

Risk IT and Operations: Strengthening capabilities

June 17, 2011



McKinsey & Company

Preface

The board of directors of the Institute of International Finance (IIF) and members of the Steering Committee on Implementation (SCI) are pleased to present *Risk IT and Operations: Strengthening Capabilities* (the Report) to the international financial community. This Report aims to assist the industry in addressing weaknesses identified in the recent financial crisis, particularly in the technology and processes that financial-services firms use to support risk management.

The Senior Supervisors' Group (SSG), in its December 2010 report *Observations on Developments in Risk Appetite Frameworks and IT Infrastructure*, acknowledged the progress firms have made in undertaking significant IT projects to improve risk-data aggregation. However, it also pointed out that considerable work needs to be done to continue to address weaknesses identified during the height of the crisis.

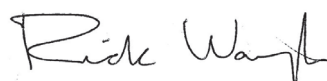
The industry recognizes that inadequate risk IT infrastructure and processes can pose challenges to improving risk-management systems. The IIF has long stressed that a resilient financial system depends equally on appropriate and balanced regulation, sound supervision, credible resolution, and sound internal risk management and governance in firms. Improving banks' risk IT infrastructure is also important for financial stability because it facilitates the provision of accurate risk information for use by bank management and by the micro- and macroprudential supervisors.

We believe this Report provides useful insights and recommendations to both individual firms and supervisors as they work to improve risk IT practices in the industry. It discusses the results of the review undertaken by the SCI, with the help of McKinsey and of firms' Risk IT/Ops practices. In particular, the Report develops an understanding of the expected impact of regulatory changes on risk IT requirements and assesses the current status of industry practices. More importantly, it provides pragmatic industry principles and recommendations that will facilitate each firm's decisions on sound risk IT/Ops practices.

The IIF is grateful for member firms' participation in the review. We are especially appreciative of the invaluable support extended by McKinsey, both in conducting the survey and in the development of this Report. The lists of members of the IIF board of directors, the SCI, and the Risk IT Working Group are included in the Report.



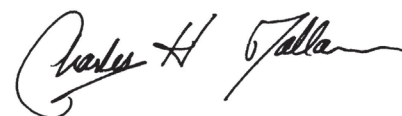
Josef Ackermann
Chairman of the IIF Board
Chairman of the Management Board
and the Group Executive Committee
Deutsche Bank AG
Co-chair, SCI



Rick Waugh
Member of the IIF Board
President and Chief Executive Officer
Scotiabank
Co-chair, SCI



Klaus-Peter Müller
Member of the IIF Board
Chairman of the Supervisory Board
Commerzbank AG



Charles H. Dallara
Managing Director
Institute of International Finance

Contents

List of members of the Board of Directors	5
List of members of the Steering Committee on Implementation	7
List of members of the Working Groups	10
Executive summary	13
Introduction	17
Insights from the research	22
Five themes to achieve sound industry practice	36
Theme I: Data standardization and risk aggregation for monitoring and reporting	38
Theme II: Front-to-back operating model	49
Theme III: Applications, architecture, and infrastructure	60
Theme IV: Organization, governance, and security	78
Theme V: Interactions with supervisors	92
Next steps for the industry	103
Appendix 1: A Table of Principles and Recommendations	105
Appendix 2: Comparing the guidance of the SSG with this Report's Principles and Recommendations	116
Appendix 3: A closer look at the survey's detailed assessment grid	125
Appendix 4: A look at further findings of the survey	127
Appendix 5. Risk IT/Ops data requirements	143



IIF Board of Directors

Chairman

Josef Ackermann*

Chairman of the Management Board and
the Group Executive Committee
Deutsche Bank AG

Vice Chairman

Roberto E. Setubal*

President and Chief Executive
Officer, *Itaú Unibanco Banco S/A*
and Vice Chairman of the Board
of *Itaú Unibanco Holding S/A*

Vice Chairman

Francisco González*

Chairman and Chief
Executive Officer
BBVA

Vice Chairman

Rick Waugh*

President and Chief
Executive Officer
Scotiabank

Treasurer

Marcus Wallenberg*

Chairman of the Board
SEB

Ms. Suzan Sabanci Dincer

Chairman and Executive Board Member
Akbank T.A.S.

Mr. Walter Bayly

Chief Executive Officer
Banco de Crédito del Perú (BCP)

Mr. Yannis S. Costopoulos*

Chairman of the Board of Directors
Alpha Bank A.E.

Mr. Baudouin Prot*

Chief Executive Officer
BNP Paribas

Mr. Peter Wallison

Senior Fellow
Financial Policy Studies
American Enterprise Institute

Mr. Robert P. Kelly*

Chairman and Chief Executive Officer
BNY Mellon

Mr. Hassan El Sayed Abdalla

Vice Chairman and Managing Director
Arab African International Bank

Mr. Vikram Pandit

Chief Executive Officer
Citigroup, Inc.

Mr. Michael Smith

Chief Executive Officer
Australia and New Zealand Banking Group Limited

Mr. Martin Blessing

Chairman of the Board of Managing Directors
Commerzbank AG

Mr. Urs Rohner

Chairman of the Board of Directors
Credit Suisse Group AG

Mr. Andreas Treichl

Chairman of the Management Board and Chief Executive Officer
Erste Group Bank AG

Mr. Gary D. Cohn

President and Chief Operating Officer
Goldman, Sachs & Co.

Mr. Douglas Flint

Group Chairman
HSBC Holdings plc

Mr. K.Vaman Kamath

Chairman of the Board
ICICI Bank Ltd.

Mr. Jiang Jianqing

Chairman of the Board of Directors and President
Industrial and Commercial Bank of China

Mr. Jan Hommen

Chairman of the Executive Board
ING Group

Mr. Charles H. Dallara (ex officio)*

Managing Director
Institute of International Finance

Mr. Corrado Passera

Managing Director and Chief Executive Officer
Intesa Sanpaolo S.p.A.

Mr. Jes Staley

Chief Executive Officer
Investment Bank
J.P. Morgan Chase & Co.

Mr. Yoon-dae Euh

Chairman
KB Financial Group Inc.

Mr. Yasuhiro Sato

President and Chief Executive Officer
Mizuho Corporate Bank, Ltd.

Mr. James Gorman

President and Chief Executive Officer
Morgan Stanley

Mr. Ibrahim S. Dabdoub

Group Chief Executive Officer
National Bank of Kuwait

Mr. Frédéric Oudéa

Chairman and Chief Executive Officer
Société Générale

Mr. Peter Sands

Group Chief Executive
Standard Chartered, PLC

Mr. Walter B. Kielholz

Chairman of the Board of Directors
Swiss Reinsurance Company Ltd.

Mr. Nobuo Kuroyanagi*

Chairman
The Bank of Tokyo-Mitsubishi UFJ, Ltd.

Mr. Oswald Gruebel

Group Chief Executive Officer
UBS AG

Mr. Martin Senn

Chief Executive Officer
Zurich Financial Services

*Member of the Administrative and Nominations Committee



Steering Committee on Implementation Chairmen

Mr. Rick Waugh
President and Chief Executive Officer
Scotiabank

Mr. Klaus-Peter Müller
Chairman of the Supervisory Board
Commerzbank AG

Members

Mr. Kevin Garvey
Head of Group Credit Review & Reporting
AIB Group

Mr. Edward Murray
Partner
Allen & Overy LLP

Mr. Roberto Sobral Hollander
Director
Dep. Gestao de Riscos e Compliance
Banco Bradesco

Ms. Barbara Frohn Verheij
Managing Director
Banco Santander

Mr. Alex Wolff
Head, Risk Strategy
Bank of Ireland

Mr. Robert Pitfield
Group Head, Chief Risk Officer
Scotiabank

Mr. Desmond McNamara
Managing Director Capital & Analytics
Group Risk
Barclays PLC

Mrs. Mayte Ledo Turiel
Chief Economist
Chief Economist for Economic, Financial Scenarios,
and Regulation
BBVA

Mr. Christian Lajoie
Head of Group Prudential Affairs/Co-head
of Group
Prudential and Public Affairs
BNP Paribas

Mr. Brian Rogan
Vice Chairman and Chief Risk Officer
BNY Mellon

Mr. James Garnett
Head of Risk Architecture
Citigroup, Inc.

Mr. Edward Greene
Partner
Cleary Gottlieb Steen & Hamilton LLP

Mr. Christian Wältermann
Director
Group Risk Management and Market Risk
Operations
Commerzbank AG

Mr. Andreas Blatt

Head Risk IT
CRO IT
Credit Suisse

Mr. Tonny Andersen

Member of the Board & Head of Danske Bank DK
Danske Bank A/S

Mr. Andrew Procter

Global Head of Government & Regulatory Affairs
Government & Regulatory Affairs
Deutsche Bank AG

Mr. Bjørn Erik Næss

Group Executive Vice President
Group Finance and Risk Management
DnB NOR

Dr. Florian Strassberger

General Manager
Head of North America
DZ Bank

Ms. Patricia Jackson

Partner
FS Risk
Ernst & Young

Mr. JB King

Director
Ernst & Young

Mr. Robin Vince

Head of Operations
Goldman Sachs & Co.

Mr. Rakesh Jha

Deputy CFO
ICICI Bank

Mr. Alex Van der Laan

Head of Credit Capitals
ING Group

Mr. Mauro Maccarinelli

Head of Market Risk Management
Risk Management Department
Intesa Sanpaolo S.p.A

Mr. Adam Gilbert

Managing Director
Regulatory Policy
JPMorgan Chase

Dr. Mark Lawrence

Managing Director
Mark Lawrence Group

Dr. Philipp Härle

Director
McKinsey & Company

Mr. Fernando Figueredo Marquez

Global Chief Risk Officer
Global Risk Management
Mercantil Servicios Financieros

Mr. Akihiro Kitano

Senior Manager
Basel 2 Implementation Office
Mitsubishi UFJ Financial Group, Inc.

Mr. Masao Hasegawa

Managing Director, CRO, & CCO
Mitsubishi UFJ Financial Group, Inc.

Mr. Hideyuki Toriumi

Senior Manager
Basel II Implementation Office
Mitsubishi UFJ Financial Group, Inc.

Mr. Tsuyoshi Monri

President and CEO
Mizuho Corporate Bank (USA)

Mr. Naoaki Chisaka

Vice President
Corporate Planning Division
Mizuho Financial Group, Inc.

Mr. Kenji Fujii

Joint Head of Global Risk Management Group
Global Risk Management
Mizuho Securities Co., Ltd.

Ms. Jane Carlin

Managing Director
Morgan Stanley

Mr. Paul Mylonas

General Manager of Strategy and Governance,
Chief Economist of the Group, and Secretary of
the Executive Committee
National Bank of Greece

Mr. Parkson Cheong

General Manager and Group Chief Risk Officer
Group Risk Management
National Bank of Kuwait S.A.K.

Mr. Scott McDonald

Managing Partner
Financial Services
Oliver Wyman

Ms. Monika Mars

Director
Financial Services
PricewaterhouseCoopers AG

Mr. Morten Friis

Chief Risk Officer
Royal Bank of Canada

Mr. Nathan Bostock

Head of Restructuring and Risk
Royal Bank of Scotland

Mr. John Cummins

Group Treasurer
Royal Bank of Scotland

Mr. Steven Oon

Head of Firm-wide Risk Management
Royal Bank of Scotland

Mr. Pierre Mina

Head of Group Regulation Coordination
DGLE/CRG
Société Générale

Mr. Clifford Griep

Executive Managing Director, Risk & Policy Officer
Ratings Group
Standard & Poor's

Mr. Paul Smith

Group Chief Risk Officer
Group Risk
Standard Bank of South Africa

Mr. Robert Scanlon

Group Chief Credit Officer
Risk
Standard Chartered Bank

Mr. Nobuaki Kurumatani

Managing Director
Sumitomo Mitsui Banking Corporation

Mr. Philippe Brahin

Director
Risk Management
Swiss Reinsurance Company Ltd

Ms. Ozlem Oner Ernart

Manager
Risk Management – Credit & Subsidiaries Risk
T.Garanti Bankasi

Mr. Takashi Oyama

Counsellor on Global Strategy to President and
the Board of Directors
The Norinchukin Bank

Mr. Richard Metcalf

Managing Director and Group Risk Chief
Operating Officer
UBS AG

Mr. Sergio Lugaresi

Senior Vice President Head of Regulatory Affairs
Institutional and Regulatory Strategic Advisory
UniCredit Group

Dr. Peter Buomberger

Group Head of Government and Industry Affairs
Zurich Financial Services



Risk IT Working Group Members

Mr. Carlos Eduardo Lara
General Manager
Treasury
Banco Itaú S.A.

Ms. Barbara Frohn Verheij
Managing Director
Banco Santander

Mr. Rui Barrento
Banco Santander

Mr. Alex Wolff
Head, Risk Strategy
Bank of Ireland

Mr. Damien Pidgeon
Bank of Ireland

Mr. Lawrence Uhlick
Chairman
BBVA Compass

Mr. Christian Lajoie
Head of Group Prudential Affairs/Co-head of
Group
Prudential and Public Affairs
BNP Paribas

Mr. Gary Gegick
Executive Vice President & Managing Director
Enterprise Risk Architecture
BNY Mellon

Ms. Jennifer Courant
Managing Director
Corporate Center Risk Architecture
Citigroup, Inc.

Mr. Bill Cronin
Managing Director
Corporate Center IT
Citigroup, Inc.

Mr. Christian Wältermann
Director
Group Risk Management and Market Risk
Operations
Commerzbank AG

Mr. Thomas Windel
Group Risk Management and Market Risk
Operations
Commerzbank AG

Mr. Andreas Blatt
Head Risk IT
CRO IT
Credit Suisse

Mr. Roland Schmid
Managing Director
Chief Risk Office
Credit Suisse

Mr. Andrew Procter
Global Head of Government & Regulatory Affairs
Government & Regulatory Affairs
Deutsche Bank AG

Mr. Jonas Slørdahl Skjærpe
IT Manager Business Intelligence & Compliance
DnB NOR

Mr. Daniel Higgins
Ernst & Young

Mr. Phil Venables

Managing Director, Technology
Goldman Sachs & Co.

Mr. Ed Flanders

Head of Wholesale Credit Policy and Projects
Wholesale and Market Risk, Group Risk
HSBC Holdings plc

Mr. Gianni Ferrari

Senior IT Specialist
Risk Management
Intesa Sanpaolo S.p.A

Mr. Domenico Fileppo

Chief of IT Risk Management Office
IT Department
Intesa Sanpaolo S.p.A

Ms. Cristina Cestari

Integrated Risk Management
Itaú Unibanco

Mr. Rodrigo Couto

Superintendent
Integrated Risk Management
Itaú Unibanco

Dr. Sérgio Werlang

Executive Vice President
Risk and Financial Control
Itaú Unibanco S/A

Mr. Takehiro Kabata

Joint General Manager
Corporate Planning
Mizuho Financial Group

Mr. Naoaki Chisaka

Vice President
Corporate Planning Division
Mizuho Financial Group, Inc.

Mr. Kouhei Kuroda

General Manager
Risk Management
Mizuho Financial Group, Inc.

Mr. Satoshi Matsui

Senior Manager
IT, Systems, and Planning
Mizuho Financial Group, Inc.

Mr. David Buckley

Managing Director
Treasury
Morgan Stanley

Mr. Paul Mee

Partner
Financial Services
Oliver Wyman

Ms. Monika Mars

Director
Financial Services
PricewaterhouseCoopers AG

Mr. Joe Sniado

Head of Ratings Services IT
Standard & Poor's

Mr. Paul Smith

Group Chief Risk Officer
Group Risk
Standard Bank of South Africa

Ms. Riana du Plessis

Standard Bank of South Africa

Ms. Erna Solomon

CIO Group Functions IT
Standard Bank of South Africa

Mr. Robert Scanlon

Group Chief Credit Officer Risk
Standard Chartered Bank

Mr. Hiroaki Demizu

Senior Manager of Corporate Risk Management
Division
The Bank of Tokyo-Mitsubishi UFJ, Ltd.

Mr. Akihiko Kabe

Adviser for Risk Management
Risk Management Division
The Norinchukin Bank

Mr. Marc Baumslag

Global Head of Risk IT
UBS Investment Bank IT
UBS AG

Executive summary

In the recent financial crisis, many firms' risk management performed ably. At other firms, however, risk management stumbled. One problem was that some firms could not always aggregate risks they were accumulating quickly and accurately, and, as a result, they could not manage and mitigate them effectively. In other cases, data problems sometimes prevented timely identification or appreciation of the magnitude of risks. As everyone acknowledges, the consequences were severe.

In response, financial supervisors have analyzed the problems in risk management and issued guidance on many specific concerns; the Institute of International Finance (IIF) has published Principles and Recommendations for improvement of internal practices, and firms have undertaken substantive efforts to remedy their deficits. As the crisis recedes, supervisors and firms now seek to establish a sound basis of risk management in firms to support institutional and systemic stability for the foreseeable future.

To help the industry and its supervisors move to this "next normal" of risk management, the Institute of International Finance (IIF) and its Steering Committee on Implementation (SCI) have set in motion several initiatives, on both the broad field of risk management and governance and on specific topics such as risk appetite, risk culture, stress testing, risk models, and Risk IT and Operations, which is the subject of this Report. Almost every commercial activity of financial firms is underpinned by Risk IT and Operations ("Risk IT/Ops"), the information technologies that financial firms use to measure, monitor, and manage their risk, and the operational

processes that gather risk data and convert it into information for decision making. Improved Risk IT/Ops is essential to the success of the industry's and supervisors' largest aspirations.

In collaboration with McKinsey & Company, the IIF has drawn detailed information from 44 member firms, including a formal survey of 39 firms, and lengthy interviews with executives at 10 of the surveyed firms and 5 additional firms. The information gathered was discussed in eight roundtable discussions attended by several financial Risk executives, and the findings of these roundtables have had the benefit of further discussion by the SCI itself. The research centered on establishing an understanding of the current state of Risk IT/Ops and the future to which the industry should aspire.

This Report documents the findings of that research effort. Three main findings emerged, along with a welter of detailed insights. First, firms broadly agree that the most serious shortcomings exposed by the crisis have largely been addressed.

Firms now have a much more detailed understanding of the risks they incur and are better able to manage them. Second, firms agree that the job is far from done and there are significant opportunities to improve Risk IT/Ops, in which they are already investing; by 2015 the collective industry practice is likely to be materially better than today. Third, firms believe that Risk IT/Ops needs sustained organizational focus, including the active engagement of the chief risk officer (CRO),

chief information officer (CIO), and the board, and stronger capabilities, among other things, if it is to achieve the next level of success.

In this Report, the SCl presents 64 Recommendations to provide detail and guidance to firms as they continue to improve Risk IT/Ops. These Recommendations and the Principles that underlie them are presented in five Themes, addressing discrete aspects of Risk IT/Ops. Firms are very actively preparing to follow through on these Recommendations; most firms plan to make substantial investments—an average of \$390 million—in that work over the next five years. For most firms, this represents an increase of spending on the order of 50 percent, and will raise Risk IT/Ops' share of average firm outlays on all IT and operations from 14 to 20 percent.

Risk IT/Ops developments require substantial financial investments but also use scarce human-resources experts in information technology and risk and consume technology resources; moreover, it is highly important not to destabilize the highly effective existing systems that run basic businesses and functions—including payment systems—while adding improved Risk overlays. For these reasons, carrying out the Recommendations made here in the manner appropriate for each firm is likely to take careful planning and often considerable time.

The following summarizes for each Theme the most significant research findings and SCl Recommendations.

Risk data

Firms identified data as one of two priority areas for improvement; 92 percent of firms think that new regulations will have a high impact on the way firms collect and use their risk data. Improvements to data design

and storage will radiate throughout the Risk business system and empower the critical task of risk aggregation. The SCl recommends each firm aim for a common data model as universally as possible. This presents multiple challenges, will take a protracted effort for most firms, and ultimately requires a formidable effort toward standardization by the official sector as well, but the pursuit is worthwhile. If every business within a firm creates its data in the same way, all the downstream tasks become that much simpler. This means numerous changes in the way firms generate and organize data, but it also depends on the consistency of official-sector requirements where data points are used for regulatory reporting in multiple jurisdictions. Firms should also weigh the benefits of consolidated data warehouses, another challenging but worthwhile aspiration. A single trusted source of data within the firm can vastly simplify the Risk IT architecture and make application development and maintenance more straightforward. Moreover, industry-wide efforts to increase data standardization would pay efficiency and comparability benefits to both firms and supervisors. Data quality can be improved by making quality assurance a bigger component of more roles; incentives can also have a powerful beneficial effect. Even as firms pursue these initiatives to strengthen their data, many will continue to find that in certain well-defined circumstances, risk reports will be better served by speedy approximations than by slower, if more precise calculations.

Risk operations

Too often, Risk processes have been built ad hoc to accommodate change, and they suffer from inefficiencies and disruptions that were not conceivable to the original process designer. Firms should reimagine these processes to achieve a seamless flow

of Risk-related responsibilities and data from one end of the process (the front office, typically) to the other (back-office settlement and clearing) and from side to side, as Risk interacts with other functions such as Finance, IT, and Treasury. High-performing processes can help not only to clear inefficiencies, but more importantly to knock down the “silos” that artificially confine processes and interactions within functions, to the detriment of firm performance. Joint design of processes by the relevant functions can get firms over these barriers. The SCl recommends that firms pay special attention to risk aggregation and limit management, critical processes that can benefit from focused improvements.

Risk technologies

Changes in regulation, products, and markets put new demands on Risk IT. Firms believe that while they currently meet essential needs, the burden will grow, making this the other priority for firms, in addition to data: 84 percent expect major new demands in coming years that will have implications for Risk IT. To prepare, the SCl recommends that firms continue to invest in applications that can adapt to cover new needs imposed by business and regulatory change. A clear design of the Risk IT architecture can help improve flexibility, essential to keep up with the accelerating pace of change. Design and enforcement of architectural and technological standards will guard against a relapse. Greater automation is essential, given the number of manual interventions firms currently perform. Middleware can give firms the flexibility and modularity that makes everyday operations simpler and future developments much easier. Finally, firms must ensure that Risk IT infrastructure is flexibly deployed and has ample reserves of capacity.

Risk organization

Firms think that their current organization and governance are robust. Notwithstanding that confidence, firms also believe that segregating Risk IT/Ops into a distinct organizational unit should be seriously evaluated. Several Recommendations outline the things that firms can do to cultivate the right mix of skills in Risk IT/Ops staff, including technical-, business-, risk-, and process-management capabilities. Finally, given the significant number of older yet vital applications that dominate many firms' Risk IT, the SCl recommends that integration planning for Risk IT systems should begin when firms first contemplate a merger or acquisition, and that investment in Risk IT/Ops should be explicitly addressed in firms' strategic planning, and strategies should recognize Risk IT capabilities and constraints.

Interactions with supervisors

Firms note that supervisory interactions could be improved in many ways. The SCl recommends that the industry and its supervisors collaborate to increase the standardization of report content, formats, timing, and prioritization. Additionally, the SCl envisions a cross-jurisdiction initiative to harmonize risk reporting across borders, ideally with leadership from supervisors. And firms and supervisors might spur greater exchange of ideas through their supervisory colleges, and through staff secondments in which managers of firms and supervisors spend time in each other's organizations.

The IIF believes that regular dialogue between supervisors and industry is necessary to continued progress and hopes that this Report will contribute to constructive discussions aimed at strengthening the industry's already considerable Risk IT/Ops capabilities over the coming years.

Introduction

RISK IT/OPS TODAY

Today's financial services firms are among the most technologically complex institutions in existence.¹ This industry, whose core activity is the accumulation and transfer of risk, spends more on technology than any other industry.² In the words of one firm's chief technology officer, "banks are essentially technology firms."³ By definition, then, the measuring and management of risk at Banks and insurers is fundamentally a technological and operational activity. It is not an overstatement to say that Risk IT and Operations is the "engine" that drives superior risk management.

Because of that, Risk IT and operations (defined as the technologies and processes that financial services firms use to identify, monitor, and mitigate risk), along with the management information systems (MIS) that provide firm leaders with risk information (collectively, "Risk IT/Ops") has always been an important focus. Risk IT/Ops underpins almost everything the firm does.

Consider an example. The rating systems that automatically judge the creditworthiness of prospective exposures—a Risk IT application—not only support the core lending activity, greatly increasing efficiency and objectivity by automating part of the credit decision; they also have a substantial impact on the quality of the resulting loan portfolio and the firm's profits.

Another Risk IT tool, risk-based pricing, can in its most sophisticated form give firms a substantial competitive edge across a broad swathe of products. In recent months, new risk tools to forecast cash flows and simulate the impact of a stressed market environment on a firm's liquidity have become more important than ever.

As a result of the recent crisis in the financial system, Risk IT/Ops is now receiving heightened attention from supervisors. It is under significant pressure on two fronts. First, the financial crisis and supervisory influence have permanently altered many risk-management practices. Risk IT/Ops is under pressure to keep pace with the changes in the broader sphere of risk management. This might be considered the indirect pressure on Risk IT/Ops, and is one that firms have already made great progress in addressing.

Second, the technologies and processes that comprise Risk IT/Ops are coming under direct scrutiny from supervisors. In many countries, supervisors are reviewing systems in increasingly detailed ways. The new Basel III framework, for example, requires new and enhanced calculation engines that use new risk methodologies. Regulators are also requiring top-down as well as internal stress tests and incorporation of the results in firms' risk planning, and they are making more frequent and more detailed ad hoc requests.

¹ General notes: (1) The term "firm" is used in this Report as a generic term and may refer to the parent firm and group on a global, cross-border basis or to a subsidiary on a solo basis, as appropriate. Whenever pertinent, references are made to specific entities, such as "branches." (2) Throughout this Report, "Risk" and "Risk management" are capitalized in usages that refer to firms' organizational units, and are not capitalized in more general usages.

² Gartner, Inc., as cited in "Silo but deadly," *The Economist*, December 23, 2009.

³ "Silo but deadly," *The Economist*, December 23, 2009.

