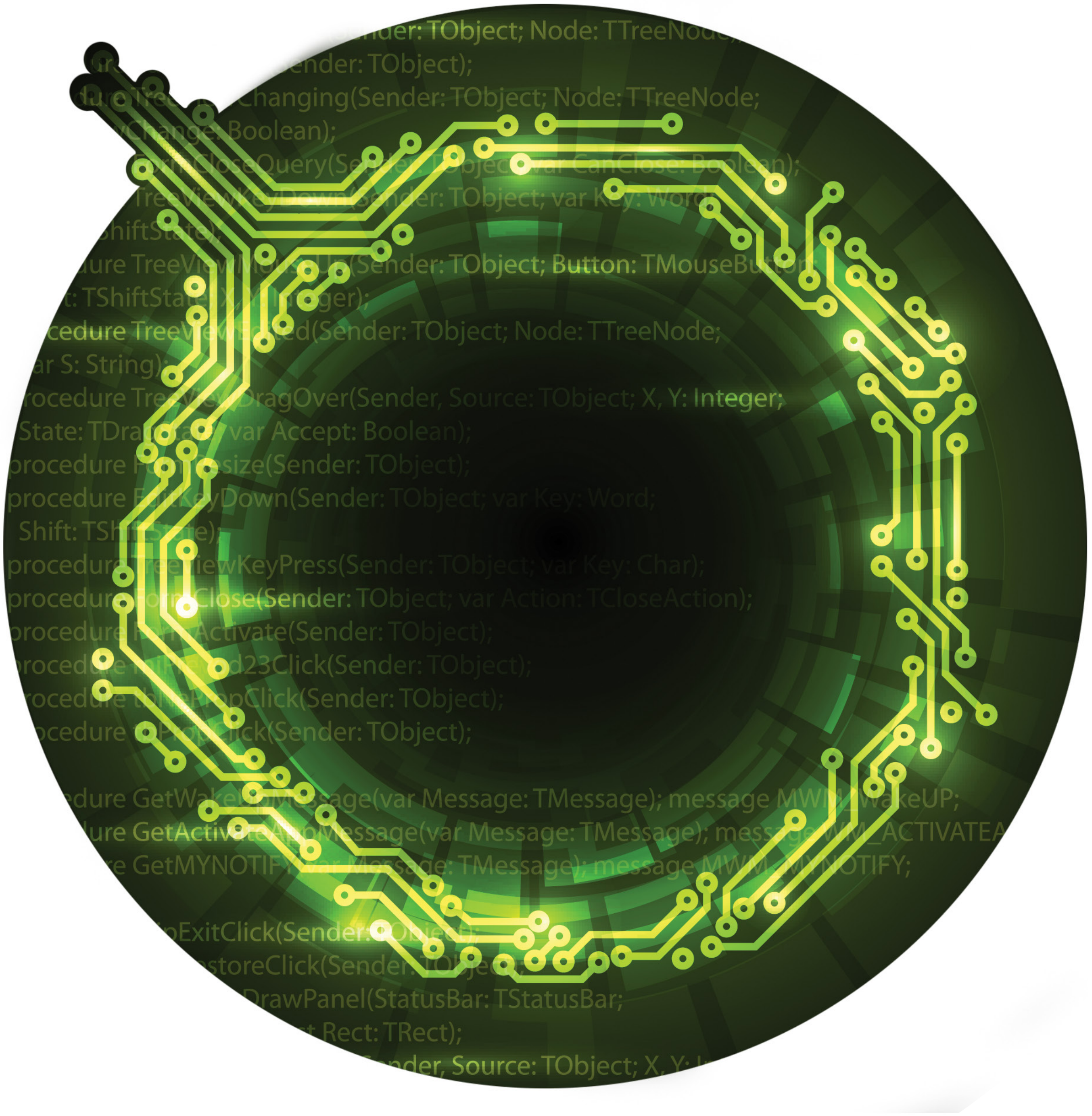
Deloitte.



