accenture

Strategy | Consulting | Digital | Technology | Operations

High performance. Delivered.

Reaping the Benefits of Operational Risk Management

Introduction

Following the introduction of operational risk as a dedicated risk category in Pillar 1 of the Basel II Framework concept of January 2001, as required, banks began to implement an operational risk framework.

This consisted of an operational risk policy including the operational risk management (ORM) process, loss data collection databases, self-assessments, scenario-analysis methods and key risk indicators.[1] We also observed that banks opting for an "Advanced Measurement Approach" implemented internal models and corresponding validation methods to help achieve appropriate risk capital levels for operational risk.

While the original focus of operational risk management was on regulatory compliance, operational risk is mostly about human behavior. This aspect of ORM, however – encompassing matters such as changing a bank's risk culture and risk appetite, and incorporating a risk focus in day-to-day business decisions – appears to have received little consideration. Moreover, in our view, given the focus of the regulatory requirements, they tend to downplay the magnitude of risks associated with lost income opportunities, reputational issues and credit defaults caused by operational risk events.

This also meant that ORM functions were often staffed with people lacking the necessary domain knowledge, putting them at a disadvantage when working with business department colleagues. This lack of knowledge also kept operational risk managers from asking the right questions and from proposing the right action steps, keeping ORM from contributing fully to the benefit of the organization by establishing the right kind of risk culture, freeing up capital resources, and minimizing surprises (and losses).

Stakeholders in Operational Risk Management

Key stakeholders in ORM can be separated into internal and external groups. Internal stakeholders include the bank's supervisory board, executive board, risk committee, senior management of business units, and teams responsible for process management, as well as the general employee population. External stakeholders include regulatory supervisors, rating agencies, insurance companies, outsourcing services companies, investors and clients.

Stakeholders, depending on their roles and responsibilities, have different expectations regarding operational risk deliverables. For example, the supervisory board and the executive board (which comprise what might be called the "management body") have responsibility for the bank's overall business strategy as well as risk strategy and policy, capital strategy, and the organizational structure to name a few. This management body also has oversight over credit risk, market risk, liquidity risk, business risk and reputational risk in addition to operational risk, key to determining the institution's capital and liquidity needs.

We believe the operational risk management function should support the bank's management body by providing the following services:

- Risk culture change programs
- Defining risk appetite and risk tolerance for operational risk and conducting regular reviews
- Analyzing deviations between the institution's risk profile and its appetite including the changes in risk capital for addressing operational risks
- Analyzing internal and external factors and trends which affect the institution's risk profile
- Improving the overall internal control framework in terms of both effectiveness and efficiency, including removal of obsolete internal controls
- Analyzing the operational risk implications of strategic changes in product mix, outsourcing, and entry into new markets
- Risk capital budgeting
- Helping to assure compliance with regulatory requirements

The operational risk management function can provide the same level of support to other internal and external stakeholders. For example, operational risk management can deliver to senior management an in-depth analysis of changes and trends in the operational risk profile of a business unit or of the company as a whole, or it can identify and analyze the dependencies among various operational risk factors.

In larger financial institutions, the operational risk management function is often centralized but also has decentralized resources in each division. The decentralized elements, which are closer to business processes and practices, can better undertake analyses such as a regular review of the division's internal control framework.

As mentioned, operational risk management also supports external stakeholders such as rating agencies and insurers. The operational risk management function supports the rating/review process, for example, by establishing a sound operational risk management and measurement system, and by collecting information and data relevant to the rating/review process.

Similarly, institutions often buy insurance coverage for certain operational risks like internal fraud or professional indemnity. The amounts spent for insurance premiums can be significant. The better the institution understands its risk situation, the better its negotiation position. Insurance coverage can be considered in risk capital calculations and can therefore help free up capital to be used to create value. The operational risk management function can also support the insurance procurement process by helping to assess the risk exposure to be insured (including the capital cost involved); helping ensure that the insurance policy meets regulatory criteria; and simulating reductions in capital and capital cost charges.

