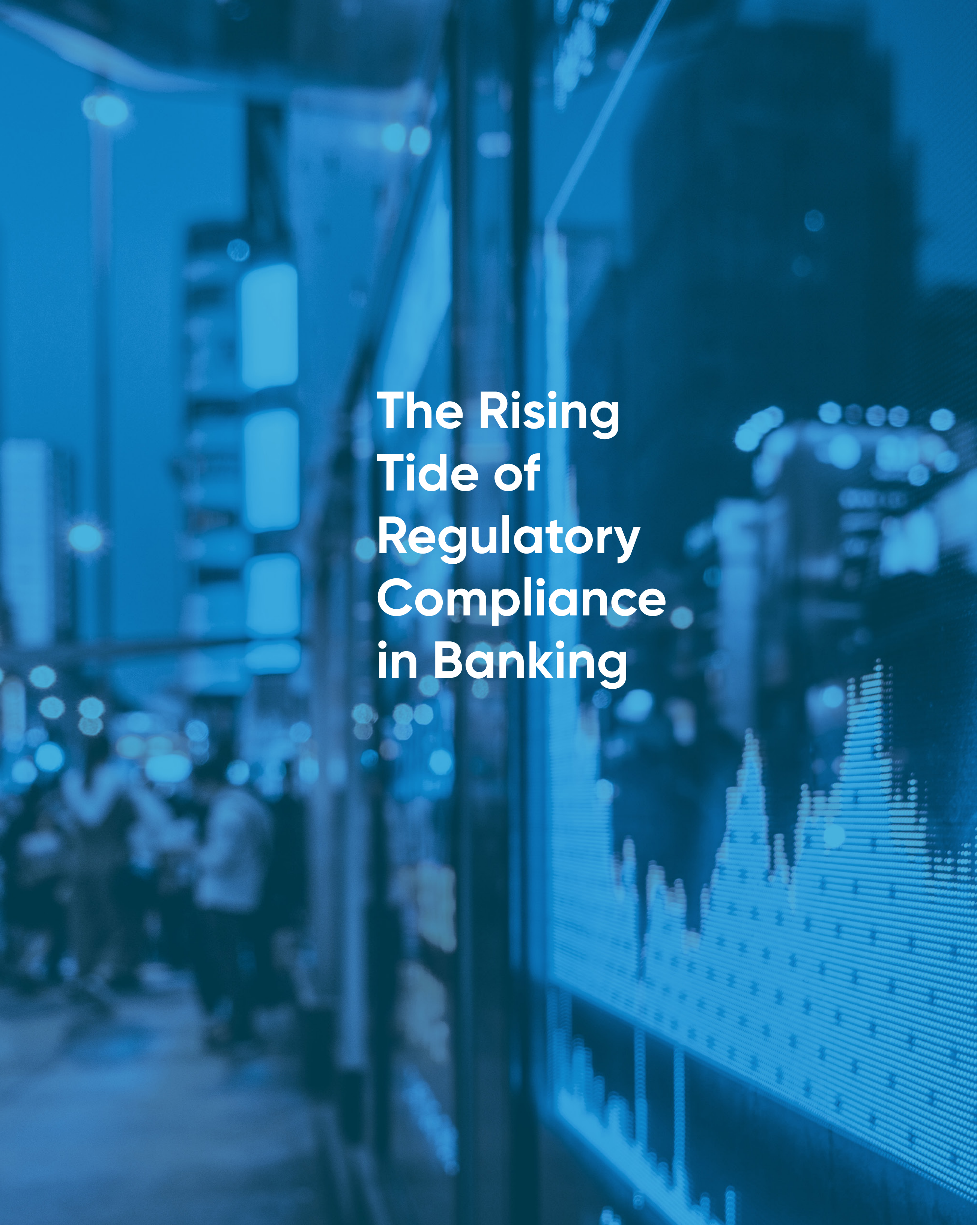
DELPHIX

Tackling The Data Challenge For Regulatory Compliance in Banking

3 Ways to Rethink Data Management to Comply Faster and Smarter



The Rising Tide of Regulatory Compliance in Banking

We'll cut to the chase—staying above the rising tide of banking compliance requires data: Securing it, integrating it, sharing a new level of detail with regulators, and developing with it to build banking, trading and customer processes that meet regulatory requirements. Data is the fuel that internal development teams, risk management analysts and other stakeholders need to update both technology and process—to not only report on to comply but to model the financial impact of compliance rules.