Implementing risk transformation in financial institutions

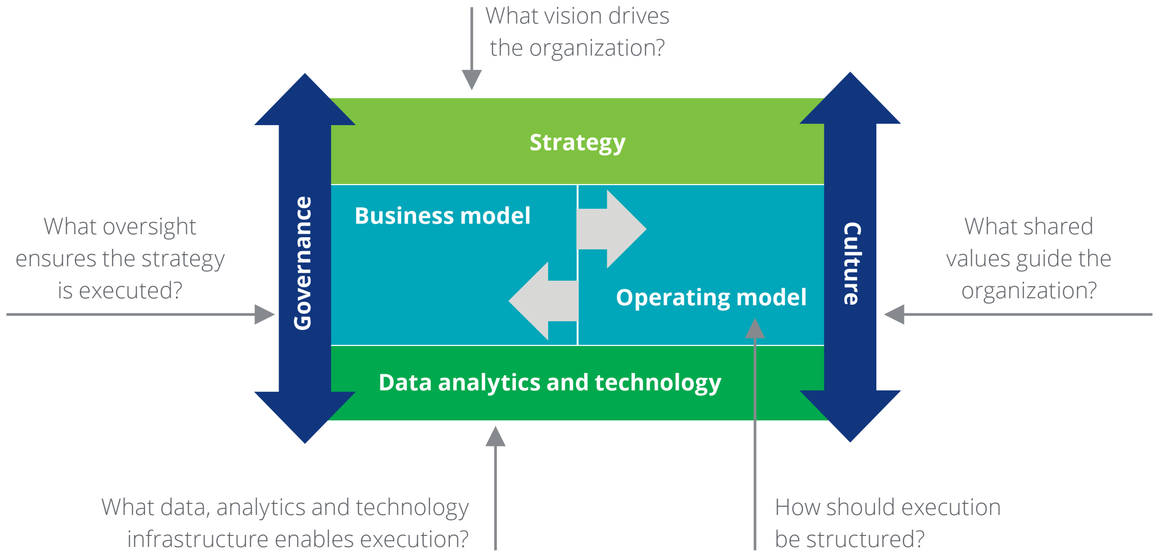
Data, analytics, and technology

Risk transformation can enable a financial institution to elevate risk management from a functional capability to an enterprise responsibility that permeates the entire organization. When that happens, every business, function, and individual becomes responsible for, accountable for, and capable of recognizing and addressing the risks within their purview. Moreover, risk awareness and appropriate risk-related skills can become an integral component of every individual's responsibilities at every level. In these ways, risk transformation can enhance the organization's ability to implement business strategies and achieve goals while addressing risks and complying with evolving regulations.

This document is one in a series of four highlighting the cornerstones of risk transformation (see Figure 1):

- Strategy
- Governance and culture
- Business and operating models
- Data, analytics, and technology

Figure 1
The cornerstones of risk transformation


What vision drives the organization?
Strategy
Business model
Operating model
Governance
Culture
What oversight ensures the strategy is executed?
What shared values guide the organization?
Data analytics and technology
What data, analytics and technology infrastructure enables execution?
How should execution be structured?

As explained in *Aligning risk and the pursuit of shareholder value: Risk transformation in financial institutions*[1], when these cornerstone frameworks and capabilities are in place, risk management, risk governance, and regulatory compliance can be implemented in a more aligned and integrated manner.

As Figure 1 shows, data, analytics, and technology are foundational elements in risk transformation, which also involves strategy, governance and culture, and business and operating models.

Each document in this series focuses on a single cornerstone so that leaders gain insight to help them launch risk transformation initiatives across all four cornerstones or start with a single one. This document discusses the importance and workings of data, analytics, and technology.

[1] Aligning risk and the pursuit of shareholder value: Risk transformation in financial institutions, 2013, Deloitte <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/finance/us-finance-implementing-risk-transformation.pdf>

Data, analytics, and technology as a cornerstone

As financial institutions cope with new regulatory and competitive challenges, some are finding their past approaches to be suboptimal, particularly in the area of data, analytics, and technology.

Key among those regulatory and competitive challenges are the following:

- **Many regulations directly affect data, analytics, and technology.** Regulators are focused on risk data quality, consistency with financial data, methods of aggregation and reporting, and related processes. The Federal Reserve's Comprehensive Capital Analysis and Review (CCAR) increases regulators' visibility into risk data, as do the FR Y-14 Capital Assessments and Stress Testing detailed data submissions for the top 30 US banks, the Basel Committee's Risk Data Aggregation and Risk Reporting (RDARR) Principles, and the European Union's (EU) stress testing requirements. Such regulatory demands must be met, and many institutions are scrambling to meet them.
- **Institutions need to optimize risk, not simply lower risk.** More detailed and immediate data can be used to enhance allocation of capital and manage liquidity, increase capital efficiency and return on risk weighted assets (RWA), and optimize products and relationships. While institutional safety and soundness is one of the primary goals of the regulations, these risk-related business goals are realistic and achievable for institutions. Meeting these risk-related business goals will also establish a foundation for future risk management and governance efforts.
- **Costs are rising and profits are threatened.** Against this regulatory landscape, costs, competition, and pressures on profits are skyrocketing. Institutions that attempt to employ tactical responses to these regulatory changes could find themselves wasting resources. Grasping this, a number of institutions are recasting data improvement or IT architecting programs within their regulatory compliance programs—or vice versa—with the goal of applying resources to enhance the long-term efficiency of technology.
- **Information technology (IT) has become a valuable enabler.** IT is enabling risk data aggregation and repositories, structured and unstructured data aggregation, real-time risk reporting, and visualization tools. However, many financial institutions have only begun to face the challenges of formulating data integration strategies and data governance processes needed if they are to employ evolving technologies in truly useful ways.

Historically, many financial institutions have responded to new regulations with ad hoc, bolted-on, or piecemeal solutions. Such fragmented approaches have created gaps, overlaps, redundancies, and manual tasks which have in turn led to inefficiencies, increased costs, and even increased risks in control, reporting, and IT systems. Given today's volume of regulatory demands, reactive efforts either won't work or may likely be unsustainable.

Three specific drivers
Though they vary by jurisdiction, certain regulatory requirements are driving the need for better data:

- **Reporting requirements:** The European Union Basel's RDARR principles, the United States Federal Reserve's CCAR, and Canadian metrics such as the liquidity coverage ratio (LCR) and net cumulative cash flow (NCCF) all dictate a need for more detailed, current, and higher quality data. This calls for breaking down silos to generate an enterprise view of risk, while meeting jurisdictional reporting requirements.
- **Living wills:** In the United States, The Dodd–Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank) requires certain major institutions to prepare resolution plans, known as living wills, which describe the company's strategy for rapid, orderly resolution in the event of material financial distress or failure. Thus, for example, a bank holding company needs separate, as well as consolidated, views of positions, conditions, and risks. Individual companies need the infrastructure to operate independently, and management needs to monitor them and take action when necessary and as planned.
- **Legal entity issues:** Legal entity issues arise around living wills from the monitoring, systems, and financial standpoints, and around matters such as geographic and client constraints and collateral positions. A number of organizations seek to simplify and rationalize their structures, which has implications for data, analytics, and technology in that a business unit may differ from a legal entity. For example, reducing the number of legal entities and their reporting will typically require reorganization of the data-related processes and systems underlying their reporting.