Good operational risk management can also help reduce the number of incidents related to the institution's financial results, which will be positively reflected under Pillar 3 of the Basel regulatory framework.

Figure 1 below summarizes the key deliverables of a typical operational risk management function by stakeholders.

Figure 1. Overview of deliverables by stakeholders

Deliverables	Board	Risk committee	Senior management	Process management	Staff members
Proposed operational risk strategy including risk appetite	✓	✓			
Risk capital budgeting	✓	✓	✓		
Action plan regarding changes in the risk profile	✓	✓	✓	✓	
Simulation of effects on risk profile due to strategic or organizational changes	✓	✓	✓	✓	
Continuous improvement of internal control framework	✓	✓	✓	✓	
Monitoring of organizational weak points				✓	
Tools and training				✓	✓
Regulatory compliance	✓	✓	✓	✓	✓

Source: Accenture, May 2014

Benefits of Strong Operational Risk Management

There are numerous potential benefits derived from a well-structured and efficiently run operational risk management approach, including:

1. Freeing up capital

Capital is a scarce resource, especially under the new Basel III capital requirements. Capital determines the organization's earnings capacity, since each risk taken requires a corresponding level of capital. The more organized an institution is from an operational risk perspective, the more capital it can allocate to income-earning activities.

2. Better decision making

Simulation results can support better decision-making by providing new insights; for example, a simulation can indicate the likely outcome of the bank entering a new market with a different legal system.

3. Lower cost of funds

Since rating agencies consider effective risk management in their rating process, there is a direct link between the quality of risk management and the rating of the institution. This can have an immediate effect on the cost of funds.

4. Lower operating costs

Improved controls and monitoring tools can help organizations identify potential risk events before they cause losses. In many cases, the number of potential risk events the bank faces can be reduced, increasing overall operations efficiency, as transactions do not need to be dealt with multiple times.

5. Less profit and loss volatility

Large operational risk loss events can have a significant impact on the volatility of the profit and loss account, resulting, in some cases, in failure to meet earnings expectations. This can result in a drop in market value. Sound operational risk management can help minimize volatility, especially as it relates to meeting revenue and profit targets.

6. Increased customer and staff satisfaction

It is generally understood that customers and employees prefer to work with/for a financial institution with a low error rate and a reputation for high quality. Weaker institutions and less performing banks are more prone to losing customers. Losing customers means losing their contribution to margin, and the cost of finding new customers is often higher than the cost of keeping existing customers.

Employees are sensitive to quality issues in their work environment and good employees may feel the need to leave and seek work with competitors if they see problems and issues around their current situation, especially if the problems might affect their future opportunities in the labor market.

7. Optimized insurance coverage and insurance premiums

The more an institution is familiar with its risk profile, the better it can identify its needs in terms of insurance coverage. In most cases, better risk information can allow for a better negotiating position on premiums paid.

8. Better regulatory compliance

Regulatory compliance is an indispensable part of doing business and can be a source of competitive advantage. The operational risk management function has an important role in helping to assure regulatory compliance.

Establishing a Risk Culture

Operational risk is a learnable risk,[2] which means that better knowledge and experience can allow for better management, and, ultimately, higher institutional returns. This knowledge and experience, however, needs to be accepted and incorporated into employee behavior – the hallmark of a strong risk culture.

Risk culture is essential to the success of operational risk management. For example, banks may undertake high-risk activities and see good initial returns. However, as clients become more familiar with the risk profile of the institution's products, they may stop buying the products or following an unforeseen negative financial experience, legal claims may result. The net result is reduced sales and depressed bank returns.

A bank's risk culture needs to be communicated throughout the organization, with staffers at all levels sensitive to risky situations that can arise. This requires a strong foundation, put in place through the firm's strategy and risk appetite. These create benchmarks for future actions and encourage the right behavior among employees. Compensation policy also plays a key role in deterring undesired risk-taking behavior by employees.

