

BCG

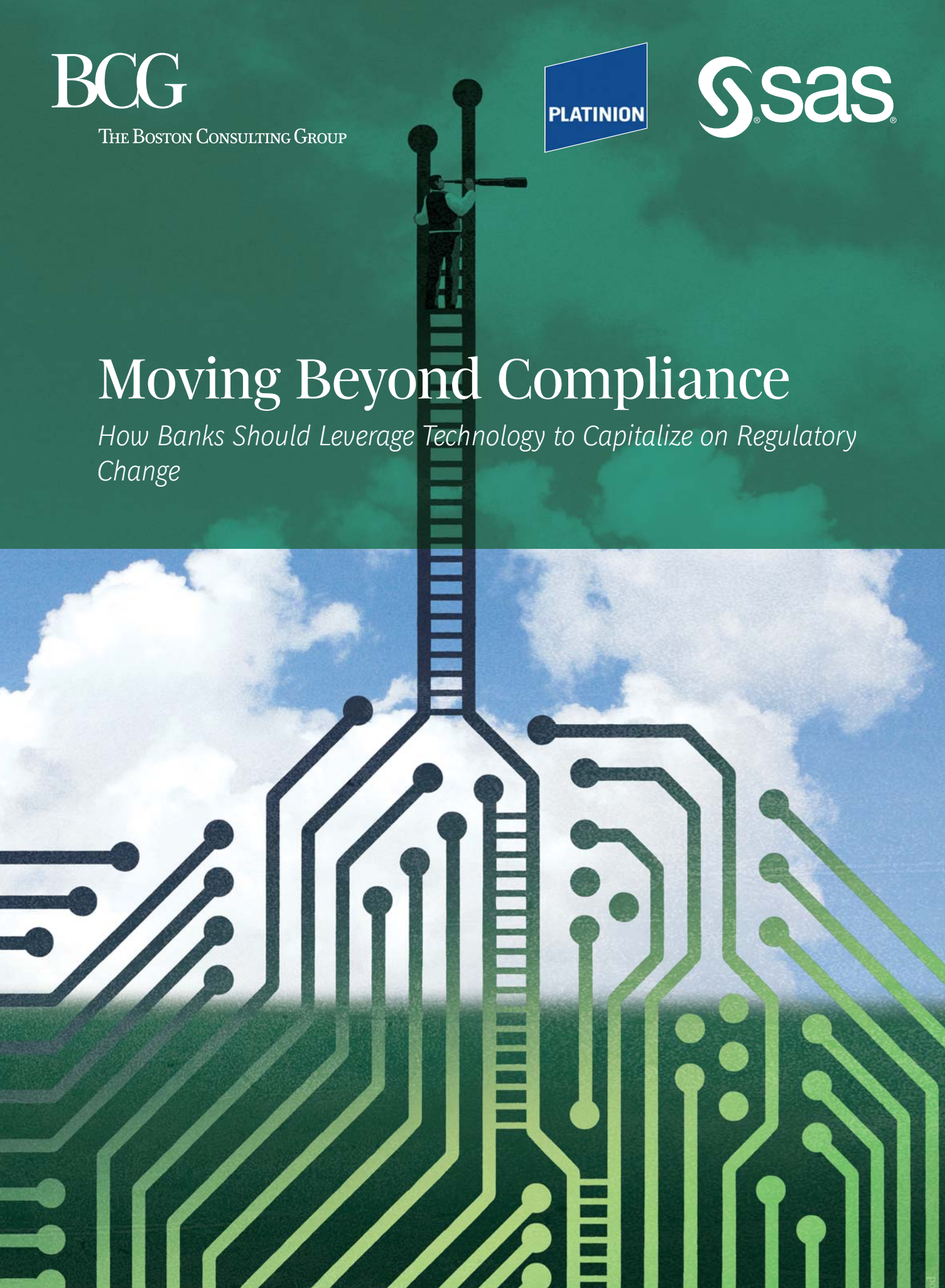
THE BOSTON CONSULTING GROUP

PLATINION

sas

Moving Beyond Compliance

How Banks Should Leverage Technology to Capitalize on Regulatory Change



The Boston Consulting Group (BCG) is a global management consulting firm and the world's leading advisor on business strategy. We partner with clients in all sectors and regions to identify their highest-value opportunities, address their most critical challenges, and transform their businesses. Our customized approach combines deep insight into the dynamics of companies and markets with close collaboration at all levels of the client organization. This ensures that our clients achieve sustainable competitive advantage, build more capable organizations, and secure lasting results. Founded in 1963, BCG is a private company with 74 offices in 42 countries. For more information, please visit www.bcg.com.

Platinion is a wholly owned subsidiary of BCG whose consulting services focus on developing and implementing business-critical IT concepts. Platinion supports clients from diverse business sectors and has a particularly strong presence in financial services. Seamlessly integrated into BCG's worldwide network, Platinion helps its clients define individual IT architectures, restructure IT processes, manage implementation, and—together with BCG—develop IT strategies. Our work is characterized by a close connection between technology and business strategy. After all, IT is generally not an end in itself: an effective IT setup can be developed only by considering the overall company perspective. For more information, please visit www.platinion.de.

With annual revenues of \$2.43 billion, SAS is the leader in business analytics software and services and the largest independent vendor in the business intelligence market. Through innovative solutions, SAS allows companies to transform data about customers, performance, financials, and more into information and insight that lay the groundwork for solid and coherent decisions. SAS's products are used at more than 50,000 sites in over 100 countries. The headquarters of the U.S. parent company, founded in 1976, are in Cary, North Carolina. SAS Germany has its main office in Heidelberg and regional offices in Berlin, Cologne, Frankfurt, Hamburg, and Munich. For more information, please visit www.sas.com.



Moving Beyond Compliance

How Banks Should Leverage Technology to Capitalize on Regulatory Change

BCG

Walter Bohmayr, Peter Neu, Michael Grebe, Kai-Oliver Müller, and Amarendran Subramanian

Platinion

Christoph Geier and Jens Müller

SAS

Christoph Benzinger, Frank Hansen, and Carsten Krahl

October 2011

AT A GLANCE

A wave of regulatory reform is forcing banks to revisit the technology used to measure and manage risk. This presents an opportunity to develop IT capabilities that provide a more nuanced view of how and where banks utilize financial resources.

UNDERSTANDING THE IMPLICATIONS OF REGULATORY REFORM

The new rules will affect and potentially reshape banks' business models and put much greater demands on risk IT functionality and infrastructure. Three areas, in particular, will require significant upgrades: data gathering, models and calculation engines, and reporting capabilities.