In tandem with such regulatory issues, institutions want to understand capital and liquidity needs, marginal profitability and returns, and risk positions and resource allocations. This information improves decisions about products, services, markets, customers, resources, and risks.

The above trends signal the need for a far more integrated and strategic approach to data, analytics, and technology—in general—and in responding to regulatory change. For example, RDARR principles present opportunities to address not only risk-data issues but also operational data aggregation and reporting issues, and, potentially, to redirect the enterprise toward more strategic management of data. CCAR presents an opportunity, and a need, to reconcile financial and risk data. Regulatory principles for stress testing and capital adequacy, planning, and management affect decisions from the front lines all the way to the C-Suite and the board. And these are just a few of the regulatory issues affecting functions at every level in financial institutions (see sidebar).

Fortunately, the need for aggregated views of risk is driving the breakdown of silos. Silos formed by organizational and technological barriers between and within finance, risk management, and the front office impede optimal compliance, risk management, and capital allocation. Barriers exist between finance and the treasury function (generally part of finance) and within risk management, for example between people monitoring credit, liquidity, market, currency, counterparty, and other risks.

While the fundamental rationale for change is regulatory compliance, forward-thinking leadership teams are taking regulatory demands as an opportunity to control compliance costs, lower the total cost of ownership (TCO) of technology, and realize operational efficiencies—while improving risk management and capital allocation. In addition, enhanced competitiveness and shareholder value can be expected over time.

This requires a transformative approach, with senior management, particularly the chief information officer (CIO) and chief risk officer (CRO), leading the way. Regulatory, strategic, operating, governance, risk management, and business needs have converged to make an unprecedented case for transformation in financial institutions. The regulatory demands are far-reaching, the need for risk-based decision-making pervasive, and the threat to competitiveness serious that institutions must take a transformative approach to risk.

Risk transformation is strategic rather than tactical, integrated rather than fragmented, and systematic rather than bolted-on. Anything less will likely waste resources as well as opportunities to position the institution for future growth and competitiveness. The next three sections briefly review data, analytics, and technology in the context of risk transformation.

Data: Improving quality, access, and integration

A transformative approach to data potentially involves three shifts. The first shift concerns ownership of risk data, which affects the institution's ability to address regulatory and risk-management requirements. Data is most often perceived as owned by IT because IT owns the technology. However, IT usually should not and usually would not prefer to own the data. Risk management may logically own risk data, although the businesses must be engaged in data quality, governance, stewardship, and, preferably, ownership.

There is no single answer to the question, "Who should own the data?" Each organization must answer it, and in answering it, some institutions have established a chief data officer (CDO) to manage a data management/data quality function. A CDO can work with the CRO to meet risk's needs, with the businesses to meet their needs, and with the chief compliance officer (CCO) to meet the regulators' needs—and interface with the chief technology officer (CTO) or equivalent.

Key issues in risk data

The CDO, CRO, and other senior executives must foster an understanding of data issues facing the organization. Broadly, these issues may include:

- **Regulatory requirements:** Regulators want more granular data, better data, and greater visibility into data sources—and relevant parties must understand this. They must also grasp the need for consistent business terms and rules, sound data processes, and data governance. In other words, every party that touches data, in businesses, risk management, compliance, or third parties has a role to play.
- **Data quality:** The businesses within an organization should arguably own data quality, given that they own the processes that produce the data and quality is use-case driven. Data quality must be addressed in the relevant end-to-end business processes as well as in the technology architecture. When it comes to enhancing data quality, specific IT tools (discussed below) are often secondary to business rules and disciplined processes.
- **Meta data:** Meta data (or "data about data") is essential to understanding data in various repositories and therefore is a key determinant of the quality of risk measures and reports. Meta data emanates from multiple processes, and its quality can be compromised at various points through misinterpretation, misrouting, or other errors. Again, disciplined processes and data stewardship are essential.
- **Financial versus risk data:** Financial reporting occurs at the end of the day, week, month, or quarter while risk data should be reported on intraday or, if possible, real time (particularly for market and liquidity risks). If financial and risk data are interdependent, problems can arise around the timeliness of risk data, given that financial reporting follows its own (slower) cadence.

Regulators want access to data, and the ability to drill down into data on a risk basis. They want to be able to ascertain data integrity, preferably via self-service. The more that business processes, data governance, and IT architecture support these needs, as well as business needs, the better.

A CDO should not own risk data because the data—and the definition of quality—are specific to its uses. Data quality also depends on business processes that the CDO cannot control. A CDO can raise awareness of data quality, sustain data governance and improvement, and foster data stewardship. In addition, a CDO can serve as a change agent regarding key data issues in the institution (see sidebar).

The second shift concerns the residence of data. Risk data originates in transactions, customer data, credit reports, ledgers, news feeds, cyberspace, and other sources. Yet if management takes this to mean that risk data cannot be centrally managed, then data quality and aggregation problems will persist. In addition, management must address data privacy rules and storage, access, and compliance issues.

