoing organizational reconfiguration efforts. There are, moreover, amplified risks resulting from technology disruptions and threats associated with firms embracing digital technologies and changing how they go-to-market in the so-called “digital world”.

With intense regulatory scrutiny around strong governance and sound internal controls on both group-level and ring-fenced subsidiaries, firms are compelled to accelerate their efforts to address the ongoing shortcomings associated with the three lines of defense control activities, including lack of overall governance, insufficient first line accountability, insufficient coordination of control functions and new investments in next-generation risk management tools and data.

Celent undertook in-depth interviews with close to 30 Tier 1 financial institutions globally to better understand the challenges facing risk and compliance executives, as well as the technology improvements that are needed to support an integrated GRC paradigm to overcome these issues.

Risk and compliance executives expect to see real benefits from digital technologies, such as big data, artificial intelligence (AI) and machine learning, and even distributed ledger technology (blockchain) to bring measurable increases in efficiency to risk management operations. At the same time, many firms are facing challenges in moving toward the future. At a fundamental level, risk operations are having trouble developing agile capabilities and continue to be hampered by inflexible technology. In our interviews, study participants offered their strategic wish-list of requirements for a fit-for-purpose, integrated risk ecosystem. These requirements fall into five key areas:

- *Information & data congruence*: Applications employed to capture and report information for various risk assessments and controls management activities, such as risk control self-assessments (RCSAs), key risk indicators (KRIs), risk appetite parameters and loss events. These should be connected, aligned and congruent with a firm’s taxonomy and framework.
- *Adaptability*: Flexible, business-user centric capabilities to respond to evolving requirements, without the need for protracted cycles of IT development, coding and testing.
- *Rich visualization, usability and collaboration*: Next-generation platforms should possess the ability to quickly analyse, chart and exchange operational and risk-related insights based on modern and intuitive user interfaces.

- *Dynamic, event-centric and timely*: Ability to support multiple modes of operation, including triggering by events and operating in near-real time in order to monitor and report on the state of affairs in a firm's risk profile in a dynamic manner.
- *Open and seamless co-existence*: Platform should be open and extensible enough to connect and co-exist with other non-risk IT applications (HR, sales, security) using modular, flexible interfacing mechanisms.

In the years ahead, the various lines of defense with responsibilities for risk management and control must think of their next-generation risk platforms as being a technology-enabled business ecosystem that acts more like a central nervous system — one that governs the health of an organization through responsive two-way feedback and risk mitigation mechanisms, yet (as required) can be managed and operated in a decentralized way by various stakeholders and end-users.

Firms must execute to ambitions to govern well and operate resiliently not merely because they "have to" under regulatory compulsion, but rather because they "want to" since it makes good business sense. This will increasingly differentiate winners from losers.

KEEPING PACE WITH BUSINESS DYNAMICS, REGULATORY CHANGES AND EMERGING RISKS

The environment for financial institutions is rapidly changing and becoming more complex, not only due to the impact of regulation, but also from ongoing organizational reconfiguration efforts. There are, moreover, amplified risks resulting from technology disruptions and threats associated with firms embracing digital technologies and changing how they go-to-market in the so-called "digital world".

Key Research Question 1

What are the main challenges facing risk and compliance offices today?

CROs continue to face the mainstay factors of regulatory scrutiny and cost pressures. At the same time, they must navigate new operating models such as business modularization, as well as the changes and risks wrought by digitization.

THE AGENDA OF THE RISK AND COMPLIANCE OFFICE

Taking a big picture view of the themes that are impacting risk and compliance functions, we see mainstay factors that will continue to exert pressures on firms, primarily the twin poles of regulatory requirements and cost pressures. At the same time, emerging trends such as digitization are increasingly shaping the CRO's agenda.

- In terms of the mainstay factors, there continues to be a heavy regulatory environment. Despite the US administration promising to cut red tape and new regulation, the existing pipeline of regulations still weighs heavily on financial institutions in various areas related to capital, margining and other areas. Supervisors, not surprisingly, have paid considerable attention to financial institutions' risk and control environment. There is also an increasing focus on transparency, investor/ client protection, conduct risk and more granular reporting. In addition, regulators continue to focus on thematic areas such as risk culture, model risk and cyber.

  For the foreseeable future, we expect these regulation-induced activities to continue in those areas where supervisory pressures remain, therefore requiring risk and compliance functions to sustain high levels of spending and resourcing in order to meet these ongoing obligations.

- At the same time, from a cost perspective, risk and control functions are not shielded from ongoing cost pressures (especially with significant amounts of dollars already spent). We see continued expectations to "do more with less;" for example, to use improvements in data and process infrastructure for value added business activities such as budgeting, forecasting, and scenario planning.

"Firms do a lot of talk about enterprise risk, but it has only grown in the last five years. Businesses now get it because the regulators are now taking a more active look at a ring-fenced organization's enterprise risk & governance framework, and the heads of businesses are now being exposed to regulatory calls."