THE CTF FRAMEWORK: DEFINING A PATHWAY FOR RISK IT

The Compliance–Transparency–Forecast framework helps banks set clear goals for enhancing their risk-related IT capabilities, with a view toward not simply ensuring compliance but also generating a more incisive perspective on risk.

UPGRADING THE RISK IT ARCHITECTURE

To support their evolution along the CTF framework, banks will need to make changes throughout the various layers of their risk-IT architectures, with an emphasis on improving consistency, performance, and transparency.

OVER THE NEXT SEVERAL years, regulators will implement a range of risk management reforms designed to lend greater transparency and stability to the global banking system. The new regulatory environment will have a significant impact on the industry, changing not just the way banks measure and manage risk but also how they run their businesses. From a technology perspective, the task of accommodating these new requirements is a steep challenge.

If banks were to focus only on compliance, however, they would forgo gaining a much more nuanced, forward-looking view of how and where they utilize their financial resources—namely, capital and liquidity. This would be a costly missed opportunity. One way or another, most banks will need to retool their risk-IT architectures. An IT overhaul provides a chance to develop capabilities that will generate not only information—as mandated by the new rules—but also insight.

To leverage technology in a way that capitalizes on regulatory reform, banks must answer the following questions:

- How will the new regulations change the processes used to manage risk and steer financial resources within the bank?
- How high should we aim, in terms of leveraging our risk-management and steering capabilities, to stay not just compliant but also competitive?
- What are the specific business and IT requirements stemming from this aspiration, and what do they mean for the bank's risk-IT architecture?
- What is the best approach—and the most suitable transformation sequence—to close the gap between the current and target risk-IT architectures?

This report addresses these questions, primarily in the context of a framework and a process designed explicitly to help banks improve their risk-IT architectures. The practical application—and benefits—of such an approach are illustrated by a case study of a major European bank that transformed its risk-IT architecture as part of an effort to enhance its approach to managing risk.

Understanding the Implications of Regulatory Reform

The banking industry is in the midst of a regulatory overhaul. As the new requirements come into force, the effective management of scarce financial resources will

become an increasingly important source of competitive advantage. The stakes are high: these resources have remained in short supply since the onset of the financial crisis. As a result, banks will need to develop a more accurate reading of the capital and liquidity implications of their business strategies and product portfolios.

The effective management of scarce financial resources will become an increasingly important source of competitive advantage.

The growing importance of managing financial resources is being driven by three sets of regulatory changes: the introduction of Basel III (which entails both capital and liquidity requirements); the ongoing implementation and enhancement of the Internal Capital Adequacy Assessment Process (ICAAP); and revisions to the International Financial Reporting Standards (IFRS 9), which aim to simplify the classification and measurement of financial instruments.¹ (For more on these changes, see the sidebar “The Changing Regulatory Environment.”)

THE CHANGING REGULATORY ENVIRONMENT

Regulators have developed a broad set of reforms designed to lend greater stability to the banking sector.

Basel III. Basel III defines new requirements regarding the amount and quality of capital that banks must hold. It also introduces new ratios for managing liquidity risk, along with the so-called leverage ratio, which compares Tier 1 capital with total assets and off-balance-sheet items.

Banks need to generate a comprehensive view of their risk coverage and regulatory capital usage, from the portfolio down to the position level. They should also ensure that capital is allocated efficiently and risks are adequately priced. These overarching goals give rise to three sets of imperatives relating to risk coverage, the capital base, and leverage.

- To enhance their risk coverage, banks must develop a stressed-market VaR model and calculate the incremental risk capital (IRC) charges for default and migration risk. Banks also need to calculate higher capital requirements for

counterparty credit risk (factoring in increased risk weights), additional capital for credit value adjustment, and increased risk weights for (re-)securitization and financial institutions.

- The capital calculation model needs to be changed according to the new rules (for example, by excluding hybrid instruments in core Tier 1 capital and phasing out public-sector capital and silent participations). In addition, banks need to implement new minimum values in the capital ratio calculations for core Tier 1, Tier 1, and total capital, and calculate conservation buffers and countercyclical buffers on the rate of credit growth. For systematically relevant banks, the model also needs to calculate the additional capital buffer.
- Banks need to calculate the leverage ratio, which is the Tier 1 capital ratio versus the gross balance sheet (including off-balance-sheet items), with the appropriate credit-conversion factor.

THE CHANGING REGULATORY ENVIRONMENT

(continued)

By making their short-term and structural liquidity positions more transparent (down to the level of individual cash flows), banks can enhance their liquidity-management and fund-pricing capabilities. The new rules regarding liquidity have implications on short-term liquidity, structural liquidity, and funds transfer pricing (FTP).

- Banks must calculate two new ratios—the liquidity coverage ratio (LCR) and the net stable funding ratio (NSFR)—and integrate them into regulatory reporting. Furthermore, banks need to implement new monitoring tools.
- Banks also must ensure that the FTP model accounts for the true costs of liquidity—in other words, that it factors in funding curves, behavioral adjustments of cash flows, and the costs of the liquidity reserve.

ICAAP (Basel II). ICAAP sets guidelines for the internal assessment of a bank's overall capital adequacy as well as its strategies for maintaining adequate capital levels. The push by regulators to improve banks' capital-assessment processes has been driven by several factors.¹

- The global financial crisis highlighted the shortcomings of banks' internal capital-assessment processes. As a result, many banks have already started upgrading their ICAAP frameworks (as requested by regulators) by, among other things, better

integrating key steering processes, incorporating additional risk types, defining more realistic scenarios, and reviewing economic capital components.

- The new standards for stress-testing, which were put in place in 2009 and 2010, have a direct bearing on banks' internal capital-assessment processes. The stress tests carried out by the European Banking Authority (EBA) for regulatory capital—based on Basel II, Pillar 1—also underscore the need for banks to run macroeconomic scenarios as part of their capital-adequacy assessment.

IFRS 9. In April 2009, the IASB announced an accelerated timetable for replacing IAS 39 Financial Instruments with IFRS 9, which aims to move accounting rules closer to the economic perspective. The new accounting rules are intended to come into full effect in January 2013. The project to replace IAS 39 has been divided into three phases:

- *Classification and Measurement.* According to the new regulations, the number of accounting categories of financial instruments (financial assets and liabilities) will be reduced from four (held for trading, available for sale, loans and receivables, hold to maturity) to two (at fair value and at amortized costs). The requirements related to the fair-value option for financial liabilities were also changed.

The global financial crisis highlighted the shortcomings of banks' internal capital-assessment processes.