The following steps can help companies strengthen their risk cultures:

1. Align the risk culture to the company's strategy and risk appetite

2. Adjust staff compensation to match the risk appetite of the organization

3. Prepare a communication program targeting all staff members including the use of "risk ambassadors" to explain the company's risk appetite and culture

4. Ensure the new risk culture is reflected in decision making tools, for example, by requiring that risk assessments be completed before transactions are closed

Business Domain Knowledge

Effective operational risk management depends upon having a clear understanding of the strategy, products and processes of the business units. This can enable the operational risk management function to identify the real risk issues, properly assess identified risks, and add value by giving practical advice.

Banks can improve business domain knowledge by conducting workshops within each business area to analyze specific risks; by training risk teams on the inherent risks of banking products and processes; and by seconding risk staffers in business units to enhance their practical experience.

Operational Risk Management and Other Corporate Functions

In addition to the operational risk management function, other corporate functions such as compliance, business continuity management, IT risk, internal control framework, corporate security, legal, audit and insurance have many of the same needs in relation to data and information required and the risks to be identified, reported and managed.

All of these corporate functions share the need for a risk-based approach; they need their own risk assessment and/or monitoring activities; and they have their own reporting requirements related to assessment and monitoring results.

As seen in Figure 2 below, each function has a dedicated scope determined by internal and regulatory requirements.

Banks can develop a common approach to be used across these functions, with a uniform standard for data and information collection and consistent reporting. To achieve this, the requirements of each function should be identified and matched to the information needs of the business. The process is shown in Figure 3.

The detailed data collected should be addressed in such a way that the information needed by the lower organizational levels can be aggregated to the next higher level. For example, the operational risk management function can use the information captured from control effectiveness testing to assess the frequency of corresponding operational risks. A business impact study from the business continuity management function can be used by the operational risk management function to assess the severity of potential losses in the business disruption and system failure scenarios. As seen in Figure 4, access to consistent information in each function is essential for aggregation.

Figure 2. Scope of operational risk management and other corporate functions (German focus)

Subject	Operational risk	Business continuity management	Compliance	IT risk	Internal control framework
1. Regulatory requirements	CRD/Solvency MaRisk	MaRisk	EBA guidelines on internal governance MaComp GWG (anti-money laundering law) Kriegswaffenkontrollgesetz (Military Weapons Control Act) Dual use enactments	MaRisk	MaRisk EBA guidelines on internal governances Sarbanes-Oxley Act
2. Standards	Loss data collection Standards	BSI standards		Cobit	COSO
3. Scope					
3.1 Organizational	Full coverage of all processes, all units on an aggregated level	All processes containing material business disruption risks on a detailed level	Dedicated parts of the organization depending upon requirements	IT organization and processes	Key controls within main processes
3.2 Risk types	All operational risk categories, according to regulatory and internal definitions	Business disruption risk	Compliance risk	IT risk	Risk of failing internal controls due to human, system and process errors
4. Observations	Business units	Processes	Processes Activities	Processes Activities Systems and their components	Key process controls

Source: Accenture, May 2014

The following identifies key steps for developing a common approach to producing consistent information across all levels:

1. Define a detailed information need matrix covering each function's requirements, including reporting delivery frequencies

2. Define metrics which allow an aggregation of information to the next operating level (Figure 4 pyramid)

3. Define an aggregation mechanism to transfer the information to the next organizational level

4. Identify the sources of information

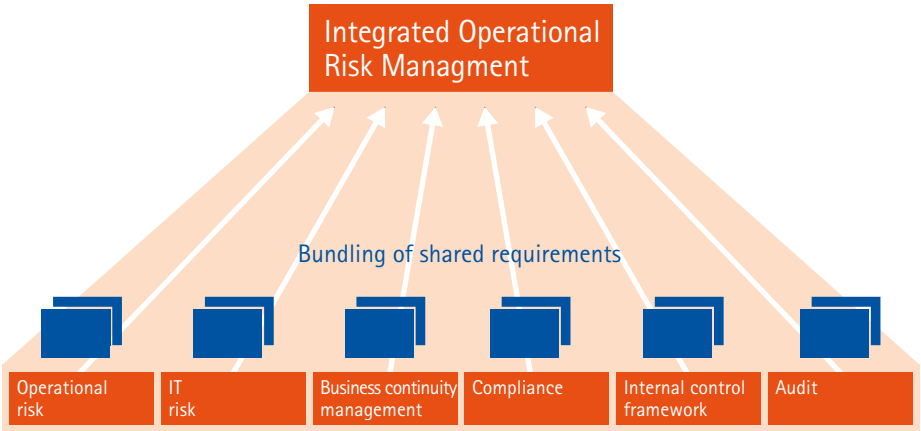
5. Define the collection methods to be used