Director, Head of Compliance, US IHC, Global European Universal Bank

Regulatory and cost pressures are ineluctable and will not go away anytime soon. On the other hand there are likely to be opportunities for firms to differentiate themselves competitively as they develop risk frameworks to handle new digital business models and emerging technology ris*ks.*

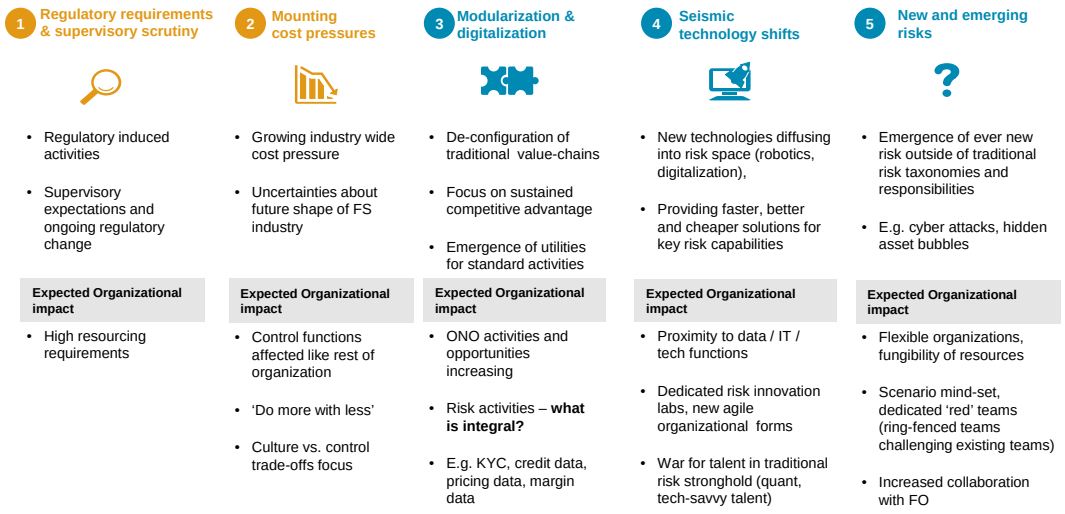
- Business modularization: As they focus on sustained competitive advantage, banks are rethinking what it means to be flexible and agile through the reconfiguration of their current value chains. Traditional activities, previously viewed as integral, are being re-examined, with industry utilities emerging to take on some functions; for example, corporate data collection for KYC purposes.

"We have a variety of legacy enterprise risk management tools that were internally designed to collect inputs for Basel AMA operational risk capital calculation, less for monitoring and managing risk. The biggest challenge is to get integrated reporting quickly, breaking it down to the many businesses to track ongoing trends. With an organization of our size, the question is how do we do it most efficiently?"

Head of Operational Risk Management, European Subsidiary of Global Bank

- Current shifts in technology and the thrust towards digitization are resulting in new and emerging risks outside of traditional risk taxonomies, such as cyber-attacks and hidden asset bubbles. These new risks are not necessarily quantifiable, or may not fall under current risk management remits.

Figure 1: The CRO Agenda of Keeping Up with Business and Regulatory Change



Source: Celent

As regulatory and cost pressures mount and the business environment continue to evolve, new digital technologies are diffusing into the risk space to provide faster, better and cheaper solutions for key risk capabilities. These technologies include robotic process automation (RPA), big data, advanced analytics, and AI.

These traditional and emerging themes are having a significant organizational impact on financial institutions:

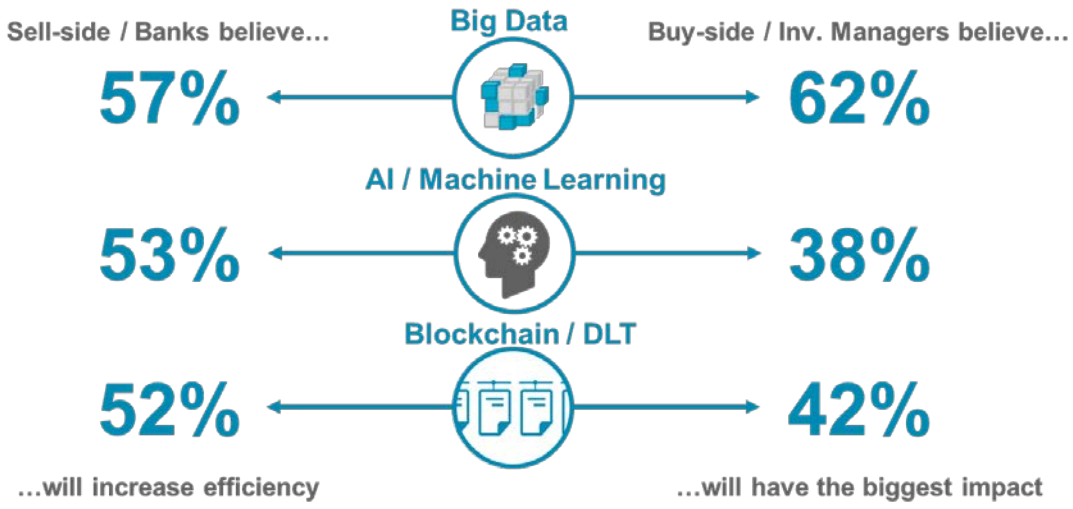
- Ongoing regulation and supervisory scrutiny continue to place high resourcing requirements on firms.
- The pressure to reduce cost is affecting control functions as it does the rest of the organization, placing the risk and compliance office in the position of having to "do more with less."
- Business modularization is making the risk office reassess what risk activities are truly integral to the firm (and which can be outsourced) among, for example, credit data, pricing data, margin data, and KYC data.
- To keep up with new and emerging risks requires organizations to be agile and flexible, with some firms setting up ring-fenced "challenger" teams to spearhead innovative approaches.