THE CHANGING REGULATORY ENVIRONMENT

(continued)

- *Impairment Methodology.* There will be a shift away from the current incurred-loss concept toward an expected-loss view. Depending on the risk profile of the financial asset, the cumulative expected loss has to be considered at once or on a pro rata temporis basis.
 - *Hedge Accounting.* The new rules aim to narrow the gap between economic hedging under a risk perspective and hedge accounting. The current draft of IFRS 9 focuses on the possibility of hedging only some risk categories as well as net positions, instead of
- single assets. The proposed standards also aim to reduce the complexity arising from different kinds of portfolio hedges (fair-value hedges versus cash flow hedges) by introducing one kind of portfolio hedge.

NOTE

1. There are wide variations in how European regulators assess capital requirements. In some countries, such as France, Spain, and the United Kingdom, regulators rely on their own models, scorecards, and stress scenarios. In other countries, such as Austria, Belgium, and Germany, the supervisory review process is based on the bank's ICAAP.

IT REQUIREMENTS STEMMING FROM THE NEW REGULATIONS

The new rules, particularly the capital and liquidity requirements imposed by Basel III, will change the competitive dynamics of the industry and force many banks to revisit their business models. As profound as these changes are, banks must not lose sight of the technical side of reform, which is essential to their ability to stay compliant—and competitive—in the new regulatory environment.

Banks must not lose sight of the technical side of reform, which is essential to their ability to stay compliant—and competitive.

On the technology front, the changes range from new demands on functionality, including calculations and reporting, to increased pressure on the underlying infrastructure, especially data storage and computing capacity. Three areas, in particular, will require significant upgrades: data gathering, models and calculation engines, and reporting capabilities.

Data gathering is certain to become more demanding and complex, with substantially more data to consolidate, greater demands on data availability, and a pressing need to ensure consistency across expansive data sets. Specific requirements for static, position, and market data include the following:

- Integrate all static and position data at the transaction level into the data warehouse. The data should cover all on-balance-sheet (assets and liabilities) and off-balance-sheet items, and should be consistent, aligned, and unique. Current and historical data need to be accessible. Users should be able to aggregate transaction data to provide a portfolio view.
- Integrate data derived and calculated from position data (for example, present value, sensitivities, exposure, PD, LGD, EL, or EAD) into the data warehouse.

Calculated data, including cash flows at the single-transaction level, must be explicitly linked to their underlying transaction data.

- Integrate present and historical market data, including macroeconomic data (such as market credit volumes) and institution-specific data (such as CDS spreads and funding curves), into the market data warehouse.

Banks will have to expand and strengthen the functionality and flexibility of their *models and calculation engines*. In the new regulatory environment, these tools will need to provide not only more metrics but also more frequent updates. Specific requirements include the following:

- Provide calculation engines for risk assessment (for example, present value, sensitivities, exposure, or EPE), capital ratios, the leverage ratio, and liquidity ratios (LCR and NSFR). The engines must be implemented within the risk IT infrastructure and be audit-proof (including versioning). They should enable the monitoring, planning, and forecasting (through scenario analyses) of figures.
- Enhance the ICAAP model by assessing and including all material risks in the risk models, defining adequate capital components qualified to cover the risks, and further incorporating stress tests into the model. In addition to gone-concern analyses, which aim to protect a bank's creditors, going-concern concepts and calculations should be implemented.
- Develop a cash flow generator that can roll out multiple sets of cash flows (contractual cash flows, behavioral adjustments, and stress scenarios) at the transaction level on a daily basis. Cash flows should be stored and made accessible in the data warehouse.
- Expand the calculation engine for credit provisioning to include expected loss at the transaction level. The hedge accounting tool should be enhanced to calculate accounting hedges (effectiveness and values) according to the new rules (for example, combination of deals or single risk types).

Enhanced *reporting capabilities* will be critical to steering financial resources. Risk IT infrastructures will need to provide dynamic front-end systems that display aggregated data and allow users to drill down into the details. Specific requirements include the following:

- Provide regular internal and external capital and liquidity reports (for example, capital ratios, leverage ratio, LCR, NSFR, liquidity reserve, or monitoring tools), including limits and limit utilization for all relevant figures. The reporting tools should provide access to current and historical data and reports.
- Provide consolidated reports on both the accounting and economic views of expected losses, valuations, and hedges, including hedge effectiveness analyses for single risk types.

Banks will have to expand and strengthen the functionality and flexibility of their models and calculation engines.

- Provide full access to all portfolio data (static, position, and derived or calculated data on assets, liabilities, and off-balance-sheet items) at the single-transaction level as well as at different aggregation levels (for example, portfolios, business units, or the overall bank). The results of calculations, scenarios, and stress tests should be accessible on different aggregation levels, as required.

COMPLIANCE VERSUS COMPETITIVE ADVANTAGE

The new requirements provide the impetus for developing a much more sophisticated approach to steering financial resources. Banks that push beyond compliance to create greater transparency and enhanced forecasting capabilities will therefore realize a much higher return from the investments necessitated by the new requirements. Conversely, banks that focus only on compliance will find themselves at a disadvantage. The difference between these two approaches—compliance versus competitive advantage—boils down to the difference between gathering information about the bank on the one hand and leveraging insights to actively *steer* the bank on the other.

To generate such insights, banks first need to understand how the new regulations will affect, and potentially reshape, their business models and overall steering processes. On the basis of these changes, banks will invariably have to revisit their risk-IT architectures—the collection of systems used to measure, monitor, and manage the data associated with a bank’s risk position. An enhanced risk-IT architecture, linked with the bank’s financial systems, will provide a powerful platform for steering financial resources.

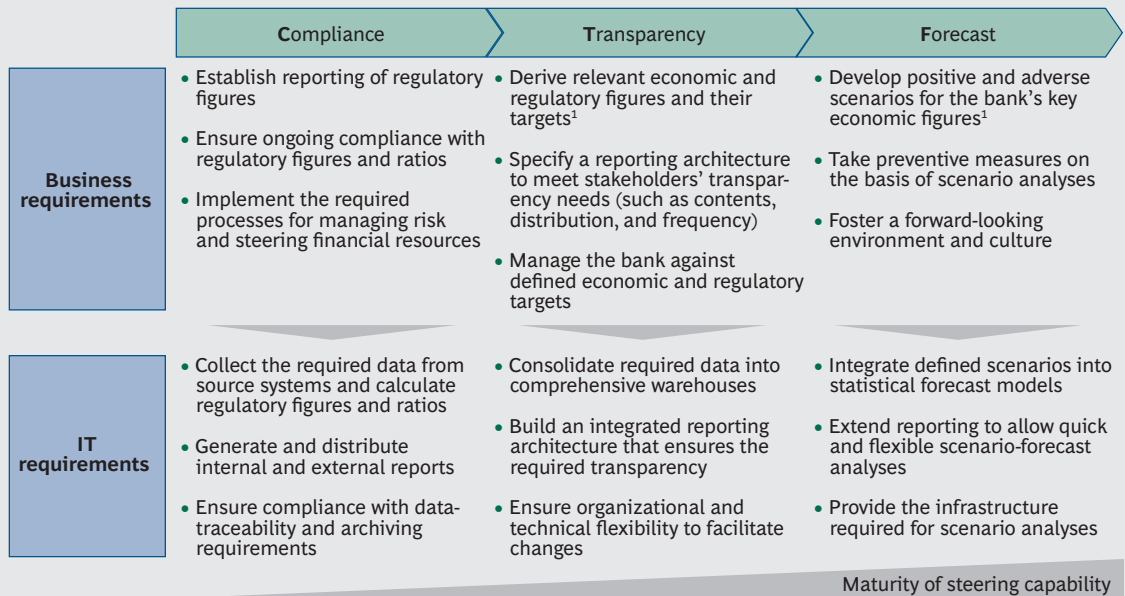
The CTF Framework: Defining a Pathway for Risk IT