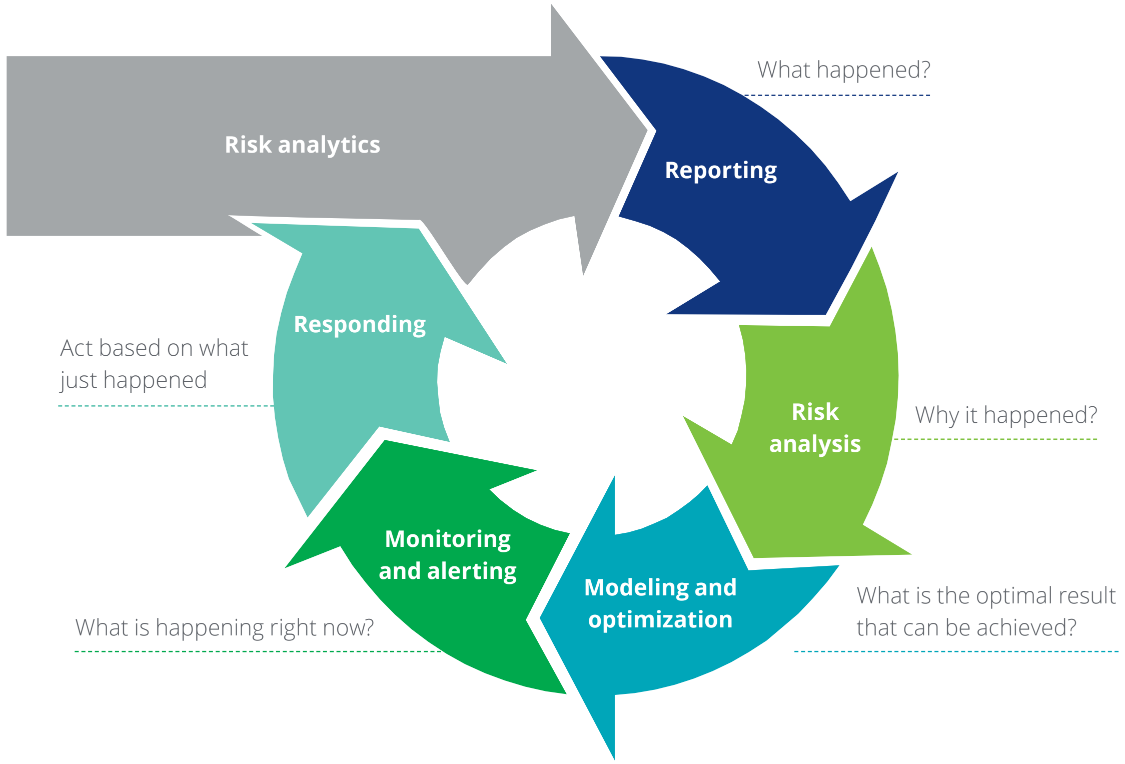
One potential solution, prompted by the Basel RDARR principles and by operational needs, is to establish (at an appropriate organizational level or levels) a single repository of risk data. Risk data can be entered into that repository, and curated by people responsible for its quality. This "clean room" or "file cabinet" approach comes closer than many alternatives to ensuring quality risk data for all users—but it's not the only alternative. Sound data governance and management remain paramount regardless of whether risk data is centralized into one or more repositories.

Another solution many institutions are employing is moving from databases geared to storage and integration to solutions that integrate business rules and support analytics and reporting. This represents a significant shift. Rather than distributing data and then applying business rules, a business unit can bring applications to a single point, perform calculations, and generate reports. The recursive or cumulative processes needed for internal or regulatory reports can now be performed without pipelines and multiple platforms, and without a single risk-data repository.

The third, potentially most challenging shift concerns risk data standards. Risk calculations use reference data, transaction data, and market data as inputs, and the various types, forms, and sources of data make aggregation a huge challenge. Meaningful aggregation requires a standard risk language or taxonomy and risk semantics. Transaction, market, and reference data must be well-defined and consistently managed. Risk data should also include financial instrument lifecycle data, such as trade lifecycle data on a security or option, in a usable form.

Risk identification, measurement, monitoring, assessment, and reporting often employ data from external sources. Choosing and using this data, and determining its quality and reliability, can present further challenges. For example, data on emerging strategic and reputational risks can take highly unstructured forms, such as blog postings, social media, and online journalism, as well as structured forms, such as economic data, earnings reports, and public filings. Fortunately, the cost of technologies for analyzing and integrating this data has plummeted while innovations, such as risk sensing capabilities aimed at parsing big data, continue to emerge.

Figure 2
Foundational components of analytics


Risk analytics
What happened?
Reporting
Responding
Act based on what just happened
Risk analysis
Why it happened?
Monitoring and alerting
Modeling and optimization
What is the optimal result that can be achieved?
What is happening right now?

Key trends in advanced analytics

Advanced analytical models apply rules to massive data sets to detect risks, answer questions, and assist in decision making. Cognitive analytics—machine learning, natural language processing, and artificial intelligence—enable analytical engines to adapt on the basis of new data and analyses and operate beyond predefined rules and structured queries[2]. Such capabilities combine lightning fast computing power with oceans of data to generate hypotheses, propose recommendations, and make decisions.

Trends worth following in this area, which might be termed Analytics 2.0, include these ongoing shifts:

- **From off-line to real-time analytics:** Advanced analytics move monitoring, analytics, and decisions from post-event into real time or near real time.
- **From structured to unstructured data:** Unstructured data in emails, text, graphics, and video can now be analyzed and, when useful, combined with structured data.
- **From internal to external data:** Data in newsfeeds, press releases, podcasts, and other web-based content, as well as social media and data flowing between organizations, can now be continuously monitored and analyzed.
- **From defined analytics to cognitive analytics:** Cognitive learning technologies enable applications to be trained, or to train themselves, to become more accurate and predictive.

One exemplary use-case centers on trading activity, a key source of risk in financial institutions. Certain trader behaviors, such as unauthorized trades or collusion, can generate conduct, regulatory, fraud, and other risks. As trade surveillance becomes more important, so does the ability to monitor and analyze the huge amounts of data that trading activity depends on and generates. While much of this data is structured (pricing data, trading limits), a good amount is not (patterns of trading activity, traders' online behavior).