Indirect pressure: Risk management is rapidly evolving

In the crisis, financial firms' risk management did much of what it was asked to do. Many firms' Risk systems foresaw to some extent the trouble brewing in various markets, and several firms were able to avoid the worst of the damage.

Unfortunately, the crisis also revealed some deficiencies in firms' risk management. The Senior Supervisors' Group (SSG) has focused on risk management as an area with an important, ongoing need for improvement. Its findings are documented in three reports: "Observations on risk management practices during the recent market turbulence," March 2008; "Risk management lessons from the global banking crisis of 2008," October 2009, which cited problems in the aggregation of risk, among others; and "Observations on developments in risk appetite frameworks and IT infrastructure," December 2010.

The IIF has also addressed the deficiencies in two reports that provide guidance to firms on addressing Risk shortcomings: "Final report of the IIF Committee on Market Best Practices: Principles of conduct and best practice recommendations," July 2008 (the "CMBP Report"); and the "IIF report on reform in the financial services industry: Strengthening practices for a more stable system," December 2009 (the "SCI Report"). These reports established a set of Principles of Conduct and a substantial body of Recommendations for the industry to use as it improves its risk management. The present Report is intended to augment these Principles and Recommendations and extend them into the realm of Risk IT/Ops.

The industry has been engaged for some time in continual improvement of its Risk practices.

The crisis has accelerated that process, and firms have mobilized to act on the lessons learned, as outlined in these reports. To take just one example, we see much more discussion of Risk topics at the board level; this in turn places a call on Risk IT/Ops to generate more frequent and more accurate reports. The IIF has recently published a report, "Making Strides in Financial Services Risk Management," that documents the considerable ground gained in firms' pursuit of the Recommendations issued in the 2008 and 2009 Reports, as well as gaps that remain to be filled.

The result, an internally driven and rapid development in risk management practices, is putting pressure on Risk IT/Ops. Other pressures are coming from the outside. Basel III in particular is creating change in Risk practices that have knock-on effects on Risk IT/Ops. Consider these examples:

Other supervisory bodies, notably the European Banking Authority, the Federal Reserve, and the UK's Financial Services Authority, are compelling firms to conduct stress tests, which will require Risk IT/Ops to support some new and cumbersome calculations. Many new microprudential and macroprudential reports are or will be required, as will many new ad hoc reports in connection with the "more intensive" supervision mandated by the G20.

In another development, the newly created Office of Financial Research of the United States Treasury is mandating a system of standard Legal Entity Identifiers, which it sees as a key requirement for analyzing and preventing the accumulation of systemic risks. Data standardization is a worthwhile goal, and it is advocated by this Report, but Risk IT/Ops will bear the brunt of the transition to new standards.

All in all, this pressure on Risk IT/Ops is significant. With very few exceptions, all of the needed new abilities can only be enabled through Risk IT/Ops. One visible expression of these new pressures is the cost to firms. In a November 2010 white paper, McKinsey & Company estimated that the Risk IT implications of Basel III will account for between 25 and 50 percent of the European banking industry's total cost to reach compliance.⁴

Direct regulatory focus on Risk IT/Ops

Whereas before the crisis, regulators were concerned largely with the broader issues of risk management, today they are intensely probing the technical realm of Risk IT/Ops. We see evidence of this in several arenas: some content in the formal reports issued by supervisors, a few features of the new regulatory regimes, a newfound interest on the part of supervisors in technical topics, and a change in the consistency and tonality of supervisors' discussions with firms, all aimed squarely at Risk IT/Ops.

Consider the 2009 Senior Supervisors Group report, which in one section deals explicitly with Risk IT/Ops. It states:

The importance of a resilient IT environment with sufficient processing capacity in periods of stress is becoming increasingly evident. Firms are constrained in their ability to effectively aggregate and monitor exposures across counterparties, businesses, risk strands, and other

dimensions because of ineffective information technology and supporting infrastructure.

A more recent report from the SSG, the "Report on observations on developments in risk appetite frameworks and IT infrastructure," from December 2010, deals directly with Risk IT/Ops, and identifies four outstanding areas for improvement: IT governance, data quality and consistency for risk aggregation and automation levels, system capacity, and the integration of IT systems and platforms. More particularly, the SSG urges firms to strengthen Risk IT governance processes by aligning IT and strategic planning, mobilizing sufficient resources (for instance for integration projects), and establishing strong project management offices. The report says firms should strengthen data governance by assigning data owners. Another area of opportunity is further automation to reduce reliance on manual interventions. Finally, the SSG urges firms to continue their efforts to integrate the disparate IT systems that many firms in mature markets have accumulated through a series of mergers and acquisitions.⁵

In the area of reporting, the newly created European Banking Authority has specified the frameworks FINREP and COREP along with the technical language XBRL and has encouraged local supervisors to use these standards in their reporting requirements to firms.⁶

In over-the-counter (OTC) derivatives, regulators and market participants have been engaged in initiatives to improve the levels of standardization, central clearing, bilateral risk

⁴ See "Basel III and European banking: Its impact, how banks might respond, and the challenges of implementation," www.mckinsey.com.

⁵ Appendix 2 of this Report provides the SSG's specific recommendations.

⁶ FINREP is the Standard Financial Reporting Framework; COREP is the Common Solvency Reporting Framework; XBRL (eXtensive Business Reporting Language) is an open-source standard computing language.

management, and transparency. Standardization in data, processes, and products is seen as a key enabler for the other improvement areas.⁷ Another example comes from Germany, where in the current consultation process for the new “MaRisk” (minimum requirements for risk management in financial firms), specific formulations regarding IT, such as the definition and enforcement of access rights and the enforced separation of production, test, and development systems, are being discussed.

In addition to all the regulatory demands on Risk/IT development time and resources, it must be recognized that accounting is also undergoing radical change in most major markets, and especially in areas critical to the financial-services industry. While a number of very significant issues remain to be resolved by the International Accounting Standards Board and the US Financial Accounting Standards Board, some of the changes being planned (impairment and provisioning, netting, and hedge accounting, to give three examples) will be very significant and will require significant systems efforts and phase-in times.

Other changes are also afoot. Many firms report that in their interactions with supervisors and regulators, Risk IT has become more prominent in four ways.

First, discussions on Risk IT/Ops are happening more often and more regularly.

Second, the discussions are reported to focus much more consistently on specific topics such as firms’ strategy for choosing locations for data backup facilities, software implementation standards, Risk IT architecture design and long-term strategies, user account management, separation of development and production systems, IT risk management, outsourcing

strategies and locations, the operational risk arising from IT, data access protocols, the number of people working on specific Risk IT projects, and so on.

Third, discussions are now much more detailed than before, and are rigorously followed up by supervisors, resulting in much more cautious audit reports on Risk IT/Ops.

Fourth, firms have also reported an increase in the number of ad hoc requests specifically on the status of Risk IT and Risk IT projects. Firms also say that, because of a newly urgent tone in their discussions with regulators, they conclude that Risk IT/Ops is now one of regulators’ top priorities.

To be sure, firms’ recent experience with supervisors varies significantly; for one thing, supervisors in different jurisdictions are emphasizing quite different points at the moment. Yet a strong general impression remains that Risk IT/Ops’s status has changed from a supplier of commodity goods to the critical constituent in enabling strong risk management practices.

The IIF’s initiative

In response to these changes and challenges, the IIF set up a global initiative on Risk IT/Ops, with three objectives: to assess the current state of the industry’s Risk IT/Ops activities and understand the implications of new regulations; to understand the industry’s perspective on the target for sound practice to which the industry should aspire; and to help the industry work with its regulators to plot a course to complete the journey toward that aspiration.

⁷ International Swaps and Derivatives Association.

The initiative was spearheaded by a working team of representatives from 12 IIF member firms. The working team met several times to set objectives, design the initiative, and develop initial hypotheses on the current status of Risk IT/Ops and on the target state of sound industry practice. The team was overseen by the IIF's Steering Committee on Implementation (SCI), a body consisting of senior executives of 40 IIF member firms and chaired by Rick Waugh (president and chief executive officer, Scotiabank) and Klaus-Peter Müller (chairman of the supervisory board, Commerzbank). The SCI is also overseeing IIF initiatives to strengthen risk-management practices.

At the center of the initiative was a survey of IIF member firms. The survey asked firms around the world to share their views on Risk IT/Ops practices, the implications they expect from new regulation, their vision for sound industry practice in the future, the resources they expected to invest to achieve this end state, and the benefits they hoped to derive from the work.

The survey began in November 2010 and concluded in April 2011; 44 firms participated in the survey and other parts of the initiative. Surveys were completed by senior Risk IT and risk-management executives. In many instances they coordinated a broader survey response for their firm; given the depth and breadth of Risk IT/Ops at most firms, the views of several people were required to provide a comprehensive response.

The survey was complemented by two additional research efforts. First, the working team conducted interviews with Risk and Risk IT executives from 15 firms. These interviews delved into Risk IT and risk-management topics in greater detail, focusing in particular on the impact of regulations, interactions with regulators, future investments and projects

related to Risk IT and risk aggregation. These have helped to provide examples and, in general, have been consistent with the results of the survey.

Second, the working team expanded slightly and then divided into two smaller working groups, each with representatives from 10 IIF member firms. The working groups constituted a representative sample of the IIF membership; executives present came from both large and small banks, investment and retail banks, and many different regions. These working groups helped to formulate, debate, and provide examples and explanatory discussion for each of the Principles and Recommendations contained in this document.

This Report

This Report summarizes the work of the IIF's initiative on Risk IT/Ops. In the following sections, the document will present:

- The high-level findings of the survey, interviews, and discussions
- The Principles and Recommendations that firms can draw on to move the industry to a target of sound practice, organized in five action Themes
- Next steps for firms' immediate consideration
- Five appendices that provide:
 - A reference guide to the Principles and Recommendations
 - A comparison of the SSG's guidelines with the Principles and Recommendations
 - A closer look at how the survey works
 - An overview of additional survey findings
 - A summary of the data requirements of Risk IT/Ops

Insights from the research

METHODOLOGY, PARTICIPANTS, AND PEER GROUPS

As described in the previous chapter, the IIF and McKinsey jointly developed a comprehensive survey covering Risk IT/Ops. The survey involved a detailed self-evaluation. The results, combined with interviews and working-group discussions, were used to understand firms' views on four topics: regulatory impact, the current status of firms' Risk IT/Ops, a possible target state for Risk IT/Ops, and the investments they expect to make. In this chapter, we outline the questions that were asked of firms and the high-level insights that came out of their

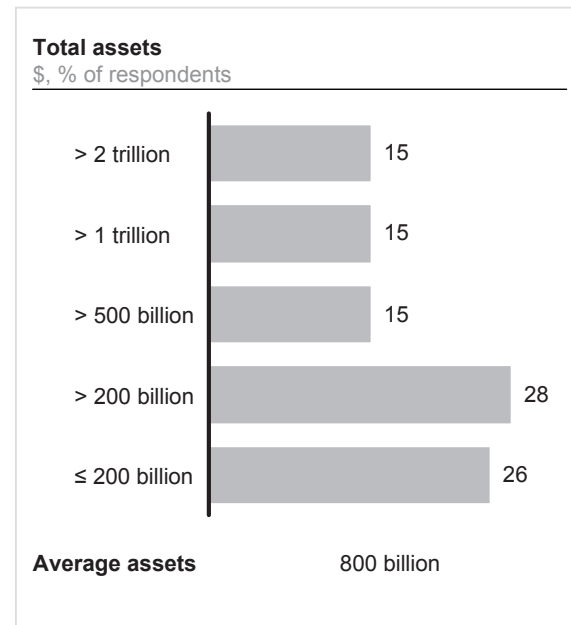
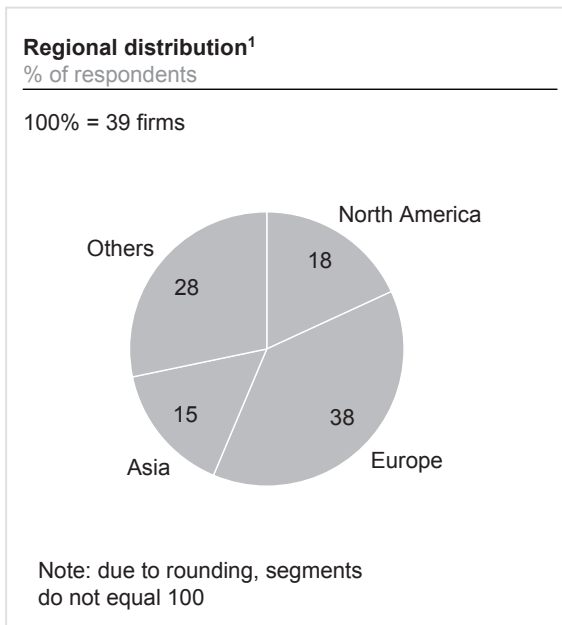
responses. The Themes that follow this chapter delve in much greater detail into the findings of the research, as does Appendix 4.

Forty-four firms participated in the research. The respondents to the survey are a representative sample of 39 firms from around the world (Exhibit 1). Fifteen firms, ten that completed the survey and five that did not, contributed in-depth interviews conducted by McKinsey; information from those interviews is included in the analysis.

The largest group of firms, 38 percent, is headquartered in Europe; North America

Exhibit 1

Survey participants are based around the globe and are of all sizes



¹ Based on location of bank headquarters.
Source: IIF/McKinsey Risk IT/Ops survey

and Asia are well represented; and nearly 30 percent are headquartered in Latin America, South America, Australia, and Africa. With respect to “footprint” (that is, geographic extent of operations), the respondents are about evenly divided into global institutions (those with branches on six continents), multiregional (on four or five continents), and regional (on three or fewer continents). Thirty-three percent are retail-oriented; 13 percent say they are investment-banking heavy; the remainder, 54 percent, are mixed. About half of the respondents have \$500 billion or more in assets.

Based on these demographics, the firms were divided into four peer groups (Exhibit 2):

- Global reach, IB franchise: Large, developed-market firms with a global footprint and an established investment-banking franchise
- Multiregional: Large, developed-market firms with a strong multi-continental or regional presence
- Regional focus: Smaller developed-world firms with a strong regional focus
- Emerging markets: Firms of all kinds and sizes, united by their location in emerging markets

Exhibit 2

Survey participants were divided into 4 peer groups

	Global reach, investment-banking (IB) franchise	Multiregional	Regional focus	Emerging markets
Description	Large, developed-market banks with global reach and established IB franchise	Large, developed-market banks with strong local/regional presence and additional presence in other regions	Developed-world banks with strong local focus	Emerging-markets banks
Members	<ul style="list-style-type: none"> ▪ Bank of America ▪ Barclays ▪ BNP Paribas ▪ Credit Suisse ▪ HSBC Group ▪ Royal Bank of Scotland ▪ Santander ▪ Société Générale ▪ UBS 	<ul style="list-style-type: none"> ▪ Scotiabank ▪ BBVA ▪ Commerzbank ▪ Intesa SanPaolo ▪ Mitsubishi UFJ Financial Group ▪ Mizuho Financial Group ▪ Royal Bank of Canada ▪ Standard Chartered 	<ul style="list-style-type: none"> ▪ ANZ Bank ▪ Bank of Ireland ▪ BMO ▪ BNY Mellon ▪ Commonwealth Bank ▪ DnB NOR ASA ▪ Erste ▪ FirstRand ▪ KookMin Bank ▪ The Norinchukin Bank ▪ PNC ▪ Suncorp ▪ State Street Bank 	<ul style="list-style-type: none"> ▪ Akbank ▪ Banco de Credito BCP ▪ Bancolombia ▪ Bank of China ▪ Garanti Bank ▪ ICICI Bank ▪ Itau Unibanco ▪ Mercantil Banco ▪ Qatar National Bank

Source: IIF/McKinsey Risk IT/Ops survey

IMPACT OF REGULATION

The survey asked firms to assess the impact of 13 newly emerging regulatory topics in four categories (Exhibit 3). Firms were asked to assess the impact of each topic on 10 areas—their core business activities, and 9 areas related to Risk Management and Risk IT/Ops: risk management, measurement and controlling; risk reporting; stress-testing and simulation; Risk Operations; Risk organization and governance; applications; data and its integration; infrastructure; and Risk IT organization, governance, and security.¹ Firms measured impact from 1 point (low) to 4 points (high). To aggregate ratings across firms, these self-assessments were indexed to a scale of 0 (no impact) to 100 (maximum possible impact).

Regulation's impact on various parts of the firm

Firms expect significant impact from regulatory changes across all areas: on the business, Risk Management, and Risk IT/Ops (Exhibit 4). The impact is clearly expected to be highest on the business. Differences in headquarters, business model, or footprint did not affect this result, although there were differences in the magnitude of impact.

The level of the expected impact on Risk IT/Ops, and the breadth of those expectations, are important signs of firms' concern about both the effects on Risk IT/Ops and the perceived shift of supervisors to a greater focus on Risk IT/Ops.

Exhibit 3
There are 13 regulatory topics, in 4 broad categories

Categories	Topics
Higher capital requirements	<ul style="list-style-type: none"> ▪ Increased quality, consistency, and transparency of capital base (e.g., new capital deductions, including the exclusion of some forms of hybrid capital) ▪ Increased minimum Tier 1 and core Tier 1 ratios ▪ New market risk and securitization framework, counterparty credit risk capital charges ▪ Non-risk-based leverage ratio as a backstop to the risk base measure
New liquidity management	<ul style="list-style-type: none"> ▪ 30-day liquidity coverage ratio to ensure short-term resilience ▪ Net stable funding ratio to ensure long-term liquidity
Modified market structures	<ul style="list-style-type: none"> ▪ Central clearing of over-the-counter (OTC) derivatives ▪ Stronger "subsidiarization" (a move to ensure local entities are operated and capitalized as subsidiaries of bank holding companies, rather than branches)
Stricter supervision	<ul style="list-style-type: none"> ▪ Increased supervisory oversight of risk-management capabilities/practices ▪ Capital surcharge for systemically important firms ("too big to fail") ▪ Stricter regulations on consumer protection (e.g., prescriptions on products, information, and consumer right of withdrawal) ▪ Extended fair value reporting, introduction of expected loss model, and enhanced and more frequent disclosures ▪ Supervisory review of new remuneration policies

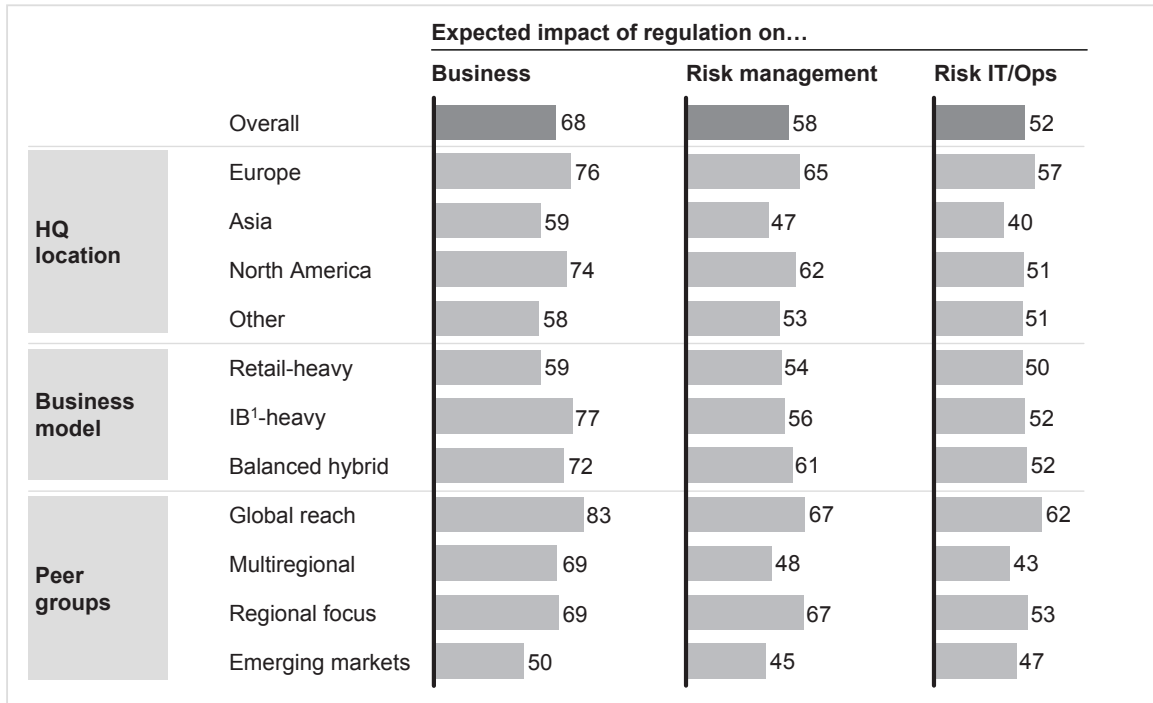
Source: IIF/McKinsey Risk IT/Ops survey

¹ Includes two accounting changes (introduction of expected-loss model for provisioning and fair-value reporting) that many firms consider of a piece with the broader body of regulatory changes.

Exhibit 4

Expectations of impact from regulation vary; firms are consistently most concerned about business impact

Indexed assessment (0 = low, 100 = high)



¹Investment banking
Source: IIF/McKinsey Risk IT/Ops survey

With respect to the four categories of regulation, firms expect higher capital requirements to have the greatest effect on the business (Exhibit 5). But in risk management and Risk IT/Ops, new rules on liquidity management will have the greatest effect (63 and 53 out of 100, respectively), firms say.

Looking more closely at Risk IT/Ops, firms expect the highest impact (53 of a possible 100) to come from liquidity management; however, the other three categories showed practically identical expectations.

There was a strong correlation between impact on risk management and Risk IT/Ops: the two fields are of course closely connected, and it is likely that firms see that regulations that affect risk management will have at least an indirect impact on Risk IT/Ops.

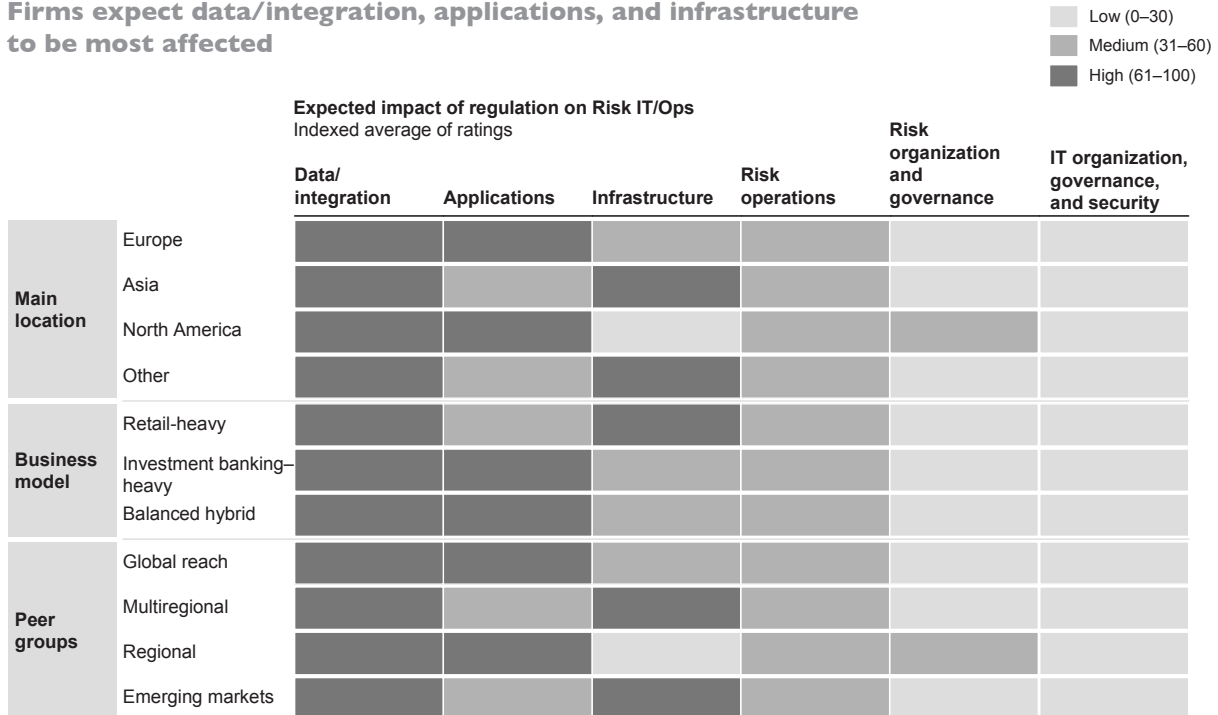
Interviews enhanced the picture from the survey, and revealed similar perspectives. Firms thought there was significant uncertainty regarding future regulation (especially the still-to-be defined details of Basel III and, in the US, the Dodd-Frank Act). They thought these emerging requirements would impact Risk IT/Ops significantly but indirectly, with few mandates specifically targeted at Risk IT/Ops. Many of those interviewed, however, expressed particular concern about meeting a perceived desire on the part of supervisors for greater real-time reporting and analysis capabilities, which will have significant impact on data, applications, architecture, and infrastructure. Indeed these are the areas that firms believe will be most affected by regulatory change (Exhibit 6).