The complex and evolving factors driving the risk and compliance agenda is inevitably leading risk officers to seek new approaches and technologies upon which to anchor non-financial risk management and controls to cope with the "mainstay" challenges, new business models and emerging risks.

Navigating Change: Business-as-Usual Change vs. Disruptive Inflection Points

Financial firms, indeed, appear poised to leverage emerging technologies to pursue next generation, digital operating models for risk management. Risk professionals are following the trends closely. Already, some areas of operational risk, such as anti-money laundering (AML) operations, are enlisting big data analysis techniques and conducting proof-of-concept trials to insert AI tools into the AML/KYC value chain.

Figure 2: Digital Tools for Risk Management: Ripe for Change



Source: AFP/ Oliver Wyman 2018 survey, Celent Buyside 2017 survey

Risk and compliance executives expect to see real benefits from digital technologies. A majority of sell-side organizations, commercial banks and asset management firms surveyed recently expect big data, AI and machine learning, and even distributed ledger technology (blockchain) to bring measurable increases in efficiency to risk management operations.

- Risk managers see the explosion, as well as the exploitation, of data using big data technologies impacting or improving how they manage risk.
- Many believe the use of AI and machine learning (that is, cognitive AI and learning-based AI algorithms) will change the way risks are managed and/or how risks manifest themselves.
- Distributed ledger technology is seen as potentially increasing the efficiency of managing risks, through its inherent ability to replicate data records within the firm and across enterprise boundaries in a secure and almost instantaneous manner.

"Big banks like ourselves, if we do not move quickly enough, we are dead. Compared to start-up banks, we have existing mindsets and infrastructures that limit us. We officially claim to be doing Agile methods and it's fashionable, but I see no sign of it."

Director, Operational Risk,
Leading Regional Banking Group

At the same time, many firms are facing challenges in moving towards the future. The majority of firms are only beginning to scratch the surface, especially in the context of risk management and control functions.

At a fundamental level, risk operations are having trouble developing agile capabilities and continue to be hampered by inflexible technology with few value-added features. The disjunction between the potential of digital technologies and agile approaches on the one hand, and the current reality of entrenched operations and slow technology on the other, is increasingly clear to risk and compliance offices.

Risk organizations continue to face the hard pains and pressures associated with operating in a fast changing, yet highly regulated environment — one that demands various risk and control groups within the institution develop the ability to deliver new changes in a responsive manner, against a backdrop of existing workloads and efficiency demands of their day-to-day functions. As a director of operational risk at a leading regional banking group put it, speaking of the technology and operational challenges posed by digital technologies, "Big banks like ourselves, if we do not move quickly enough, we are dead."

EXAMINING ISSUES AND FOCUS AREAS IN ENTERPRISE-WIDE GRC

Key Research Question

2

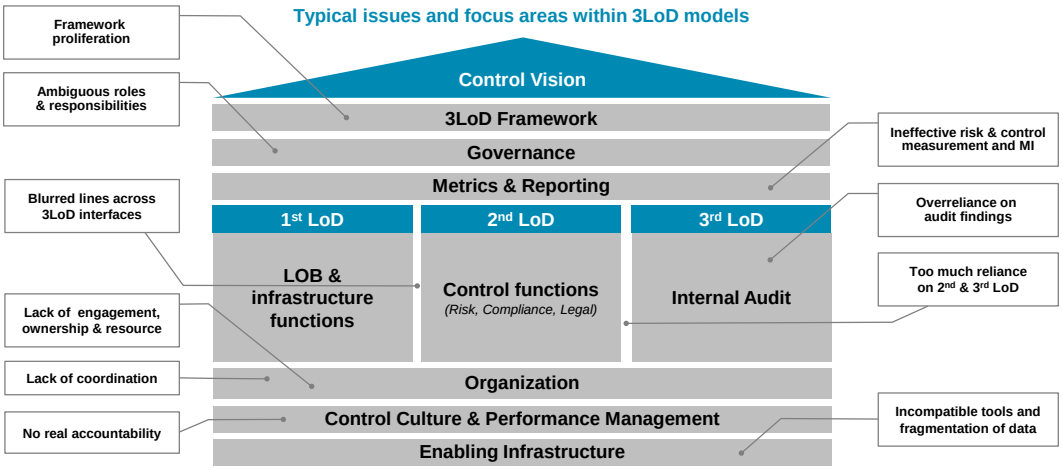
What are the limitations of current approaches to governance, risk and compliance (GRC?)

The industry standard paradigm of the Three Lines of Defense faces a number of implementation shortcomings, including a proliferation of frameworks, ambiguous roles and responsibilities, and ineffective management information reporting. GRC platforms are limited in their capacity to provide timely, accurate data and analytics, to support integrated reporting and model management, or to align with a financial institution's organizational and operational frameworks.

THREE LINES OF DEFENSE FRAMEWORK IMPLEMENTATION

The Three Lines of Defense (3LoD) approach is the industry standard paradigm for governance, risk and compliance (GRC). Financial institutions, however, still face shortcomings when implementing 3LoD models, including lack of overall governance, insufficient first line accountability, and insufficient coordination of control functions.