Analytics: Enhancing risk management and governance

Regulators' focus on risk analytics complements their focus on capital and liquidity. From management's perspective, analytics enable the organization to improve risk-based decision making and performance monitoring and reporting. Analytics also assist organizations in managing financial, market, operational, regulatory, and security risks. Analytics establish a baseline for tracking risk in business units and, through aggregation, across the organization. Rapidly evolving advanced analytics are increasingly being applied in financial services (see sidebar).

Deloitte has identified the following foundational components of risk analytics (Figure 2):

- Reporting entails generating information for management and regulators based on specific views of data.
- Risk analysis correlates disparate data on risk and drills down into specific factors to illuminate drivers of risk.
- Modeling and optimization enable, respectively, forecasting of risk events, such as default or loss, and formulating responses, such as proper pricing of risk.
- Monitoring and alerting employs risk models embedded in manual or automated systems to track risks and exposures.
- Responding means deciding what action to take on the basis of analysis, designing effective, efficient responses, and monitoring the outcomes. It also means analyzing the outcomes and making improvements. For example, response to a breach of a risk limit (such as a value at risk (VaR) limit) still occurs largely via manual intervention, although automated responses are becoming attractive for low-impact/high-frequency events.

[2] Cognitive analytics: Wow me with blinding insights, HAL, Tech trends 2014: Inspiring Disruption, pg. 18, Deloitte University Press <http://d27n205l7rookf.cloudfront.net/wp-content/uploads/2014/02/Tech-Trends-2014_FINAL-ELECTRONIC_single.2.24.pdf>

To accurately portray risks and exposures, certain analytics, such as dynamic recalibration of credit risk scores, should be as close to real time as possible. As the mix of customers changes, so does the organization's risk profile, and such changes should be taken into account. In addition, self-service and visualization technologies (discussed below) can put analytics into the hands of users, both accelerating and improving responses.

A commitment to risk analytics also supports risk governance, oversight, and management in ways that directly impact operations, capital allocation, and profitability.

Monitoring key risks

Improved data integration and analytics generally lead to enhanced stress testing and monitoring and reporting of key risks—a chief aim of regulators. The risks in question include those that financial institutions work within their core businesses: credit, market, liquidity, currency, interest rate, and other financial risks, as well as strategic risks, third-party risks, cyber risks, and conduct risk.

Monitoring nonfinancial risks often involves scanning high volumes of unstructured data from diverse sources (e.g., big data). This calls for addressing structured and unstructured data in an integrated manner, although, as discussed below, no technology vendor can as yet supply a stand-alone solution.

Consider conduct risk, a major focus of regulators (particularly UK and, increasingly, US and Canadian regulators). Monitoring conduct risk, even in the traditional sense of fraud and other illegal activities, demands surveillance of transactions, preferably in real time.

[3] "The Global Cost Of Anti-Money-Laundering Efforts". http://www.pymnts.com/news/2015/the-global-cost-of-anti-money-laundering-efforts/. February 24, 2015. PYMNTS.com.

[4] Deloitte Touche Tohmatsu Limited Global risk management survey, ninth edition: Operating in the new normal: Increased regulation and heightened expectations <http://d27n205l7rookf.cloudfront.net/wp-content/uploads/2015/05/DUP_GlobalRiskManagementSurvey9.pdf>

In implementing trade surveillance capabilities that address such behaviors and data challenges an organization could:

1. Monitor trading activity in real time to identify behaviors before they do damage or in time to limit potential damage, and prevent the behaviors in the future. The sooner risk or undesirable behavior is detected, the better.
2. Identify patterns between structured and unstructured data—for example, between trades booked and traders' emails—to uncover anomalous trades and trading behavior.
3. Use of data outside the organization, for example in a trader's social media profile, to gain insight into their behavior within the organization.
4. Employ cognitive analytics in the form of an application that can adapt on the basis of new analyses to identify anomalies with less human intervention.

Anti-money laundering (AML) efforts offer another compelling use-case. According to Charles Kenny, a senior fellow at the Center for Global Development, AML programs cost the financial services industry billions each year to run, and the talent needed to manage AML programs is in short supply. Traditional monitoring and analysis can generate staggering numbers of false positive alerts, which require manual review to clear.

Recognizing the need for far greater efficiency in this area, many banks are adopting advanced analytics in AML programs. Such analytics can automatically clear large percentages of false positive alerts, freeing up talent for cases that truly warrant investigation.

Advanced analytics are now beyond the "promising" stage. They are real and the case for adoption is strong: 62 percent of companies consider their risk information system or technology infrastructure to be extremely or very challenging[3][4] . A move from traditional to advanced analytics can often generate more accurate and predictive analysis with less human intervention and lower long-term cost.

Monitoring conduct risk can also involve unstructured data, which provides the context of transactions, as well as more structured data on accounts, amounts, controls, and access patterns. At the same time, institutions need to understand credit, liquidity, market, and other risks at the transaction level.

This presents a strong rationale for integrating data sets, or at least for capabilities that enable analysis of disparate data sets on an integrated basis. This means understanding business and risk management objectives and technology architecture options. The relevant business processes must then be structured to enable proper data governance and stewardship and continuous improvement.

Analytics must not only enable risk reporting, stress testing, and model validation, but also monitoring of transactions, positions, and risks on individual and aggregated levels. The results must then be viewed in the context of risk appetite, risk tolerances, risk/reward tradeoffs, and risk management options. Institutions possess widely varying capabilities in these areas, and some fall short when it comes to incorporating unstructured data into analysis and monitoring operational and conduct risks.