Overcoming the data roadblock to compliance has become a profound issue for banking industry executives as they struggle to meet the wave of regulations hitting the industry. Transactional, customer, institutional, FX, counterparty and numerous other datasets that are core to compliance remain buried trading platforms, proprietary and legacy applications. Tapping into it is manually intensive, often creates duplicative effort, and each data extract poses its own risk because mishandling data in a rush to meet banking compliance rules can create data privacy jeopardy, or increase the risk of a breach. Banks are facing a rising tide of compliance costs—from internal costs, to fees, to penalties. Since 2009, fines and settlements have increased almost 45X(2). Putting processes and reporting in place to reduce regulatory risk requires getting data to the right people at the right time—from internal teams to outside industry regulators.

And with ever increasing regulation, the need to improve data agility to cope with change has never been more pressing. Gaining Perspective. Taking Action. It's why Delphix commissioned market research firm, Vanson Bourne, to investigate the regulatory compliance hurdles around data facing banks today. As part of the research, they interviewed 90 banking executives with commercial and corporate responsibility, IT roles, or in risk, compliance and legal. This eBook highlights the three most pressing concerns around data for compliance, specific regulations that require data process overhaul, and a plan for where you can employ the latest data management best practices to use data to not only comply faster but do so with less cost.

"Around the globe, most bank executives believe regulators will continue to increase requirements for data capabilities."

McKinsey[1]

What We Heard: Three Data Strategies to Comply Smarter

Secure Data. Everywhere.

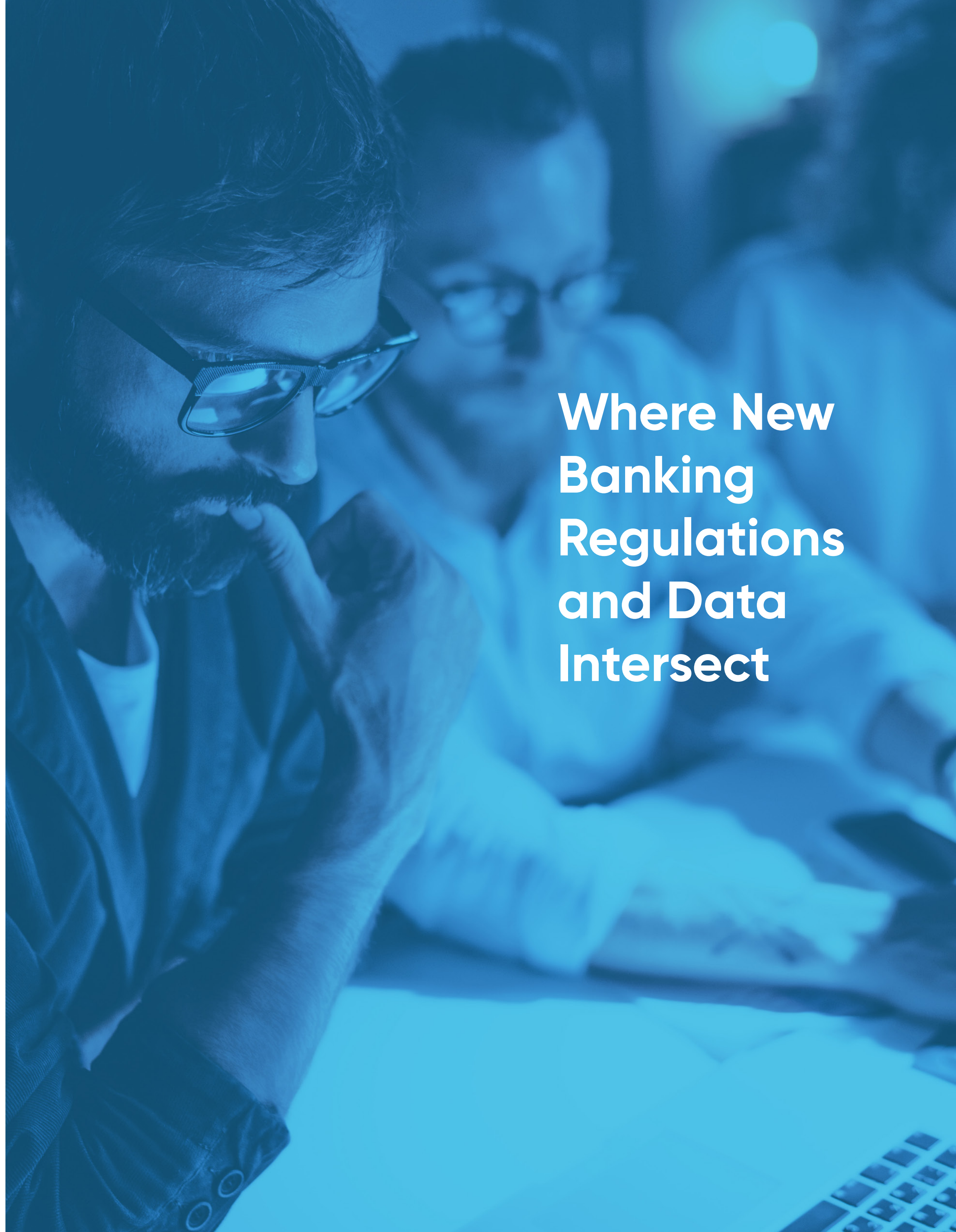
And by everywhere, we mean not only production but non-production too. For many organizations, about 80% of sensitive data resides in sub-secure environments—like dev, test, or ad hoc silos—and four out of five Bankers surveyed (81 per cent) tell us they face data security challenges in their compliance journey. In fact, that's likely where most of your risk is too. UK financial firms alone suffer at least 800 data breaches per year, and the costs range from penalties to lack of trust—and the average cost of a breach is about $3M (€2.7M) With developers, test teams all working with potentially sensitive data as they create new reports, risk models, and build new integrations, it's essential data is masked wherever possible.