Figure 3: Typical Key Issues and Focus Areas for 3LOD Models



Source: Celent

These continuing issues are an impediment to firms seeking to update their risk operations to cope with the broader business, environmental, and technology changes. Firms need to address the ongoing shortcomings associated with three lines of defense control activities not because the model does not work, but because actual implementations at present still leave more to be desired.

- *Proliferation of frameworks*. The pace of change from different regulatory regimes with tight delivery pressures has led firms to develop specialist frameworks for areas

such as cyber risk, conduct risk, and model risk. These frameworks may not necessarily be meaningfully aligned with operational risk and audit building blocks, which then create further proliferation of disjointed frameworks.

- *Ambiguous roles and responsibilities*. Blurred roles and responsibilities within governance reduce efficacy, while at the same time compounding the shortcomings of inadequate first line ownership of and accountability for risks.

  Institutions need to evolve from merely executing tick-the-box exercises that carry limited accountability for the management of risks, to addressing cultural and organizational challenges to get the first line of defense (front office) to *"walk the walk"* rather than merely *"talking the talk"*. Firms have moved forward in terms of senior frontline executives having more "skin in the game" from a risk and control perspective, but there is still some way to go.

TOOLS, DATA AND RISK REPORTING

- *Ineffective management information reporting (MI)*. This can stem from ineffective design of MI, whether with too much or too little detail, that lacks meaningful "so what" analysis linked to risk appetite.

- The report production process can also be overly cumbersome and manual due to incompatible tools and fragmented risk data taxonomies across disparate toolsets, such as spreadsheets and governance, risk and compliance (GRC) applications.

"Our 1500+ live users detest our current GRC platform. It has a user interface which is dated, poor; user experience is dreadful, management of data objects weak with data validation issues, and it's painful to retrofit. It is a deterrent to shaping a stronger risk culture and perception of being in control of our control environment."

ORM Director,
Regional UK Bank

- As an influencer and advisor, the second line of defense, particularly operational risk roles, need timely, accurate data and analytics to be able to play their roles more effectively. Operational risk and non-financial risk managers tend to be profoundly dissatisfied with their incumbent systems. There often isn't an integrated or connected way of running the needed analysis or report, or of managing models. Even if the system is capable of delivering the needed functionality, it takes too long or requires significant changes to the system. Having tools that cannot meaningfully connect and analyze data is seen as a big impediment to achieving risk and governance goals.

"At the moment, we build our ORM system in-house but it is not integrated and we are facing issues here. All our metrics are a hodgepodge of items and there is too much information. I see a lot of risk data mapping & consolidation, cleaning up of policies/ procedures, and 'risk appetite on a page' type activities. But what else can be done? The "so what" question is not there. I do not see information being used – e.g. in order to understand correlations with other types of (financial) risks and linking it to economic capital. I do not see anyone exploring that and is what I believe is missing in the industry."

Senior Manager, Financial Markets Operational Risk,
International Bank, Asia division

MODEL RISK MANAGEMENT

Model risk management is one area where Tier 1 banks have been putting effort into aligning and integrating specific risk functions within a firmwide control framework. At the same time, platform support for integrated management of models across risk is limited.

In the area of financial crime, for example, the risk may be owned by the lines of business (for example, retail and corporate banking and capital markets), while oversight is performed by a central control function. Financial crime risk models at large banks are becoming more sophisticated, employing regression models and other advanced analytic techniques, which has led some banks to integrate risk model activities for financial crime with the central risk function. In this way, shared resources might support areas such as model development and validation across non-financial and financial risk functions.

At the same time, model management remains the responsibility of the line function. Model management platforms are often employed on a siloed basis, leading to redundancy of these systems across risk functions. Approval procedures for models may also be fragmented even within silos, with different model types requiring separate line approvals. Platform support for managing such processes is typically limited and highly manual.

In this way, while banks are making progress in aligning controls for various risk functions at a high level, coordination relies on largely manual processes and system support is often limited. In high—profile, high-risk areas such as financial crime, risk analytics managers are seeking solutions to increase efficiencies and support integrated model risk management processes.

ANTICIPATING AND PREPARING FOR THE FUTURE

STRATEGIC CAPABILITIES, TRENDS AND CHANGING PARADIGMS

With governance, risk, and compliance, there is no one-size fits all. It entails a journey where firms need to examine where they are, their own ambitions, the complexity of their business and operations, global commonalities and regional/local regulator expectations, as well as the scope and velocity of risk factors that they are exposed to. In the years ahead, in order to deliver further value to the business, we expect the scope and characteristics of three lines of defense functions to evolve as follows:

- Firms will increasingly be expected to demonstrate "one view" of their risk profile and control management activities, yet granular enough to have "sharper sub-views" into different ring-fenced/legal entities, business units, geography and processes.

- Streamlined, coordinated efforts between the 1st LoD and control groups (operational risk, aligned with other risk groups, as well as audit and compliance functions) will be a key focus.

- Non-financial risk and control applications will evolve to more flexibly deliver the provision of specific and customized operational intelligence, with a strong line of business “flavour”.

- Operational risk, control managers and compliance staff will need to play a key role to promote awareness and champion the development of risk culture and robust management practices at all levels.

