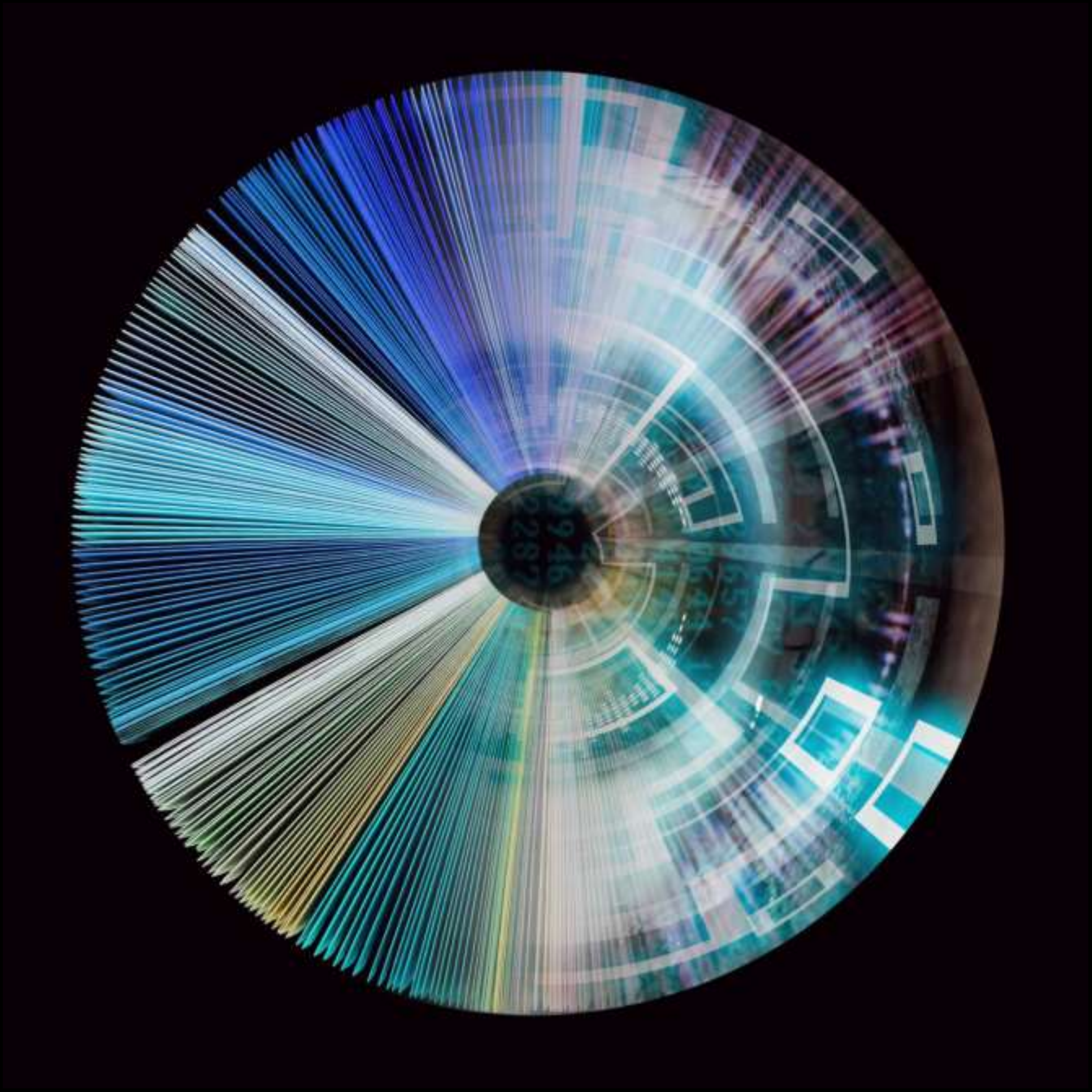
Deloitte.



# The future of operational risk in financial services

## A new approach to operational risk capital management

# Understanding the implications of the new Standard Measurement Approach, and using it as a catalyst to enhance operational risk management programs

As part of its completion of post-crisis reforms, the Basel Committee on Banking Supervision (Basel Committee) recently finalized its Basel III standard, which complements its previously published initial phase of Basel III reforms.

The new standard fundamentally changes how Operational Risk Capital (ORC) is calculated. This shift has major implications for banks' internal loss data, and how it could be used to derive business value and risk management insight.