Deliver Data to Where it Matters. Fast.

Data delivery is the biggest reporting barrier faced by banks as almost all (92 per cent) said they face it. It's not only for reporting—finance and risk management teams need better data faster to feed and update their risk models. Relying on DBAs to pull data manually, IT-centric reporting processes, multiple copies of the same data, increasing data volumes are all slowing down projects. No surprise then that our survey found that 36 per cent of financial services professionals are at high risk of missing reporting deadlines due to data issues.

Test with Fresh Data. Continuously.

40-percent of survey respondents said they have testing roadblocks. Overcoming those issues means the opportunity to test more, build more robust regulatory reports, and have more accuracy in risk models. It's why banks are shifting towards real-time data to feed testing processes, with nearly one-third (31 per cent) of respondents indicating they need real-time copies of data for testing. The reason is that regulatory reports, redeveloped business processes, updated risk models, and redefined integrations all require rigorous and continuous testing. Data is often hard to extract from applications like Murex, Calypso, Front Arena, Summit, Mysis, and others, never mind continually refreshing downstream testing and reporting environments.



Where New Banking Regulations and Data Intersect

In the survey, banking executives commented that compliance failure isn't only about financial risk in terms of penalties, as 53 percent noted, it's also about losing the banks competitive position in a much more fluid marketplace, as 51 percent indicated too. But what regulations put the most pressure on data? Below are some of the top regulations that have big implications on your data strategy.

Banking executives are responding: A recent Global Risk Data and Technology Benchmarking survey conducted by the Institute of International Finance (IIF) found that two-thirds4 indicated that they are aligning their regulatory programs with a strong focus on using data for the fundamentals: improving operations and IT, enhancing risk management and to better support the business.