For most banks, the task of transforming the risk IT architecture to comply with the new regulations is bound to be complex and resource intensive, and is likely to keep the bank’s risk and IT experts busy. The prospect of pushing the transformation further—so that the bank is not just gathering and reporting data but actually using the information to steer its activities and businesses with greater precision and purpose—may therefore seem like an unattainable goal. Banks can make this transformation far more manageable by setting clearly defined, business-driven goals for their risk-IT architectures.

The Compliance–Transparency–Forecast (CTF) framework helps banks to make the all-important connection between business and IT requirements—and then move beyond compliance. The framework itself describes the level of sophistication of a bank’s steering processes. (See Exhibit 1.) Banks that progress to the far end of the CTF spectrum will find themselves in an advantageous position: they will know exactly where they stand in terms of their current and projected use of scarce financial resources. Such knowledge seems basic enough to be nearly universal—more a prerequisite than a potential point of differentiation. Nevertheless, many banks have difficulty extracting this information from their systems—at least in a way that is both comprehensive and routine. As a result, they often lack a clear and current perspective on how and where their financial resources are consumed or allocated.

Many banks lack a clear and current perspective on how and where their financial resources are consumed or allocated.

EXHIBIT 1 | The CTF Framework Defines a Pathway for Enhancing the Risk IT Architecture



Source: BCG and Platinion analysis.

¹Figures and targets may vary by business segment, product, instrument, and region.

When it comes to measuring risk, many banks are operating with imprecise metrics—or ones they simply do not trust. As a result, they rely on a patchwork of ad hoc technical solutions, often called workarounds, to comply with current regulations. The burden of compliance falls more on the bank's business side, where the workarounds are initiated, than on the IT architecture. The cost of using temporary fixes to compensate for unsophisticated architectures is certain to rise, particularly as forward-looking banks begin to deploy and leverage IT solutions that allow them to use their financial resources as efficiently as possible.

The CTF framework will help banks develop a plan for resolving these compromises. The road map will vary from bank to bank, depending on each institution's business model, strategic goals, and risk profile, as well as its current IT infrastructure. In general, however, the CTF framework will revolve around a core set of business and IT requirements associated with three successive levels of risk-related capabilities.

Compliance. This is the baseline for improving the risk IT architecture—the bare minimum that banks must do. It provides a foundation for the enhancements that follow.

- *Business Requirements.* Banks must adhere to regulatory figures and ratios, and implement the required risk-management processes, including regulatory reporting.
- *IT Requirements.* Changes to the IT architecture would be required to identify or

define (if data are stored in several systems) the leading data marts with the required data. Banks will also need to collect and consolidate the data from the data marts, calculate the necessary figures and ratios, and generate and distribute reports.

Transparency. Simply by complying with the new regulations, banks will improve transparency (improved transparency is, after all, a goal of regulatory reform), but they should aim for an even greater degree of clarity.

- *Business Requirements.* Banks should derive economic figures and develop a reporting architecture that increases transparency in terms of the parameters, value drivers, and timeliness of data. They also need to manage the business against defined economic figures, making the necessary adjustments to meet those targets and reconcile the different views on the data (economic versus accounting).
- *IT Requirements.* To fulfill these business requirements, banks will have to consolidate data into warehouses, using highly automated systems. They will also need to build an integrated reporting architecture and ensure both organizational and technical flexibility so that the business can respond to issues uncovered by the enhanced transparency.

Forecast. Banks should aim to make the most of the raw materials at hand (the data), with a view toward becoming not only more prepared but also more agile.

- *Business Requirements.* Banks should develop scenarios to understand how certain events might affect key economic and regulatory figures. This will highlight what needs to be done to mitigate potential threats while fostering a more forward-looking, risk-conscious culture.
- *IT Requirements.* The IT architecture should allow scenarios to be integrated into models. It should also extend the bank's reporting capabilities to include forecast analyses, while ensuring that people on the business side—those responsible for steering financial resources and managing risk—have the tools to develop and run scenarios as needed, without having to involve the bank's IT department.

Banks should aim to make the most of the data at hand, with a view toward becoming not only more prepared but also more agile.

Upgrading the Risk IT Architecture

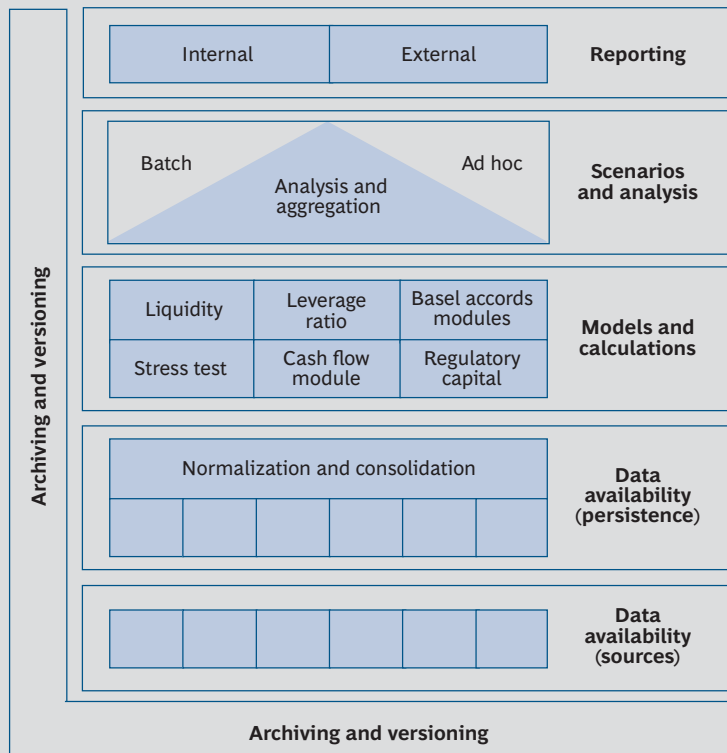
To support their evolution along the CTF framework, banks need to adapt—and in some cases transform—their risk-IT architectures. This architecture can be deconstructed into six main layers, each with its own distinct functional and technical characteristics. Stratifying the complex architecture makes it easier to design the target state—how it should look if it were to fully support all the requirements stemming from the regulatory changes. It also allows banks to define a series of interim stages between the current and target states, and thus avoid the pitfalls of a single “big bang” transformation. (For more on the architecture, see the sidebar “The Six Layers of the Risk IT Architecture.”)