- Personnel will need to move “closer to the front” with a sharper understanding of business unit processes and nuances. 2nd and 3rd LoD staff will also need to develop sharper consulting competencies and play roles as “advisors” to proactively avoid threats within specific business domains, support various aspects of non-financial risk and compliance operations improvement efforts, and reduce risk capital charges.

“The most effective 2nd lines are those that challenge the frontline well, at the same time, can subject themselves to practical business considerations, but yet help guide business decision-making based on credible data.”

Director, Head of Compliance & Operational Risk,
US IHC, Global European Universal Bank

- In order to gain credibility with stakeholders within the various lines of business and divisions, operational risk personnel will need to understand the business and move beyond merely the “people with the risk tools, techniques and methodologies” to “strategic partners who know my business and can add value to my decisions.”

- IT applications and tools (GRC/ORM/ERM) will need to evolve to drive measurable and value-based operational improvement decisions across the business.

Aligning Risk Platform Requirements With Regulatory and Business Realities

Key Research Question 3

What capabilities are needed to support a next-generation, integrated GRC paradigm?

A fit-for-purpose, integrated risk platform should be flexible and agile; support information and data congruence; provide rich visualization and usability; promote collaboration and seamless integration with **ecosystems**; and deliver dynamic, event-driven, and timely insights.

The preceding section explored how proliferation of frameworks, blurred roles, and fragmented data and technology pose challenges to firms seeking to modernize their non-financial risk management infrastructure and operations. Establishing integrated risk management and controls are key to meeting these challenges, ideally supported by a flexible, integrated risk platform. Study participants offered their wish-list of requirements for a fit-for-purpose, integrated risk infrastructure, which fall generally into five areas.

1  Information and Data Congruence

Applications employed to capture and report information for various risk assessments and controls management activities, such as RCSAs, KRIs, risk appetite parameters and loss events. These should be connected, aligned and congruent with a firm's taxonomy and framework. While this may seem an obvious point, many firms have yet to achieve coordinating their risk activities with the business in this manner.

Considerations: *To what degree are elements of the risk framework, taxonomy and assessments aligned from an information and reporting standpoint (without unnecessary data replication and massaging)?*

2  Adaptability

A platform should have the flexibility to respond to evolving requirements, without the need for protracted cycles of IT development, coding and testing. This could also help alleviate the challenge many firms have of prioritizing IT resources for risk and compliance programs.

Considerations: *How easily can the apps and 'processing engines' be adapted to fit data, validation and process nuances of different units, geos and control groups? To what extent can customization be achieved without IT code-based changes?*

3  RICH VISUALIZATION, USABILITY AND COLLABORATION

Next generation platforms should possess the ability to quickly analyse, chart and exchange operational and risk-related insights based on modern and intuitive user interfaces; again without the need for extensive programming and data reformatting.

Considerations: *How rich are the facilities for analysis and insight generation in terms of usability, visualization, data lineage and analytical capabilities? To what degree is the user experience intuitive, collaborative and touch-point agnostic?*

4  DYNAMIC, EVENT-CENTRIC AND TIMELY

The underlying architecture of the platform should support multiple modes of operation. This includes triggering by events and operating in near-real time in order to monitor and report on the state of affairs in a firm's risk profile in a dynamic manner.

Considerations: *To what degree can the underlying architecture and apps 'throttle' in different modes — on demand, near real-time and responsive to events — related to data ingestion, processing and delivery?*

5  OPEN AND SEAMLESS CO-EXISTENCE

Due to the broad nature of non-financial risk management, platforms should not be confined to the boundaries of risk and control information. The platform should be open and extensible enough to connect and co-exist with other non-risk IT applications (HR, sales, security) using modular, flexible interfacing mechanisms. This final point is important as risk and control functions are increasingly expected to connect risk- and control-related insights, with broader business/organizational information in order to add value to the front line.

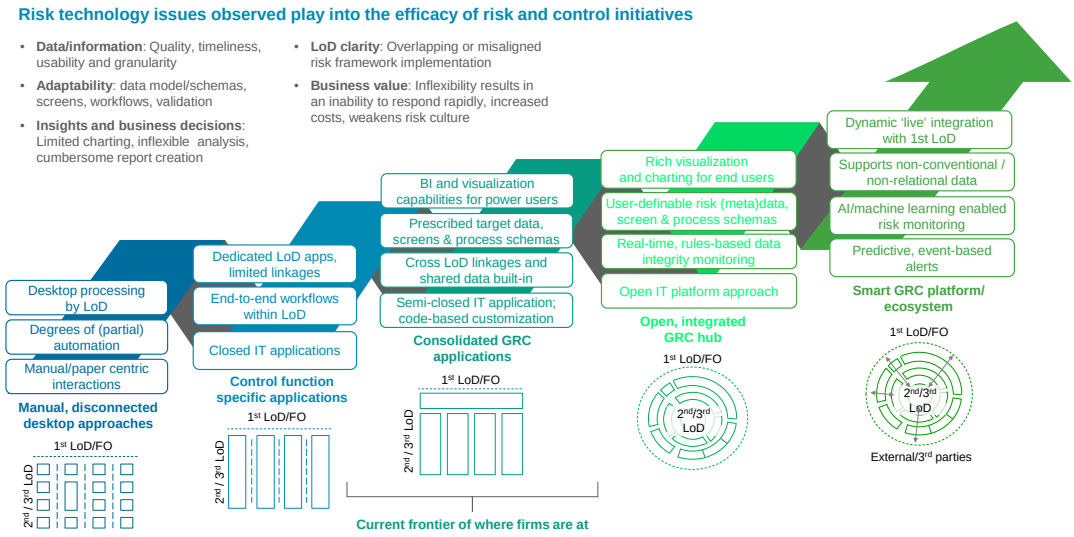
Considerations: *How can the new platform blend and co-exist seamlessly with what we have, rather than rip and replace? To what extent does it support modern agile/modular mechanisms of app-to-app interfacing to ensure future-readiness?*