Exhibit 5
Firms expect significant impact on business, risk management, and Risk IT/Ops



Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 6
Firms expect data/integration, applications, and infrastructure to be most affected



Source: IIF/McKinsey Risk IT/Ops survey

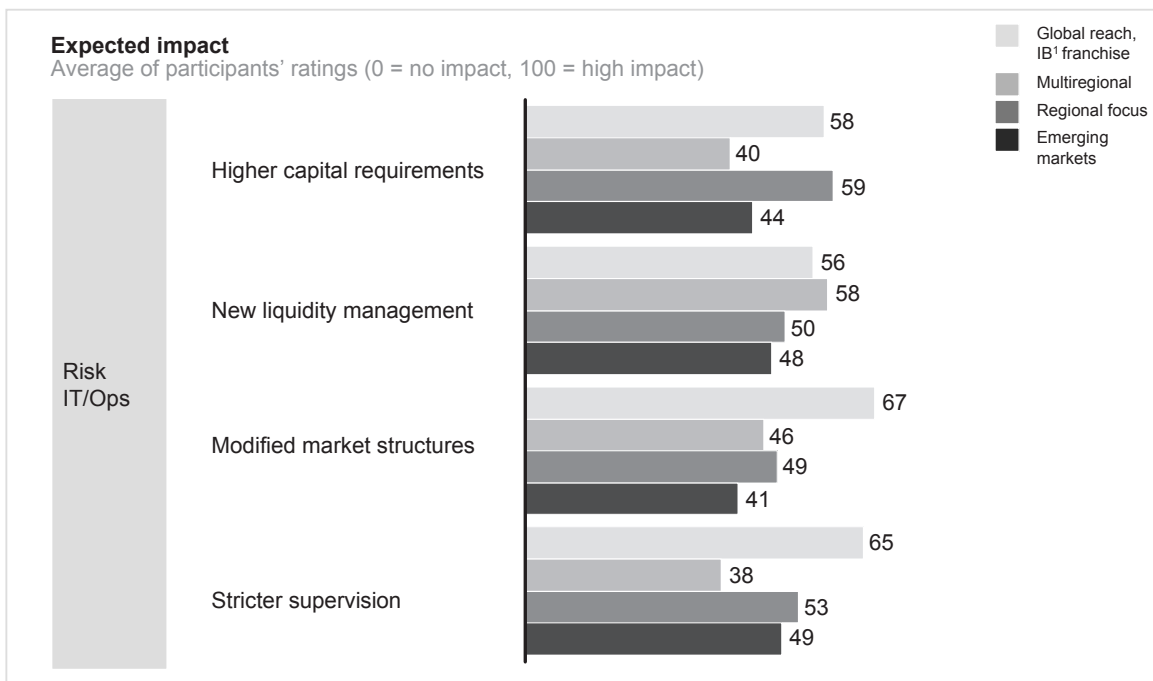
The categories of regulation with greatest impact on Risk IT/Ops

Firms in all peer groups expect a substantial impact on Risk IT/Ops from the new regulatory liquidity and funding ratios, as well as from the extensive development of liquidity-risk management that has been driven by the fallout from the crisis, including the IIF and Basel principles on liquidity risk management published in 2007–08 (Exhibit 7). While further changes in these rules may be desirable from a substantive point of view, the potential for change also causes concern because of the need for planning of Risk IT/Ops to support these requirements at a time when the final complex of rules remains unclear.

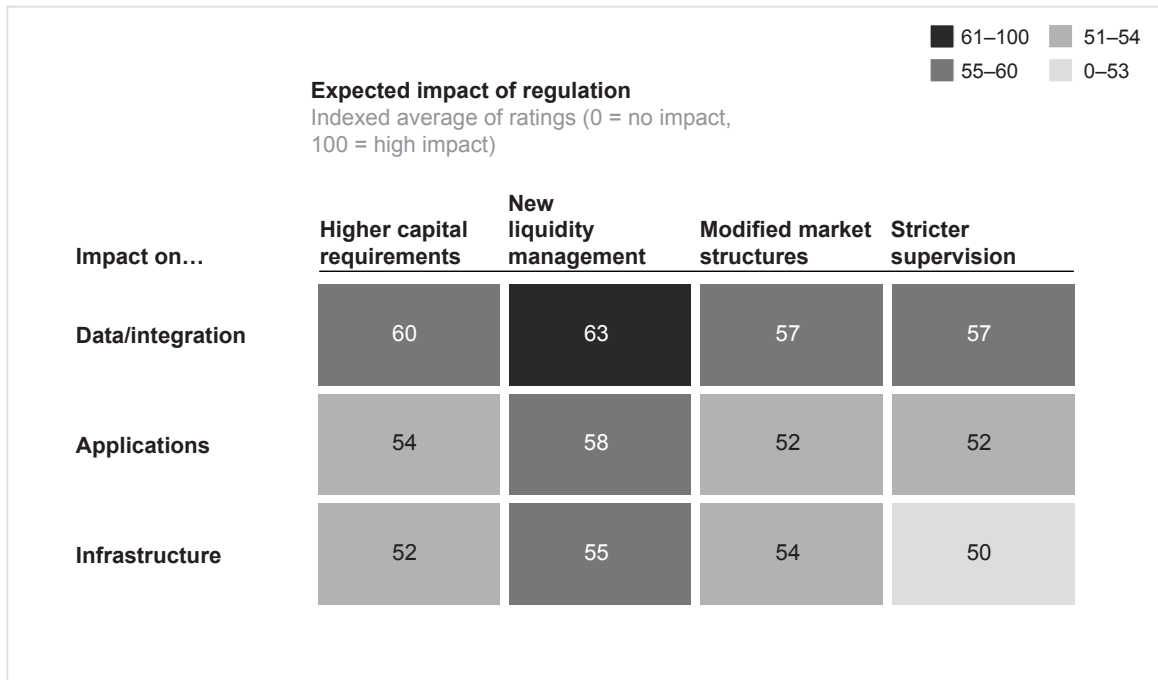
Generally speaking, global firms expected higher impact than the other peer groups. In two of the four categories, emerging-markets firms expected the least impact. Regional firms say higher capital requirements will have the greatest effect (59).

Exhibit 8 summarizes the expectations of all firms for regulatory impact on the three most affected areas of Risk IT/Ops: data and integration, applications, and infrastructure. These areas are consistently the top concern for firms in every peer group and across all demographic divisions. Here too, it is clear that liquidity management is arousing the highest expectations for impact. Further, we see that, across all four categories, firms expect greatest impact on data and integration.

Exhibit 7
Global firms are most concerned and emerging-markets firms are the least concerned about regulatory impact on Risk IT/Ops



¹Investment banking.
 Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 8**There are four drivers of impact for the three most affected areas of Risk IT/Ops**

Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 9 shows the three regulatory topics that firms expect to have greatest impact. Surprisingly, none of these topics are drawn from liquidity management. That anomaly is an artifact of the wide range of expected impact in some categories; while liquidity management was highest on average, other categories had some elements whose impact was very highly rated and some whose impact was rated quite low.

Firms expect one topic categorized under higher capital requirements (that is, “new market risk and securitization framework, counterparty credit risk capital charges”) to have greatest impact on Risk IT/Ops. Other topics in this category, such as the new capital ratios, will have less effect, firms say.

Two topics under increased supervision are also in the top three (“extended fair-value reporting, introduction of an expected loss model for provisioning, and enhanced and more frequent disclosures” and “increased supervisory oversight of risk management capabilities/practices”).² The other elements grouped under stricter supervision, including new rules regarding capital surcharges, customer protection, and remuneration review, are expected by firms to be the most straightforward to implement.

Some changes that will have substantial import for the business, such as rules that afford customers greater protection, are not expected to tax current information technology, at least

² As noted, for sake of completeness some prominent accounting changes have been included in the 13 regulatory topics.

as they are now understood. Should further consumer-protection measures be proposed in future, that perception may change.

Alignment with regulators

Firms have mixed views on their interactions with regulators regarding Risk IT/Ops. Firms' greatest concern is the transparency of the process of defining new regulatory requirements for Risk IT/Ops. While 36 percent of firms rate this transparency of regulators in defining new rules highly (above 4 on a 7-point scale) and 26 percent of firms believe that supervisors regularly seek discussion, only 11 percent say that Risk IT/Ops requirements are well defined.

CURRENT PRACTICE AND TARGET FOR THE FUTURE

The survey asked firms to rate the current state of their risk management and Risk IT/Ops practices, including their capabilities in credit risk, market risk, operational risk, and liquidity risk. It also asked firms for their views about the current state of sound practice in the industry in both these areas, and about their expectations for the target state for industry sound practice in 2015. Because these topics are closely related, we treat them together in this section.

In this section of the survey, respondents provided ratings on a scale from 1 to 7, with 7 the most positive appraisal. To help calibrate their rating, they were provided 75-word descriptions of levels 2, 4 and 6. The survey thus sought to convert subjective assessments into quantitative answers and provide an objective and effective way to compare firms' responses. Appendix 3 provides more information on the assessment grid that enabled this objectivity.

Gaps between firm practice and current sound industry practice

Most firms believe they are close to current sound industry practice. In fact, 63 percent of firms rate themselves within half a rating point of current industry sound practice, and none rate themselves more than 1 rating point below. In some areas, however, firms believe they are behind current industry sound practice.

Two of the bigger risks where many firms believe they are behind are liquidity and operational risk, especially in relation to applications, timing capabilities in monitoring and reporting, flexibility of MIS, the prevalence of an end-to-end process view, and real-time data capabilities. This is to be expected, as these risks have recently become more important for both management and supervisors.

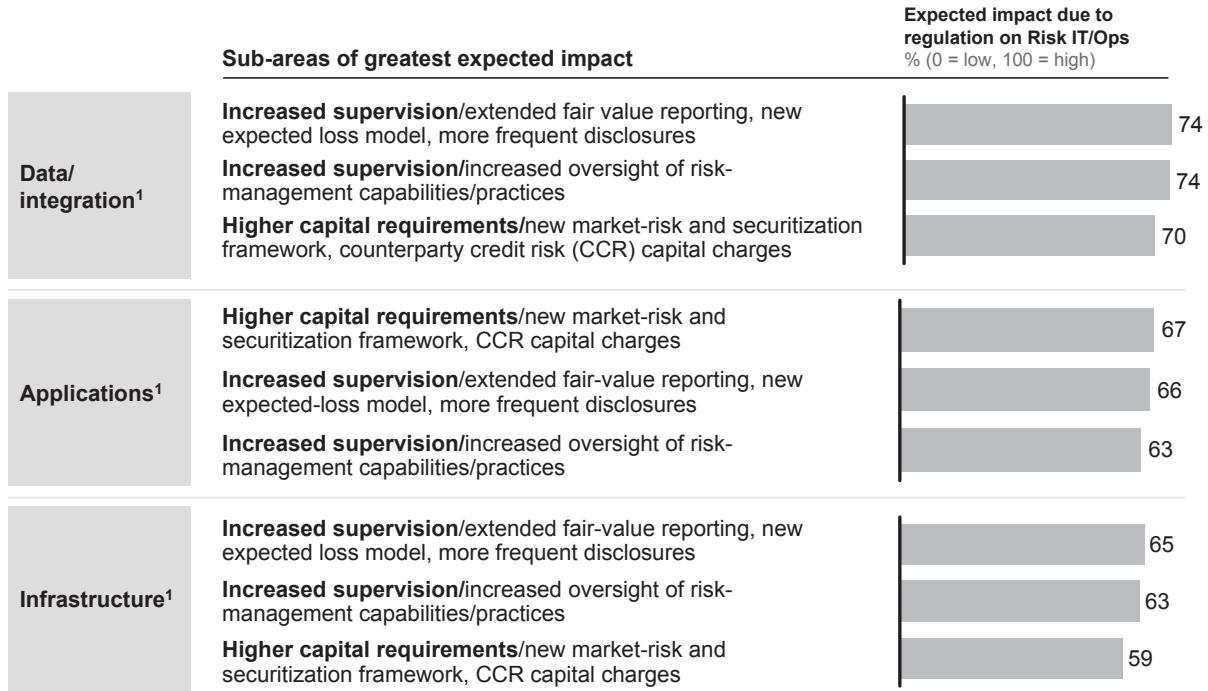
In both the survey and interviews, some firms made clear that they consider themselves to be far ahead of current industry practice. Thirteen percent of survey participants rated themselves at least half a point above current industry sound practice. On average, global and multi-regional firms are the most confident about their current practices, perhaps due to their scale and greater IT resources. The multiregional firms say they are particularly strong in risk reporting and risk operations. Interviews confirmed this, with some firms reporting they are "ahead of the game" and that their "internal requirements [are] above regulatory needs."

Sound industry practice: Gaps between today and the future

The greatest self-reported gaps are in risk analytics for simulations (2.1 rating points) and real-time capabilities (2.0 points), and a related issue, MIS flexibility (also 2.0 points; Exhibit 10).

Exhibit 9

Top three drivers of impact are relatively consistent for the most affected areas of Risk IT/Ops

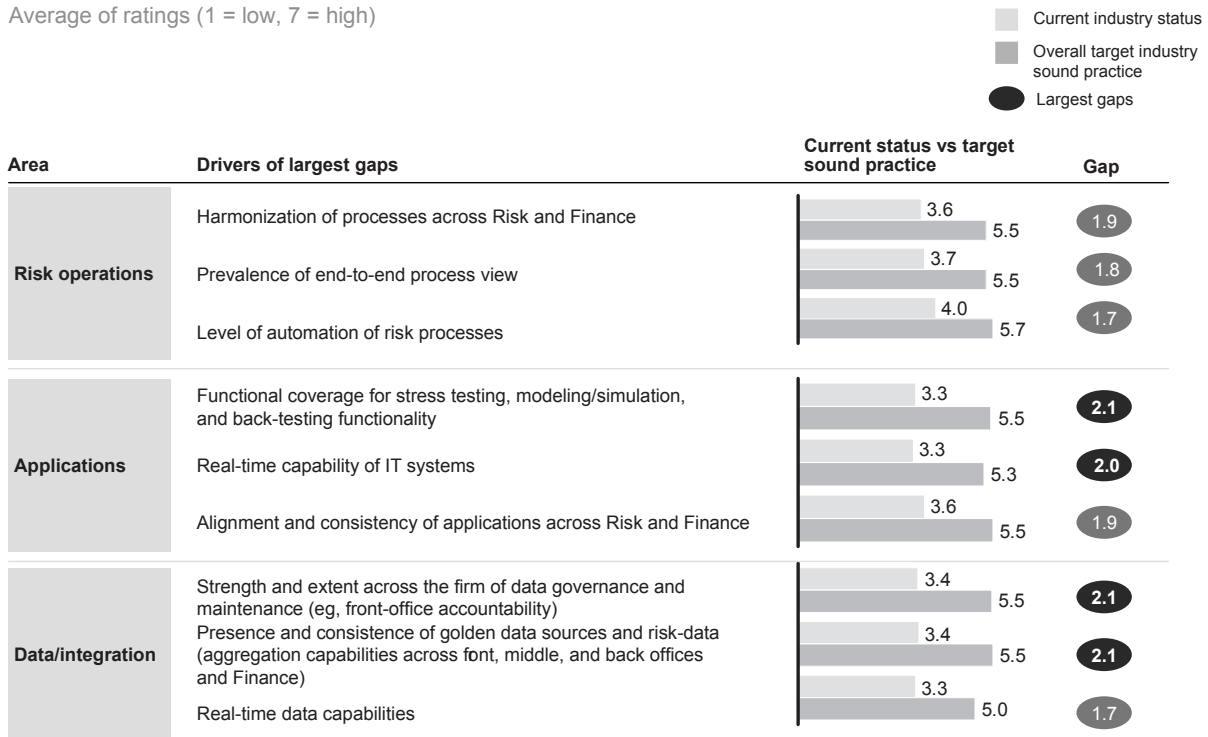


¹ Only top three key drivers shown.
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 10

Largest gaps are in applications coverage for risk analytics and real-time capabilities

Average of ratings (1 = low, 7 = high)



Source: IIF/McKinsey Risk IT/Ops survey

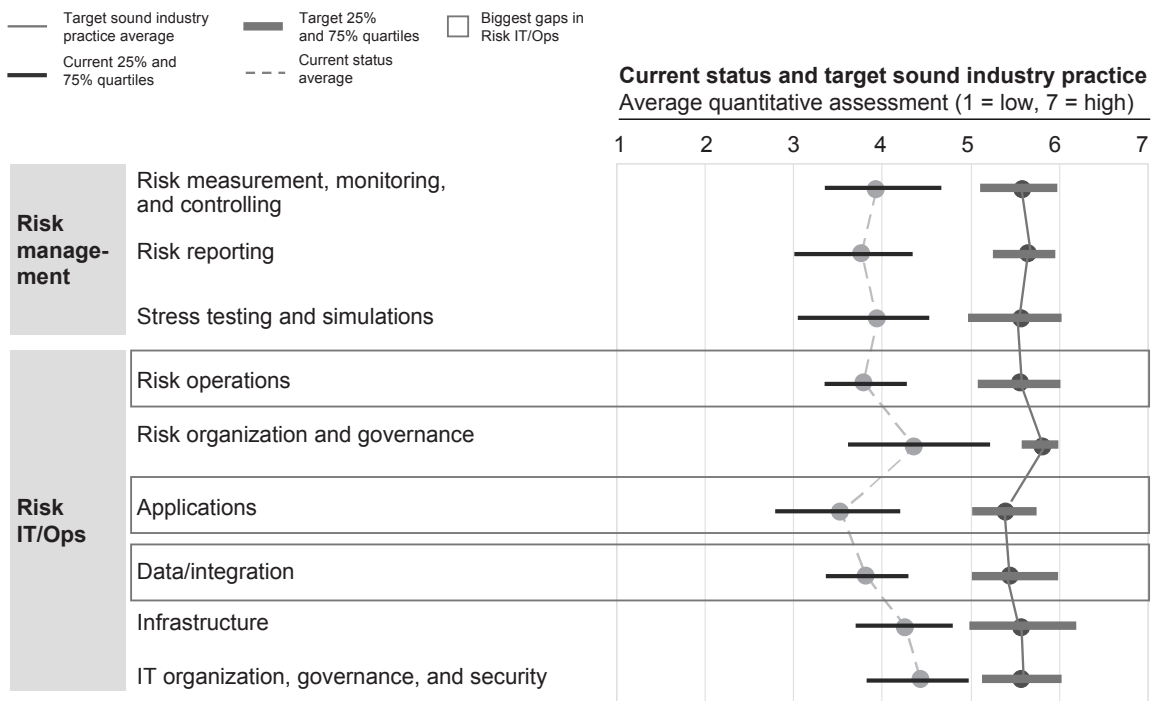
Firms strongly agree that improvements are needed by 2015: 84 percent expect at least a full-point improvement from their current status. The firms that are most confident today are also the most ambitious about the future. But there is significant divergence in firms' views of the future state of sound industry practice, especially in reporting, operations, and applications (Exhibit 11). Firms agreed most about organization, governance, and Risk IT security.

Of the four peer groups, global firms expect the industry to achieve a higher level of sophistication in risk monitoring and reporting than other firms. Most likely this is driven by

the higher regulatory requirements on these firms. Emerging-market firms have higher expectations for infrastructure, possibly because of a focus on growth and consequent need to expand capacity rapidly.

The areas of highest ambition and largest gaps helped determine the survey's conclusions about the priorities for improving Risk IT/Ops practices. Some of these are the aggregation of all risk types, strengthening data integrity through greater accountability and improved governance, and developing coverage in Risk IT applications for critical regulatory requirements. These priorities are expressed in the Themes, Principles, and Recommendations that comprise the bulk of this paper.

Exhibit 11
Firms universally expect progress in Risk Management and Risk IT/Ops but vary on specifics



Source: IIF/McKinsey Risk IT/Ops survey

INVESTMENTS AND EXPECTED BENEFITS

The survey asked firms to provide their current spending range in Risk IT/Ops and the share of Risk IT/Ops in all IT/Ops spending. They were also asked to state their expected investment in the next five years in Risk IT/Ops to close the gap between their current status and target industry sound practice. Finally, firms described the expected benefits and payoffs from these investments.

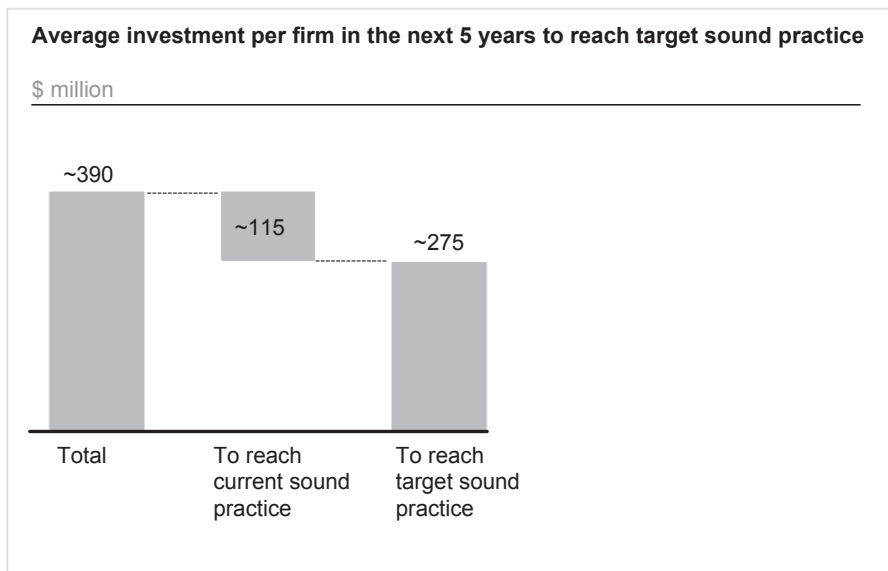
Additional investments of approximately \$390 million on average are required for each firm to continue its journey toward the target state over the next five years (Exhibit 12). At an annualized figure of approximately \$78 million, this represents an increase of about 46 percent

in firms' current spending on Risk IT/Ops, which averages \$170 million annually. The increase will take Risk IT/Ops' share of all IT and operations spending from about 14 percent currently, to 20 percent in 2015.

European and North American firms plan high future IT investments to continue the journey toward a reasonable target level of sound industry practice (Exhibit 11 and 12). European firms are the most ambitious. North American firms currently spend the least on Risk IT/Ops but plan to spend relatively more in the future. This may of course reflect prior investments and the timing of meeting perceived needs. Asian firms have the highest current self-assessments (approximately 10 percent higher than the average of the others), and the lowest expected investment levels.

Exhibit 12

To close the gaps, firms will invest \$390 million on average over the next five years



Source: IIF/McKinsey Risk IT/Ops survey

While the regional patterns are reasonably clear, other investment trends are hard to detect. There is a limited correlation between the amount of planned spending and firm size. Many very large firms (those with over \$2 trillion in assets) planned to spend more than \$500 million over the next five years, while several smaller firms expected to spend less than \$100 million. For the majority of firms in the middle, the correlation breaks down. Risk IT systems appear to have relatively fixed costs, and most firms need to buy or build similar systems, so firms with more resources and greater needs are better positioned to spend the funds necessary to meet those needs.

The amount that firms expect to spend also has little to do with their views on current status and future industry sound practice. In fact, there was no correlation between the size of the gap to target sound practice and future spending. Much

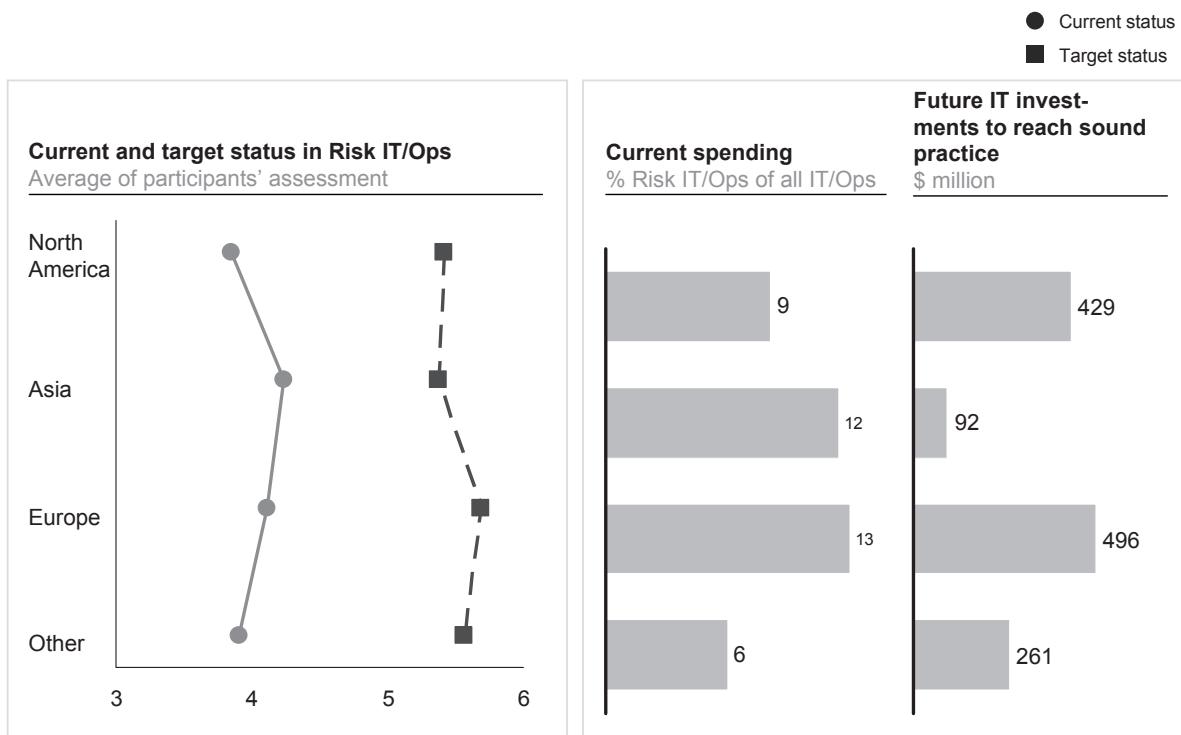
naturally depends on each firm's starting point, and perhaps also the resources it currently has available for this purpose.

Nor was there any correlation between current annual spending and investment need. Part of the reason for this is the fact that some firms have already invested significantly in improving their systems, as certain firms mentioned during interviews. As a result, future investments will look small relative to current or past investments for such firms.