As with data integration and aggregation capabilities, analytical capabilities are constantly expanding with the ongoing evolution of technology.

Technology: Getting there, but not there yet

While observations regarding IT can become rapidly outdated, the needs of institutions are fairly clear and vendors have been working to meet them, with partial success.

Traditionally, databases have been geared primarily to storage and, secondarily, integration. Combining business rules and standardization in appliances represents a shift away from applying business rules and standards after data was centrally stored. The storage-and-integration approach is giving way to approaches that aggregate data and views to support specific analytics and reporting, such as stress testing. This supports recursive processes and does away with pipelines; instead, applications are brought to a single point and reporting occurs at the back-end as reporting, rather than calculation and reporting.

Relational databases will not go the way of the punch card and vacuum tube. Financial institutions (and organizations in other industries) have too much data in relational databases, which handle storage, maintenance, and query too well for them to become obsolete anytime soon, despite statements to the contrary. Of course, database vendors will feel pressure from those selling hierarchical and open source systems, an aspect of the ongoing flux in the IT marketplace.

However, relational databases have their limits and sequential or batch processing and static reporting tools cannot fulfill dynamic, on-demand risk-related requirements. The following emerging technologies, can to some extent, enable the kind of data access, integration, and analytics that institutions now seek:

- **Streaming technology and event processing technology:** These technologies are still limited to high velocity, smaller volume trading situations and have yet to see widespread application. Yet they have the potential for broader adoption, particularly in transaction and conduct surveillance and financial risk monitoring.
- **Open source:** These technologies can enable access to data in its native form and provide analytical capabilities to users. However, analytical capabilities must usually be developed by the institutions. That said, these technologies can enable queries on large, unstructured data sets as well as solutions for more structured data.
- **In-memory technologies:** The major enterprise resource planning (ERP) vendors and emerging companies provide in-memory or equivalent solutions, which are gradually being adopted in many financial institutions (see sidebar). These technologies may help overcome the limits of relational databases, allowing for less structure and providing more flexibility.

Self-service and visualization tools are also winning acceptance. These put analytical and monitoring capabilities into the hands of users, thus eliminating the need to transfer data to other platforms or to analysts. Indeed, the output of most real-time, on-demand risk calculations can be readily understood only by means of graphical visualization tools.

Significantly, self-service and visualization capabilities can also enable institutions to provide regulators with the transparency they seek into risk data and positions.

In general, enterprise governance, risk and compliance (GRC) solutions are now starting to come of age. Many organizations have traditionally employed three or more GRC solutions to address their operational risk, Sarbanes Oxley Act of 2002 controls, and IT risk areas. However, due to the regulatory imperative to aggregate risk data across operational risk areas and the push to automate more control processes, compliance and control areas are migrating toward a single enterprise GRC tool. This enables a single source of authoritative information to report to the audit committee and allows for a standardized definition of issue-criticality across different types of operational risk.

By the same token, in light of stress-testing requirements, many ERP vendors are starting to extend their solutions to address the challenges of data convergence across finance, risk, and treasury. The same business case for a common data model and a single reconciled data repository (both of which ERPs historically have delivered across accounts payable, accounts receivable, and billing) is being applied to risk, liquidity, funds transfer pricing, and anti-money laundering needs. As with any system, a solution entails entering the original transactions correctly with all of the data elements required to meet the needs of various business areas. The success of these projects therefore depends on disciplined data governance and management processes.

These ERP programs are still relatively new and thus unproven in delivering the promised benefits. However, assuming the vendors bring the same discipline to these new areas that they have made routine elsewhere, these solutions could become the new standard in the future.

In sum, technology is undergoing a generational change with short, intermediate, and long-term implications for the ways in which institutions structure, store, access, and analyze data. Any transformation of—or adjustment to—this cornerstone must account for this while recognizing that the IT marketplace will remain in flux and that complete, off-the-shelf solutions are—at least for now—rare.

In-memory databases and analytics

It's useful to grasp the distinction between in-memory database and in-memory analytical capabilities:

- **In-memory database** mimics a parallel or serial database but has the advantage of real time, on-demand data. There is, however, a cost penalty, and most in-memory appliances lack applications and leave users to create solutions. There are technologies offering performance equal to that of in-memory databases, which function like traditional databases with more real-time capabilities. These solutions tend to be used to monitor market and liquidity risks.
- **In-memory analytics** overlap in-memory databases, but aim to provide complex analytics not supported in the existing environment. These products can work where there is a shallow environment and no centralized data warehouse. Although they can provide good departmental solutions, they don't promote accuracy and consistency nor do they work well across the organization. Some solutions are being used for meta data, but they currently tend to be expensive for what they do.

In-memory, online analytical processing tools (and technologies such as column-based databases and complex-event processing technologies) can potentially address issues beyond the capabilities of relational databases and static reporting tools. Such issues include aggregating large volumes of intermediate results while accounting for complex rules in legal agreements, monitoring exposures across multiple legal entities, currencies, and countries, or analyzing market prices from multiple sources.

These technologies warrant continued monitoring, and organizations may wish to consider judicious experimentation and application.

Implications for three lines of defense

Risk transformation can strengthen the three lines of defense—the business units, risk management function, and internal audit function—a generally accepted industry framework (see Figure 3). Transforming data, analytics, and technology strengthens the three lines of defense by improving the risk-related information that each line depends on in its work.