THE SIX LAYERS OF THE RISK IT ARCHITECTURE

The risk IT architecture comprises six discrete layers, each with its own well-defined functionality. (See the exhibit below.)

- Reporting.** This layer ensures that information collected across all other layers is presented in a user-centric format. It updates predefined reporting information, including tables and management-oriented dashboards, at regular intervals. Internal reporting focuses on the needs of various stakeholders, such as the finance and risk-controlling departments. External reporting is generally based on templates defined by regulators.
- Scenarios and Analysis.** This layer provides a framework for defining various regulatory and custom-made scenarios and analysis paths, aggregating the results of calculation engines, and managing temporal data. It provides OLAP and other technologies to support ad hoc analysis, along with high-performance analytic engines to support efficient nightly batch

The Risk IT Architecture Has Six Main Layers



Source: BCG and Platinion analysis.

THE SIX LAYERS OF THE RISK IT ARCHITECTURE

(continued)

- and ad hoc analysis, as well as simulations.
- *Models and Calculations.* This layer supports the definition and management of analytic and simulation data models. It also provides powerful and flexible calculation engines for simple and derived risk figures.
- *Data Availability (Persistence).* All data for risk analysis are reconciled and stored on this layer. It aggregates discrete but consistent data views—for example, HGB versus IFRS accounting, and economic P&L data for trading book versus IFRS P&L data. Other functions include data consolidation and normalization, data access optimization, data quality assurance, data life-cycle management, and data enrichment based on external sources.
- *Data Availability (Sources).* This layer handles the often complex tasks of data extraction, transformation, and loading (ETL) into the persistence layer. It covers data collection from various sources, including position and transaction data from front- and back-end systems, collaterals, and market data. Its main focus is on establishing efficient procedures for all ETL capabilities.
- *Archiving and Versioning.* This layer maintains versions and backups of data across all other layers. To ensure that data are not lost, they are stored at defined intervals on separate media. This layer also provides audit trails and data versioning on all layers, to ensure that any entity—for example, a management report or an analytic formula—can be retrieved for a given point in time.

BUILDING A FOUNDATION FOR IMPROVED CAPABILITIES

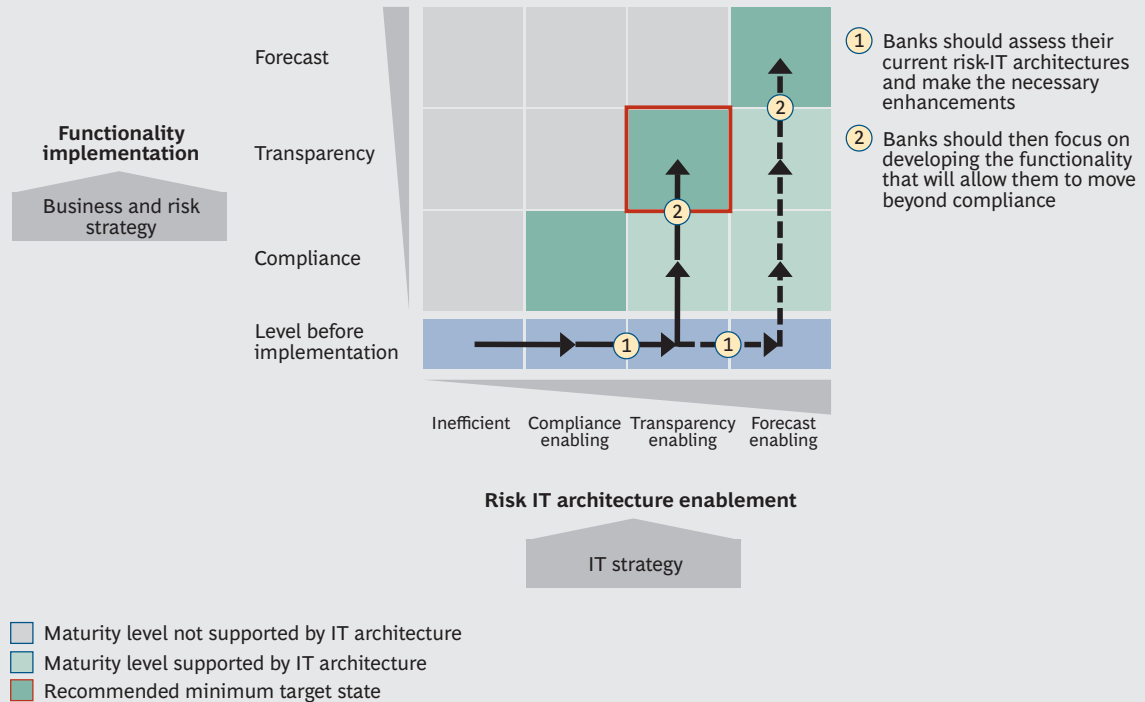
The technical implementation of the new regulations should unfold over two discrete phases. (See Exhibit 2.) First, the bank needs to *enhance the enablement level* of its risk architecture, moving along a spectrum that begins with “inefficient” (the bank has to rely on workarounds to ensure compliance) and peaks at “forecast enabling” (the architecture can support the types of processes and functions necessary to regularly forecast potential risk scenarios). Advancing along the spectrum might entail replacing single components within the architecture, implementing new software across one or several layers, or even establishing a new data warehouse for the bank.

Once the bank has developed its risk-IT architecture to the target enablement level, it needs to *implement the functionality* necessary both to meet regulatory requirements and to fulfill its “above and beyond” objectives—namely, increased transparency or sophisticated forecasting.

A bank’s progress along the functionality axis is driven mainly by its business and risk strategies, whereas changes in the enablement axis are driven mainly by its IT

EXHIBIT 2 | Banks Should Aim to Move Beyond Compliance

The enablement and functionality of the risk IT architecture



Source: BCG and Platinion analysis.

strategy—which should be derived from the business and risk strategies. The principle of first enabling the architecture and then building functionality on top of it is critical to aligning the bank’s business and IT requirements.