In many of our conversations, firms were candid about the fact that there is much work to do. Common challenges around the technology for integrated risk and controls reflect the need for the modernization of non-financial risk management infrastructure. At the same time, there is also a sense of a growing momentum for change in the *years* ahead.

CURRENT STATE OF THE INDUSTRY

It is clear that financial firms see the value in integrated risk management. What is the current state, and what advancements can be expected over the next three to five years?

Figure 4: Steps towards Best Practice in Integrated GRC



Source: Celent analysis

Governance, risk and compliance operations were at their start characterized by **manual, disconnected desktop approaches**. Desktop work implies fragmentation of processes, and in this model controls were siloed by functional risk area, and processes were divided according to the three lines of defense. Automation was limited and interactions were dominated by manual and paper-centric activities.

"In the course of employing different commercial ORM systems, I have found them to be typically inflexible (for things such as screen customization, report creation, data manipulation). One often has to trade-off between functionality-rich solutions that are based on legacy technology, vs. the newer ones that are more flexible and fast, yet lacks coverage"

Director - Risk Management, Top 10 Global Bank

The next stage saw the emergence of **applications to support specific risk and control functions**. These solutions established end-to-end line of defense workflows within each silo, but tended to be closed applications with limited linkages across GRC domains and with the front office (first line of defense).

At present, the industry is dominated by **consolidated GRC applications**. Although applications may be built on somewhat dated technologies, these solutions have the ambitious goal of providing an enterprise-wide platform to support shared data and processes across the various non-financial risk and control functions, as well as across the three lines of defense. GRC platforms are based on prescribed target data, screens and process schemas (workflows). Business intelligence (BI) and visualization capabilities provide power users with a cross-functional view of risks, controls, and performance metrics. GRC platforms can be customized to align with the needs and

frameworks of the firm, but this typically requires modification of the code and prolonged testing cycles before being moved into production.

The current state of the art is aimed at further realizing the vision of enterprise GRC by overcoming the limitations of incumbent platforms through an **open, integrated GRC hub**. This platform supports real-time, rules-based monitoring of data and models, enabling an integrated, dynamic approach to managing risk and controls across functional areas and lines of defense. User-definable risk data and metadata, user-configurable screens and workflows, and rich visualization and charting capabilities provide the agility that is often lacking in incumbent systems.

"With digital trends, there are lots of potential to enhance what we do, especially to access and exploit data through data warehouses, Big Data tools. At the moment, our data is relatively siloed. This slows down reporting and decision-making processes, devalues ORM; and encourages decision-makers to commit to decisions based on gut feel, or based on singular dimensions of value"

VP, Internal Audit Manager,
Global Corporate and Investment Bank

The next stage of development will leverage digital technologies to increase automation of processes and deliver enhanced insights. **Smart GRC platforms** will apply AI and machine learning to a spectrum of data sources including non-conventional and non-relational data to risk monitoring and generate predictive, event-based alerts. These extensible and agile platforms will enable dynamic, live integration with the front office (first line of defense) as well as a growing ecosystem of third party services.

IMPLEMENTATION CONSIDERATIONS

When considering next-generation capabilities, firms need to enhance and/or rationalize their risk data and systems, guided by a cohesive vision that explicitly aligns business and risk management priorities, risk appetite statements, and a converged framework — one that enables a risk management and its ecosystem capabilities to be extended tactically in parts towards a strategic whole.

- **Evolve towards an integrated GRC framework and platform capabilities**. Different firms are at varying levels of maturity and approaches differ for GRC activities. Financial firms looking to centralize risk and controls across the organization need to examine next-generation solutions that demonstrate a cohesive "one platform" capability based on modern architectural components. Alternatively, for financial firms that have made investments in separate GRC tools/applications, it may make sense to implement a top-down governance dashboard layer that can integrate data from (disparate) GRC tools and applications. With the latter, underlying GRC data definitions and taxonomies are likely to differ, and firms will need to ensure an appropriate level of uniformity such that information can be interpreted consistently and quality of data is high.

- **Underlying architectural components and data model flexibility and responsiveness are key strategic capabilities**. Modern "digital' systems are often built on technologies that can support iterative, agile methodologies. Whether financial firms are procuring third party solutions or designing their own, they should look towards modern architectural and data models that can be designed and deployed with *"as little IT programming as possible"*. Any customization related to new risk data elements, screens, data capture/validation, data portability and risk process workflows should not involve protracted cycles of IT development, coding & testing.