6. Define information quality assurance (approach and metrics)

7. Define ownership

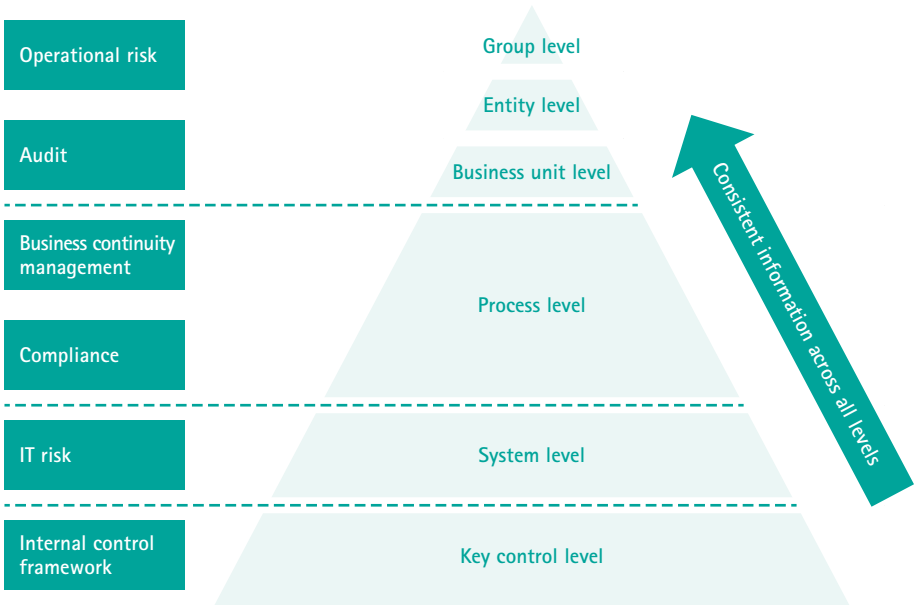
The in-depth analysis of changes and trends in the operational risk profile of the division and analysis of dependencies among various operational risk factors should also be connected to a report matrix to help ensure that consistent information is used and synergy effects are realized.