To start this transition, banks need to gauge the sophistication of their current risk-IT architecture by assessing their capabilities across the six layers. They can then determine whether their architecture enables compliance, transparency, or forecasting.

Compliance. At this level of development, the risk IT architecture provides basic reporting formats and tools, the models and capabilities necessary to make the requisite calculations, and access to all relevant data. There may, however, be a lack of consistency or harmonization, particularly in terms of data and reporting. The outputs may be correct, but they are often incomplete. Moreover, they rely on domain-specific interpretations of data, which might be partially inconsistent and not fully transparent to end users. The lack of transparency means that analysts may not fully appreciate the implications of changes in the outputs of certain models or calculations.

Transparency. The risk IT architecture provides sophisticated bankwide reporting capabilities and accessible functionality. Data are not only captured and consolidated but also carefully cataloged and managed. For each data point—for example, a

payment transaction or a customer data record—there is a single verifiable source. In addition, relevant models and analytic functions are implemented transparently and are well understood, so analysts immediately recognize the implications of changes in key outputs. The bank not only knows the answers to questions posed by the new regulations (for example, What is the current core Tier 1 capital ratio?), but it also understands the composition of the figures (for example, by product, region, or business segment).

Forecasting. Banks that have the most advanced risk-IT architectures can develop and run simulations on demand, provide frequent updates, define and generate reports, and take targeted action on the basis of the results. Such functionality is supported by a dedicated simulation infrastructure that provides calculation capabilities and databases that can be extended or modified on demand. The bank has a clear view of its current position, along with an informed perspective on how its position might evolve, depending on the impact of a host of variables and trends (such as changes in capital and liquidity ratios under certain adverse macroeconomic scenarios).

COMMON STARTING POINTS AND PRIORITIES

Most banks will find that their risk-IT architectures are at or below the level of compliance. If the architecture is inefficient, IT departments will have to find makeshift solutions to problems such as data not being digitized or aggregated across risk domains, which can lead to inconsistencies. They will also confront a lack of harmonization across reporting technologies and approaches.

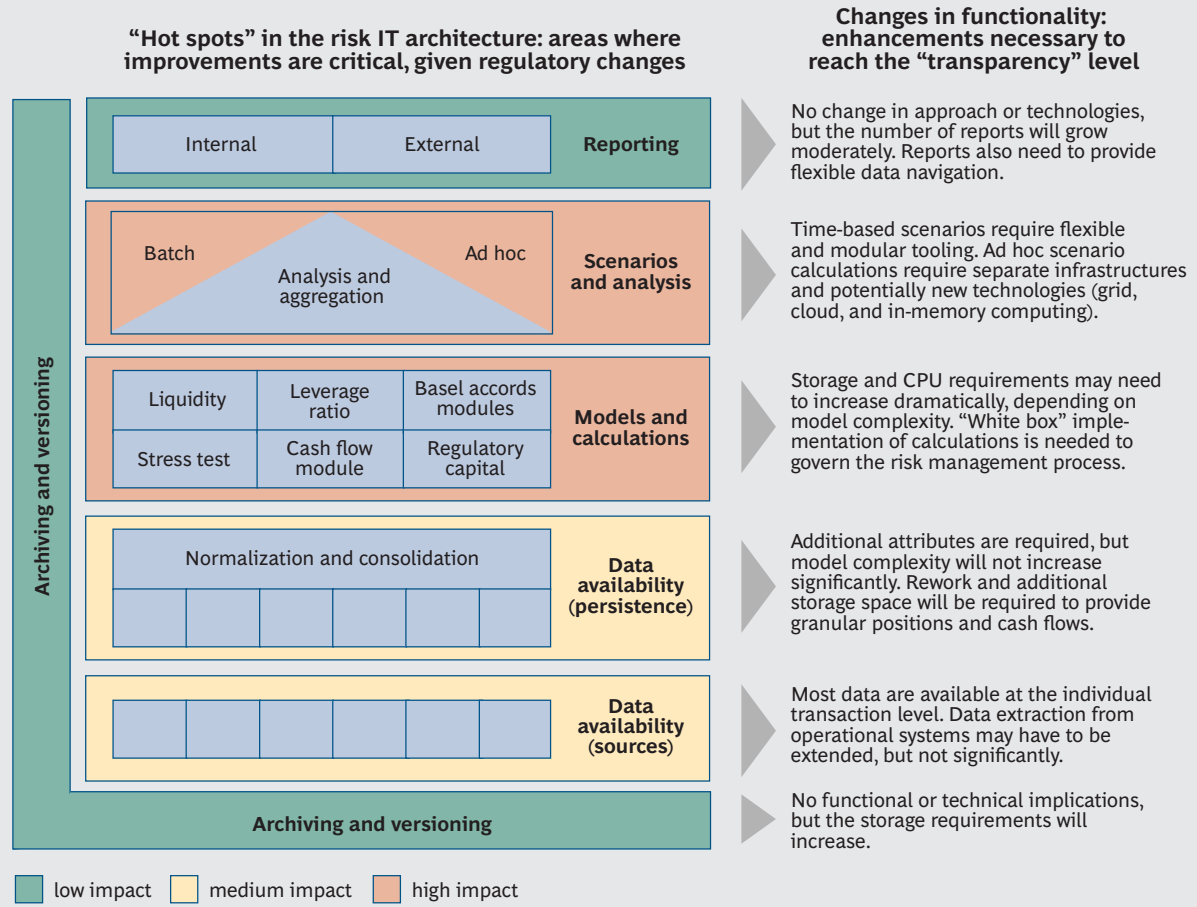
Improving data accessibility and consistency will be a priority.

Banks in this position will need to pursue initiatives across each of the six layers, but improving data accessibility and consistency will be a priority. They should focus on developing data warehouse standards, which will harmonize existing data marts and eliminate inconsistencies. They should also roll out core data marts for risk domains, such as credit risk, market risk, liquidity risk, and operational risk. In addition, they will have to reconcile the various methods of collecting data in order to lay the foundation for a risk management platform that is capable of more than just ensuring compliance.

Banks that are already at the “compliance enabling” level most likely used Basel II as a catalyst to establish a solid data-warehouse platform. Their starting point provides a foundation to create new risk functionality. Their main focus should be on improving the capabilities that support the second and third layers: scenarios and analysis, and models and calculations. (See Exhibit 3.) They need a flexible infrastructure to keep up with the calculations and storage requirements necessary to run multiple simulations. Such banks will also need to provide missing liquidity data (especially for disaggregated cash-flow positions) and further enhance data availability.