  The system should be able to adapt to the organization's evolving framework, rather than needing the organization to conform rigidly to the system's way of operating. There are typically trade-offs between functionality-rich, legacy solutions that are based on less flexible technology; compared to newer platforms that are more flexible and fast, yet lack "out of the box" coverage. We would argue that the latter category is becoming more important, given regulatory nuances and fast changing business and integration requirements.

  "Having multiple systems without a centralized tool is not an optimal solution at all. We have to urgently improve our technology to support activities like for RCSAs and loss events — it's currently difficult to extract and manipulate data to create charts and lists and monitor trends. It's not user friendly and not adaptable to local realities without extensive customization."

  Senior VP, Operational Risk Management
  US IHC, Global European Bank

- **Adopt a flexible, component-based integration strategy**. As the remit for GRC ecosystems is expected to broaden, a component-based middleware and integration layer to cohesively integrate data and connect to upstream and downstream systems will be paramount. GRC solutions have the opportunity to be the "operations control and monitoring" hub in a federated model if the architectural foundations are right. Firms must insist that their vendors and internal solutions adopt a strategy to expand off-the-shelf component adapters and where possible, employ open / microservice-based interfacing to external systems.

- **User experience of applications should be "digital app-like", intuitive and interactive**. Given GRC's mandate to facilitate cultural change and information sharing across various business units and divisions, GRC applications can benefit from user interfaces that have social media, digitally-oriented features around information sharing, connecting, and collaboration. Service providers and financial firms can build communities of GRC groups around domain and content areas between front office, product control, and risk groups, where people can follow/share information, add their own tags and comments to "personalized versions" of the reports they are following, set individual "limit triggers" (beyond the firm's formal limits), etc.

"I have been following our internal initiatives that are using data lakes and clever machine learning tools to bring data from various channels (incorporating information from human resource systems, chat data, security logs) to monitor and detect inappropriate conduct. I see this as an opportunity for my group to potentially follow a similar path to be able to link, correlate and analyse multiple, diverse data sets. However, unlike technology firms, banks nowadays are not necessarily cash rich and purse strings are tight. To get something working as sexy as an iPhone takes a lot of investment"

Head of Operational Risk, Australian Bank

- **Experiment, infuse and use Big Data paradigms selectively as required**. Underlying Big Data technologies around machine learning and unstructured data will add another dimension to activities within operational risk, compliance, and reputational and audit management, especially if processing involves unstructured documents. These technologies enable firms to better monitor and automate information within unstructured data sets, as well as gather timely intelligence around emerging risk factors.

From a technology standpoint, real "innovation stories" that we expect to play out in the coming years are not necessarily tied to individual technologies alone. Real breakthroughs come by collectively integrating and employing an ecosystem of technologies to enable a firm to effectively join up, analyze, and more importantly, act in a timely manner to prevent and mitigate vulnerabilities.

A true integrated approach for managing operational risk, control, and compliance is one that is unified across business entities, risk types and regulatory mandates. The emerging best practice here is for integrated GRC applications to be positioned as a key component of a "dynamic ecosystem" with responsive alerting mechanisms, supported by timely information exchanges with upstream and downstream systems and a rapid delivery of analytics. This will mean that firms will need to "design in" measures and application capabilities that support cultural and conduct change.

"The industry is focused on framework components that are seen to be mandatory in order to keep regulators satisfied, and this can translate into a tick-box compliance exercise, all of which do not necessarily add value to managing the risks that we face. We are looking to do something different.
In our organization, my concern is that too many resources are focused on bottom-level risks, the 'small stuff' – whereas not enough on the material risks that will actually kill you. Currently, 90% of my resources are focused on low-level risks whilst only 10% on top risks. I would rather it be the other way round."

Chief Risk Officer, Global Japanese Bank

CONCLUSION

In the years ahead, we expect risk management approaches and industry practices to evolve from a paradigm of fragmented frameworks, tools and data to one of greater cohesion. Integrated risk management is no longer just a “nice to have”. With intense regulatory scrutiny around strong governance and sound internal controls on both group-level and ring-fenced subsidiaries, firms are compelled to accelerate their efforts to address the ongoing shortcomings associated with the three lines of defense control activities, including greater investments in next-generation risk management tools and data. However, based on our conversations with financial institutions, it is evident that there is still much work to do in adopting a more integrated approach to risk, especially for non-financial risk and controls management.

The various lines of defense with responsibilities for risk management and control must think of their next-generation risk platforms as being a technology-enabled business ecosystem that acts more like a central nervous system — one that governs the health of an organization through responsive two-way feedback and risk mitigation mechanisms, yet (as required) can be managed and operated in a decentralized way by various stakeholders and end-users.

Given the continued pace of innovation around digital financial services and emerging technologies, what seems like a far-fetched vision could be closer than we think. The limiting factor, however, could be implementation and execution capabilities within financial firms to invest appropriately to strengthen various lines of defenses within the GRC ecosystem.

Firms must execute to ambitions to govern well and operate resiliently not merely because they “have to” under regulatory compulsion, but rather because they “want to” since it makes good business sense. This will increasingly differentiate winners from losers.

Was this report useful to you? Please send any comments, questions, or suggestions for upcoming research topics to info@celent.com.