Benefits

Most firms expect investments to pay off beyond improving regulatory compliance (Exhibit 13). A bare majority of respondents are generally optimistic about monetary return from the investment; 51 percent say they expect their investment will pay off. But

Exhibit 13
Western firms are to invest more; North American firms are starting from a lower base



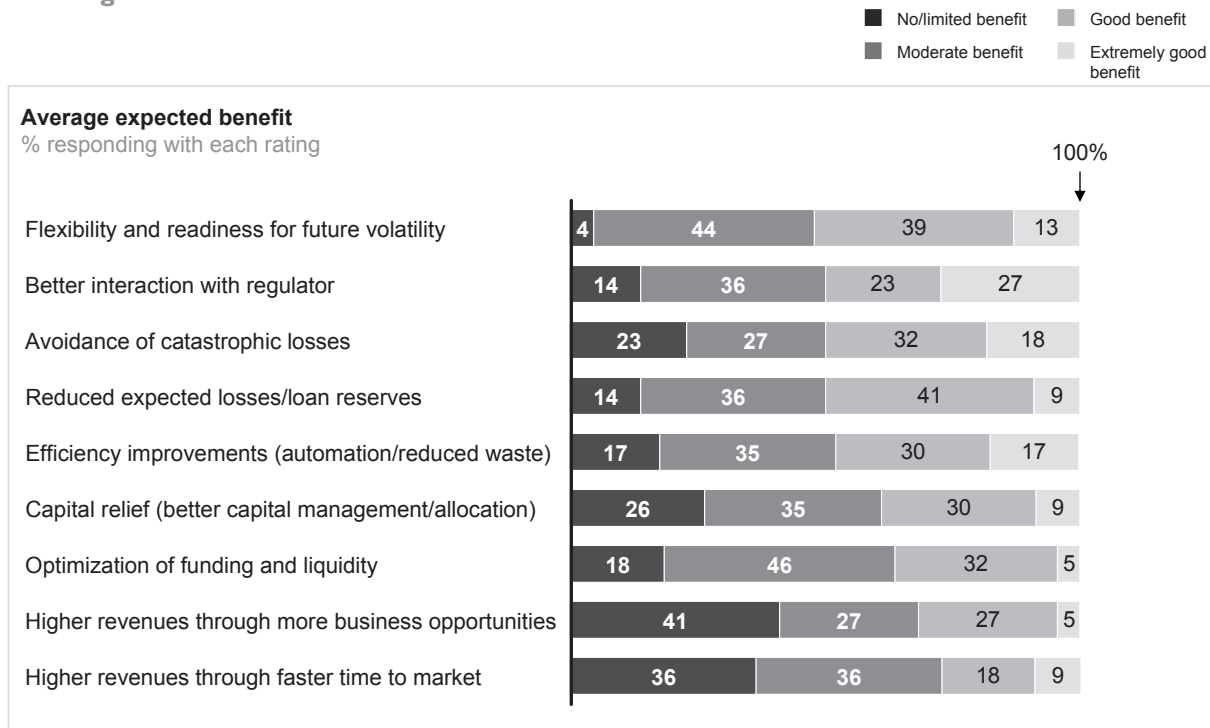
Source: IIF/McKinsey Risk IT/Ops survey

firms that are spending the most are the least certain about expected nonregulatory benefits, perhaps because they are in the midst of major projects or because the investments are being driven by supervisory or regulatory rather than business reasons.

The most-anticipated business benefits (Exhibit 14) are greater flexibility and ability to adapt to a volatile business and regulatory

environment, and improved interactions with supervisors. On that point, firms may reasonably hope that supervisors will react positively to what firms say will be significant improvements in IT-intensive areas. Firms are clear that supervisory and business benefits can be aligned; for example, a supervisory emphasis on stress testing appears to have led to reduced probability of catastrophic losses.

Exhibit 14
Most firms expect returns on their investments – especially better interactions with regulators



Source: IIF/McKinsey Risk IT/Ops survey

Where do firms plan to spend the money?

Nearly all firms participating in the survey, interviews, and working-group discussions report ongoing, large-scale investment in Risk IT/Ops. This includes several firms spending hundreds of millions annually to bring their IT capabilities forward. One source of uncertainty in peer-to-peer comparisons is that some organizations count only the direct IT costs, while others include the investments in governance, training, and cultural change that are natural complements of technology evolution.

These investments are being made in an uncertain regulatory environment, leading firms to prioritize architectural flexibility, but also causing firms to worry that investments may be out of step with the “new normal” of financial regulation. That normality will not take hold until final rules are available, especially in areas known to be under reconsideration, such as liquidity, the leverage ratio, and trading-book rules, and even then many rules will remain susceptible to ongoing, substantial change, such as major accounting programs.

Several common threads emerged in firms' planned investments:

- To “de-Excel” modeling and monitoring processes driven by both regulatory pressure and internal needs for speed, scale, and reliability. This applies to both “business as usual” processes such as stress testing and specialty processes such as cross-risk exposure integration.
- To develop or enhance data warehouses both to broaden access to key information and to ensure that all parties (for example, Risk and Finance) are using the same information for analysis and reporting.
- To make greater use of automation in feeding market and trading data, which will enable better (and more real-time) reporting, and to deliver a comprehensive counterparty perspective (that is, to combine the credit and market views of a particular corporate name)
- To complete postmerger integration projects, with some adopting the “best-of-breed” of the premerger systems and some opting to design and implement completely new systems.

These issues are treated in some detail in the balance of this Report.

Five themes to achieve sound industry practice

ABOUT THE THEMES, PRINCIPLES, AND RECOMMENDATIONS

The survey, interviews, and working-group discussions revealed considerable work under way, but also and importantly revealed the extent of the variance between current industry practice and the “target state.” We define target state as the situation in which a firm’s Risk IT/Ops (a) fully supports its post-crisis risk-management and related control needs and (b) is sufficiently resilient and adaptable to changes in the environment to sustain a high quality of risk management. For 2015, the target state is equivalent to the highest rating on each aspect of Risk IT/Ops, as expressed in the survey. We anticipate that as firms approach their target states, market changes and other environmental factors will compel yet further changes. The target state is an absolute that firms endeavor to approach but which is always receding. To describe the collective of firms’ target states, we use the term “sound industry practice.”

The variances at firms range from small to large; the most advanced and proactive institutions already exceed in some ways the target state, while others have some ground to make up. These differences between current practice and the target state present a challenge to the day-to-day management of a firm’s risks. It is important to keep in mind that the issues described here, though common, arise in different ways in different firms. In many cases, this is because IT systems have grown and adapted to meet specific business and control goals. Some firms may already have resolved

some of these issues while others are just beginning to confront them.

The goal for many firms—the target state—is now to knit together these systems to satisfy broader, group-wide needs; and to achieve the degree of performance and resilience of Risk IT required for both regulatory and business reasons in the post-crisis environment.

Based on the analysis of the survey (including the prioritization of areas with the largest gaps and greatest ambitions) and the interviews, working-team discussions, and discussions within the SCI about these priorities, the IIF has developed Principles and specific Recommendations to achieve sound practice, building on the progress firms have made since the crisis. These Principles and Recommendations are grouped in five action Themes:

- Data standardization and risk aggregation for reporting and monitoring
- Front-to-back operating model
- Applications, architecture, and infrastructure
- IT organization, governance, and security
- Interaction with supervisors

The Principles and Recommendations are intended as guidelines that each firm can draw on, as appropriate to its particular circumstances. The IIF encourages the industry to take these as a basis for further discussions both internally and with supervisors. These Principles and Recommendations augment the related Principles and Recommendations

published by the IIF in 2008 in the CMBP Report, as updated in 2009 in the SCI Report.

The Principles and Recommendations will, of necessity, be implemented in different ways, depending on a firm's starting position (as noted, some firms have made more progress than others), its business model (for example, investment banks will make different choices than retail banks), and the mix of risks it must manage (firms whose exposure is dominated by market risk will draw more heavily on some Principles than firms with mainly credit risk). The implementation timeline will also vary by these factors. As an example, a local retail bank, with its characteristic risk-aggregation needs and reporting needs, may well be able to reach its target state more quickly than a global investment bank.

Theme I: Data standardization and risk aggregation for monitoring and reporting

In the survey, interviews, and discussions, many firms mentioned the importance of standardization and aggregation of the firm's risk information. (Standardization across the industry, particularly of taxonomies and reporting, is addressed in Theme III). Data standardization refers to the extent to which data from different parts of the organization conforms to established norms. Risk aggregation is the ability of firms to sum risks across different business areas and, to a lesser extent, across risk types such as market and credit risk. For example, a firm operating in two different countries may want to understand the total value at risk in its interest-rate products books; to gain that understanding, it must aggregate the risks.

Although these are distinct issues, they are very much linked. Data standardization is an essential prerequisite to excellence in risk aggregation. In a working session, a common view was that data standardization was the base on which to build other Risk IT improvements.

Firms think that solving the two issues is important, for business and regulatory reasons. As noted, businesses' needs are evolving quickly. Moreover, 92 percent of firms thought at least one of the new regulatory regimes would have a high impact on risk aggregation and data standardization. Of course, many firm efforts at standardization will meet both internal and regulatory needs. In one example, the International Swaps and Derivatives Association (ISDA)—itself the product of one of the

industry's early pushes for standardization—is coordinating efforts to further standardize products covered by its standard agreements, and automate their processing, in advance of new rules affecting these products.

CHALLENGES AND POTENTIAL AREAS FOR IMPROVEMENT

The issues affecting data standardization break down into concerns about data's granularity, quality, consistency, completeness, and timeliness. Firms cited businesses' disparate IT practices and the volume of data, as two factors that, in addition to nonstandard data, hinder risk aggregation.

Improving data “granularity”

Several firms noted insufficient granularity in their data, leaving them to estimate exposures that could be more precisely quantified if more detail were available. Drill-downs are often available only for some “cuts” (for example, risk type or line of business) and not necessarily for, say, a specific counterparty. To be sure, this data issue has been recognized in connection with Basel II for some time, and most firms have been working diligently to improve their data collection and granularity. In an interview, one firm reports it now has the ability to “slice and dice” the data in over 125 different ways.

Insufficient granularity in data can be caused by a number of factors. Most often, it is due to the evolutionary way in which firms have

expanded their portfolio of businesses, a tendency to collect only the kind of data they have historically collected, and the expedients that are sometimes used to make it simpler for systems to store or process that data.

Raising data quality

Ensuring data quality is a significant challenge for institutions. This is another complex problem with historical, organizational, and technological dimensions. There is a fairly wide variation in firms' experiences with data quality, but indications are that inadequate data quality is a widespread problem, albeit of widely varying intensity. Most firms report they already have efforts under way to address the issue.

The challenge has two dimensions: weak incentives for data quality and problems with data entry. On the first, it appears that data quality has often been given insufficient attention by the front office—the frontline units that commit the institution's capital. Data quality control is sometimes not formally included in front-office duties; in other cases front-office employees are not incentivized to give high attention to data quality. In the survey, 33 percent of firms believe they had not reached the level where front-office was accountable for any risk-relevant data. In such circumstances, data integrity tends to be monitored only as needed—when there's a problem—rather than early and proactively.

On the second issue, firms concede that quality of data entry is sometimes low. In an interview, one firm described the thousands of people involved in the input of data, a number so large, entailing so many handoffs, that ensuring quality is difficult. Establishing a clear owner of such cumbersome data-entry processes is difficult. Another data-entry problem that firms cited is the uncertain or insufficiently specific definition of data fields. For example, some firms

reported that counterparty reference data sometimes did not allow for the identification of legal entities within a counterparty group.

Data quality is taking on a higher profile as regulatory and management changes create new pressures. In a time of higher capital requirements and, perhaps, a concomitant scarcity of capital, a business that is unable to cross-net as a result of such data deficiencies may find that the resulting higher capital requirements can be onerous. Many firms that did not have adequate data-quality controls before (some did) report, perhaps with these new incentives in mind, that they have started to change their thinking on this topic; at least one firm is experimenting with a scheme to include data quality as one component in determining front-office employees' compensation.

Data inconsistency

Another cause of difficulty in aggregating and reporting risk information on a quick and highly automated basis is variability in the data sets. Variability and inconsistency arise within a business when, for example, data rules and codes change (such as when new business rules are put in place). In addition, each business may have its own set of rules, data models, and taxonomies. This can occur because of the different ways businesses think about and assess risk (commodities businesses conceive of risk differently than interest-rate businesses, for example), but it can also occur because of merger-and-acquisition activity.

As an illustration, consider this example of data inconsistency. Some desks within the same firm define the delta of an interest rate swap as the change related to a 1 basis point (bp) change in the underlying, while other desks run their calculations on a delta that corresponds to a 10 bps change. These differences may have

been established for good reasons; nonetheless, because the definitions are not always linearly related, aggregating across businesses becomes a problem.

Such problems can also appear in retail-oriented firms. For example, in calculating risk-weighted assets, small and medium enterprises of much the same size and risk profile are sometimes classified as retail customers and sometimes as corporate customers. Of course, the risk weights assigned to these classes are very different, and so retail banks can wind up with either too much or too little capital reserved. To some extent, the Basel III capital and liquidity requirements will catalyze change in this regard; even so, problems will likely remain, as Basel's categories may not line up with firm's current definitions, and, at least on the liquidity side, those requirements remain subject to change.

Data inconsistency can result in the need for ad hoc reconciliations and manual adjustments. Both are not only inefficient but also significantly increase operational risk from errors. Firms report significant progress at automating their risk-aggregation processes, but concede that more remains to be done.

Incomplete data sets

A lack of complete time series is a long-standing challenge that the industry continues to wrestle with. Not every data set has been collected and kept consistently over time, although Basel II and III have created strong incentives, to which firms are responding. A patchy data history makes it difficult in many cases to model future exposures well. It also poses a significant constraint for back-testing the validity of models, a fact that is increasingly a focus of supervisory attention and demands. Regulators are apt to look askance, for example, at short or patchy data sets for credit portfolios in retail banks.

Patchy or incomplete data histories can have several root causes. The same changes in product definitions, business rules, and data codes that drive inconsistent data can also result in incomplete histories. Sometimes external data providers cease to publish the same data or may not publish it in the same format. Internal data may similarly not be collected in the same way over time.

Timeliness of data views

Fast turnarounds of data requests are difficult for many firms, especially when requests differ from the firm's standard reporting formats or methodology. Real-time views, which, while desirable, are not necessary for all businesses or risk types, are generally more difficult. Aggregating the necessary data, for example for stress tests, requires several ad hoc data "pulls," which then must typically be manually adjusted. Lack of timeliness can be challenging for all types of firms. In our survey, 20 percent of firms with investment-banking franchises and 33 percent of retail-focused firms thought that their risk reporting was below the level of having "reporting available for consolidated risk positions on a T+5 basis in select asset classes or lines of business only."

Lack of timeliness is caused by many of the factors mentioned previously, the most significant of which is nonstandard data and the need to access many different systems to deliver the required data.

Difficulties in aggregating risk

Not every firm has reported all the issues described here, but most have reported at least one. Several firms find it complicated to tie the exposures of their various businesses or geographical locations into a single, integrated view. Some firms reported that they can achieve an integrated view of exposure to

certain standard risks, and are working toward a similarly integrated view of others, but they are not yet able to do it for all risks, nor can they do it as rapidly and automatically as they would like. Forty-one percent of firms in the survey thought that their aggregation capabilities were not yet ready to achieve “an integrated view on standard risks across desks and asset classes . . . using automated scripts but requiring time lag and integration from disparate sources.”

More positively, some firms reported that they are working on implementing goals such as “risk aggregation on demand,” a capability that would allow them to produce an aggregated view on, say, market and credit counterparty risk by simply pressing a button. Clearly, this capability will not be required by all firms—a local, retail-heavy bank could very well reach a sound target state with much more manual operations, conducted over more time.

For those firms that are experiencing difficulties, two factors seem to be at work: the historically “siloesd” nature of firms’ businesses and the sheer volume of data.

Many business units maintain their own repositories and different, nonstandardized IT infrastructures, largely for historical reasons. This poses a major technical hurdle to the rapid and automated aggregation of data across business units, geographies, and even desks. Fifty-eight percent of firms reported not having “consistent integrated ‘golden’ sources of data for subareas,” with most reporting that their “data [are] extracted from different sources.” Siloes within the firm also lead to different approaches to data governance, and differences in timing created by batch processing. These may also be mandated by external requirements such as clearing system procedures. And of course, many siloes are the result of mergers and acquisitions that have left some IT infrastructure not fully integrated.

These “islands of information” and other legacy systems are discussed further in Theme IV.

Aggregation is made more difficult by the volume of data that most firms have. In an interview, one firm described the “hundreds of millions of rows of data that are collected every few months” through the normal course of business.

PRINCIPLES

In describing target industry sound practices, the Steering Committee has identified, on the basis of the survey and industry discussions, five Principles of risk aggregation and data standardization. These Principles, when fully incorporated in firms’ Risk IT implementation, will enable Risk IT to support more accurate, rapid, and timely risk reporting and monitoring. These Principles describe end states that will take time to reach. They should not be applied uniformly at the same time to all firms, as there is a wide range of starting positions, risk profiles, and requirements from regulators with respect to risk aggregation and standardization. Different Principles will have higher or lower priority depending on the situation of each firm. Overall, they describe goals that all firms should pursue.

Firms should therefore define their own bespoke journeys to achieve maximum focused impact in reaching better risk-management practices through better Risk IT. Some firms will pursue a root-and-branch redesign of their Risk IT infrastructure, while others will decide to pursue a more incremental strategy that builds on existing infrastructure. The decision requires a careful cost-benefit analysis that considers the long-term total cost of ownership of the different approaches. Potential business benefits include faster time-to-market and greater flexibility to accommodate fast-changing business strategies. As a general guideline, it

might be said that firms with a multinational or global operation and an investment-banking franchise should consider eliminating legacy systems as part of a root-and-branch redesign. Careful attention should be paid to the design of a “road map” with explicit intermediate “go/no-go” decision points. Firms with less risk-intense business models may in many cases opt for an incremental approach.

This chapter presents the Principles, followed by more detailed Recommendations that describe actions that might be taken to implement them. Examples that illustrate differences in application are detailed in the discussion of each Principle and Recommendation.

Principle I-i. The ability to achieve an integrated view of exposures for major risk types is essential. Standardized data—across trading desks, asset classes, product classes, counterparties, and legal entities—that can be readily and rapidly aggregated without extensive manual intervention are fundamental.

Discussion of Principle I-i

This Principle aims to orient efforts to overcome the difficulties now experienced in aggregating risks, described above. In implementing this Principle, firms will need to consider how those difficulties appear in their own business and proceed accordingly.

At most firms, the major risk types—market, liquidity, credit, and counterparty—are subject to the Principle. The firm’s business model will, however, affect aggregation requirements. As an example, a retail bank operating on a local level whose risk exposure consists mainly of credit risk might reasonably decide to first develop the capability to aggregate its credit

risk routinely, with less attention to its other risks. An investment bank with a global reach, on the other hand, would more likely need to give priority to building capabilities to routinely aggregate all its major risks across its entire operation.

The aggregation of liquidity risk merits firms’ careful attention. Liquidity risk is subject to all of the same issues of aggregation as other risks, but it also raises specific issues; among other things, firms must heed rules governing the transferability of funds among legal entities. Many of the specific issues raised by liquidity risk have been addressed in prior IIF reports and Basel guidance.³

Operational risk is another special case: it is harder to quantify, there are fewer accepted methodologies to treat it, and, while it is often necessary to respond very quickly to specific instances of operational risk, the need to react quickly to aggregate reports of operational risk is generally lower than for other risks, among other reasons because operational risk is more independent of general market and economic conditions than, for example, credit, or market risk. Accordingly, the firm may conclude that it is not meaningful to aggregate operational risk data in the same way as other risk types.

It is important, however, to define and collect operational-risk data as uniformly as possible; the industry has invested considerably in this effort, through initiatives such as the Operational Riskdata eXchange Association (ORX). Operational risk reporting, including the aggregation of operational risk data, requires separate analysis by operational-risk specialists and, hence, development of appropriate dedicated systems.

³ For more, see the following IIF reports: “Principles of liquidity risk management,” March 2007; the CMBP report; and the SCI report; all available at www.iif.com; and “Liquidity risk: Management and supervisory challenges,” February 2008, Basel Committee for Banking Supervision, www.bis.org.

Principle I-ii. Sufficient granularity, down to the level relevant for risk management and supervisory analysis (generally, the counterparty and product-class levels), must be easily and readily available for all material risks.

Discussion of Principle I-ii

The required level of granularity depends on the institution and the type of risk. Granularity requirements need to be tailored to the type of risk, the type of obligors or counterparties, and the nature of portfolios. The right level of granularity will allow the firm to generate an accurate picture of risk without information overload or “noise.” For example, for many firms, it will be enough to have detailed information on exposure to the largest counterparties rather than to all. Firms note, however, that the set of largest counterparties is fluid; a firm might have very little exposure to a counterparty today but significant exposure tomorrow. Risk IT/Ops will need the flexibility to capture these dynamics.

The benefits of having the right level of granularity include the ability to isolate particular portions of a portfolio, especially a given counterparty, and much better understanding of risk exposures, resulting in better decision making. Management can also fine-tune its actions to target particular problem areas that are pinpointed by more granular data.

Principle I-iii. Data quality standards must be clearly defined and enforced for internal data. For external data, quality checks must be designed and consistently applied.

Principle I-iv. Data used in all control, risk-management, compliance, and supervisory functions must be defined consistently.

Discussion of Principles I-iii and I-iv

High data quality should be a goal for all firms across all risk types. However, with the number of reports firms produce for different purposes, it is reasonable to expect that developing consistency between, say, Finance and Risk will take significant time (often a period of years, according to IIF working teams) and require an ambitious work program.

There are several obvious benefits of high data quality. First, data quality is an integral requirement for all risk-management and other banking activities. As such, high data quality and consistency build trust in risk reports among senior decision makers and among supervisors. Firms will also benefit from loss avoidance through better counterparty risk management. Higher data quality will also lead to a range of benefits for the business, including lower capital requirements and better capital and liquidity management, a more realistic view of key business drivers, higher revenues through better risk selection, and more accurate loan-loss provisions.

In future, firms’ understanding of the requirements of data quality must always include the needs of risk management, in ways perhaps not always conceived of in the past.

Principle I-v. Sufficient data history for more important risk factors and comprehensive data sets for such risks are important to risk management and meeting supervisory requirements. Requirements for the depth and comprehensiveness of data history should be defined conservatively, in consultation with the firm's supervisors. Where necessary and possible, missing internal data values should be filled in with high-quality proxies or external data sources, to be agreed on between the firm and its supervisors.

Discussion of Principle I-v

Incomplete data histories should be completed where necessary on terms that are well understood between the firm and its supervisors. Where firms have not in the past collected information that they now use to produce risk calculations, they cannot be expected to obtain complete internal data immediately. For credit risk in particular, firms can reasonably aim for a lighter implementation; many will likely find that monthly data collected over a business cycle are sufficient. For market risk, data histories should also span at least a business cycle but should be logged more often to capture relevant volatilities.

Firms recognize that longer data histories can without question provide a richer understanding of risk. The longer the data history, the better the calibration of risk models and thus the more precise the risk forecasts. At present, some supervisors have determined that the length of available data histories is insufficient to establish a reliable loss rate for the future. Firms are motivated to change on this front, but it is necessarily a long effort. See Theme V for more on firms' interactions with supervisors.

Principle I-vi. The speed with which consistent data (including aggregated data across businesses, legal entities, and so on) must be delivered should be defined for each relevant risk type. The definition will depend on the materiality and type of risk, and the risk profile and structure of each institution.

Discussion of Principle I-vi

Required delivery or "turnaround" times for aggregated data should depend on the type of risk (particularly its variability) and the type of business unit within an institution. Data on traded counterparty risk or market risk for an investment bank must be turned around more quickly than data on risk-weighted assets for a retail bank. Operational risks generally do not require a rapid turnaround for aggregation across businesses, although it may be important to collect data on certain developing operational risks very promptly within specific businesses.

Frequency of reporting will likewise depend on the institution and the risk type. Risks that are subject to high volatility should generally be aggregated more frequently than less volatile risks. Credit risks, for example, do not need to be available so frequently. Each firm will need to determine its optimal reporting cycle for each type of risk.

In addition, the firm's ability to generate ad hoc aggregate reports for each type of risk upon demand or in a crisis should also be identified, analyzed for adequacy in light of its particular needs, and disclosed to its regulators.

The chief benefits of rapid turnaround times in risk reporting are, of course, stronger compliance, and, on the business side, the essential ability to react quickly to market shocks, including extreme scenarios such as the events of September 2008. In such situations, every firm should have the ability to know its exposures with confidence, so that they may wind down positions, establish hedges, and take other mitigating measures.

RECOMMENDATIONS

The IIF working groups on Risk IT/Ops have established a number of specific Recommendations that firms can use to implement these Principles. These Recommendations encompass changes to IT infrastructure, organization, and processes. Many of these Recommendations are complex, and will require 5-to-10-year efforts to complete.

- **Recommendation I-1.** Firms should aim to create a common data model as universally as possible, including standard definitions of all risk-related data.
- **Recommendation I-2.** Firms should develop clear governance practices to encourage the use of the common data model among all data users.
- **Recommendation I-3.** Firms should develop a reasonable timetable for the transition to the new common data model.
- **Recommendation I-4.** Firms should conduct systemic checks of data quality (e.g., automatic checks against acceptable data ranges during data entry).
- **Recommendation I-5.** Firms should build front-office interfaces that will ensure high quality of risk information.
- **Recommendation I-6.** When external data fails a quality check, firms should bring it up to standard as soon as practicable.
- **Recommendation I-7.** Where appropriate, firms should consider the consolidation of their data into a small number of data warehouses.

Discussion of Recommendations I-1 to I-7

Many firms have suggested that a common data model is a logical prerequisite for many other infrastructure and process improvements. A data model is the abstract description of how a firm stores and works with data. As such, a common data model is an

important IT enabler to reach target industry sound practice, supporting implementation of all the Principles in this Theme, in particular Principles I-ii and I-vi.