More specifically, improved risk data and analytics can impact each line of defense in the following ways:

- **Business units:** Risk-based decision making demands timely, reliable information at the right level of detail. The more granular that data can be while remaining comprehensible, the better the front offices can manage products, choose customers, and price risk. Self-service and visualization tools can enable that kind of comprehension and decision making.
- **Risk management:** To gauge risk positions and tolerances, risk managers use much of the same data as the businesses, but usually with separate processes and a need to reconcile differences at various points. The technology architecture will dictate the extent to which risk management can run off the same systems as front office functions and affect the level of integration between finance and risk data. The greater the level of integration throughout, the better the processes and systems will be.
- **Internal audit:** Assessing risk management, control, and compliance systems—the chief responsibility of internal audit—becomes more efficient and effective when data is more accessible, controls are rationalized, and risk management and governance processes are more transparent.

In addition, attention to the other cornerstones of risk transformation more closely aligns the lines of defense. A clearly understood, consistently implemented strategy provides a strong sense of direction and common purpose. Strong governance and culture enable the business units and risk management to balance risks taken in creating value against anticipated rewards. Practical, rationalized business and operating models establish the role of each line in implementing strategies and achieving goals.

The business case

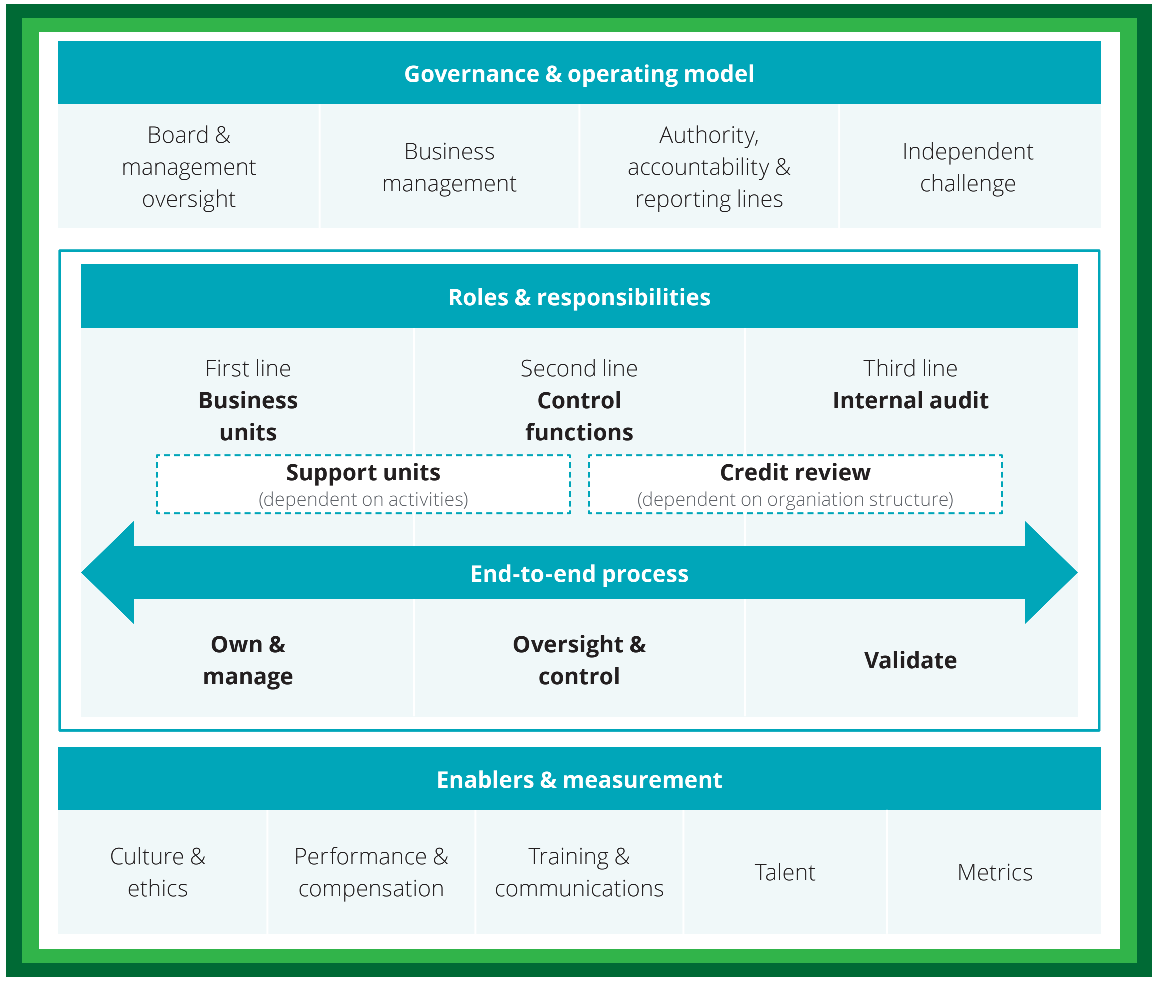
It may be best for an organization to recognize the business case for transformation as distinct from the regulatory imperative. The two are intertwined in that compliance is not optional for the institution, which must meet the regulatory requirements and adjust business practices accordingly. Yet the case for business transformation of the data, analytical, and technology cornerstone goes beyond the regulatory imperative.

The business case rests on using regulatory demands as an opportunity to transform risk-related capabilities—not overnight, but over time as regulatory, operational, and risk-related needs, and the technologies, evolve. Thus the initiative may originate with the need to upgrade capabilities so as to meet regulatory requirements, but management should consider these needs in the context of the institution's goals, business, and competitive position. That is, organizations should consider whether their risk transformation should aim not only to address regulatory issues, but to enhance insight, decision making, and competitiveness.