APPENDIX

ACKNOWLEDGEMENTS

For this study, we interviewed close to 30 Tier 1 financial institutions across North America, Western Europe and parts of developed Asia. Most of these were structurally significant financial institutions with assets of more than US$100 billion.

Celent would like to thank the individuals and industry practitioners for their time in providing ground-level and future-oriented perspectives across the various lines of defense on how to best navigate the challenges and opportunities across operational risk, compliance, audit and governance activities; along with the threats and implications for risk and control functions as a result of digitization trends across the industry.

RESEARCH BACKGROUND

This report was commissioned by Thomson Reuters; however, the analysis and conclusions are Celent's alone, and Thomson Reuters had no editorial control over report contents.

About Thomson Reuters

Thomson Reuters is the world's leading source of news and information for professional markets. Our customers rely on us to deliver the intelligence, technology and expertise they need to find trusted answers. The business has operated in more than 100 countries for more than 100 years. Thomson Reuters shares are listed on the Toronto and New York Stock Exchanges. For more information, visit www.thomsonreuters.com

Thomson Reuters Connected Risk

Thomson Reuters Connected Risk is the firm's next-generation risk management software platform designed to help identify, assess, manage and monitor risk across the enterprise. Flexible and customizable with seamless integration of key data, the platform provides a dashboard view of an organization's holistic risk profile. For more information, visit risk.tr.com/connected-risk

LEVERAGING CELENT'S EXPERTISE

If you found this report valuable, you might consider engaging with Celent for custom analysis and research. Our collective experience and the knowledge we gained while working on this report can help you streamline the creation, refinement, or execution of your strategies.

SUPPORT FOR FINANCIAL INSTITUTIONS

Typical projects we support related to governance, risk, and compliance include:

Vendor short listing and selection. We perform discovery specific to you and your business to better understand your unique needs. We then create and administer a custom RFI to selected vendors to assist you in making rapid and accurate vendor choices.

Business practice evaluations. We spend time evaluating your business processes. Based on our knowledge of the market, we identify potential process or technology constraints and provide clear insights that will help you implement industry best practices.

IT and business strategy creation. We collect perspectives from your executive team, your front line business and IT staff, and your customers. We then analyze your current position, institutional capabilities, and technology against your goals. If necessary, we help you reformulate your technology and business plans to address short-term and long-term needs.

SUPPORT FOR VENDORS

We provide services that help you refine your product and service offerings. Examples include:

Product and service strategy evaluation. We help you assess your market position in terms of functionality, technology, and services. Our strategy workshops will help you target the right customers and map your offerings to their needs.

Market messaging and collateral review. Based on our extensive experience with your potential clients, we assess your marketing and sales materials — including your website and any collateral.

RELATED CELENT RESEARCH

Stronger Together: The Bank Imperative for Cyberthreat Intelligence Sharing
March 2018

Innovations in AML and KYC Platforms: New Models Powered by Advanced Computing
January 2018

Innovation in AML Technology: New Tools for Optimizing Compliance Efficiency
November 2017

Buy Side Investment Risk Management Part 1: A Survey of Business Priorities, Risk Hotspots, and Operational Alpha Opportunities
November 2017

Buy Side Investment Risk Management Part 2: A Survey of Risk Technology and Innovation Imperatives
November 2017

Cloud-Enabled Governance, Risk, and Compliance Solutions
October 2017

Innovation in Compliance Technology: Emerging Themes and Vendor Solutions
June 2017

Bank of America: In Pursuit of Operational Risk and Compliance Excellence
April 2017

Artificial Intelligence in KYC-AML: Enabling the Next Level of Operational Efficiency
August 2016

Market Surveillance in Capital Markets: The Growing Role of Artificial Intelligence
August 2016

Copyright Notice

Prepared by

Celent, a division of Oliver Wyman, Inc.

For more information please contact info@celent.com or:

Cubillas Ding	cding@celent.com
Neil Katkov, PhD	nkatkov@celent.com

AMERICAS

USA

200 Clarendon Street, 12th Floor
Boston, MA 02116

Tel.: +1.617.262.3120
Fax: +1.617.262.3121

USA

1166 Avenue of the Americas
New York, NY 10036

Tel.: +1.212.541.8100
Fax: +1.212.541.8957

USA

Four Embarcadero Center, Suite 1100
San Francisco, CA 94111

Tel.: +1.415.743.7900
Fax: +1.415.743.7950

Brazil

Av. Doutor Chucri Zaidan, 920 –
4º andar
Market Place Tower I
São Paulo SP 04578-903

Tel.: +55.11.5501.1100
Fax: +55.11.5501.1110

EUROPE

France

1 Rue Euler
Paris
75008

Tel.: +33.1.45.02.30.00
Fax: +33.1.45.02.30.01

United Kingdom

55 Baker Street
London W1U 8EW

Tel.: +44.20.7333.8333
Fax: +44.20.7333.8334

Italy

Galleria San Babila 4B
Milan 20122

Tel.: +39.02.305.771
Fax: +39.02.303.040.44

Switzerland

Tessinerplatz 5
Zurich 8027

Tel.: +41.44.5533.333

ASIA

Japan

The Imperial Hotel Tower, 13th Floor
1-1-1 Uchisaiwai-cho
Chiyoda-ku, Tokyo 100-0011

Tel: +81.3.3500.3023
Fax: +81.3.3500.3059