In the past, many internationally active banks, based on requirements of their primary regulator, used a model-based approach that included a number of variables that determined the ORC they were required to hold. Under the new standard, that model-based Advanced Measurement Approach (AMA) is being replaced by the Standardized Measurement Approach (SMA), which essentially limits a bank's influence over ORC to a single variable: the Internal Loss Multiplier (ILM), which is in turn based on the bank's actual loss history.

The focus on internal losses when determining a bank's ORC requirement has two important implications. First, banks need to ensure their internal loss data—and the systems, processes and controls associated with building internal loss databases—are as accurate and robust as possible in order to support and substantiate their calculated ILM. Second, banks have a tremendous opportunity to reduce the existing and future ORC by focusing effort on managing and reducing actual operational losses, thereby reducing the impact of the ILM factor in the calculation of ORC.

The latter will likely require new behaviors and a new mindset, since many banks have traditionally viewed internal operational risk incidents—and the corresponding losses—as unavoidable costs of doing business, and something over which banks have had little control. However, with the addition of strong capital incentives to improve, banks may likely discover that internal losses can, in fact, be actively reduced, particularly with the help from new analytic and predictive technologies that make it possible to identify root causes and mitigate potential problems and risks before they result in major losses.

This point of view highlights essential components of a mature operational risk management framework that goes beyond compliance with the new standard. We describe how firms can leverage anticipated investments to derive risk intelligence from existing data to produce insight and reduce internal losses. By building an operational risk management framework that goes beyond compliance, banks can better navigate operational risk incidents by actively reducing their impact, allowing them to lead in their industry.

# The new formula-based approach for calculating Operational Risk Capital

In December 2017, the Basel Committee issued revised standards that finalized its post-crisis reforms and new Basel III framework. The revised standards include a new way to measure the amount of ORC that banks are required to hold. This new SMA seeks to restore credibility in the calculation of risk weighted assets (RWAs) and to improve the comparability of banks' capital ratios. Specific objectives of the reform include:

- Simplifying the Basel framework by replacing the four current approaches with a single standardized approach
- Making the framework more risk-sensitive by combining a refined measure of gross income with a bank's own internal 10-year loss history
- Making it easier to compare RWAs from bank to bank by removing the option to use multiple approaches and internal models

The SMA is based on the following components: (i) the Business Indicator (BI), which is a financial-statement-based proxy for operational risk; (ii) the Business Indicator Component ("BIC"), which is calculated by multiplying the BI by a set of regulatory determined marginal coefficients ($\alpha_i$); and (iii) the ILM, which is a scaling factor that is based on a bank's average historical losses and the BIC.

In practical terms, the ILM is the only variable a bank has significant control over, but its impact can be significant. The revised operational risk framework does not take effect until January 1, 2022. This gives banks time to improve their processes for collecting, managing, and analyzing internal loss data to reduce their ILM and thus the ORC they are required to hold.

# Improving the quality of historical loss data

Given the new standardized formula for calculating ORC, banks will likely scale back on their advanced modeling efforts and instead pivot those resources to improve the quality of their internal loss history through activities such as formalizing definitions of operational risk events, and improving incident identification and reporting.

Basel has provided specific guidelines and criteria for data quality. In particular:

- Banks are expected to base their ORC calculations on 10 years of data. During the transition period, five years of data is acceptable. However, for large institutions that previously used the AMA, 10 years of data should not pose a significant challenge as the required incident reporting processes and data quality procedures should already be in place.

- Data is most relevant when it can be directly linked to a bank's current businesses and internal operating environment. Extra consideration should be given to historical losses in businesses and activities that have been carved out and sold, or in businesses being wound down.

- Banks must have documented procedures and processes for the identification, collection and treatment of internal loss data – including documented de minimis thresholds. Documented policies and procedures for identifying and reporting operational risk events must serve as the starting point for managing data capture and quality.

- Associated procedures and processes must be validated before a bank's loss data can be used to calculate its ILM and ORC. Regular independent reviews by corporate audit functions and external organization are also required.

- Specific information and attributes should be collected as part of the data for individual operational risk events. These data elements include: gross loss amounts, and key reference dates such as the date of occurrence, date of discovery, and date of accounting. In addition, banks must collect information on recoveries of gross loss amounts as well as descriptive information about the causes and drivers of the loss event.

Basel has specified that banks failing to meet the minimum loss data standards might be subjected to severe penalties, including the requirement to hold capital that is at a minimum equal to 100% of their BIC.

# Changing behaviors and culture

In the financial services industry, the past decade has seen numerous well-publicized and damaging misconduct scandals, both institutional and retail. As a result, improving conduct is at the top of most firms' agendas.