While firms recognize the value of a common data model, the obstacles to achieving it are sizable. Large firms especially will find it challenging to create and enforce a common data model throughout enterprises that encompass hundreds or thousands of offices in dozens of countries, a problem that is often compounded by the need to meet data specifications that often vary across jurisdictions. And all firms will find that creating a common data model requires a mature organization that prioritizes data architecture and data governance. Many firms will find this comparatively easy to achieve in their Finance and Risk functions, and possibly also Marketing. Business units on the other hand will likely not put equivalent importance on this—but their involvement is essential if the common data model is to succeed. Creating a truly comprehensive common data model could take time to accomplish and may be difficult to achieve, although the effort should be useful. In addition, achieving the organizational maturity to use it consistently and effectively in the business is if anything an even harder and more complex task. Finally, a common data model depends, to some extent, on greater harmonization of reporting requirements and timelines, as discussed extensively in Theme V. A pragmatic solution for many firms may be to drive a certain degree of commonality in the data model while acknowledging that some variation is inevitable and can be accommodated.

Firms should also be mindful of the cost/benefit balance that should be achieved before they start such an undertaking. This includes having common data taxonomies across the organization, which ensure everyone (and

more importantly, every system) within a firm speaks the same data language, including the front office. For example, the definition of the word “balance” should be consistent across businesses. In this way, the common language supports Principle I-iv, on data quality, and the realignment of incentives discussed below in Recommendation I-8.

Arriving at this common language is a difficult task. A firm faces two options: it can make adjustments to outputs from the business units at the time of aggregation or it can ask front-office or business units to change the way they make certain calculations. The right choice depends on the nature of the discrepancy and the risk type.

Better front-office interfaces can drive success in Principle I-iv. If frontline staff can view and use risk information, their interest in and demand for accurate data will naturally increase. For example, if the connection between daily limits and front-line data is clear, traders would be strongly incentivized to ensure the accuracy of those limit calculations. The tighter the feedback loop, and the greater integration of risk data into frontline uses, the more effective these efforts will be.

Recently, some firms have gone a step further and tried to consolidate their data into a single data “warehouse,” with links to all their disparate systems and with data stored at a granular level for every trade. With such a single or “golden” source of data, applications then interact exclusively with it and not with other applications. When they need to use or manipulate data that have historically resided in other applications, they can now turn to the warehouse. This, of course, makes aggregation and consistency that much easier to achieve; moreover, the consolidated warehouse can help firms enforce a common data model.

This is an ongoing and complex task for many firms. Several firms are currently trying to consolidate data warehouses, as well as their counterparty reference models, while also aligning their key performance indicators (KPIs) for risk. Some firms have been very successful at implementing a consolidated data warehouse for particular risk types, such as credit (see sidebar). When they need to aggregate across risk types, they do so through more manual means, collecting risk information from each warehouse.

The Principles can be achieved without necessarily creating a single data warehouse. Some firms can create a common data model and then implement that model across several warehouses. For these firms, the focus is no longer on establishing a single “golden” source, but on building a robust data “fabric” to support the needs of different users (for example, the business, Risk, or Finance) for reference data. Some firms are pursuing a “metadata” repository, a kind of master data layer that allows users to navigate reference data effectively. Such solutions might be more pragmatic for some firms and reduce costs. Larger firms may decide that being able to consolidate quickly across several data warehouses is the right way to apply this Principle.

A globally consolidated view of credit risk at a large firm with international operations

One firm that participated in the deep-dive interviews has set up a globally consolidated data warehouse across the entire banking group for credit risk. It did this over a period of several years. This firm had the challenge of operating in numerous countries in several different regions around the world.

The data in the warehouse is accessible to thousands of employees and offers more than 100 different cuts and data views, typically available one day after data entry. To get to this, the firm created a standard data model with over 100 fields. This has been in place across the organization for many years, with both the front office and risk management understanding what the fields mean. For instance, each transaction or legal entity will have the same identifier, allowing front-office employees and risk managers to recognize their data input in analytics tools. As a result of these efforts, the firm says, no new fields have been added, and there has been no need to re-collect data.

While this foundation is already quite sound, the firm is doing further work to improve the system's capabilities; solid investment plans are in place.

- **Recommendation I-8.** Firms should realign roles, responsibilities, and incentives throughout the business system to improve data integrity.
- **Recommendation I-9.** Firms should consider the establishment of a dedicated team to manage risk data quality.

data fields; it does this by applying artificially conservative values to missing fields.

Some firms have established owners of every data domain, such as interest-rate-market risk data, ensuring a single point of accountability for all data-related issues.

Discussion of Recommendations I-8 and I-9

Fulfillment of the ideas entailed in these Recommendations will support all the Principles, especially Principles I-i, I-iv, and I-v. Roles and responsibilities need to be reconsidered throughout the risk system, in back-office and control functions, and especially in the front office. Many firms are increasing their focus on data quality and integrity at the source, by appropriately incentivizing front-office staff. One, for example, applies capital-usage penalties to business units that have too many missing

Another measure that firms are starting to explore is the creation of a dedicated function to manage data quality, either as part of the firm's Risk Management function or as the foundation of a cross-business-unit Risk team (see sidebar). A dedicated team manages routine data aggregation and also assures fulfillment of specific requests. Its tasks include ensuring the consistency of data from various risk systems on the same risk type (credit, for example), delivering comprehensive aggregated exposure reports for all risk types for each counterparty, producing regular reports on limits and exposures by subcategory (such as industry

and region), and performing monthly cross-checks with the firm's Finance group on limit and exposure data, taking any necessary steps to achieve consistency. For certain firms, this unit will need to work closely with front-office quantitative teams to align on methodologies across businesses.

Governance measures for higher data integrity at a large investment bank

In one interview, a large investment bank described the challenge of data consistency and its approach to tackling it. The firm is establishing a unit to take charge of risk-methodology standards. This unit will define and monitor requirements for all front-office analytics so that the risk methodology is aligned across businesses. While closely collaborating with front-office Risk teams, the unit reports to central Risk control.

A particular challenge has been to find the right set of skills: team members need subject-matter expertise on data usage while also being able to understand the capabilities of the underlying systems and navigate them well.

In addition to the new unit, other changes to the process are being implemented to ensure greater data integrity. For example, an end-to-end governance process will require traders to validate warehouse information. Other more infrastructure-related measures include the reduction of overlapping data streams (both external and internal).

- **Recommendation I-10.** Firms should define service-level agreements (SLAs) for report turnarounds.
- **Recommendation I-11.** Where appropriate, firms should analyze the trade-offs between accuracy and speed of risk

reporting and consider the use of speedy approximations rather than delayed reports of greater precision. Such approximations, as well as their merits and flaws, should be thoroughly understood and discussed with supervisors.

Discussion of Recommendations I-10 and I-11

Recommendation 10 is an important enabler of the other Recommendations in this Theme. An understanding of reporting and timing needs will help firms to define other Risk IT/Ops requirements.

Implementation of Principle I-vi will generally require specific protocols, such as standard cut-off times for aggregation, and the right balance of report frequencies and turnaround times. Firms should develop strong service-level agreements (SLAs) between business units and the Risk function and between the firm and its supervisors (as discussed in Theme V) about turnaround times. These SLAs could, for example, call for different response times based on the type of risk and the nature of the request (for example, routine versus bespoke). This would enable better prioritization when fulfilling requests.

For more on SLAs, see also Recommendation V-16.

In some instances, approximate rather than to-the-dollar numbers will more than meet the need. Such approximations are more readily producible in the form of ad hoc reports. While it is important to understand the limitations of such reports, there is no reason to let the perfect be the enemy of the good. Firms should exercise appropriate judgment to decide the degree of precision or approximation that is adequate for such reports.

Theme II: Front-to-back operating model

The survey, interviews, and working-group sessions revealed that integration of the Risk IT/Ops operating model, from the front office through analysis and reporting, could often be improved. An operating model is defined as the way firms coordinate processes and the flow of tasks and information between parts of the organization. The emphasis here is on risk-related processes—the operations part of Risk IT/Ops; the technology that facilitates these flows is also implicated to an extent. (Theme III focuses explicitly on technology.)

This Theme primarily discusses the “front-to-back” operating model, the flow of information and tasks between the front office and back office (and in some cases back again to the front office). It also seeks to shed light on the broader alignment of risk-related processes, especially the links between risk operations and Finance, and Risk IT/Ops planning and the firm’s strategic planning.

It is clear that the seamless design of these processes and flows, and their full alignment with the systems that support them, can help improve efficiency and also lower operational risk. When the operating model is so designed and aligned, with an end-to-end consistency, the quality and speed of management information and reporting are greatly helped, as is the efficacy of key risk processes such as limit management.

The absence of such alignment became visible during the crisis and demonstrated how much difference an aligned front-to-back operating model can make. Supervisors noted that during

the crisis, when firms were asked to produce reports on their top five exposures, misaligned processes and data flows meant that some firms took two weeks to respond—too long for the reports to still be valid, or to provide a basis for mitigation, or indeed for supervisors to analyze broader industry issues. Firms have begun to address these challenges, with some success. This Theme will discuss that success and what firms see as outstanding challenges, and provide Principles and Recommendations to suggest ways to further the industry’s progress.

CHALLENGES AND POTENTIAL AREAS FOR IMPROVEMENT

The survey, interviews, and working-group discussions revealed four challenges in the design and implementation of an efficient and integrated operating model.

Making greater use of end-to-end design principles

Not all risk-related processes are designed with an end-to-end perspective. In the survey, 64 percent of firms say that only “some critical processes are...designed and managed with an end-to-end perspective across the entire firm.” Firms with a local focus were particularly self-critical; 54 percent rated themselves below this level. Firms report that among the processes that are often not yet designed and managed end-to-end are counterparty risk management, early-warning routines, approvals, and new-product development. The result in many cases is duplication and inefficiency,

with business implications; more critically, in some cases, there are disruptions or outright breaches in processes and data flows that engender operational risk.

One prominent example is the early-warning process many firms use in counterparty risk management. At one firm in 2008, at the depth of the crisis, an early-warning trigger about a counterparty was not communicated in time to the clearing and settlement department. A material sum was sent by wire transfer to another firm, which went into default just hours later. A postmortem analysis showed that the problem would have been readily fixed with a stringently aligned end-to-end process and corresponding data flow.

One of the most important processes that at times suffers from a lack of end-to-end design is limit management—a core process for Risk, Risk IT/Ops, and the front office. Managing risk in trades and portfolios depends on a widely shared, agreed, and detailed understanding of the risk appetite, and the limits to risk that management and the board are prepared to assume. It is the limit-management system that communicates and enforces that understanding.

The majority of firms consider their limit-management process to be quite mature. In fact, 77 percent of firms think they are at or above the level of having a “consistent limit-management framework for some asset classes,” while 87 percent think they are at or above the level of having “escalation procedures defined” and “automated escalation procedures and triggers in place for most critical areas.” Spurred by both internal requirements and supervisory challenge, firms have worked hard over the last several years to achieve this maturity, by improving their limit-management frameworks and procedures.

Some firms, however, believe that their limit-management process is inconsistent across the enterprise; some say that their process lacks the capability to produce near-real-time and real-time reports on exposure and limit usage. Other firms report that some activities in the limit-management process are done manually, because front-office system interfaces are not fully automated.

Approvals processes are also not always sufficiently integrated. Some firms report having little transparency into the impact of potential transactions on the risk position of the portfolio. Some firms also thought that the Risk function did not participate in the approval process until quite late.

Manual data entries (as discussed in Theme I) are also a symptom of a lack of end-to-end process optimization. Firms use many disparate systems in front, middle, and back offices; because of the difficulty in communicating between these systems, manual handoffs are often made. These increase operational risk.

The challenge also extends into new product development. Product launches are not always coordinated across the business, Risk, and IT functions. Some business units may not fully account for the IT requirements of new products. At one firm, an asset-management business unit that was trying to aggressively expand into new areas found after launch, that its systems were not able to support that move.

Improving the alignment of Risk and Finance

Many firms think that the alignment of their Risk, Risk IT/Ops, and Finance processes could be improved. Forty-six percent of firms surveyed think they are not yet at the level where “most steps and interfaces between Risk and Finance are identified and defined

with clear ownership and responsibility.” Sixty-nine percent of firms with a local focus thought they were below this level.

Risk, Risk IT/Ops, and Finance have historically often acted independently when designing the information they require, and when collecting it. This leads to inefficiencies, and, worse, inconsistencies, especially where the firm uses different definitions for some concepts and quantities. In a working group session, one firm cited different definitions for “balance” within the firm. In a deep-dive interview, one firm described how Risk and Finance “do not even look at the same data.” The reality seems to be that at some firms, the operating model is not designed with that goal in mind.

As a result of unaligned processes and data across Risk and Finance, manual reconciliations between Risk and Finance are common. Especially prevalent are the often time-consuming ex-post reconciliations between financial accounts and risk reports. These are often done on the basis of irregular reviews of, and cross-checks between, the two system landscapes. Forty-one percent of firms thought they were below the level of having “most critical applications well aligned [with] some interfaces necessitating manual reconciliations.” Firms with a global reach were particularly concerned, with 56 percent believing they were below this level.

Integrating Risk IT/Ops with firm planning processes

An end-to-end alignment also means linking planning processes, in particular those of Risk IT/Ops and the firm’s strategic planning. In interviews, firms note that these are not always intimately connected, resulting in poor alignment of budgets, strategic priorities, change plans, and long-term road maps. Risk IT projects can be overwhelmed by other

IT projects, pushing them down the list of priorities and making it hard for firms to monitor their spending (and progress) in Risk IT/Ops.

A primary cause of these loose connections is the historical view, at some firms, of Risk IT/Ops as a mere support rather than a true partner and enabler of firm business.

Progress is being made, however. As firms report in interviews, with the size of investment currently being planned or undertaken in Risk IT/Ops and the strategic opportunities presented by these investments, attitudes are changing, with Risk IT/Ops beginning to be seen as a partner.

PRINCIPLES

To guide firms as they continue toward the target for industry sound practice, the Steering Committee on Implementation has identified, on the basis of the survey, interviews, and industry discussions, four Principles that can further promote the development of firms’ front-to-back operating model. These Principles should help improve the efficiency and accuracy of firms’ risk management, as supported by Risk IT/Ops, and reduce the operational risks that arise from process and data-flow disruptions.

These Principles, like the others in this Report, cannot be applied uniformly; currently there is a wide range of practices across the industry, with some firms being much more advanced than others. As noted, for example, the majority of firms think that their limit-management frameworks and procedures are at an advanced level, although even these firms also think there is room for improvement. Firms should view these Principles as guideposts as they continue their journey to the target state.

For each Principle, examples of application and illustrations of concepts are provided in the subsequent discussion.

Principle II-i. Risk-related processes should be designed and managed with an end-to-end perspective, and designed for enablement by Risk IT.

Principle II-ii. All risk-related processes should be aligned with the firm's risk appetite. Risk IT should facilitate the process of developing and enforcing the firm's risk appetite.

Discussion of Principle II-i and II-ii

At many firms, the Principles will apply to numerous processes within or affecting risk management and IT. Processes such as counterparty risk management, early-warning routines, approvals processes, limit management, and new-product development should likely all be designed and managed with an end-to-end perspective.

There are clear business, operational, and risk benefits that firms will derive from these Principles. Principle II-i will allow firms to make fewer manual interventions and handovers, and will lower their operational risk. The same Principle will also help firms to access more accurate and timely data and management information. Processes that have been aligned front-to-back are easier to "sync" with the global risk-appetite framework, the rationale for Principle II-ii; and that syncing will help ensure that decisions taken on all levels are consistent with the risk appetite. This will not only help management steer the firm in safe as well as troubled waters, but also further facilitate discussions between the firm and IT supervisors. Risk appetite is currently a high-profile concern of supervisors. To supplement past advice about risk appetite (see especially the CMBP Report and its Recommendations

I.9–I.14, which established the necessity of a well-managed and considered risk appetite statement), the Institute is publishing a report on risk appetite simultaneously with this Report.⁴

These Principles are highly relevant to firms of all sizes and in all locations. Implementation will vary, naturally; larger firms with many different business units and more trading desks may find it more difficult to improve key processes from end to end. And firms' needs will vary depending on their starting position. The 64 percent of firms that only have some processes aligned end-to-end agree that further improvements are realistic. Also, as should be evident, these are Principles that embody the idea of continuous improvement. Firms will need to revisit their processes periodically to ensure that, for example, changes to definitions and systems do not result in inefficiencies or inconsistencies between front and back office.

Principle II-iii. To the extent practical, Risk and Finance processes and data should be aligned for seamless transfers and consistency between the two groups.

Discussion of Principle II-iii

Greater harmonization between Risk and Finance is a goal for many firms; in interviews, firms spoke of the benefits to be gained, including the easier reconciliation of reports, and a more consistent and timely provision of data and information. This will help supervisors and management create a unified view of the firm that includes both risk-management and finance perspectives.

There are several prerequisites to the full implementation of this Principle, including a degree of data standardization and strong data governance including potentially a common

⁴ For more, see "Implementing robust risk appetite frameworks to strengthen financial institutions," www.iif.com.

data model, as discussed in Theme I. Even before such a model is adopted, Risk and Finance can agree on a common “language” on risk-related concepts. Implementing this Principle could take time for many firms. Most firms are, however, at least considering it, and some have already begun. The exact timeline to implementation will thus depend on firms’ current status.

Some more advanced firms expressed the intent to extend this Principle to include Treasury. Harmonizing with Treasury could have an added benefit. Better steering of the firm could lead to potentially lower capital requirements. Aligning processes among Risk, Finance, and Treasury will make it a more challenging task since issues of liquidity and funding would also need to be considered in data models and reports.

The limit-management system is so important that the SCI believes it should be identified as a particular interest in the broader context of improving risk-related processes generally. Many firms agree, saying they intend to reap the benefits of a better limit-management process. They state that they would like not only to meet regulatory requirements, but also to have greater confidence, through more precise and timely reports, that they are not taking on risks larger than they planned. An end-to-end alignment, linked to the risk appetite, will let firms understand how much of a given limit they have consumed; greater automation will help achieve that in near-real-time or real-time. As a result, firms will make better decisions about transactions to enter and deals to avoid.

While this Principle should apply to all firms, the extent of its application will vary. Greater automation (an outcome of Principle II-i) is particularly relevant to those firms with larger trading units; for others, it may not always be necessary. For example, for small retail banks,

automation of, say, the escalation of limit breaches may require too great an investment to be justified.

Principle II-iv. Firms’ strategic planning should have Risk IT/Ops (as well as IT more broadly) as an integral component.

Principle II-v. Risk IT should be a critical, independent category of information technology.

Discussion of Principle II-iv and II-v

Firms have several planning processes, including strategic planning at the group level, business unit planning, and firm IT planning. For most firms, as they invest more heavily in technology to enable better risk-management decisions, it will be increasingly important to ensure that this spending on Risk IT is considered in other planning processes. Not only has the size of spend increased, but Risk IT is taking an ever-greater role as an enabler of decision making for both Risk and front-office desks. This means that investments and resources for Risk IT need to be incorporated into business strategy planning.

The benefits of integrating the various planning processes are many. Business units will better understand the constraints and opportunities afforded by Risk IT. Businesses will also understand what it will take from IT to deliver their critical business requirements. The Risk IT/Ops group will become more of a peer to businesses; it will be able to advise on business possibilities from the standpoint of Risk IT. Risk IT/Ops will be able to stage and prioritize its investments across the business to meet group requirements.

Principle II-v, which carries both operational and organizational implications, will foster sustained prioritization of Risk IT projects and will focus the attention of senior firm and IT leaders on the needs of Risk IT. With that, the SCI believes

that firms will find it easier to deliver these increasingly complex projects in a timely fashion.

RECOMMENDATIONS

The SCl has established specific Recommendations that firms can use to advance the ideas embodied in the Principles. These Recommendations represent primarily changes to processes and will affect Risk IT/Ops, Finance, and Risk.

- **Recommendation II-1.** Firms should use joint teams from the relevant businesses and functions, including people from front, middle, and back offices, to design risk-related processes and data flows with an end-to-end perspective.
- **Recommendation II-2.** Firms should define clear ownership of end-to-end risk-related processes and indicators to help the owner manage the process and assess her performance.
- **Recommendation II-3.** Firms should establish ownership for the task of continually reviewing, redesigning, and implementing improvements in processes that will enhance their end-to-end consistency and efficiency.
- **Recommendation II-4.** Firms should consider the use of workflow-management tools in all relevant risk-related processes.
- **Recommendation II-5.** As firms realign risk-related processes, and particularly the limit management process, they should ensure that the new design is motivated by and closely connected to the firm's risk appetite.

Discussion of Recommendations II-1 to II-5

These Recommendations will help firms achieve Principles II-i and II-ii in particular. Several key processes should come under the scope of these Recommendations,

including counterparty risk management, limit management, collateral and netting management, early warning routines, monitoring, approvals, and new product launches. All should be designed with a clear end-to-end alignment in mind. As some firms rightly point out, end-to-end process design is not a goal only for internal processes; outsourced processes should also be submitted to redesign efforts.

Clear process ownership, accountability for continual end-to-end improvement, and new workflow-management tools are three necessary and complementary techniques firms should use to improve processes and information flows.

- Firms can analyze steps in processes and data flows, grouping similar activities, to determine genuine process ownership. They should then formalize this by charging owners with their redesign (where needed) and management, documenting the new processes, drafting performance management principles, and so on. In many instances, conducting this analysis and assigning ownership can mean a radical redesign of the whole process layout.
- Another important ingredient is establishing clear accountability for the continual improvement of processes, now and in the future. Firms have tackled this in different ways. Several firms talked about conducting comprehensive reviews and revisions of processes and structures, with the intent of assigning accountabilities for improvement of processes. Some have gone further and centralized the task of improving processes. At one European firm, a central operational unit has been established with the specific responsibility to design processes with an end-to-end view and to own the task of designing and implementing improvements to those processes in the future.

- A third component builds on the first two and therefore should likely be introduced later. Firms can make more use of workflow management systems. In such systems, firms can have all available data populated automatically, making handovers from one person to the next simple and clear. For example, in credit applications, many firms already have systems in which information about the applicant is displayed on the screen of the frontline seller. His first-stage approval then triggers a flow of the same information to the next person in the credit-approval process; the information also populates relevant screens of Risk controllers.

These workflow management tools can be extended to other risk processes (see sidebar 1). Such systems could help reduce the need for manual interventions and reduce the chances of errors creeping in along the chain. A prerequisite for making this a success is to have carefully designed the processes in an efficient end-to-end way before implementing this in IT (see sidebar 2).

Sidebar 1: Workflow management in Risk: An example

One firm has placed particular emphasis on making its Risk IT systems cover processes from end to end. For instance, a central workflow tool is used for all large corporate customer credit applications. The tool includes a database of corporate ratings and information on customer behavior supplied by the frontline seller; customer-relationship information, a pricing engine, contract-management functions, monitoring and review of the outstanding credit, and renewal processing. The tool maintains and updates all relevant information for several million companies. Most of the customer ratings are automatically updated every month in a batch process. Users get notified of these updates.

Frontline users input the basic data for the loan application. The application file is forwarded by the workflow tool to the responsible credit manager for approval. After approval the file is sent to securities valuation, legal, and loan administration, entirely in electronic form within the workflow system. Finally, the workflow tool automatically forwards data to the central customer database and to the local product systems (for uses such as limit updates).

Sidebar 2: Using technology to link process steps: An example

One firm has recognized a “disconnect” between the front office as it produced risk data and the Risk group monitoring it. Risk analysts perceived that the quality of data received from the front office was not adequate to produce the reliable risk reports required by management. As a result, the firm spent a large amount of time and effort on manual data adjustments and ex post reconciliations. However, after the adjustments, the front office did not recognize its data in the produced reports. Consequently, the front office felt little ownership in the outcome and only weakly supported measures to mitigate risks identified as excessive.

To bridge this disconnect, the firm invested heavily in technology to reduce manual interventions. In addition, the firm has developed an end-to-end governance framework; traders continue to provide all the feeds necessary for the risk-aggregation platform, but now also validate warehouse information and configure risk-calculation applications. This effectively eliminated Risk from the process and led to a much stronger sense in the front office of ownership and accountability for risk reporting and steering.

- **Recommendation II-6.** Firms should clearly define the essential characteristics of processes that involve both Risk and Finance.
- **Recommendation II-7.** Firms should consider the design of a consistent taxonomy and data model for both Risk and Finance.
- **Recommendation II-8.** Within the firm IT architecture, firms should manage applications for Risk and Finance coherently, seeking consistency wherever possible. In

the absence of an independent Risk IT/Ops unit, this should be a clearly established task within firm IT.

- **Recommendation II-9.** Risk and Finance should jointly design their reconciliation processes.

Discussion of Recommendations II-6–II-9

In interviews, working-group sessions, and in the survey, firms overwhelmingly wanted to improve the consistency between Risk and Finance, the object of Principle II-iii. Consistency requires both a greater coordination of Risk and Finance processes and the alignment of applications and data between Risk and Finance. Both of these are significant challenges for most firms because of the historically different ways Risk and Finance think about and use data for their reports, as discussed above.

Coordination between Risk and Finance processes requires a clear definition of ownership on either side of a defined interface, roles and responsibilities, service levels, and escalation mechanisms for process disruptions.

In most firms, Risk will likely own risk reporting and controls. Risk should also provide firm-wide standards on methodology. Finance will likely own balance-sheet and asset-liability management, and the firm’s performance-management process. For this split of responsibilities to work effectively, the groups must effectively and frequently interact. The groups should also conduct an annual planning session to address their joint requirements.

Alignment of applications and data is the more difficult challenge. It entails both organizational changes and changes to tools, systems, and underlying infrastructure. For example, many

firms have not yet founded an independent Risk IT/Ops unit, as discussed in Theme IV. At these firms, the IT unit that looks after Risk and Finance application development and maintenance (ADM) should, at a minimum, plan changes in a collaborative and coherent way and ensure change requests from Risk and Finance are integrated, to reduce inconsistencies or duplication.