More Transparency: Dodd-Frank, SFTR

The Dodd-Frank Act (known as the Dodd-Frank Wall Street Reform and Consumer Protection Act) is a US federal law enacted in July 2010 to limit risk by enforcing transparency and accountability in banking and financial securities trading. The main purpose is to help prevent another deep financial recession in the US. Dodd-Frank created the Consumer Financial Protection Bureau (CFPB) to protect consumers from large, unregulated banks and consolidate the consumer protection responsibilities of a number of existing bureaus.

The EU has similar initiative in place to increase transparency in the Securities Financing Transactions market called the Securities Financing Transactions Regulation (SFTR), which requires securities trading firms to report Securities Financing Transactions.

More Data Granularity: MiFID II

The Markets in Financial Instruments Directive II (MiFID II) was originally conceived to bolster investor confidence in reaction to the financial crisis and is affecting everyone in the industry. The new rules put a substantial burden on reporting and in turn trading platforms, creating potentially petabytes of data. For example, some trades must be time stamped to 100 microseconds, while some transactional reports must stretch to 60+ fields, and the data itself must be stored for 5+ years.

More Data Connectedness: PSD II

The Payment Services Directive 2 (PSD II) poses a significant technical challenge because it requires banks to open their payments infrastructure and customer data assets to third parties, while all mandating enhanced security and strong customer protection.
Third party access to customer data is a clear concern for banks and legal experts, especially with the advent of GDPR. Legacy banking applications were simply never designed to be so open, and often lack the APIs for the degree of integration necessary.

More Data Quality: BASEL 3

Complying with Basel 3, and the Basel Committee on Banking Supervision (BCBS) rule 239 ‘Principles for effective risk data aggregation and risk reporting’ creates a profound data management challenge for Global Systemically Important Banks (G-SIBS) and Domestically Systemically Important Banks (D-SIBS) alike. BCBS 239 ups that ante for the velocity and breadth of data to drive risk models. First, risk models must have more and better-quality risk data. Second, banks need to roll up and report on risk data from systems within hours rather than days or longer.

More Data Volume: IFRS 9

International Financial Reporting Standards (IFRS 9) impacts both Risk and Finance functions, changing the way credit losses are recognized and requiring more modelling around the bank’s assets, and potential future losses. It not only hikes modelling complexity but also increases data volumes with the need to model at the individual asset level of detail.

More Data Privacy: GDPR

No doubt you're familiar with the General Data Protection Regulation (GDPR) that creates a further privacy and data security framework that financial services institutions must consider as part of all production and non-production processes. In the rush to integrate and develop new apps and reporting to meet other banking regulatory requirements, GDPR represents a significant landmine. Penalties can run as high as 4% of annual turnover, and there is only a small 72-hour window to report a breach. It's a potential landmine with so many non-production environments that have duplicated copies of data.

More and more US states and countries around the world are enacting data privacy laws. One stringent new law was enacted in California, called the California Consumer Privacy Act (CCPA), mandates that companies doing business in California must comply with a new set of sweeping provisions designed to protect the privacy of consumer data.

According to the data privacy laws, organizations must implement new processes and technologies that govern how sensitive data is processed, shared, and secured. Those that fail to adopt an enterprise-wide strategy data privacy compliance risk fines, lawsuits, and reputational damage.

5

More Regulations

Depending on your banking sector, you may have different regulations, including meeting the new Insolvency Hierarchy Directive, potential updates to the European Deposit Insurance Scheme (EDIS), New York Department of Financial Services Cybersecurity Regulation, the Anti-Money Laundering Directive (AML), CRD IV, the new EU Benchmarks Regulation and more. But what they all have in common is handling data better, faster, putting it in the hands of IT, finance, risk teams, to build systems, update models, and exchange it, securely and reliably.

"Data management at the heart of regulatory compliance"

British Bankers Association[5]

Drilling Down

Secure Data. Everywhere.

Data masking helps shield sensitive business and personal information, so even in the event of a data breach, hackers gain nothing of value. While nearly half of respondents (49 per cent) believe better data masking will improve their organization's compliance journey, 59 per cent said data masking remains troublesome.