Figure 3. Integrated operational risk management



Source: Accenture, May 2014

Figure 4. Information Pyramid



Source: Accenture, May 2014

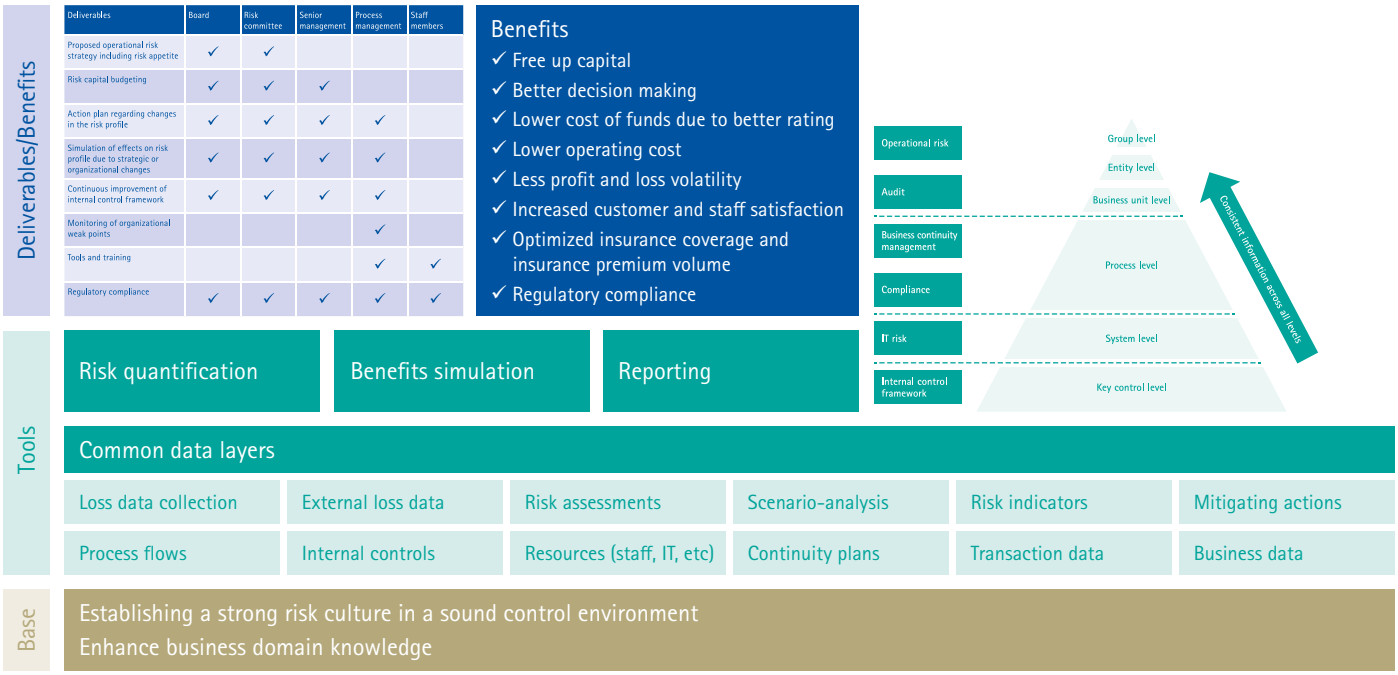
Operational Risk Management Road Map

A road map such as the one shown in Figure 5 below can serve as the starting point for banks wishing to obtain the benefits of an operational risk transformation.

While tools may be implemented in existing operational risk management functions, the scope of the tools should be expanded in some cases. For example, tools should be used to examine all loss severity components beyond the regulators' purview, such as missed income, credit losses caused by operational risk, and financial losses caused by reputational damage.

A road map, combined with the internal requirements of the institution, can function as the target model for conducting a gap analysis.

Figure 5. Operational risk management road map



Source: Accenture, May 2014

Accenture Approach to Operational Risk Management

Accenture's approach is focused on helping banks optimize their operational risk management capabilities by implementing or reshaping the ORM function's ability to effectively and efficiently deliver on business needs.

In order to minimize project risks, a phased approach is suggested with clear deliverables as stated in Figure 6 below.

Phase I: Maturity Assessment

Identifying business needs is the key step in this phase. This is done through interviews with the business managers ultimately responsible for managing operational risks. This step will help ensure that the operational risk management process and the corresponding tools and reports are properly focused on the business needs, and thus delivering business value as described in the target model.

The next step during this phase is the analysis of the current toolset. The toolset, as defined in the operational risk management road map, consists of the operational risk management capabilities. These should meet the criteria set by the target model, which goes beyond the regulatory requirements.

Assessment of the corporate risk culture is next, with an examination of the maturity of the risk culture and the pace at which actions are taken and completed. Following the assessment of the risk culture, synergies for data collection (including data quality assurance and risk reporting) are identified and validated. Finally, business domain knowledge, essential for the proper function of operational risk management, is evaluated.