Advanced operational risk management programs with predictive risk capabilities can provide intelligence on changes in employee sentiments and behaviors that might be early indicators of potential conduct lapses. However, deep-rooted changes at the culture level are also needed.

Many organizations have no pre-defined incentives or consequences related to high-frequency, low-impact operational losses. Typically, only massive loss events have any consequences for management. This is likely due to the fact that operational losses have traditionally been viewed as an unavoidable cost of doing business, and there is a common perception that management has no control over such losses (unlike credit and market risk which have standard levers for managing and mitigating risk).

In the wake of the financial crisis, some local regulators introduced 'claw back' frameworks and longer term incentive compensation linked to risk adjusted performance; however, these limited efforts have not had a significant impact on reducing the industry's overall operational losses. More recently, the introduction of conduct risk frameworks, and a renewed focus on culture risk, has helped some organizations begin to better understand the link between product design, compensation and sales incentives, management objectives, and employee behavior.

What is still missing in many cases is direct accountability for operational risk losses, specifically, consequences that have a meaningful impact on first line management, whether by affecting the size of their operating budgets and available investment funds or, more personally, by affecting their performance evaluations and compensation. These types of consequence and incentives can help establish a culture where operational losses are not just glossed over as a write-off in financial statements.

The SMA makes the long-term capital and business consequences of operational losses more significant for banks, and thus it is only common sense for banks to try and change behavior by aligning operational losses with business unit and executive performance. This will require institutions to empower their managers with enough authority and flexibility to change their business environment—including the underlying process and tools—and to manage risks more proactively.

# Gaining efficiency by automating data collection and aggregation from multiple sources

Cost efficiency is becoming a higher priority in risk management and compliance, with risk managers increasingly being expected to do more with less. This pressure is creating an incentive for risk leaders to explore and embrace new technologies and techniques that can help improve the efficiency and effectiveness of their programs.

A bank’s infrastructure for operational risk management should leverage automated workflows to continuously monitor for emerging problems and ensure the right people receive the right information in a timely manner, enabling them to respond quickly and effectively.

Banks can consider taking advantage of the latest advances in Robotic Process Automation (RPA) and cognitive technology to streamline and automate routine activities such as data collection, cleansing, and storage - for both structured and unstructured data. RPA ‘bots’ can be created to continuously scan the internal environment and collect data from pre-determined sources. In conjunction with increased information standardization and more intelligent optical character recognition (OCR) and cognitive technologies, these innovations can transform data into a powerful tool for real-time production and monitoring of key risk indicators, management information, and internal risk and control reporting.

A valuable byproduct of introducing these methods and technologies into operational risk management is the alignment of expectations and outcomes across the three lines of defense: the first-line businesses and functions where the risk originates; the second-line risk and compliance groups; and the third-line internal audit function. Once all three lines of defense agree on a solution and its inputs and outputs – for example, agreeing on what an RPA bot will do, what data it will use, and what reports it will generate – everyone should be able to use the same results, leading to synchronous and seamless alignment.

# Creating an effective infrastructure for aggregated risk data and risk reporting

When designing an infrastructure for operational risk data and reporting, institutions should consider the principles issued by the Basel Committee for effective risk data aggregation and risk reporting. Also known as BCBS 239, these principles apply to all key internal risk management models for regulatory capital, including the AMA for operational risk. Although the AMA is being replaced by the SMA, BCBS 239 will continue to be relevant to the design of an operational risk data infrastructure, given the importance of internal loss data to an institution's calculation of its operational risk capital using the SMA.

The principles outlined in BCBS 239 aim to strengthen banks' risk data aggregation capabilities and internal risk reporting practices. Broad areas covered by the principles include:

Overarching governance and infrastructure
Risk data aggregation capabilities
Risk reporting practices
Supervisory review, tools, and cooperation

According to BCBS 239, the term "risk data aggregation" refers to defining, gathering, and processing risk data. For operational risk, key activities include establishing policies that define operational risk incidents; specifying attributes to be collected for each event that is considered an operational risk incident; and building an internal loss history as part of an institution's operational risk database.

As we describe in more detail later in this point of view, moving forward, banks should consider expanding the attributes collected for operational risk events and include a broader range of data elements included in operational risk databases to enable more advanced data modeling and analytics.

**"Although the AMA is being replaced by the SMA, BCBS 239 will continue to be relevant to the design of an operational risk data infrastructure, given the importance of internal loss data to an institution's calculation of its operational risk capital using the SMA."**

# Developing advanced capabilities in risk analytics and predictive risk intelligence

Armed with aggregated historical data about internal losses (along with robust automated processes for data collection and management) banks will be better positioned to capitalize on advanced capabilities such as big data analytics, correlation and root cause analysis, and predictive risk intelligence, enabling them to identify patterns and trends that may help reduce internal losses in the future.