Firms should also consider changes to tools, systems, and infrastructure. An aligned data model and taxonomy (as discussed in Theme I) would greatly reduce the amount of work required to reconcile Risk and Finance reports. This would also help firms automate data reconciliation. The required changes to tools, systems, and infrastructure might lead to a fundamental redesign of Risk IT applications and architecture. Some firms may also choose to go one step further by integrating Risk and Finance data warehouses, a topic discussed in Theme I. It should be noted, however, that this is not necessary to ensure consistency and harmonization.

Implementation of these Recommendations will not be easy and could take several years. Most firms suggest that reconciling the vast amounts of data and the numerous ways that the data are reported across the two units will take considerable time, recognizing as well the need not to destabilize vital systems and processes when making the requisite changes.

■ **Recommendation II-10.** Firms' enterprise-wide risk-limit management systems should in an automated way enforce local limits, monitor limit utilization and adherence, and trigger escalation procedures. Automation should be appropriate to the constitution of the firm's risk portfolio; firms with less volatile risks should ensure that their manual predeal simulations are as accurate as possible.

■ **Recommendation II-11.** Front-to-back escalation procedures should be clearly defined and embedded in Risk IT systems.

Discussion of Recommendations II-10 to II-11

These Recommendations apply in particular to Principles II-i and II-ii. While most firms report their limit-management practices are advanced, they also think there is room for improvement. In particular, they think that a more centralized limit management approach that "cascades" from the top of the house and the firm's risk appetite statement to the frontline would be a good end state. Such an approach needs to be supported by IT systems to ensure limits are obeyed and breaches escalated in a timely fashion.

Cascading limit-management frameworks should be based on a firm's risk appetite, with appropriate interpolation for the group, business unit, and desk levels. IT systems should be built with sufficient flexibility to cater to changing definitions of limits. In addition to enforcing risk appetite and limits from the top down, the systems should enable frontline business and Risk staff to request exceptions and escalations. Embedding these front-to-back information flows in the limit system greatly speeds the process and helps ensure that decisions are well-documented and in accordance with governance guidelines.

Automated systems should be a goal for most firms, but firms should evaluate whether it is necessary to have highly precise measurements of limit exposures in real time, predeal, or whether it may be equally effective and more efficient to allow some approximation in predeal reports, with slightly longer timelines for precise, detailed information. The complexity of simulations

varies between asset classes, making it difficult for firms to provide accurate and comprehensive aggregate views on limits in the required time. As described in Theme I, market risk limits are more complex and may need more frequent calculation than those for credit risk. Firms with greater concentrations of market risk may find the benefits of automation greater than those whose books consist mainly of credit risk.

Most firms, however, think that full granularity is not strictly necessary for appropriate limit management. In fact, to be able to take into account volatility, correlations, and “wrong way” risk, most firms prefer approximations to comprehensive simulations. (Moreover,

The limit framework as a core risk-management tool: An example

One firm interviewed uses its limit management framework as a key tool to manage financial-market volatility. The framework has 500 limits in place for wholesale credit, describing in detail what business units can do. The limits might, for instance, limit the amount of total commercial property lending or the volume of illiquid repo transactions with hedge-fund clients.

The limits are derived from the firm’s risk appetite, created in an approach the firm has used for nearly a decade. Limits are defined at the group, business unit, and desk levels. Besides central limits, business units also set their own limits for groups within the BU, based on the central allocation. Group Risk and Finance, in their budgeting process, determine the level of detail of limits, loss exposures, and the distribution of probability of default within portfolios. The board’s Risk committee reviews annually and also reviews any proposed deviation from the framework.

some firms also believe that a world in which most major firms rely on highly automated limit management systems may make them vulnerable to market shocks that trigger widespread limit breaches and consequent waves of position liquidation.) Firms should therefore work to provide good approximations of limit exposures predeal that will let them make confident decisions.

- **Recommendation II-12.** Firms should ensure that both enterprise- and business-level strategic-planning processes incorporate regular input from Risk and IT groups, and, where one exists, the Risk IT/Ops unit.
- **Recommendation II-13.** Risk IT should be a critical and independent category in firm IT’s planning.
- **Recommendation II-14.** In new-product development processes, firms should include in their due diligence an assessment from Risk IT/Ops of the ability to support the product from a Risk IT perspective.

Discussion of Recommendations II-12-II-14

These Recommendations suggest ways for firms to meet Principles II-iv and II-v. These Recommendations consider firm and business strategic-planning processes as well as other planning processes, such as new-product development, all of which should integrate a consideration of the implications from strategy for Risk IT/Ops. In every case, Risk, IT, and Risk IT/Ops personnel, where they exist, should be involved in the planning process.

To achieve this, firms should consider setting up a regular meeting schedule to bring together strategic and IT planners; these groups should be charged with unearthing critical dependencies between business

strategy and Risk or Risk IT strategy. A regular meeting will also help determine the appropriate allocation of resources to projects and help firms find the opportunities presented by new IT capabilities.

In the case of new product launches, Risk IT requirements should be considered in advance. This will ensure any system gaps are addressed before products go to market.

Theme III: Applications, architecture, and infrastructure

Risk IT/Ops is the union of Risk IT—the systems used to collect and store data and calculate, manage, and report on risk—with Ops—the comprehensive set of processes used to manage and steer risk that are the engine of financial risk management. This section focuses on Risk IT, which depends critically on three elements:

- Applications—the software programs that typically perform narrowly defined sets of functions
- Architecture—the construct in which the firm designs the relationships among applications, and the data they use and generate. The Risk IT architecture is a subset of the firm's larger IT architecture. Within the Risk IT architecture, we distinguish several "layers," including data, integration, results, and business intelligence
- Infrastructure—the hardware on which applications reside, the physical connections between components of this hardware, and services to support and maintain this equipment.

CHALLENGES AND POTENTIAL AREAS FOR IMPROVEMENT

Risk IT systems have come in for heavy criticism in the wake of the crisis. Regulators have found several potential areas for improvement. An important report from the SSG ("Observations on developments in risk appetite frameworks and IT infrastructure," December 23, 2010) cited four such: improving IT governance for strategic planning and decision making, automating risk-data aggregation capabilities, prioritizing the

integration of IT systems and platforms, and maintaining appropriate systems capacity.

Interviews with firms indicate that firms have continued to invest in remediating these and other problems in Risk IT, and that considerable progress has been made. As noted in Chapter 2, however, the survey revealed variations in practices across the industry. After standardization of data and risk aggregation, discussed in Theme I, Risk IT applications and architecture in particular were the areas most frequently cited by firms as needing improvement. The survey, interviews, and discussions highlighted five particular challenges:

- Widening the functional range of Risk IT systems (the number of business processes that risk systems cover and the range of activities that risk applications can perform)
- Resolving the fragmentation of the data layer in the Risk IT architecture
- Improving the flexibility and modularity of Risk IT architecture, especially in cases where postmerger integration has never been completed
- Maintaining infrastructure capacity—a lesser challenge than the others, but still important
- Managing the migration of applications, architecture, and infrastructure on the journey toward the target state

Widening the functional coverage of systems

Even without the impetus of regulatory pressure, many risk-management groups

in recent years have aspired to more comprehensive support of functionality by Risk IT systems, to replace the multitude of Excel workbooks and macros with which their firms have performed many tasks. With the more complex requests that regulators are now making, demands for more comprehensive and usable information from boards, and the demands of firms' top management for greater sophistication, firms are now pouring more resources into this development. In interviews, firms' main theme is closing their "white spaces"—the next round of gaps to be filled— either with new functionality or by significantly extending the abilities of current applications.

Of course, firms' starting points vary widely; some firms are already confident in the adequacy of their Risk IT systems' functional coverage. However, 84 percent expect major new demands in coming years that will have implications for their applications.

The three areas most often cited as needing coverage are some new (or substantially changed or newly important) risk indicators, such as Basel III's liquidity coverage ratio and net stable funding ratio, and indicators used to support recovery and resolution plans; simulations, including stress testing, back-testing, and predeal assessments; and the functional demands of new market structures.

- Basel III will require the monitoring of a number of new indicators beginning in 2012. Many of these will have significant implications for the functionality of Risk IT systems. Of these, liquidity-management indicators are probably the most important and will become part of standard regulatory reporting. Although the

requirements will be phased in gradually, eventually firms would, if the requirements are finalized as currently proposed, be required to maintain and report a minimum 30-day liquidity ratio to ensure short-term resilience, and a net stable funding ratio to ensure long-term liquidity. This requires new data-aggregation capabilities across the enterprise, new calculation engines, and new reporting capabilities in addition to the developments required to support generally improved liquidity-risk management and better internal pricing of liquidity. Another new Basel-driven indicator concerns counterparty credit risk, where firms will need to create new methodologies to calculate credit-valuation adjustments (CVAs) and other complex and sophisticated market-risk measures. Requirements from "Basel II.5," the updated framework on market risk, will include new calculations on stressed value at risk (VAR) and incremental risk charges.

Preparing for the introduction of these indicators is complicated by uncertainty about their final form. Important parts of Basel III, including the two liquidity ratios and the leverage ratio, are subject to revision after monitoring and observation periods. Basel II.5 is subject to revision after a "fundamental review" of market-risk requirements. Thus, a significant degree of uncertainty remains, and some developments done to meet interim reporting requirements may need to be revised once the authorities settle on final rules.

Other indicators firms are concerned about are those needed to support recovery and resolution plans (so-called living wills), which are becoming the bedrock foundation of supervision.⁵ These will place demands on Risk

⁵ For more, see a white paper co-authored by Davis Polk Wardwell LLP and McKinsey & Company, "Credible living wills: The first generation," April 25, 2011, www.davispolk.com.

IT/Ops and call on firms to understand their IT structures, which must be flexible enough to disaggregate in the event of a resolution.

- Simulations are the second area of concern. Firms already conduct an array of simulations and expect to do even more in the future. Yet 30 percent of firms in the survey believe that their IT cannot provide advanced analysis on demand for various simulation needs, including:
 - Scenario analyses, in which effects on P&L, liquidity, and business-level balance sheets are calculated according to a range of assumptions, typically statistical distributions or expert judgments. The goal is to create transparency on risk drivers and sensitivities.
 - Classical stress tests, in which the impact of specific stress scenarios on a company's capital, profitability, and liquidity is estimated. The goal is typically to understand the development and implications of specific triggers of financial crisis and assess the sufficiency of capital and liquidity to cover these events.
 - Reverse stress tests, in which the firm is assumed to be bankrupt or illiquid and scenarios are reverse-engineered that might have brought about these states. The goal is to develop an understanding of the nature and likelihood of potential crises.
 - Back tests, in which new models, products, trading strategies, and so on are supplied with historical data to assess how well they would have predicted actual outcomes.
 - Predeal simulation, in which the effects on exposure and other characteristics of a potential deal are calculated before the deal is concluded. Firms find this difficult for all but the simplest "plain vanilla" products. Simulation

software must have automated links to systems with the relevant data. Without such links, firms must resort to manual processing, with its attendant problems.

- New market structures are also putting demands on functional coverage. The Dodd-Frank Act and the new European Market Infrastructure regulation (Emir) mandate central clearing of certain derivatives and reporting of some over-the-counter (OTC) trades to electronic trade repositories. New regulation is also shifting some products to trading through centralized trading facilities. Risk IT systems will need to respond, to meet enhanced margin and collateral requirements, and support adequate risk management of exposures to bilateral counterparties and to the central counterparties (CCPs) themselves.

In addition to these specific changes, regulators across the globe are requiring more timely, more granular, and more frequent reporting of large amounts of data. Much of this is in the form of familiar microprudential requirements from firms' supervisors (a requirement that may be multiplied by the number of agencies and jurisdictions with which they deal). Additionally, data demands are expected to increase in coming years as the Group of 20's demand for more macroprudential oversight is translated into tangible requirements by the new authorities just now taking up and defining their tasks. Many of these requests can no longer be handled using manual models and ad hoc fixes and instead require a higher level of automation and greater functional coverage from applications.

The survey shows that many of these functionality gaps are already being filled or are well on their way to being filled. IT departments and external vendors at

many firms have begun to develop the new functionality, though the process will take some time. The SCI's working teams noted that much of the needed functionality has only recently become available in the market.

Other gaps will not be filled, however, until some methodological challenges are fully resolved, such as determining the influence of changing correlations in times of stress, or the treatment of wrong-way risk. These methodological challenges are greatest at investment-banking-oriented firms, which need to run numerous and varied simulations more frequently.

Resolving the fragmented data layer

As discussed in Theme I, most business units still hold their own data. That same fragmentation extends to the Risk IT architecture and especially the data layer. At many firms, applications originally defined and “owned” by individual businesses typically hold their own data. They may also copy and modify their data according to algorithms that are unique to each application. The result is data that are in many cases totally incompatible, residing in discrete and unconnected sources.

Even in the abstract, data under such conditions are likely to be incompatible. Typically, each system uses a unique data model—that is, it stores and works with data in unique ways. Even where data models are similar, they are not always aligned. With each system marching to a different drummer, the structure of the data, the applicable taxonomy, and the methods with which data are used and processed, differ from application to application.

This puts enormous strain on the links between applications. Links are commonly custom-made for each connection, with developers writing extensive code to make the data from the source application compatible with the application that draws from it. In some cases, especially where legacy systems are involved, some functionality is coded into the interface; data are processed and not merely transferred. This muddies the distinction between applications (which manipulate and calculate data) and interfaces (which transfer it). Firms then have to spend time and resources to analyze systematically the different data models used by applications; the interfaces, because they cannot be sure that the data definitions used by the source application are equal to the data definitions of the receiving application; and so on. In some cases, weak or missing documentation means that firms must spend even more time reverse-engineering data to understand how it is being used and transformed.

All this makes reconciliations quite challenging, and does so as well for the upgrade or replacement of applications. Flaws in the data layer make it harder to convert data into insightful information, and contribute to delays in the creation of risk reports. Point-to-point interfaces are a hindrance to risk aggregation, as discussed in Theme I, and to other activities carried out within the Risk IT architecture.

Increasing the flexibility and modularity of systems and architecture

Many firms' Risk IT architectures are dominated by legacy applications or systems—older programs that are typically custom-designed to support a narrow business activity. These applications have many strengths: they

do what they have been designed to do very well and are highly reliable. Because they are the basis on which firms, and indeed the financial system, run, they can only be changed with great caution and deliberation, and must not be destabilized.

But they may present problems. They are often not modular—that is, they are not easily divided into sections that can be readily upgraded, replaced, or reconnected to each other and to other applications. Legacy applications may be written in old programming languages that few IT developers now know, and have been amended over the years with dozens of bespoke upgrades. Finally, firms sometimes have few skilled resources for these systems. Legacy applications persist, however, because they perform basic functions well and because the costs and risks of replacement outweigh their disadvantages.

In the broader IT architecture, some of the same problems crop up. Like Risk, many businesses and functions rely on massive legacy applications. As noted, these applications are often unique, with little or no alignment between them. Firms' IT architectures are thus fragmented or siloed.

Finally, both the IT and the Risk IT architectures are often characterized by point-to-point interfaces—a sometimes bewildering array of connections from applications to their own data tables, reference data, and input systems; to other business support systems; and to the firm's core risk and financial systems.

Firms with a topology composed mainly of point-to-point interfaces face a problem: as more nodes (new systems, new connections) are added to the architecture, the number of point-to-point interfaces rises exponentially. The combination of point-to-point interfaces and legacy systems leads to redundancies

in applications, as each business despairs of the difficulty of using other applications and applets and builds its own. In a kind of vicious cycle, these duplicate applications become even harder to manage. In the survey, 38 percent of firms reported that they had not yet achieved the modest goal of an “integration layer implemented with limited scope, [and with a] high proportion of point-to-point interfaces.”

The problem is most acute in organizationally complex firms that have grown as a result of mergers and acquisitions and today have several business lines and business units. These firms typically have a fragmented architecture with a high number of interfaces and legacy applications. At its core, the accretion of legacy systems from M&A is often the result of political compromises made during these corporate events. Sometimes the acquirer's system is inferior but is allowed to continue. Sometimes firms agree to a “best of breed” approach; even when this succeeds and identifies the best applications, they do not often fit well together. A best systems/worst architecture paradigm can be the unintended result.

Enhancing the flexibility and performance of Risk IT infrastructure

While survey participants did not report large variances in the current state of their Risk IT infrastructure, several noted that increasing demands for risk modeling and reporting require planning to ensure sufficient computing capacity for risk applications. Only 23 percent of firms reported that they are managing computing power in a very flexible way, with dynamic allocation to user needs, and are covering peaks of utilization (from stress testing, for example). Fifty-six percent of firms reported

that while computing power is well managed, capacity for each application area is mostly fixed; as a result, shift or upgrade of capacity is typically possible only in special situations.

Less positively, working teams noted that the infrastructure available today may not be configured well for future business needs, especially if some applications considered noncritical today become so in the future, or vice versa.

A more flexible infrastructure might be most difficult to achieve for smaller firms that do not have the scale within which flexibility becomes possible. The greater the scale of the firm's infrastructure, the more feasible it is to allocate capacity dynamically as required.

As extensively discussed in this report, trends are putting greater demands on Risk IT infrastructure at present. One is the shift of some products to central counterparties, and a related requirement of reporting other OTC products to central trade repositories. Another is the expected alignment of settlement periods for various products. This will pose new challenges to internal processing power and external interfaces for these trades, possibly increasing the volume of transactions and information Risk IT systems must handle.

Finally, regulators are working on ensuring orderly resolution if a firm fails. These living wills, or recovery and resolution plans, are still under discussion. For purposes of this Report, it is important that a firm's Risk IT be adequate to support not only the analysis required for such plans and the requisite provision of information to supervisors but that Risk IT have the capability to allow such plans to be carried out expeditiously and

effectively if they ever need to be triggered. Requirements for recovery and resolution plans will certainly have large implications for the way data is stored and made accessible, and the way systems are designed. It will be in the interest of firms to develop systems that can be carried through a reorganization or resolution without compromising essential functions or contributing to systemic problems, among other things to avoid inappropriate and inefficient demands to "ring-fence" some activities during ordinary operations. Thus the infrastructure and the entire Risk IT architecture might need the flexibility to be split up, to accompany the pieces of the business as they may be reorganized or spun off in a resolution situation. The IIF published on May 9, 2011 an updated report on resolution issues entitled "Addressing priorities in cross-border resolution."⁶

Managing the migration

Many firms point out the difficulties involved in improving and replacing applications, architecture, and infrastructure. Firms find it especially difficult to replace critical systems; more often than not these are multiyear and highly complex projects. In interviews, several firms mentioned in particular the extraordinary time requirements, saying that five-to-ten year time frames are not implausible for major projects. Such project also require very significant resources from firm IT and the business, and pose substantial project-management challenges for firms and their IT departments.

Firms cite the difficulties involved in working on critical risk systems that are in use around the clock. Some have likened this to changing engines while the plane is flying: firms must

⁶ www.iif.com.

proceed in small steps with even more thorough testing than is typically done in application development done from scratch.

PRINCIPLES

To help firms respond to these challenges in applications, architecture, and infrastructure, the IIF has defined, on the basis of the survey findings, six Principles intended to help firms approach sound industry practice. Given the complexity and heterogeneity of firms' systems and the requirements of their business models, firms might apply these Principles in different ways, at different intensities, and probably at different speeds as well.

For example, a local or regional retail bank might already have an appropriate set of applications covering its needs now and for the foreseeable future, whereas a firm in the same jurisdiction with a significant investment banking franchise might have many white spaces to fill.

Principle III-i. Risk IT systems and applications should comprehensively cover all material regulatory and management requirements, recognizing that in the current environment and the foreseeable future, firms will have a broadened roster of fundamental risk requirements and simulation needs.

Discussion of Principle III-i

This Principle supports the firm's capability for the generation of enterprise-wide aggregation of risk across risk types. It should apply to credit and market risk, and should also support liquidity and capital management.

The crisis has in effect introduced a new set of broadly applicable KPIs (key performance indicators) that firms must meet generally. While the specific KPIs to which a particular firm must give priority will vary, as a general

matter, such KPIs include those introduced by Basel III, such as the liquidity coverage ratio (LCR), the net stable funding ratio (NSFR), and the incremental risk charge; and credit VAR and stressed VAR. (See Appendix 5 for an overview of these and other indicators that Risk IT/Ops must provide.)

In addition to such KPIs, the Principle implies that functional coverage should also include security applications to ensure fraud detection, monitoring, and reporting; similarly firms should have coverage that will adequately detect and report rogue or other suspicious activity.

As discussed in Theme I, it will be essential to increase substantially most firms' capabilities to produce enterprise-wide aggregation of risk information on a very timely basis. The Principle implies that the most material functions, those that would be most important to understand quickly in a crisis, and those that have systemic implications should be covered by automated systems and applications.

The Principle does not exclude, however, that manual interventions might sometimes be used, if the firm concludes that gains through automation would not compensate for the implementation effort. This might be the case for certain unique ad hoc reports and analyses, although firms need to anticipate where time-critical analysis needs might arise ad hoc; these would be less susceptible to manual response, and firms should plan accordingly.

As discussed in Theme V, firms and supervisors both need to consider that risks have different timing implications. Market risks are volatile and are more likely to require timely data and rapid turn-around of inquiries. Credit risks are less volatile and systems and procedures may reasonably be designed accordingly. In addition, as also noted in Theme V, approximate data may be sufficient for many purposes when a rapid

response is required, and it may be perfectly reasonable to make trade-offs between quick-response capability and delivery of fully granular information.

The appropriate level of automation will vary from firm to firm. For larger firms with significant wholesale operations, automation will probably be pervasive, and will extend to stress-testing and other simulations. It is likely that smaller, retail-focused firms may be able to manage adequately with more reliance on manual analysis, as their aggregation issues are likely to be less complex and a product focus on relatively simple types of credit risk is likely to make the delays that may result from manual procedures acceptable.

Principle III-ii. The Risk IT data layer must be defined with clarity, achieved primarily through consistent data models. Such models will allow the firm to identify and verify data sources and integrate both internal and external data quickly and smoothly.

Principle III-iii. Where possible the Risk IT architecture should employ an integration layer instead of point-to-point interfaces.

Discussion of Principles III-ii and III-iii

Well-defined data architecture is particularly important for large firms with several business units. Because such firms typically have several different data silos, it is important that they have an integration “layer”—that is, a part of the Risk IT architecture that can pull data from these areas. This layer would help remove point-to-point interfaces between all applications. With this foundational layer in place, other layers, such as the business intelligence layer, can be used to further build a firm’s decision-making capabilities. A well-designed integration layer could facilitate the movement toward

consolidated data warehouses, which will usually be a feature of improved “end state” systems.

The principal benefit of a well-designed data layer is more timely risk aggregation. Therefore, of course, the investment needed in this capability, and in data warehouses where indicated (see Recommendation I-7), will depend on the complexity and business model of the given firm.

As discussed in Theme I, a simple, retail bank may have much more modest needs under this Principle than a complex, wholesale bank. A practical way forward for a smaller bank, capable of achieving the purpose of the Principle, might be to align data models and taxonomies as well as data governance across the firm. Later it could, if necessary, start moving to more consolidated data warehousing, so-called golden sources of truth. With a consolidated data warehouse, monitoring access and controlling changes to data that is used in various applications is much easier.

Principle III-iii calls for the optimization of the integration layer. Firms should strive to limit the number of point-to-point interfaces, through the use of middleware.

Principle III-iv. The Risk IT architecture should be sufficiently flexible, and Risk IT applications and architecture sufficiently modular, to keep in step with the changing needs of supervision and the business.

Discussion of Principle III-iv

Flexibility is needed to cope with changing regulatory requirements, evolving management-information requirements, shifting product definitions, and other changes in the business, such as corporate events. For example, applications should be ready to support new market structures. The second requirement of

this Principle, modularity, is needed, for example, to ensure the ability to perform analyses separately for legal entities, functions, products (for example, to accommodate the needs of CCPs, say, or to support the requirements of recovery and resolution plans).

Due to the complexity of firms' architecture and the risks of modifying "live" systems, changes to add flexibility and modularity can take significant time. Smaller banks that rely more heavily on third-party applications might focus on reviewing their vendors' standards, reference data, and service-level agreements to ensure that the software is sufficiently adaptable. Firms that have built their own systems might focus on the ongoing application of clear architecture standards, and install middleware to make connections between systems simpler.

Legacy systems also need to be accommodated in the application of this Principle; time and care must be taken to avoid destabilizing operations or useful legacy systems while, at the same time introducing more flexibility and more aggregation capability. For firms with a significant legacy presence in their architecture, it may be more important to invest in improving the point-to-point interfaces that connect them, especially if these can be made more easily configurable if changes occur.

Principle III-v. Like the Risk IT architecture, the Risk IT infrastructure should be sufficiently flexible to allow the firm to react nimbly to structural changes in markets and methods.

Principle III-vi. The Risk IT infrastructure should contain sufficient computing power to meet all business and regulatory needs.

Discussion of Principles III-v and III-vi

Risk IT infrastructure should not become a bottleneck, even in times of stress. The infrastructure must be flexible to accommodate changes in the business system, such as the ongoing shift of activities to CCPs and multilateral trading facilities. And it must have sufficient reserves of capacity to accommodate Risk IT/Ops' core activities, as well as more complex goals such as dynamic resource management.

This Principle can be applied across all firms, though the required computing power will depend on the business model. Obviously, small firms with simpler business models and, for example, fewer volatile trading positions will not need as much infrastructural capacity as large firms.

The level of sophistication deployed in managing computer power will also vary, along with the degree of flexibility in the infrastructure. Some firms may choose to build central server "farms," or data centers, with the ability to dynamically allocate resources within these. Others may opt for resources closer to, and owned by, the business units. These choices require different levels of sophistication in the management of capacity. Data centers are more efficient than distributed arrangements; they manage capacity better through load balancing and more accurate capacity projections. Many firms have had success with virtualization of servers, which greatly expand capacity, and can only be done in data centers.

RECOMMENDATIONS

To continue the journey toward the target state, many firms said in interviews that they will need to make significant changes. These

improvements touch on all aspects of Risk IT, and cover everything from data collection through analysis and reporting. From interviews and working group sessions, it is clear that most banks have already committed to and started to make improvements, and that, indeed, many have progressed a long way toward achieving their goals.