Figure 6. Accenture approach to operational risk management

	Maturity assessment	Gap analysis	Identify actions	Implementation planning
Phases	• Identify information needs at a business management level • Document current tool set • Assess risk culture maturity • Assess the cooperation-mode between operational risk and other functions • Assess the business domain knowledge within the operational risk management function	• Compare current toolset to target model including business management requirements • Compare available business knowledge to required business knowledge within the operational risk management function	• Identify actions to close gaps within: – Risk culture – Reporting – Tools – Business domain knowledge • Prepare cost-benefit analysis • Identify quick wins • Prioritize actions	• Create action plan including dependencies • Determine project staffing • Confirm plan • Develop process approval document
Deliverables	• Current situation documented	• Gaps to target model documented • Knowledge gaps documented	• Prioritized action list • Quick wins	• Implementation plan and budget • Approved document

Source: Accenture, May 2014

Phase II: Gap Analysis

Based on the information extracted in Phase I, and the defined target model, gaps will be identified and analyzed, including those in business domain knowledge among operational risk management resources.

Phase III: Identify Actions

Based on the gap analysis conducted during Phase II, actions to help close gaps are identified. Actions to help change risk culture, for example, might include:

Re-aligning compensation

Employee compensation often needs to be re-balanced to match the risk appetite of the organization. Compensation drives employees' risk appetite, especially if there are opportunities for short-term gains at the expense of possible long-term losses. There are other issues to consider, for example, if generating new business volume, rather than credit quality, determines a corporate bank account manager's bonus.

Preparing a detailed communications program

Communication and leadership are key to successfully changing the risk culture of an institution. Employees need role models (we call them risk ambassadors) who demonstrate the right behavior. A risk strategy and communications program might include briefing packages for board members, senior management, department managers and influencers, as well as a kickoff event to introduce the new risk culture. Staff meetings, written communications, and other initiatives, like round table discussions at the business unit level can help the company adopt the new risk culture.

Building risk into decision-making tools

Measures such as requiring risk assessments to be completed before transactions are closed can help reduce the number of adverse events.

For example, new products should balance client value and the value delivered to the organization; if this is not the case, the business case reporting tool should flag this as a risky initiative prior to launch.

Reporting and tools

When gaps between business needs and regulatory requirements, and existing reporting versus reporting requirements are identified, the bank's current reporting package can be enhanced in a number of ways to address this. For example, reports covering various dedicated operational risk elements can be integrated and made consistent. The reporting process can be re-defined with clear responsibilities, and reports can be enriched with analysis and recommended management actions.

A detailed reporting matrix can help a bank identify comparable information requirements and allow for streamlining of the data collection processes. Along the same lines, an aggregation mechanism can help transfer information to the next level while maintaining consistency. Information sources for each report should be identified and defined. Other areas of concern include collection methods, information quality assurance, data ownership, and the development and implementation of simulation tools.

Business domain knowledge

Banks can undertake a number of actions to help the operational risk management function (and its complementary functions) enhance their business domain knowledge. They can conduct training on banking products and processes, with a focus on identifying and understanding their inherent risks. Workshops with business areas can help analyze the identified risks in more detail. And, for highly complex products and processes, on-the-job training in the form of short-term assignments to business areas can be very helpful.

Cost-benefit analysis

The potential benefits of operational risk management improvements include freeing up capital; better decision-making based on simulation results; lower cost of funds due to better corporate ratings; and lower operating costs from improved controls and monitoring tools. Other potential benefits include reduced profit and loss volatility, increased customer and staff satisfaction, optimized insurance coverage, and improved regulatory compliance.

As for costs, these include project implementation costs for the various program elements; costs associated with adapting or upgrading the bank's IT platform; and a number of recurrent and ongoing costs when the project is moved to the production stage.

Conducting a cost-benefit analysis can help the bank identify quick wins to support the effort and shed light on how to prioritize its action steps.

Phase IV: Implementation Planning

Implementation planning addresses the time frame, the necessary resources and the costs incurred.

This last phase is also used to create the documents used to present the results to senior management in order to receive approval for the implementation of the identified action steps.

Many of these action steps, especially changing risk culture, take time and require careful organization. However, the benefits of improved operational risk management can be compelling and can help banks create and maintain competitive advantage through better performance, lower capital costs, enhanced reputation and many other elements.