Banks have long been interested in finding ways to enhance their traditional operational risk practices to predictive risk intelligence.[1] Although historical data on operational losses is still the baseline for complying with regulatory capital rules, such data has always been seen as a blunt instrument for controlling loss and risk profiles. In the past, the necessary tools and technologies to make more insightful correlations and predictions did not yet exist.

A specific challenge is that most Basel historical data models do not provide enough information for organizations to identify truly meaningful correlations between losses and other factors, leading to insights that are obscure or spurious. Occasionally, experienced operational risk practitioners—with help from data scientists–have used their intuition to identify some patterns between risk profiles, losses, and the events in legacy models. However, this generally did not happen until long after the event occurred, and often was limited to situations where extreme data variations were clearly visible – situations that were so infrequent that they had no real predictive value.

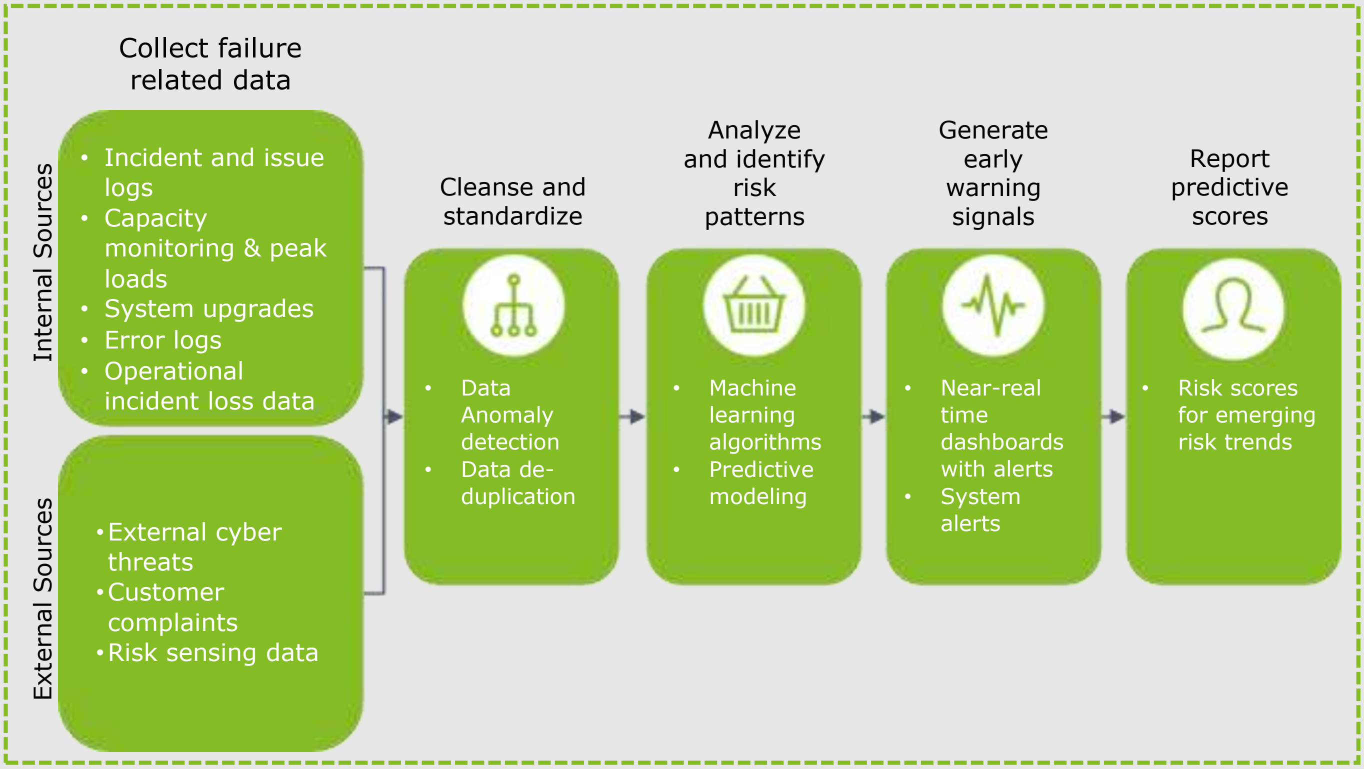
Given the advanced tools and vast amounts of data available today, banks should seize upon the valuable opportunities enabled by predictive risk intelligence, big data analytics, and other breakthrough innovations. Through techniques such as machine learning and artificial intelligence, banks now have the ability to efficiently build and mine large and complex data sets that combine traditional Basel data with transaction data, non-transaction data (e.g., HR information, compliance data, and internal management information systems), and external data (e.g., sensing data, social media, customer complaints, and regulatory actions). Such aggregated models enable vastly improved analytical results and insights by providing billions of data combinations, greatly increasing the likelihood of uncovering patterns and correlations that were previously unnoticeable or detected too late. This can help banks prevent unpredictable tail outcomes, potentially reducing operational losses and capital impacts.