- **Recommendation III-1.** Firms should analyze their Risk applications to determine gaps in their functional coverage, especially with respect to key indicators and simulation support for stress testing and other needs.
- **Recommendation III-2.** Firms should convene a dialogue across businesses, Risk, IT, and Risk IT/Ops on how to redesign the Risk IT architecture to fill the gaps.
- **Recommendation III-3.** Firms should consider establishing a single point of responsibility to oversee development of Risk applications.

Discussion of Recommendations III-1 to III-3

To expand the breadth and depth of applications' capabilities, the essence of Principle III-1, it is important for firms first to define their goals and regulatory requirements. Given the heterogeneity of business models, each firm will need to make its own assessment of the gaps in the functional range of its current risk applications—places, that is, where requirements (both regulatory and management, today and in the future) are not sufficiently covered. As financial firms return to prosperity, these Recommendations are essential to ensure that Risk IT needs are prioritized in the competition for scarce resources.

Capabilities that are becoming more important for many firms are new risk indicators, especially for liquidity management;⁷ and simulation support for scenario analysis, stress testing in all its forms, and pre-deal analysis, as discussed above. On the last point, Risk IT/Ops should integrate a new generation of front-office simulation tools. These can simulate the effect of a new product or a new deal on funding, liquidity, profitability, or the limit utilization. They can also simulate the effect of exogenous change in, say, the yield curve or credit spreads, on business P&Ls, products, and individual deals.

Because these new tools are designed to, among other tasks, measure and manage certain risks, their methodology, data model, taxonomy, and so on should be aligned with Risk standards, and they should be integrated with the Risk IT architecture. If not, firms are in danger of worsening any inconsistency in data models and methodologies from which they already suffer.

Once the firm has assessed its needs and current capabilities, it can turn to addressing any gaps. To that end, a dialogue between the business, Risk managers, the Risk IT organization, and software vendors, facilitated by the firm's IT management, is likely to be needed. Firm IT is the best convener of such a group, since it is neutral and has a profound understanding of what is possible and what is not. IT can help steer the dialogue toward ideas with maximum impact.

Risk and Risk IT, however, have equally critical roles to play, to make sure that the needs of Risk are given adequate priority, to meet the expectations of supervisors and boards,

⁷ The key performance indicators that most firms should consider include the liquidity coverage ratio (LCR), the net stable funding ratio (NSFR), the incremental risk charge, credit value at risk (VAR), and stressed VAR. See Appendix 5 for a full discussion.

fulfill the various regulatory and industry recommendations on Risk governance and risk management, and, crucially, to make sure that investment in Risk IT and support of Risk Management will be sustained given competing business demands for resources. Following those discussions, firms should design a long-term transformation plan.

Many firms have already started this journey, in various ways.

- Some firms report in interviews that they are improving their risk measurement applications, such as the algo credit suites that firms rely on to measure risks such as counterparty risk. Firms note that today many external vendors offer such technologies; the main effort now required is implementation.
 - Several firms are investing in applications that can more easily generate ad hoc reports. These have become standard practice in many firms' marketing and sales departments, to provide real-time business intelligence that does not require processing or interpretation by programming or analytical specialists. Risk departments appear ready to take the same step and are seeking quality vendors.
 - Efforts are under way at several firms to improve calculation engines and routines, in all risk types. One major firm is building a new firm-wide risk-aggregation engine and eliminating any noncompliant legacy tools, some of them introduced and owned by front-office traders.
 - Other firms are extending their capabilities for advanced stress testing and other simulations. VAR calculations, counterparty exposure, and probability of default (PD)/loss given default (LGD) calculations are also among the top simulation priorities of firms.
- Apart from the technical work and project management needed for these initiatives, firms should consider an organizational change. A single point of contact should be established in Risk IT with a mandate to manage demand and ensure architectural compliance for new development in Risk (and potentially Finance) applications. This structure will allow firms to more easily prioritize their application development. The duty might be handled well by a dedicated unit within IT responsible for Risk IT, an idea we discuss in Theme IV.
- **Recommendation III-4.** Firms should consider refreshing or redesigning their Risk IT architecture to exploit the benefits of a common data model and middleware.
 - **Recommendation III-5.** Firms' planning should, as much as possible, aim for all businesses to coalesce around a common data model.
 - **Recommendation III-6.** Firms should align their internal risk taxonomy among businesses and all Risk units.
 - **Recommendation III-7.** Firms should evaluate the benefits of a layered architectural layout—with data warehouse(s), calculation “engines,” and data integration (middleware), business intelligence/MIS, and reporting layers.
 - **Recommendation III-8.** Firms should, in particular, evaluate the benefits of consolidated data warehouses as consistent “golden” sources of data and proceed accordingly.
 - **Recommendation III-9.** For all manual reconciliations that in a firm's view consume substantial resources, the firm should construct a business case to analyze the advantages and costs of automating the reconciliation.

Discussion of Recommendations III-4 to III-9

To achieve Principle III-ii, firms must redesign their Risk IT data and integration layers. This work has several elements, including the alignment of internal risk-data taxonomies, the alignment of risk-data models, and the layering of the data architecture.

Risk-data taxonomies should be aligned across the firm. (Theme V explores how these taxonomies should also be aligned across the industry; here, our focus is on internal alignment.) Firms should clearly define their risk data, as described in detail in Theme I, and ensure consistency. This is a prerequisite for many different developments in Risk IT, including this one.

A consistent data model as described in Recommendation I-1 is the first step in moving to a superior risk-data architecture. Data models are descriptions of data structures. A common data model, with its reliance on consistent and precise data and database definitions, helps the firm integrate data from different businesses. With a common data model in place across databases and data warehouses, firms have much less need for the manual interventions that are used to make “apples-to-apples” comparisons.

Ideally, a layered data architecture should then be implemented. It should include:

- Consolidated data feeds, which provide information from both internal and external sources
- Consolidated data warehouses, as described in Recommendation I-7
- An integration layer, as described in Principle III-iii
- A results layer, which stores results of calculations produced by analytical engines

- A business intelligence/reporting layer, which runs reports using the data and results generated

The process of defining a layered data architecture might begin with a review of the ways that risk-relevant data are captured, processed, and transmitted among applications and then stored. This could inform changes required in the data architecture to remove inconsistencies and redundancies.

According to one firm, one of the major challenges it has faced from the outset of its effort to improve its data architecture is the uncertainty surrounding business and regulatory requirements for data storage and processes. The concept of living wills, for instance, could have a significant impact on data architecture and governance, by changing the way some types of data must be stored and the frequency with which they must be analyzed.

As discussed in Theme I, some firms are consolidating all the data for a given risk type into a single data warehouse; for example, one major firm is working on consolidating all its data for risk, finance, and compliance. The working groups believe this is beneficial but not necessary. In fact, as discussed in Theme I, not all firms need to fully consolidate their data in a single warehouse, or even a small number of warehouses. Identifying the data for each firm that critically require consolidation or separation is the most important task. For the selected data, a common data model can then be implemented across several warehouses, enabling fast aggregation.

Principle III-iii calls for the optimization of the integration layer. Robust yet flexible “middleware”—the software that connects front-office systems, where data are captured, with back-office systems, where data are

processed and aggregated—can help firms reduce the number of point-to-point interfaces. That in turn will help reduce or eliminate the need for manual aggregation that today often forces firms to use Excel workbooks or similar expedients.

One form of middleware that some firms are using is an enterprise architecture integration bus. This software provides a platform on which all applications can exchange data and even services. For example, a service such as “find customer” need only be designed once and implemented in one application; with middleware, it can then be used by other applications through a standardized call on the middleware. This modularization renders the architecture more flexible, making it easier to orchestrate data flows between applications, and to add, remove, or adjust applications and functionalities. Only the interactions and communication with the middleware need to be adjusted.

Several firms are already using various middleware technologies to optimize their architecture. The technology is considered mature, and several providers offer solutions. Most of the firms involved in large-scale IT transformation have taken the opportunity to move to modern middleware technology. Such transformations cannot readily be done without a migration of the middleware.

The working groups also described the integration layer in relation to the target Risk IT architecture, as discussed in the sidebar:

Finally, many firms are working to increase the level of automation to reduce reliance on manual processes and spreadsheets; indeed, the thread connecting many of the Principles and Recommendations in this Report is that a high-quality Risk IT/Ops paradigm will reduce or eliminate the need for manual processes

and spreadsheets. As firms progress toward that goal, however, such manual processes will continue. Recommendation III-9 suggests that firms should consider the benefits of automating, through custom programming, those manual processes that continue to consume inordinate resources.

As part of the calculation of benefits and costs, firms should include, as noted in Theme I, the difficulties that many firms experience in reporting risk exposure in real time and with great accuracy. Many firms are instead setting a goal of good approximations, with a conscious understanding of the implications of setting a lower bar for accuracy, trading off a degree of granularity for the benefits of timeliness. Every firm must establish a similar degree of clarity on its minimum requirements, which should be discussed with its supervisors.

Defining a target Risk IT architecture: What it might look like

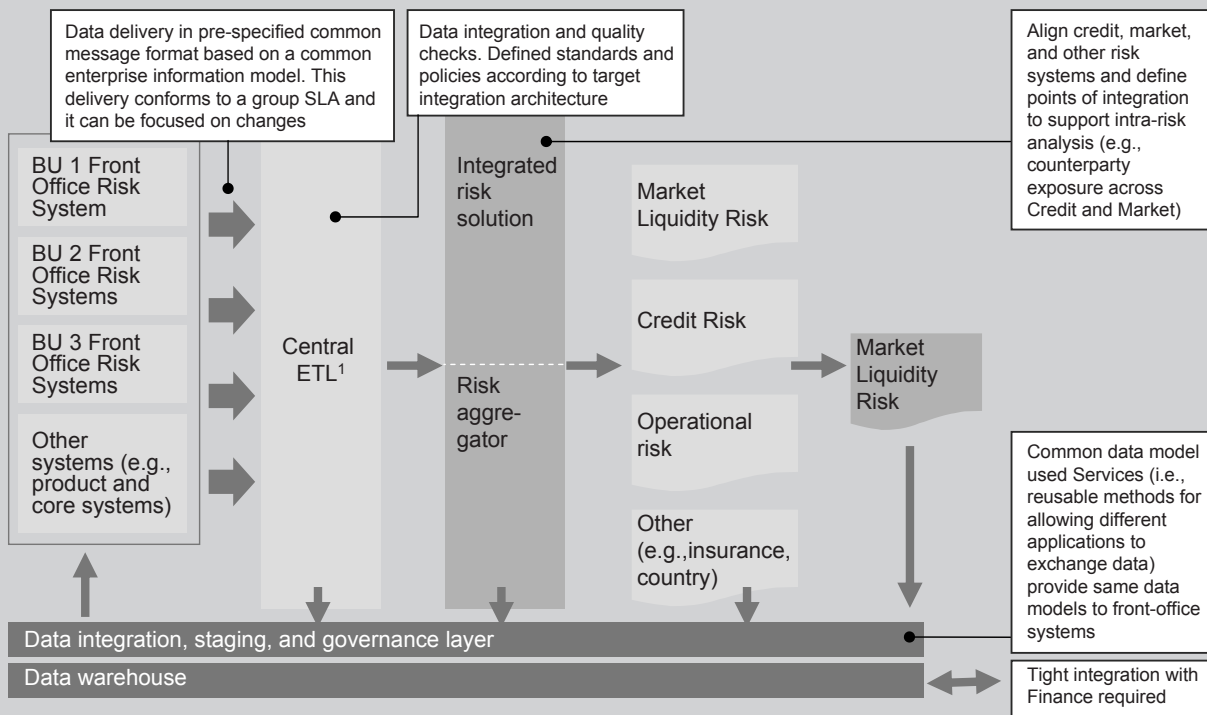
One firm has embarked on a transformation of its architecture. The effort started by establishing a common data model (Recommendation I-1) and designing a data-integration hub (Recommendation III-8). The objective was to reduce point-to-point connections and ensure that common data formats are implemented across product and core systems (Recommendation III-6). The firm is also standardizing risk applications across geographies, and it is reviewing the functionality of risk applications (for example, the adequacy of these applications to support stress testing) as outlined in Recommendation III-1.

The IIF working groups discussed in detail what a target Risk IT architecture could look like for other firms, in fulfillment primarily of Recommendation III-7 (Exhibit). Central elements include:

- A central extract, transform, and load (ETL) layer. The central ETL layer consolidates data from front-office risk and other systems that arrive in a pre-specified common message format. The ETL layer performs data integration and quality checks based on defined standards and policies.
- An integrated risk application layer with a risk-aggregation module. The integrated risk solution and the risk-aggregation module perform the calculations required for reporting on, say, a given risk type or a risk within a specific country. Credit, market, and other risk systems must have well-defined points of integration to support more complex analysis (for example, counterparty exposure across credit and market risk).
- A data integration, staging, and governance layer. This layer uses a common data model to consolidate data from different systems and hand over data to the appropriate data warehouses.

Exhibit

Most firms expect returns on their investments—especially better interactions with regulators



¹ Extract transform, and load

Source: IIF/McKinsey Risk IT/Ops interviews

- **Recommendation III-10.** Firms should develop a clear target layout of their Risk IT architecture. They should develop a manageable road map to reach this target layout, with clear intermediate milestones at which stand-alone impact will be achieved.
- **Recommendation III-11.** Within the Risk IT architecture, production and development environments should be separated.
- **Recommendation III-12.** Discrete risk functions should be provided, as much as possible, by single modules. Redundant functionality among modules should be eliminated, and modules and applications should be grouped by purpose.
- **Recommendation III-13.** Firms should establish clear architectural standards for the Risk IT architecture that will promote modular and flexible design.
- **Recommendation III-14.** Firms should establish clear technology standards for the Risk IT architecture that will promote modularity and flexibility.

Discussion of Recommendations III-10 to III-14

Some fundamental changes to the Risk IT architecture are required to increase flexibility and reduce turnaround times, for, say, adding or upgrading applications. These changes will help firms satisfy Principle III-i. There are several tangible ways that firms can make progress here. For example, within the architecture, firms should clearly separate production and development systems. Similarly a grouping of applications by their purpose can help firms identify and eliminate redundancies.

These firms are beginning by developing a clear target layout for the Risk IT architecture, which the working groups believe is the right first step. After that, firms should define standards for architecture design and standards for technology.

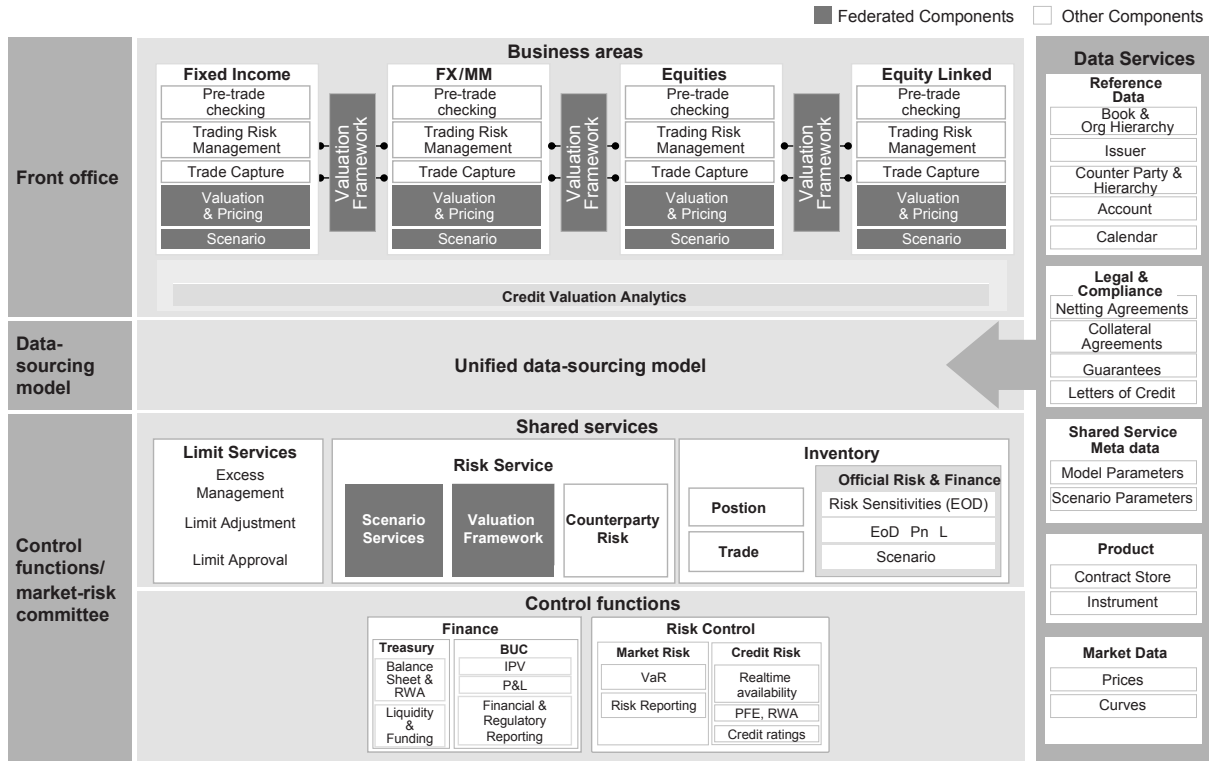
- First, firms will need to define their target Risk IT architecture and a long-term migration path to reach an appropriate degree of modularization and consolidation. In the target architecture, firms will want to ensure that functional domains are defined and their capabilities fully delineated. There should be one group of applications per domain, to avoid the redundancies that lead to inconsistent data and results. If redundancies are discovered, such as two or more applications within or across domains that perform essentially the same operation, firms should consider the creation of services. In this case, services are software modules that perform a defined operation (for example, “check a customer account balance”) that can be easily plugged into any application—current or in development—that needs to perform that operation.

One firm has made significant progress in redesigning its IT architecture (Exhibit 15). Front-office systems, business-unit control systems, and data sources are now separate. Within the front-office domain, each business has its own distinct system, and within those, clear distinctions are made among applications for pre-trade checking, trading risk management, trade capture, valuation and pricing, and scenario analysis. Risk-related tasks are centralized in a separate domain.

These are features of the target state that most firms can agree on today. Fundamentally, however, the end state will likely be a moving target; in fact it is not even an end state. Given continuous change in Risk IT requirements, there is no destination, only a journey.

The long-term migration path toward the target state should be broken down into manageable pieces, with intermediate checkpoints and clear, predefined deliverables. For each of these checkpoints IT should, along with Risk and

Exhibit 15
One firm redesigned its Risk IT architecture



Source: IIF/McKinsey Risk IT/Ops interviews

businesses, define the impact to be delivered. Doing this ensures that there is always a functioning intermediate point that delivers some value for the investments made up to that point.

- Second, firms should define clear standards for new architecture development; the standards should enforce modularity. For example, when applications are developed, IT architects should coordinate with business strategists to create modular designs from the outset.
- Third, firms should set standards for technology. This includes standards for programming languages, and should even cover such topics as the types of servers and database technologies used. Such detailed standards can then be used to

support higher degrees of standardization, making broader system changes easier. Some leading firms are looking at data-exchange standards that call for the system to deliver data in a prespecified common message format based on a common data model.

It should be noted, however, that some firms may choose to keep their legacy systems in any change of architecture. Firms should consider this especially for legacy systems that are, by definition, old and perhaps complex but may be performing well and are deeply embedded in the organization. Maintaining legacy systems should be done with eyes open, and investments made in a way to minimize any adverse effect on the firm's drive toward modularization. Should a firm decide to renew or replace a legacy system, the new software it designs or purchases should be sufficiently modular.

To manage architectural-design projects, firms should bear in mind a few guidelines. Well before launch, firms should seek a clear alignment on objectives, scope, functionality, and end products among all parties involved—businesses, Risk, Finance, IT, Risk IT/Ops. This alignment can be achieved through open and transparent discussions regarding trade-offs between functionality and design, on the one hand; and pragmatic solutions, cost-efficiency, and delivery time on the other.

During implementation, a program-management office (PMO) should be created. The PMO should have the capacity to contribute effectively to the development of solution content and to act as a sounding board and discussion partner for the leaders of the initiatives within the program. These skills are critical to keeping the project within scope. Firms often cite “mission creep” as a key risk factor that can expand budgets and timelines.

- **Recommendation III-15.** Firms should adopt a long-term perspective to plan Risk IT infrastructural capacity.
- **Recommendation III-16.** Firms should assess the requirements needed to provide Risk IT computing power as a service, including the provision of Risk IT computing capacity from an internal “cloud.”

Discussion of Recommendations III-15 and III-16

While supervisors have pointed to problems with computing capacity in the crisis, our survey indicates that most firms do not believe they have such a problem at present. In an interview, one firm cited the tens of thousands of servers to which the Risk group has access as proof of adequate capacity. However, firms believe they can do more to plan for needed capacity increases in the years ahead and manage their

usage more flexibly. Firms will need to view Risk IT as a critical business enabler and plan to provide the appropriate infrastructure.

Capacity planning therefore needs to have a longer-term perspective, in which firms factor in the increased requirements from, among other sources, Risk management—especially as more risk applications become mission-critical. A creative way of ensuring sufficient capacity is to provide “testing labs” to the business, in which the performance of new analytical models can be verified and checked with the hardware configuration that is planned for the production environment. Internal service-level agreements that explicitly state the information to be provided and the turnaround time within which it will be provided could make risk requirements more transparent and allow for more effective monitoring.

An ideal view would be to provide computing power as a service, which would be nearly as flexible in terms of capacity provided as power from the power outlet. Cloud-computing services are one measure firms are exploring. While most are familiar with these on-demand, dynamic, and measured services as offered by companies with excess computing capacity, they can also be provided by firms’ IT or Risk IT groups. Cloud services can include “infrastructure-as-a-service” offerings that provide basic computing and storage capacity for a broad range of Risk needs, and “software-as-a-service” offerings that provide fully developed applications in a standardized or metered manner. Cloud computing can greatly increase the scalability and flexibility of Risk IT, and can change the investment approach for adding additional capacity from “big step” capital investments to variable operating expenses. Users can pay for what they use, rather than for what they think might be needed, simplifying budgeting processes.

Cloud computing can also ensure that Risk IT will fulfill its role in the firm's business-continuity plans. In the event of a business or technical disruption, firms will need seamless rollovers and "warm" systems set to go live as necessary. Distributed IT deployment options (that is, cloud computing) can increase the speed and coverage of continuity delivery, by reducing the need for work on physical infrastructure. As more Risk IT applications are delivered in real time and incorporated into firms' commercial processes (for example, pricing) they must be treated as fail-proof assets, similar to transaction-processing systems.

Theme IV: Organization, governance, and security

Effective organization and good governance are essential to a high-performing Risk IT/Ops function. Investment in processes and systems is important, but it can be wasted if firms do not also have in place people with the right training who ask the right questions. To ensure that the actions described in the first three Themes, which will accomplish the technical work of advancing the firm toward the target state, are achieved, and that the gains are sustained over time, firms must also address their Risk IT organization and governance model. These must be sufficiently flexible to accept and empower the changes contemplated in data standardization, risk aggregation, operating models, applications, architecture, and infrastructure; at the same time, the organization and governance must be strong enough to ensure that the new ways of working are embedded in the firm.

The previous CMBP Report and the SCI Report dealt extensively with organization and governance of Risk. Those Reports provided guidelines to firms on establishing an organizational focus on Risk, the role of the chief risk officer and the Risk organization, and the resources needed for Risk. The present Report should be seen in a chain of continuity with the earlier Reports, especially with respect to issues of organization and governance.

Of all the thematic topics in this Report, firms believe that organization and governance, along with Risk IT security, are the most advanced, in part because of management and board attention in the wake of the financial crisis, and in part because of the stimulus of

supervisory dialogue and firms' pursuit of industry recommendations, such as those published by the IIF in 2008 and 2009. Firms perceive that progress has been substantial in the sense that the differences between the current and target states are smaller than in other areas discussed in this Report. Those differences do, however, merit discussion, and no firm can be complacent about organizational and governance issues that require constant attention if gains are to be maintained as better business conditions return. As before, the SCI has identified Principles and Recommendations that firms can draw on to help them achieve sound practice.

CHALLENGES AND POTENTIAL AREAS FOR IMPROVEMENT

Firms view the choice of organizational structure, a shortage of skilled staff, the growing complexity of Risk IT projects, the pace of change in regulatory requirements, and maintaining impregnable IT security as particular challenges.

Organizational structure and governance

Despite the overall perception that organization and governance of Risk IT/Ops have achieved new strength, many firms report that they have not yet achieved the strong, centralized responsibility that might be needed for the target state. For example, some firms report that they do not have a dedicated unit for Risk IT/Ops. Twenty-three percent of survey respondents believe they fall short of this description: "Risk IT is part of

the Risk department and leverages IT for most complex activities.” Eight percent think this description fits them exactly: “No dedicated team for Risk IT, relevant activities are assigned to IT department, no clear accountability.”

The implications of doing without a dedicated Risk IT/Ops team are everywhere. To take only one, obvious example, front-office teams may build their own tools, with little involvement from Risk IT, thereby continuing the fragmentation that has caused the Risk IT difficulties discussed in this Report and that most firms are trying to overcome. Firms believe that the Risk IT/Ops function needs strong central authority and responsibility, with (as discussed below) skilled people and superior delivery capabilities.

Similarly, firms see a need to address Risk IT/Ops more directly in their governance model. Just as the risk appetite and limits are applied at all levels of the organization and championed by a centralized Risk function, as recommended by the IIF in the CMBP report, so risk technologies and processes should be championed by Risk IT/Ops, which must be similarly incorporated into firm governance.

Broad mix of skills needed by Risk IT/Ops staff

Risk IT/Ops functions must have the appropriate skills to deliver the increasingly complex systems and applications that meet risk-management requirements, and the needs of the business. To be effective, Risk IT/Ops must possess both the control perspective of risk management and a business perspective to assure efficient but also effective integration of risk requirements into overall planning. To that must be added the ability to understand and articulate the constraints and opportunities posed by the firm’s IT infrastructure and ongoing development plans for it.