As noted, fragmented approaches to regulatory compliance often waste money and other resources, increase costs, and create gaps, redundancies, manual labor, and new risks. In contrast, an integrated, transformative approach may reduce the TCO of technology and optimize the cost of compliance. It can also lead to more streamlined and efficient business, data governance, and risk management processes.

The point of a transformative approach is to have, in addition to the regulatory imperative, a well-developed business case that permeates the organization's approach to data, analytics, and technology. This enables the organization to go beyond compliance to break down silos and align business, risk management, and internal and regulatory reporting processes and to strengthen the three lines of defense (see sidebar). Sought-for results could include wider access to data and analytics at lower levels of the organization, views of aggregated risk positions at higher levels, and greater flexibility in terms of responses to marketplace and regulatory needs going forward.

Figure 3
A depiction of the three lines of defense model of risk governance



Source: Deloitte US point of view Strategic risk: A cornerstone of risk transformation.
http://www2.deloitte.com/global/en/pages/risk/articles/implementing-risk-transformation-in-organizations.html

Institutions should also aim to position themselves to understand risks more broadly and deeply and to price risk accordingly, allocate capital and liquidity optimally, and enhance selection and management of businesses, products, and customers at every stage of their lifecycles. Other useful aims include continuous improvement in data quality, improved analytical accuracy and immediacy, greater operational efficiency, and, ultimately, enhanced competitive advantage and shareholder value.

Improved data aggregation, analytical, and risk-reporting capabilities would be expected to enhance the organization's relationships with regulators. After all, like management and the board, regulators are essentially concerned with the safety and stability of the organization.

Transformative considerations

A transformative approach to data, analytics, and technology begins with consideration of the following factors:

- **Data governance:** Strong data governance ensures that data is accurate, reliable, and handled in standard ways. This enables the organization to run the same business processes while avoiding a confusing multitude of rules.
- **Meta data:** Big data may be needed for sophisticated risk analytics, and meta data tools are essential to incorporating unstructured data into analytics. These tools enable analysts to tag raw data, and to track its origin, evolution, and users.
- **Data model:** The data model must evolve to integrate structured and unstructured data. The major ERP vendors' solutions may not be the most sophisticated, but they are working to promote data integration. Those vendors also provide a unified data model, applications, and training—all of which help in breaking down silos.
- **Awareness and teamwork:** Users need to become far more aware of data quality, ownership, and management issues. The CDO, CRO, and other leaders have to foster and sustain that awareness. They must also foster the collaboration among data architects, modelers, risk managers, and business process owners that is essential to strong data governance.

From a technology standpoint, when selecting solutions today, it is wise to consider whether the organization will need an integrated solution in the future. To meet regulatory requirements, many large institutions are using ERP solutions for integrating data and employing bolted-on analytics, a workable interim approach.

Relational databases may give way to open source and other evolving technologies, but based on knowledge and experience, Deloitte professionals indicate those databases are here to stay as general repositories. Operational data stores (ODS), data warehouses, and data marts may—repeat may—give way to data lakes, but only with strong data governance and curation (a data lake is a repository for raw data in unstructured, semi-structured, and structured forms; few vendors currently offer the equivalent of data lake solutions.)

The optimal technology posture is to remain flexible, while establishing data governance and a meta data and data integration strategy. In practice, many institutions lack sound data governance and a workable data strategy, which means these would represent an excellent starting point. Few institutions have the basic pieces in place, and even fewer have operationalized true data governance. Many institutions must go to the trouble of rewriting their interfaces so they can simply pull together the data needed to meet the new regulatory requirements.

Much of this state of affairs stems from the fragmented approaches to meeting regulatory requirements of the past, as well as past priorities, which tended to neglect these considerations. A better future will require a much different approach.

Conclusion

The decision of regulators, particularly in North America and Europe, to focus on risk data and the processes that produce it is driving activity and investment within financial institutions. A host of outcomes hinge on whether an institution takes a reactive, fragmented approach, or a transformative, integrated approach, to addressing regulatory requirements.

Those outcomes affect not only regulatory compliance, but also costs of compliance and technology ownership, as well as the organization's capital allocation, product development, customer relationship management, and risk management capabilities. Given that a financial institution manages risk as its core business, the more effective its response, the better it will position itself to meet not only future regulatory demands, but also the demands—and the risks—of the evolving global marketplace.

Contacts

Canada

Azer Hann
Partner
Deloitte Canada
ahann@deloitte.ca
+1 416 601 5777T

Paul Skippen
Partner
Deloitte Canada
pskippen@deloitte.ca
+1 416 874 4411

United Kingdom

Tom Scampion
Partner
Deloitte United Kingdom
tscampion@deloitte.co.uk
+44 20 7007 2828

Paul Garel-Jones
Partner
Deloitte United Kingdom
pgareljones@deloitte.co.uk
+44 20 7303 3069

United States

Bala Balachander
Principal
Deloitte United States
+1 212 436 5340
lbalachander@deloitte.com

Scott Baret
Partner
Deloitte United States
+1 212 436 5456
sbaret@deloitte.com

Dilip Krishna
Managing Director
Deloitte United States
dkrishna@deloitte.com
+1 212 436 7939

Rick Porter
Partner
Deloitte United States
rickporter@deloitte.com
+1 561 962 7792

Omer Sohail
Principal
Deloitte United States
+1 214 840 7220
osohail@deloitte.co

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee ("DTTL"), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as "Deloitte Global") does not provide services to clients. Please see www.deloitte.com/about for a more detailed description of DTTL and its member firms.

Deloitte provides audit, consulting, financial advisory, risk management, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries bringing world-class capabilities, insights, and high-quality service to address clients' most complex business challenges. To learn more about how Deloitte's approximately 225,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte Network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.