Banks also need to develop robust reporting capabilities that can provide early warnings about emerging situations that may exceed their risk tolerance and risk appetite. Several leading institutions are already using advanced analytics and big data techniques to improve the effectiveness of their risk programs in a wide range of areas, from trade surveillance and third-party risk management to fraud prevention, anti-money laundering and regulatory reporting.

[1] Please see our whitepaper – "Seeing the storm ahead - Predictive Risk Intelligence, 2017, "available at https://www2.deloitte.com/us/en/pages/risk/articles/predictive-risk-intelligence.html

# Predictive Risk Intelligence case study

As the world becomes more digitized and customers and counterparties continue to leverage multiple bank provided platforms for their transaction needs, banks rely heavily on the 24x7 availability of the underpinning technologies to facilitate these transactions. Regulators have also stepped up their efforts to curb technology failures in a greater effort to maintain the integrity of markets and to protect customers. The loss from a technology failure can not only damage an organization's reputation and drive away potential revenue, but could result in significant fines from regulatory agencies.



Collect failure related data
Internal Sources
• Incident and issue logs
• Capacity monitoring & peak loads
• System upgrades
• Error logs
• Operational incident loss data
External Sources
• External cyber threats
• Customer complaints
• Risk sensing data
Cleanse and standardize
• Data Anomaly detection
• Data de-duplication
Analyze and identify risk patterns
• Machine learning algorithms
• Predictive modeling
Generate early warning signals
• Near-real time dashboards with alerts
• System alerts
Report predictive scores
• Risk scores for emerging risk trends

Deloitte's Predictive Risk Intelligence (PRi) solution can help provide information on increasing risk profiles within an organizations and potentially provide advanced warning of a technology failure event. The PRi solution begins by collecting and evaluating internal and external variables that can best predict a future technology failure. Data is cleansed and standardized to remove anomalies and machine learning algorithms and other advanced analytics are applied to the data to identify potential patterns of causation and correlation to technology failures, which typically have a very short cycle to impact. Leaders can then view a near-real time dashboard that provides alerts and early warnings for the organization's critical systems.

# Looking ahead

As operational risk managers search for ways to increase the value of their programs, much of their focus should be on reducing internal losses. An essential step in achievement of that objective is to improve the quality and completeness of internal loss data and the greatest value will revolve around identifying patterns and correlations in data and predictive intelligence – aggregating internal loss data with data from a wide range of other internal and external sources, and then using the latest cognitive, machine learning, and analytics tools to identify dangerous buildups of potential risk.

These advanced capabilities can give a bank the forward-looking insights it needs to develop effective strategies for mitigating risk and reducing losses, including reducing the bank's ILM and required ORC.

# Contacts

**Monica O’Reilly, Banking and Capital Markets Advisory Leader**
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
monoreilly@deloitte.com
+1 415 783 5780

**Nicole Sandford, Regulatory and Operational Risk Leader**
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
nsandford@deloitte.com
+1 203 708 4845

**Krissy Davis, Operational Risk Leader**
Partner | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
kbdavis@deloitte.com
+1 617 437 2648

**Nitish Idnani, Operational Risk Banking Leader**
Principal | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
nidnani@deloitte.com
+1 212 436 2894

**Steve Bhatti**
Specialist Leader | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
stbhatti@deloitte.com
+1 617 437 2451

**Christopher Thackray**
Specialist Leader | Deloitte Risk and Financial Advisory
Deloitte & Touche LLP
cthackray@deloitte.com
+1 585 238 3323

**Dimitrios Goranitis**
Risk and Regulatory Advisory Partner
Deloitte Central Europe
digoranitis@deloittece.com
+40 212 075 396

This publication contains general information only and Deloitte is not, by means of this publication, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This publication is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this publication.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of our legal structure. Certain services may not be available to attest clients under the rules and regulations of public accounting.