While banks in general have much to gain from building sophisticated risk functions—particularly around modeling and calculations—they must not lose sight of the critical role of, and growing demands on, the data warehouse. The new regulatory regime has significant implications for how banks gather and store data. Calculating the LCR, for example, entails a substantial amount of data collection and consolidation.

EXHIBIT 3 | Banks with Advanced Architectures Can Focus on Improving Functionality



Source: BCG, Platinion, and SAS analysis.

Apart from the logistical challenge of storing data, most banks will also have to contend with much higher demands on their computing power, given the need to calculate sophisticated risk metrics and analytics. But simply boosting the power of the existing setup might not be economically feasible or technologically advisable, since banks will also need to support ad hoc analysis and simulations. Traditional infrastructure setups are not equipped to accommodate surges in demand for computing power—at least not in a cost-effective manner. As a result, banks must explore new approaches to providing scalable and flexible processing capacity, along with advanced technical concepts such as grid computing or in-memory databases.

Banks that continue to postpone upgrades to the data warehouse or risk management platform (including its computing power and processing capacity) will become increasingly out of step with regulatory requirements. As more rules go into effect, the capability gap will continue to widen to the point where the upgrade becomes not only massive but urgent. In the meantime, the bank will need to

implement inefficient stopgap measures in order to ensure compliance, and will likely see other banks gain a competitive edge through the use of more transparent and accurate measurements of key risk parameters.

Of course, identifying areas for improvement is one thing; actually addressing them as part of an orchestrated overhaul is another. Even when armed with the CTF framework and a clear understanding of the changes required across the six layers of the architecture, banks often face challenges in implementing so much change to such a complex web of IT components. To help manage this process, banks should follow an approach that focuses squarely on the changes that will make a significant difference to the business. (For more on this approach, see the sidebar below.)

A FOUR-STEP PROCESS FOR TRANSFORMING THE RISK IT ARCHITECTURE

Transforming the risk IT architecture is often a complex and involved undertaking. Banks can make it more manageable by following a four-step process.

- 1. Assess the current IT infrastructure.** Banks need to assess their risk-IT capabilities against the backdrop of the CTF framework, categorizing their various layers and functions somewhere along a spectrum that runs from “inefficient” to “forecast enabling.”
- 2. Define a target state.** Again using the CTF framework, banks should define an aspiration for their bank-steering capabilities somewhere along the spectrum. This aspiration sets the bar for the risk IT architecture.
- 3. Prioritize initiatives to close the gap.** Banks need to map out the most effective way to cover the distance between the current and target IT architectures. They should focus on initiatives that have a combination of high value to the business and a sense of urgency (due, for

example, to pending changes in regulations).

- 4. Develop a road map for implementation.** The previous step will provide the basis for an implementation road map—a detailed plan for transitioning to the target IT architecture, which sequences certain initiatives on the basis of their importance and urgency.

During the third step, banks might have to explore different vendor solutions, depending on the state of their current architecture and the distance they need to cover to reach the target. Some architectures can be improved; others may have to be at least partially replaced. In parallel to developing a road map, the team that is leading the transformation should develop a holistic understanding of how the new regulations will affect the bank’s business model and the processes and principles used to steer financial resources.

Case Study: Realizing the Benefits of an Enhanced Risk-IT Architecture

A recent initiative by a European universal bank illustrates the benefits of translating new regulations into marching orders for the risk IT architecture. The bank, which is active in capital markets, corporate finance, and retail banking, is a significant player in both its home country and the region. Although it complied with Basel II and was considered by the investor community to be proactive in adapting to new regulations, its risk-IT architecture lacked transparency. The “black box” nature of the bank’s risk calculations meant that the results were not always fully trusted or utilized.

The bank set out to refine its risk-IT architecture in order to achieve greater transparency. More specifically, it aspired to improve its processes for running scenarios and stress tests, which were relatively cumbersome and, in some cases, prohibitively expensive. It also wanted to build flexibility into its risk models and calculations so that business analysts could manage their calculations and understand, develop, and change key inputs without having to involve the IT department. In addition to providing drill-down capabilities, the enhanced architecture would need to enable consolidated, timely reporting in order to help the bank’s managers make informed decisions about the overall direction of the business.

SHAPING THE RISK IT ARCHITECTURE AROUND BUSINESS REQUIREMENTS

The team leading the transformation began by assessing the bank’s ability—from a technology standpoint—to comply with current and future regulations. The assessment covered each of the six main layers of the risk IT architecture. It also factored in the bank’s aspiration for its risk-IT architecture, which was guided by the aforementioned expectations for improving transparency and flexibility.

On the basis of this assessment, the team decided to focus on two main layers of the architecture: scenarios and analysis, and models and calculations. The changes made to these two elements would have substantial implications for a third part of the architecture, data availability. The objective of the transformation was to upgrade these elements so that they not only ensured compliance but also increased transparency, while providing a foundation to significantly improve the bank’s forecasting capabilities.

The bank set several criteria for a software solution that would enable the transformation. The architecture needed to be flexible and open with respect to data management and calculation routines; it had to have proven performance on large, complex analytic tasks (for example, simulation-based CVaR); and it needed to provide a vast range of off-the-shelf risk-analysis routines and valuation algorithms.

The SAS product Risk Management for Banking was chosen as a software solution. It was implemented on a hardware platform comprising two Sun servers, each with 24 cores and 64 GB RAM, to enable a calculation of economic capital requirements based on a Monte Carlo simulation. (BCG does not have a commercial interest in any third-party IT solutions, which allows us to provide unbiased advice to clients that may need to acquire new technology. Although a specific third-party solution is an integral part of this case study, BCG—in keeping with its independent stance—does not endorse the IT vendor or its solution.)

The transformation was designed to ensure compliance, increase transparency, and provide a foundation to significantly improve the bank’s forecasting capabilities.

The implementation, which took about one year, had two main phases. Each, lasting roughly six months, was managed by a core team comprising two business experts, one IT expert, and two SAS senior consultants. The core team drew additional resources from the IT division to integrate data and set up technical processes.

During the first phase, the new architecture was developed in a lab setting and then gradually refined on the basis of the results of three development cycles. Each cycle was run using a copy of live data, and the results were cross-checked against the output generated by the existing system. During the second phase, the new system was run in parallel to the existing system for approximately six months before the decision was made to go live and to replace the existing system. The testing was supported by the risk department and the end-user community.

BUILDING ENHANCED FUNCTIONALITY

After elevating key elements of the risk IT architecture, the team upgraded a range of functions to infuse various risk activities with greater clarity.