It's because for every change to processes, reporting, integrations and risk models to meet new regulatory compliance rules, real data must be copied and refreshed numerous times throughout its development and test cycle. Much of this data is highly sensitive. In fact, the bulk of sensitive data often lies outside of production systems. Data provisioning is already a highly manual process, but protecting the data adds even more complexity and cost.

Banks run 100s of non-production environments, and it's painfully easy for one of them to contain unmasked sensitive data. Masking data has always been a painful task, adding days to the provisioning process and meaning banks sometimes opt out and risk using sensitive data to feed downstream processes instead. However, with GDPR and CCPR, the legal requirement to masking sensitive data is a lot more explicit, and the potential penalties much greater.

TAKE THE MANUAL OUT OF DATA MASKING.

There's a shortcut: The latest technology enables you to automatically and irreversibly mask data just once and then deliver it repeatedly to every environment. A "maskonce, deliver-many" approach ensures data can be securely delivered on demand where it is needed, without manual human intervention.

And one more thing: Modern data masking doesn't mean randomly scrambling data. It means anonymizing it while still maintaining its integrity, so it doesn't compromise testing results.

Fail-safe protection means banks can deliver this data anywhere, across departments, third parties and cloud providers, without elevating GDPR risk, run afoul of other privacy regulations, or raise the risk of a breach.

Boeing Employees' Credit Union (BECU) Rolls Out Online Banking Enhancements Without Compromising Security

Delphix helps BECU deliver digital features to its customers faster, with higher quality, and more security. With Delphix, BECU reduced the overall time and effort to distribute securely masked data for application developers. The Delphix platform profiles and finds instances of sensitive information contained in the data and consistently masks that data across relational database platforms and flat files. BECU implemented Delphix masking in fewer than six weeks enabling them to meet internal compliance requirements ahead of schedule. In addition, Delphix virtualization reduces the overall time and effort to distribute masked data, making it possible to launch new banking products up to two times faster.

"Not only does Delphix allow us to reduce our risk footprint by masking sensitive data, but we can also give developers realistic, production-like environments, which ensures we're not introducing defects because of bad data."

KYLE WELSH
Chief Information Security Officer, BECU

Deliver Data to Where it Matters. Fast.

Copying and refreshing data is highly manual and creates process bottlenecks which can take multiple administrators several weeks to work through. In our survey, speeding up data delivery (46 per cent) is the #1 capability banks are looking for to improve their compliance obligations. It's no wonder because banking data volumes are growing exponentially—making it increasingly difficult to extract and update for downstream developers, test, modelers, who need it to create regulatory reports, develop or adjust newly compliant processes.

DELIVER DATA. VIRTUALLY.

With so many regulatory changes, risk and compliance teams need more power than ever. Modern dynamic data platforms enable data in non-production risk and compliance environments to be not only refreshed, but snapshotted, rewound to a point-in-time, and branched. It's built around new technology to efficiently deliver data for better compliance, known as a data virtualization. It cuts the need for physical copies of data that would otherwise take too long to copy, update, and just take up too much storage space. Taking a data virtualization-based approach enables teams to cut non-production data footprints by up to 80 to 90 per cent by instead storing virtual copies of data.

European Bank Automates Data Masking to Meet GDPR Compliance

A large Northern Europe bank had a six-month project to mask all sensitive data in preparation for the new EU General Data Protection Regulations (GDPR). Masking 9,500+ data sources used by 128 applications would have taken over two years using current technology and process.

Using Delphix the bank automated much of the data masking and delivery process meeting the timeline requirements and saving significant service and storage costs. Now GDPR compliant, the bank can provide masked data anywhere in the business in hours, rather than days.

Test With Fresh Data. Continuously.

Fresh data is the lifeblood of risk models and regulatory reports, for testing scenarios, testing reporting, and other compliance initiatives. Doing more testing with fewer resources is the second biggest capability (34 per cent) banks want today during the compliance journey. Simply, testing with subsets or stale data sacrifices quality.

THINK CONTINUOUS SYNCHRONISATION.

Access to data, shouldn't mean compliance teams are waiting days for a DBA to fulfil a data request. Deploying a self-service portal for data enables any team interacting with data to refresh their environment at any point in time themselves. Modern dynamic data platforms enable data in non-production environments to be continuously synchronized. Doing so not only cuts the need for data refreshes but also enables risk teams to more effectively model stress scenarios by efficiently testing models on the latest data.