Notes

1. Basel Committee on Banking Supervision, "International Convergence of Capital Measurement and Capital Standards," June, 2006. Access at: http://www.bis.org/publ/bcbs128.pdf

2. David Apgar, "Risk Intelligence, Learning to manage what we don't know," Harvard Business School Press, Boston, Massachusetts, 2006

References

Bundesanstalt für Finanzdienstleistungsaufsicht, Rundschreiben 4/2010 (WA) - Mindestanforderungen an die Compliance-Funktion und die weiteren Verhaltens-, Organisations- und Transparenzpflichten nach §§ 31 ff. WpHG für Wertpapierdienstleistungsunternehmen, Fassung 30.11.2012 (in German). Access at: http://www.bafin.de/SharedDocs/Veroeffentlichungen/DE/Rundschreiben/rs_1004_wa_macomp.html;jsessionid=283A9F204EC2D39B7EC3484108AB07B1.1_cid363

"European Banking Authority, EBA Guidelines on Internal Governance (GL 44). Access at: http://www.eba.europa.eu/regulation-and-policy/internal-governance/guidelines-on-internal-governance

Financial Stability Board, "Increasing the Intensity and Effectiveness of SIFI Supervision, Progress Report to the G20 Ministers and Governors," November 1, 2012. Access at: http://www.financialstabilityboard.org/publications/r_121031ab.pdf

Kreditwesengesetz (German Banking Act in German). Access at: http://dejure.org/gesetze/KWG

"Sarbanes-Oxley Act of 2002,"107th Congress, Senate and House of Representatives of the United States of America, Public law 107-204, July 30, 2002. Access at: http://www.sec.gov/about/laws/soa2002.pdf

About the Authors

Michael Auer

Michael is a managing director – Accenture Finance & Risk Services, responsible for banking and capital markets in Germany, Austria and Switzerland. Based in Munich, he has nearly 20 years of industry experience in risk management, including market-, credit- and operational risk. Prior to joining Accenture, Michael held a number of leading roles in the banking industry, including the head of operational risk at a major European bank.

Gerrit Jan van den Brink

Gerrit Jan is a senior manager – Accenture Finance & Risk Services. Based in Frankfurt, Jan has 26 years of industry and consulting risk management experience in the financial services sector. Prior roles included head of operational risk, head of operations and controller at global banks based in Europe. An accomplished speaker and author, he holds a PhD from Erasmus University Rotterdam and is a CPA (Registeraccountant) in the Netherlands.

Eva Mormann

Eva is a senior manager - Accenture Finance & Risk Services based in Zurich. Eva has 15 years of experience in the financial services industry and has held numerous consulting roles primarily in operational risk management and treasury management for financial institutions. Eva's present focus is on operational risk related topics including cyber-crime, reputational risk management and new developments in the operational risk management space.

About Accenture

Accenture is a global management consulting, technology services and outsourcing company, with more than 323,000 people serving clients in more than 120 countries. Combining unparalleled experience, comprehensive capabilities across all industries and business functions, and extensive research on the world's most successful companies, Accenture collaborates with clients to help them become high-performance businesses and governments. The company generated net revenues of US$30.0 billion for the fiscal year ended Aug. 31, 2014. Its home page is www.accenture.com.

Disclaimer

This document is intended for general informational purposes only and does not take into account the reader's specific circumstances, and may not reflect the most current developments. Accenture disclaims, to the fullest extent permitted by applicable law, any and all liability for the accuracy and completeness of the information in this document and for any acts or omissions made based on such information. Accenture does not provide legal, regulatory, audit, or tax advice. Readers are responsible for obtaining such advice from their own legal counsel or other licensed professionals.

Stay Connected

Join Us

https://www.facebook.com/accenturestrategy

https://www.facebook.com/accenture

Follow Us

http://twitter.com/accenture

Watch Us

www.youtube.com/accenture

Connect With Us

https://www.linkedin.com/groups?gid=3753715

Copyright © 2015 Accenture
All rights reserved.

Accenture, its logo, and
High Performance Delivered
are trademarks of Accenture.

11-8658 / 14-2954