- *Scenarios and Analysis.* The bank's simulation capabilities for credit risk were enhanced significantly. Business experts can now analyze and amend scenarios without IT support—they can simulate changes in house prices or unemployment rates, for example—while credit analysts can follow and understand all of the dynamics underpinning the simulations. Furthermore, the range and depth of scenario analysis increased, providing additional insight into the assumptions underlying various models.
- *Models and Calculations.* The bank's models and calculation engines were made more flexible, transparent, and accessible. As a result, its risk models are no longer perceived as a black box but rather as tools for identifying profitable business opportunities, and the risk profile indicated by the bank's quoted prices continues to converge with the risk profile suggested by the models. The new infrastructure can handle and simulate credit risk calculations for a range of situations, from individual exposure to group exposure. It also provides the basis for drill-down and scenario functionalities. In addition, all calculation routines and results—both interim and final—are available and linked to each other, which paves the way for enhanced reporting capabilities.
- *Data Availability.* Data were made available by means of a comprehensive warehouse and at the required granularity, including cash flows for single deals. They are also now available at a disaggregated level in the warehouse. For each deal (with any counterparty), users can see its contribution to economic capital for any risk category, making it easier to pinpoint the benefits of diversification. The input interfaces were also refined to facilitate the delivery of detailed data to the calculation engines. The new data warehouse is stable but also flexible enough to accommodate minor changes in the data delivery processes.

The bank's risk models are no longer perceived as a black box but rather as tools for identifying profitable business opportunities.

RESULTS

By enhancing the risk IT architecture and then building the functionality to leverage this capacity, the bank has realized several important benefits. It can now measure credit risks more accurately. This includes sizing up individual types of

risk—credit and market risk, for example—as well as understanding the correlations among different types of risk. The increased transparency has led to a more precise calculation of economic capital and a more efficient allocation of resources among the business units. At the same time, the bank has improved its capabilities for pricing risk.

In addition, the perception of risk has changed throughout the bank. People at all levels have a much better understanding of the factors that contribute to risk, along with greater confidence in the underlying data and calculations. Risk is seen not just as an output—something to be monitored and reported—but also as an input to business decisions. Moreover, the bank, relative to where it was before the transformation, as well as to many of its peers, is in a better position to make the most of its financial resources, thanks to a more transparent view of the relationship between risk and reward.

BANKS HAVE MUCH to gain by taking a constructive approach to adapting to the new regulatory environment. By using the CTF framework to convert their new business and IT requirements into targeted actions across the six layers of the risk IT architecture, banks can not only comply with the new rules but also generate a more incisive view of risk. Such insight, in turn, will lead to a more purposeful, efficient use of financial resources, which will become an increasingly important source of competitive advantage.

NOTE

1. These three sets of regulations are global, though their precise implementation—including the timetable for when different elements come into effect—could vary from country to country. Banks may also need to contend with country-specific reforms, such as the German Accounting Law Modernization Act (BilMoG), which will add further complexity to the process of evaluating and responding to new business and IT requirements.

Risk is seen not just as an output—something to be monitored and reported—but also as an input to business decisions.

About the Authors

BCG

Walter Bohmayr is a partner and managing director in the Vienna office of The Boston Consulting Group. You may contact him by e-mail at bohmayr.walter@bcg.com.

Peter Neu is a partner and managing director in the firm's Frankfurt office. You may contact him by e-mail at neu.peter@bcg.com.

Michael Grebe is a partner and managing director in BCG's Munich office. You may contact him by e-mail at grebe.michael@bcg.com.

Kai-Oliver Müller is a project leader in the firm's Hamburg office. You may contact him by e-mail at mueller.kai-oliver@bcg.com.

Amarendran Subramanian is a consultant in BCG's Stuttgart office. You may contact him by e-mail at subramanian.amarendran@bcg.com.

Platinion

Christoph Geier is a managing director in the Cologne office of Platinion. You may contact him by e-mail at geier.christoph@platinion.de.

Jens Müller is chief IT architect in Platinion's Cologne office. You may contact him by e-mail at mueller.jens@platinion.de.

SAS

Christoph Benzinger is an executive business advisor in the Frankfurt office of the SAS Institute, a subsidiary of SAS. You may contact him by e-mail at christoph.benzinger@ger.sas.com.

Frank Hansen is a manager in the Munich office of the SAS Institute's Risk Management Competence Center. You may contact him by e-mail at frank.hansen@ger.sas.com.

Carsten Krahl is a business expert in the Cologne office of the SAS Institute's Risk Management Competence Center. You may contact him by e-mail at carsten.krahl@ger.sas.com.

Acknowledgments

Several experts in risk management and IT made valuable contributions to this report. From BCG, the authors would like to thank Benjamin Friedrich, Bernhard Gehra, Norbert Gittfried, Jan Koserski, and Wolfgang Thiel. From Platinion, the authors are grateful to Ralf Kiessling and Marco Zimmer. Finally, we thank the following members of BCG's editorial and production teams: Gary Callahan, Daniel Coyne, Angela DiBattista, Sharon Slodki, and Sara Strassenreiter.

This Focus was sponsored by BCG's Financial Institutions and Information Technology practices.

For Further Contact

If you would like to discuss this report, please contact Walter Bohmayr or Peter Neu from BCG, Christoph Geier from Platinion, and Christoph Benzinger or Carsten Krahl from SAS.

To search for the latest BCG content, please visit one of our websites at www.bcgperspectives.com or www.bcg.com/publications.

To receive e-alerts, including the latest content on this topic or others, please register at www.bcgperspectives.com.

© The Boston Consulting Group, Inc. 2011. All rights reserved.



BCG

THE BOSTON CONSULTING GROUP

Abu Dhabi	Cologne	Kuala Lumpur	New Jersey	Stuttgart
Amsterdam	Copenhagen	Lisbon	New York	Sydney
Athens	Dallas	London	Oslo	Taipei
Atlanta	Detroit	Los Angeles	Paris	Tel Aviv
Auckland	Dubai	Madrid	Perth	Tokyo
Bangkok	Düsseldorf	Melbourne	Philadelphia	Toronto
Barcelona	Frankfurt	Mexico City	Prague	Vienna
Beijing	Geneva	Miami	Rio de Janeiro	Warsaw
Berlin	Hamburg	Milan	Rome	Washington
Boston	Helsinki	Minneapolis	San Francisco	Zurich
Brussels	Hong Kong	Monterrey	Santiago	
Budapest	Houston	Moscow	São Paulo	
Buenos Aires	Istanbul	Mumbai	Seoul	
Canberra	Jakarta	Munich	Shanghai	
Casablanca	Johannesburg	Nagoya	Singapore	
Chicago	Kiev	New Delhi	Stockholm	bcg.com