It all adds up to enabling teams to test more, and test continuously—without taxing production systems, so they can go faster and maintain quality. Testers and analysts have their own copies of real-time and historical data and can work in parallel on their immediate compliance task at hand.

Continuous Data Delivery for Regulatory Risk Modeling at Large National Bank

With regulations driving new reporting requirements for a line of business, this bank used the combination of continuous synchronization, data virtualization and data self-service to speed data access for risk modelling and reporting. They used Delphix to efficiently double the number of environments available for risk analysis, and reduced risk model time-to-market by 50% while gaining a 3X ROI based on storage savings alone.

The Road Ahead

The journey to compliance has many obstacles. Data is one of the largest: Copying and moving ever-increasing amounts of data has become riskier and more painful. At the same time, banks are under immense pressure to innovate faster. Meeting compliance obligations can take seven some of the most well resourced banks months to complete and put a strain on every team: IT, compliance, risk and reporting.

It's time to make a change.

Making data flow more easily and making it more dynamic is proven to accelerate project velocity by 2X. Data virtualization enables organizations to deliver data faster and more efficiently. Data masking has evolved too and can now be automated, and "masked-once, delivered-many". It frees banking teams to focus on delivering more value and spend less time waiting for data, so they can build compliance reports faster, model risk continuously, and even free valuable resources for innovation. Because more dynamic data is the key to faster, smarter compliance.

1. https://www.mckinsey.com/business-functions/risk/our-insights/living-with-bcbs-239
2. https://www.mckinsey.com/business-functions/risk/our-insights/a-best-practice-model-forbank-compliance
3. http://www.eweek.com/security/average-global-cost-of-a-data-breach-now-3.6m-ibmreports
4. https://www.mckinsey.com/business-functions/risk/our-insights/living-with-bcbs-239
5. https://www.bba.org.uk/news/insight/data-management-at-the-heart-of-regulatorycompliance/#.WxmcvYpKguV
6. https://www.globallegalinsights.com/practice-areas/banking-and-finance-laws-and-regulations/usa

Take The Next Step

Schedule a meeting with a Delphix solution expert and learn how to accelerate your compliance process. During the meeting, we'll discuss:

- **Your goals —like regulatory compliance, risk modelling, and improving project velocity**
- **How Delphix has helped teams like yours (and you'll see a demo too)**
- **What an initiative would look like at your organization**

REDWOOD CITY (HQ)
1400A Seaport Blvd, Suite 200
Redwood City, CA 94063
TEL: (650) 494-1645

SAN FRANCISCO
343 Sansome St, Suite 900
San Francisco, CA 94104
TEL: (415) 964-5140

ATLANTA
3600 Mansell Rd., Suite 350
Alpharetta, GA 30022

COLORADO
350 Terry St., Suite 320
Longmont, CO 80501

BOSTON
230 Congress St, Suite 200
Boston, MA 02110

TOKYO
BUREX Kyobashi 2-7-14 Kyobash
Chuo-ku, Tokyo, Japan
TEL: +813-5579-9415

LONDON (EUROPEAN HQ)
68 King William St.
London EC4N 7DZ

BASINGSTOKE
Suite 42 & 43 The Coach House
Worting Park, Basingstoke,
Hampshire, RG23 8PX

FRANKFURT
The Squaire 12
60549 Frankfurt, Germany

DELPHIX

q220-000010

ABOUT DELPHIX

Delphix unlocks enterprise data, whether on-premise or in the cloud and provides self-service, personal-data-environments that are available in minutes with full control over bookmarking, branching, sharing, refreshing, and restoring data while enabling secure masking of sensitive PII and PCI information.

With Delphix, Financial Services organizations and Banks can quickly and securely deliver data for differentiated product offerings, enhanced customer experiences, expanded partnerships, and better business modeling to protect profits and stay ahead of constantly changing regulations.

For more information visit www.delphix.com

Visit Delphix online at delphix.com.