A common view in the working group sessions was that, because of the rapid developments over the last several years in both risk and financial businesses, firms have not always been able to find sufficient numbers of experienced people who can bridge the gap between IT and Risk. Another root cause of this issue is that at many firms, IT departments have historically been considered enablers rather than partners in developing the business; at these firms, the sharing of ideas and experience between IT and the business, and between both of them and the Risk department, has been sporadic. With firms’ current focus on producing reliable, repeatable, and timely views of risk, they can ill afford such a divide.

The extent of the challenge is not the same for all firms. Some firms have made substantial strides in building capabilities, especially since the crisis, and others make effective use of vendors or other external resources to deliver projects. But use of external resources only reduces the challenge without eliminating it; some firms report that it is difficult to manage third parties given their chronic shortage of in-house staff with the requisite mix of skills and, of course, issues of embedding and sustaining structures, systems, or applications built with extensive help from the outside may arise. The mix of inside and outside resources behind any project will require management attention to assure appropriate management and governance structures that can provide continuity beyond the development phase.

Complex project demands

Risk IT projects are often complex, requiring the involvement of not only Risk and IT but also senior management and the businesses. Complexity can deepen when there are several business lines and other functions involved. Project goals need to be aligned with different stakeholders, such as front-office managers, risk

managers, top management, and regulators. One firm, for instance, has initiated a large-scale risk transformation to develop a joint Risk and Finance warehouse and further improve its risk analytics. A considerable part of the overall effort went into communicating with the main stakeholders in Risk, Finance, and the business lines to achieve consensus on goals and the means to attain them.

The SSG noted in “Observations on Developments in Risk Appetite Frameworks and IT Infrastructure” that firms with strong project-management offices have tended to do better in ensuring that IT projects meet deadlines, because of the better co-ordination that results from effective use of a PMO. The SSG also noted the need for appropriate representation from Risk IT in important firm-wide projects. As noted above, special attention is required when substantial outside resources are used.

In working-group sessions, some firms held the belief that the problem of growing complexity is exacerbated because Risk IT projects may not always have the sponsorship of senior firm leaders. Other firms reported quite different experiences; in interviews, some firms stressed the successes of their current projects, which benefited from strong high-level support. This is consistent with prior IIF work on sound practices, which has stressed the importance for senior management, under the oversight of the board, to ensure that their firms’ risk-management function has a sufficient amount and quality of resources to fulfill its roles (which of course extends to necessary IT developments).⁸

Keeping pace with regulatory requirements

The increasing demands of regulation and the accelerating pace of change create more and more demands for accurate reporting and punctual information, to which firms must respond. While this issue is discussed at length in other Themes, notably Theme V, one part of the problem is organizational.

To respond to new requirements and regulators’ requests, especially ad hoc requests, firms must convene different parts of the business quickly to form action plans and responses. Sometimes firms must make do without some of the ideal participants, including Risk IT/Ops. While most firms think they do well on this, 24 percent of firms think they have not yet achieved this description of basic proficiency: “The Risk IT/Ops unit is sometimes involved in updates, meetings, and trainings on emerging regulation [with] no dedicated resources covering the topic.”

Maintaining IT security and auditability

Firms see a need to further improve their already strong IT security. While investments have been made in security for many years, and security is generally not mentioned as a problem related to the crisis, improvements are still required. Still, the overall high standards are reflected in the fact that just 11 percent of firms thought they had more than “some relevant IT security breaches in terms of number and severity.” Retail-heavy banks were more self-critical: 15 percent made that assessment.

⁸ For the IIF’s prior work on sound practices, see the CMBP report and the SCI report, and in particular Recommendation I.I, www.iif.com. For a review of the industry’s progress on implementing these Principles and Recommendations, see “Making strides in financial risk management,” a report co-authored by the IIF and Ernst & Young, April 2011, www.iif.com.

While security is already very strong, firms recognize that it must constantly evolve. In an interview, one firm noted that for IT security to avoid fraud, constant investment is needed, as fraudsters have shown a good ability to find weaker firms and exploit their security gaps. Some of these issues can be tackled with sophisticated IT that enables antifraud and antirogue activities, as discussed in Theme III.

PRINCIPLES

In describing target-industry sound practices, the Steering Committee has identified, on the basis of the survey and industry discussions, four Principles of Risk IT organization, governance, and security. These Principles, when fully incorporated into firms' Risk IT implementation, will enable the improvements described in Themes I, II, and III to become embedded, and for the associated gains that firms envision to be fully realized. These Principles augment the related Principles and Recommendations published by the IIF in 2008 in the CMBP Report, as updated in 2009 in the SCI Report.

These Principles, like those in previous Themes, need not be applied uniformly to all firms, as there is a wide range of sound organizational structures, governance models, and related processes across the industry. As noted, a preponderance of firms believes their IT organization and governance are well advanced toward their target state. Firms should view these Principles as guideposts as they progress toward that end state. The present Principles, plus those published earlier, make clear that constant effort and vigilance are required to assure the high-quality IT necessary to support and sustain over the entire business cycle the high-quality risk management that the IIF's prior Principles and Recommendations aim to foster.

We present below the Principles and the more detailed Recommendations and describe

actions that might be taken to implement them. In the discussions of each, we will illustrate differences in application by providing examples.

Principle IV-i. A high-performing Risk IT/Ops function should be concentrated to the extent possible in a dedicated organizational unit.

Principle IV-ii. For the Risk IT/Ops group to be most effective, its staff must possess—in depth—four kinds of skills and knowledge: business, risk, technology, and project management.

Principle IV-iii. Highly specialized skills and critical knowledge should be developed and kept in-house; only noncritical activities should be outsourced.

Discussion of Principles IV-i to IV-iii

Recommendations III-13 and III-14 call on firms to design and enforce consistent standards in architectural design and technology. These standards must be supported by a strong central organization, the essence of Principle IV-i.

The application of this Principle will depend on the nature of the firm and the Risk IT operating model. For many larger firms with complex needs, this will mean a strong centralized Risk IT/Ops unit and the active involvement of top management. At other firms, it may be appropriate to have smaller teams of Risk IT/Ops specialists residing in business-specific Risk groups (that is, a group that supervises retail banking's risks). With the latter distributed arrangement, firms must also include a small Risk IT/Ops unit at the center to help the function manage the many challenges of fragmentation. In all cases, the active support of senior management and the board will be required, consistent with prior IIF Principles on risk management.

In support of Principle IV-ii, Risk IT/Ops professionals must master several forms of knowledge: risk and its management, certainly; technology and its limits; and also a strong understanding of the financial businesses in which risk is engendered. Less well understood is the need for self-knowledge among Risk IT/Ops professionals: they must understand the firm's need for them to be consultants or advisers to the business and the Risk group. They must have the confidence to reach out and speak up, and the technical knowledge and gravitas to command respect. In the view of many firms, Risk IT/Ops professionals would be well served to move past utopian thinking about ideal systems and instead help the firm understand the cost-benefit trade-offs in Risk IT/Ops, and find the firm's ideal point on those trade-offs. At the same time, they must support the strengthened role of the CRO and the Risk function that have been achieved since the crisis. The IIF established eight Recommendations on this in its 2009 report; the industry has made substantial progress on these Recommendations since that time.⁹

The application of Principle IV-ii and IV-iii will also depend to some extent on the firm's current circumstances, including its size. Larger firms may find it more practical to develop the desired range of knowledge. Smaller firms might take longer to inculcate Risk IT/Ops staff with the various forms of expertise, and might rely more on external resources to fill in gaps in expertise.

Given the complexity of the function, many firms have appropriately shifted a number of Risk IT/Ops activities out of the firm. As they do this, firms should be mindful of some of the guidelines associated with Principle IV-iii. Keeping critical capabilities in-house (see a

suggested list of core Risk IT/Ops activities in the discussion of Recommendation IV-2) helps the firm develop an independent view of potential solutions to Risk IT needs. The greater the knowledge within the firm, the easier it is to manage outsourced capabilities effectively. And keeping capabilities in-house provides significantly more flexibility to expand the function quickly in the event of regulatory changes or increased business needs. Finally, firms that rely more heavily on outsourcing more may require specialists to manage vendors and consultants.

Principle IV-iv. Strong, integrated project-delivery capabilities are fundamental to the success of cross-functional, cross-business initiatives, and are required for many Risk IT projects.

Discussion of Principles IV-iv

Strong project-management capabilities are an important element of sound practice. Risk IT/Ops professionals must know how to set up project structures along with business and Risk; develop realistic deadlines; manage the scope and budget of projects; and consistently deliver impact. The same SSG report that highlighted the importance of these capabilities mentioned that one firm that delivered its projects particularly well had a single point of accountability. The Principle is particularly relevant to firms that have recently merged or acquired others, where different, complex systems may need to be merged quickly to extract the synergies expected in such deals.

Adherence to this Principle should allow firms of all sizes to deliver their Risk IT projects in a timely manner. It should also provide boards and supervisors with the assurance of a project

⁹ See Recommendations I.15–I.22 in the CMBP Report, www.iif.com. For a review of progress since 2009, see pp. 13–14 in “Making strides in financial risk management,” a report co-authored by the IIF and Ernst & Young, April 2011, www.iif.com.

delivery that includes adequate provision for present and future risk requirements. This is especially important since many firms have reported greater regulatory scrutiny of their Risk IT project planning. In one interview, for example, a firm mentioned extensive discussions with regulators of its plans to implement Risk IT initiatives such as the consolidation of its data warehouses.

Principle IV-v. Anticipation of regulatory change can only benefit firms. Preplanning can help firms react quickly and thoughtfully to regulatory change.

Discussion of Principles IV-v

The survey results showed that firms that believe they work closely with supervisors expect less negative impact from regulation on their business. Better preparedness for regulatory change, in both the flexibility and modularity of Risk IT, as discussed in Theme III, and in the organization will help firms adjust more quickly to change when it happens, and, to the extent possible, to anticipate regulatory trends.

To achieve this organizational preparedness, firms want to improve their “reaction times” to new rules. In one interview, a firm said that its reaction to substantial regulatory change takes as long as a year to formulate. Faster response times could lead to improved interactions with supervisors (a topic discussed at length in Theme V). This could also lead to a greater ability to inform the way new regulations are applied. More fruitful consultation processes between regulators and industry could result.

It is clear from the post-crisis regulatory environment, the observations of the SSG, and the discussions of the SCl that firms must aspire to know well in advance about every development in regulation that affects them and their peers. They should have a process to analyze new proposals from a technical

as well as a policy point of view. While it is important to participate in industry debates and official-sector consultations on developing regulations, it is equally important to devote the resources needed to be ready for timely implementation (including assessment of Risk IT/Ops requirements), making allowances for areas of uncertainty. While the industry will continue to ask the official sector to provide adequate lead times on implementing new regulation, it must be recognized that there will always be a degree of uncertainty about future regulations or supervisory requirements, and this awareness must be built into the process.

Principle IV-vi. Risk IT security must remain vigilant, both for business reasons and because vigilance is a foundation of public confidence in the industry.

Principle IV-vii. Firms should ensure that changes to Risk IT/Ops, and in particular to its systems and methodologies, are auditable.

Discussion of Principles IV-vi and IV-vii

The industry clearly understands the need to keep the number of IT security breaches to the barest minimum, and to ensure the protection of data. Firms in many parts of the world described how regulators are now very interested in this issue, reflecting legal data-security requirements, the increasing importance of privacy concerns to customers, and concerns about avoiding the financial and reputational damage of major security problems. IT security is essential to confidence in the system, as well as to the health of each institution.

“Back-traceable” changes (that is, changes made in systems that record the date, time, and author of inputs, edits, and other alterations) and detailed change logs are important to

ensuring that operational risks associated with Risk and other IT projects are limited. It is therefore important for firms to decide on an appropriate process for system changes.

Only if firms can precisely back-trace their changes to Risk IT systems can they ensure high security. The benefits of such auditability are better interactions with and higher confidence from the regulators and internal auditors; stronger security, including fewer losses to fraud or rogue behavior; and a minimized risk of so-called tail losses. While auditability is important to any IT process, it is especially important for Risk IT, because Risk IT/Ops is in effect monitoring itself. Most of the time, Risk IT/Ops serves as a guardian to the rest of the firm. Here, it must guard itself; strong auditability is essential for that purpose.

RECOMMENDATIONS

The IIF working groups on Risk IT/Ops have established several specific Recommendations that firms can use to implement these Principles. These Recommendations represent change to organization and governance, with some additional change to Risk IT/Ops processes.

- **Recommendation IV-1.** Firms should consider establishing a dedicated Risk IT/Ops group with clear responsibilities, or take measures to assure that the functions that would fall to such a dedicated group in accordance with the Principles and Recommendations of this Report are adequately covered.
- **Recommendation IV-2.** Firms should cultivate the appropriate mix of technical, content, and process-management skills in the Risk IT/Ops group.
- **Recommendation IV-3.** Firms should invest in the appropriate management of vendors of Risk IT/Ops products and

services, reduce their dependency on any one vendor, and take steps to improve the speed with which third-party contractors deliver services.

Discussion of Recommendations IV-1 to IV-3

There are three important reasons to consider establishing a dedicated Risk IT team, in support of Principles IV-i and IV-ii. First, such a team is needed to conquer the many challenges of fragmentation—in data models, Risk IT architecture, and so on—discussed in Themes I and III. The core work of a central team is to break down the silos that pervade and distort Risk IT and Operations. Such a team can be established in different ways, as discussed below. Even if a firm concludes that a separate Risk IT team is not appropriate given its overall structure, the functions of such a team as discussed in this section should be adequately covered. The support of top management, including the CRO and CIO, is essential to fulfill this objective.

Second, such a team can act as a center of excellence that can interface between Risk and Risk IT functions (and Finance, at more complex firms), provide the advocacy necessary to launch and sustain important Risk IT projects, and manage some of the complex projects that take place at the intersection of these functions' responsibilities. The team should be made up of experts in the Risk IT/Ops domain, and able to "speak the languages" of both Risk and IT. This is aligned with one of the main messages of the SSG's December 2010 report, that firms should develop greater capacity to deliver important Risk IT projects. Third, a dedicated team can help firms expand Risk IT quickly if changes to business requirements or regulations occur. This is generally only possible if critical capabilities and knowledge are kept in-house.

A dedicated Risk IT/Ops team is clearly highly desirable at larger firms, and also at many smaller firms. It is possible that smaller firms will find the cost/benefit balance of such a team unpalatable and decide to rely instead on strong vendors, with well-defined SLAs and strong internal oversight and management. No matter how great or small their reliance on third-party providers, firms should ensure that they do not become overly reliant on any one vendor, whose failure to deliver could jeopardize Risk IT/Ops' mission. A multivendor model will be better for most firms. And in their contracts with vendors, firms should pay special attention to the time frame within which vendors must fix software bugs and similar problems, ensuring that such time is as short as possible, and that penalties for exceeding this time are appropriately severe.

A dedicated Risk IT/Ops group should be granted a high degree of independence, in line with Recommendations I.16 and I.17 of the CMBP report. Recommendation I.16 states that the "CRO should have a sufficient degree of autonomy" and "be independent of line business management." Risk IT/Ops should share in that independence, especially if, as discussed below, it is housed within the Risk organization.

There are several different ways to position the Risk IT/Ops unit within the organization. Firms should choose the one that fits their purpose and current starting point. Below are notional models that could be considered, and the advantages and disadvantages of each; see the sidebar for examples.

- **Risk IT/Ops within Risk.** Inclusion in the Risk function will typically result in a better understanding of that group and its needs. Such a construct could result in a better understanding of the business, as in most cases the Risk group has more expert
- **Risk IT/Ops within IT.** Placing the Risk IT/Ops unit within the corporate IT group would naturally result in a greater understanding of the larger IT architecture, and a strong alignment with the IT governance model. Oversight by the IT group would also ensure that feasibility and system capabilities, now and in the future, are taken fully into account in Risk IT decisions.
- **Hybrid.** A hybrid approach, in which some parts of Risk IT are located within Risk and others in IT, is also a possibility.

While this configuration is perfectly plausible, it should be noted that, broadly speaking, firms that use it will probably find it more difficult to secure the desired level of specialized risk skills, and, more problematically, the essential prioritization of risk issues and projects. In a working-group session, one firm observed that prioritization of risk and compliance requirements might be more difficult if the business case is uncertain or poorly understood. In addition, placing Risk IT/Ops within IT would raise issues of assuring the continuity of attaching a high priority to risk issues, given competing demands for resources, even if, in principle, senior management and the board fully support appropriate prioritization of Risk.

One firm keeps most of its Risk IT/Ops within firm IT. In Risk, it has a special, highly skilled “SWAT” team that takes care of Risk’s mission-critical applications and databases. However, this team often moves forward with a custom approach to problems and may lose track of central standards, architecture, and so on. Quite often the rest of the Risk IT/Ops group, isolated from the SWAT team, finds out about these developments only after the fact. This may create a problem that is the opposite of the risk challenge discussed in the prior section: the SWAT team may give (appropriately) high priority to critical projects but lose benefits of integration or coherent planning.

To correct this, the firm is taking steps. The organizational structure remains the same,

but the reporting lines have been clarified. The firm is insisting that the SWAT team knows its core activity well, by emphasizing the direct report to IT. The SWAT team now has an additional, dotted-line report to Risk to help it better integrate with that group and facilitate its daily work.

Recommendation IV-iii calls for firms to ensure that external suppliers are well managed. As a first step, firms should consider the right activities to entrust to third parties. Core activities that most firms might conclude should not be outsourced are listed in the discussion of Recommendation IV-4. The activities that many firms, in the interest of efficiency gains, might find appropriate to outsource include maintaining noncritical applications, supporting implementation, and time and budget controlling for projects. As

Dedicated Risk IT units

In interviews and working sessions, it became apparent that dedicated Risk IT units can take many different forms. Examples of all three of the approaches described above were evident at the firms interviewed.

One firm has several Risk IT teams (supporting retail banking, wholesale banking, and so on), all housed with the business they support. These teams report to the global CIO and are supported by a global information-security department. The firm is moving its governance toward a global IT structure consolidating architecture, processes, people management, and technology.

Another firm has a relatively small, independent Risk IT unit that closely collaborates with both the Risk and IT departments. The unit reports to the IT group; a dedicated steering committee includes the CRO and CFO. The firm has found that its “current structure works well.” The next step this firm plans to take is to give Risk IT a greater role in data governance.

In a third example, one firm is considering a hybrid model with a dedicated Market Risk IT team reporting to Risk, and a larger Credit and Operational Risk IT team reporting to IT.

This firm has also set a requirement for Risk IT staff to have specific Risk and IT experience. With this structure, the firm is trying to achieve “stronger IT/business interaction in project definition and constant feedback to achieve quickly the best solutions.” Whenever possible, the firm is trying to ensure that “project management [is not] IT-only or business-only. There should be project management with mixed skills, possibly specific to Risk (but not specific to finance or trading—because Risk is Risk).”

noted, firms might need to develop additional resources to specialize in the management of third-party providers. Firms can also draw on a range of techniques to ensure that external providers deliver the promised services, efficiency gains are captured, and execution risks are shared appropriately.

- **Recommendation IV-4.** Firms should dedicate staff to manage critical Risk and Finance IT applications and infrastructure. The staff should develop the kind of deep knowledge that is essential for getting high performance out of applications and infrastructure. Use of such specialists will provide a better result than asking Risk IT generalists to look after such critical systems.
- **Recommendation IV-5.** Firms should invest in capturing and codifying Risk IT/Ops knowledge to ensure that the group's expertise and know-how can be shared today, to generate efficiencies, and tomorrow, to ensure continuity.
- **Recommendation IV-6.** Firms should conduct regular joint meetings, across business, Risk, IT, and Risk IT/Ops, at both strategic and operational levels. Such meetings should be conducted at a sufficient level of detail to allow attendees to engage in and contribute to the thought processes of other groups.
- **Recommendation IV-7.** Firms should establish training and rotational programs to ensure Risk IT/Ops staff have sufficient understanding of Risk and business issues, and similarly to ensure that business and Risk staff develop a sufficient understanding of IT.
- **Recommendation IV-8.** Firms should consider hybrid career paths, with time spent in Risk, business, and IT. Such hybrid career paths can be thought of as a kind of

permanent rotational program.

- **Recommendation IV-9.** The CIO and CRO should jointly sponsor and actively lead major Risk IT/Ops projects within the context of the firm's Risk IT/Ops governance model, and provide active and engaged leadership for their planning and execution.
- **Recommendation IV-10.** Firms should work to create shared accountability with specified responsibilities for the design and delivery of major Risk IT projects among Risk, IT, and Risk IT/Ops.

Discussion of Recommendations IV-4 through IV-10

To deliver projects efficiently, on time, and at a high level of proficiency, as expressed in Principles IV-i and IV-ii, firms should take two steps. First, they need to embed the commitment to continuing investment in the development of Risk IT capabilities in a sustainable way, with sufficient priority to be maintained despite competing demands of businesses, especially as business opportunities increase with recovery from the crisis. Second, firms should also ensure sponsorship from senior executives for major Risk IT projects, as expressed in Principle I.4 of the IIF's 2008 report.

The dedicated Risk IT unit, as established in Recommendation IV-A, must possess several forms of knowledge: a sufficient understanding of Risk, and of IT, especially the relationship between the Risk IT architecture and the larger firm IT architecture; knowledge of financial businesses and their challenges; and the know-how needed to manage vendors. The unit should also have strong project-management capabilities. It must understand and internalize the firm's risk strategy and risk appetite.¹⁰

¹⁰ For more see Appendix 2 of the SCI report, which contains an IIF paper on risk appetite; and "Implementing robust risk appetite frameworks to strengthen financial institutions," www.iif.com.

Above all, it must be well integrated into, and a positive contributor to, the firm's risk culture.¹¹

Not every professional must possess every skill. Certainly everyone will need a fundamental mastery of both risk and IT. Beyond that, professionals can develop specialties, for example, in project management, vendor management, and so on. Such specialties should be wedded to the firm's professional-development approach and developed as distinct career tracks.

Recommendations IV-4 through IV-7 will provide firms with essential vehicles for building "content" capabilities in Risk and IT. Several firms already use one or more of these ideas. One firm has a noteworthy training program: it intensively trains its Risk IT professionals on both Risk and IT through a program in which Risk IT specialists rotate through these areas.

The best way for firms to develop the second required set of skills, in project delivery, is, first and most obviously, to manage projects well, and second, to ensure that there is a good apprenticeship for future project managers within the current projects. This requires on-the-job coaching to help groom the next generation of talent in project delivery. It also requires senior-management commitment to long-term development and sustained commitment over time and across the business cycle.

With the full set of content and delivery skills, the Risk IT unit might conduct the following activities:

- Ensure that service levels for turnaround times, prioritization, execution, and so on, as established in SLAs with Risk, are fulfilled. (For more on these SLAs, see Recommendations I-11 and III-16).

- Facilitate regular interactions between business, Risk, supervisors, and IT.
- Define the target risk architecture and ensure that new projects adhere to architectural principles.
- Gather and develop functional requirements for Risk IT systems and prioritize change needs.
- Oversee third-party risk-application development and maintenance (ADM); manage vendors to ensure sufficient flexibility, in fulfillment of Principle IV-iii.
- Lead the program-management office (PMO) for Risk IT projects, as discussed in Recommendation III-14. This is of particular importance, given the challenge posed by the highly complex nature of Risk IT projects.
- Take an active role in the PMO of large firm-wide projects, as most of these have interdependencies with Risk systems.
- Help define integration planning at the earliest stages of mergers and purposefully execute that planning (see Recommendation IV-11 for more on this topic).
- Develop systematic project-quality and delivery-control capabilities that will allow Risk IT/Ops to conduct, for example, comprehensive audits of Risk IT projects. In such audits, ongoing projects undergo a systematic review of the quality of delivered end products as well as on-time performance.
- Plan Risk IT capacity in the context of project delivery as well as business-as-usual requirements.
- Plan the integration of Risk IT/Ops in mergers and acquisitions, as discussed below.

In interviews and working sessions, a common view was that high-level executive sponsorship is required to ensure timely and effective delivery of Risk IT projects. This confirms prior

¹¹ For more see Appendix 3 of the SCI Report, which contains an IIF paper on risk culture.

ITF recommendations as to sound practice, as discussed above. At many firms, it will be appropriate for both the CIO and the CRO, with overall sponsorship from the board and senior management, to sponsor projects where risk-specific investments must be planned and sustained over time in light of competing demands on scarce resources. Leaders should sit on steering committees and allocate considerable time during projects to help with problem solving, removing bottlenecks, and providing inspiration—a departure from common practice, where leaders attend decision meetings and then wait for delivery. Discussions of the working groups and interviews with firms lead to the conclusion that IT is an essential enabler of success and a foundation of firm strategy. Therefore leaders should be trained on these topics and actively involved and engaged in Risk IT projects.

Executive sponsorship and involvement should also extend to other Risk IT-related activities. They can also sponsor holistic reviews of Risk IT projects to ensure that the firm is receiving value for money spent.

Big Risk IT projects should be genuinely shared efforts. This will require a shift in mind-sets at some firms, where too often the project consists of the CRO defining what he or she needs and the CIO leading the project to carry it out. Underlying this may be a tacit temptation for IT to be simply a delivery unit; that way, if the project fails it can claim that it received the wrong requirements. In these cases both sides must shift: the Risk group must invite the IT group to share fully in the project design, and the IT group must share in the responsibility for the project. IT can contribute early assessments on feasibility, and can even offer a “sanity check” on the project’s content. Both parties must work to make sure that any project is adequately designed to meet relevant regulatory requirements and to support the

reporting and control requirements of the firm’s risk appetite, as articulated by the board and enforced by senior management.

- **Recommendation IV-11.** Firms should consider Risk IT/Ops planning as essential to corporate transactions; they should devote the necessary time and resources to the creation of a sound Risk IT/Ops integration-planning process. In particular, this process should be deployed as major mergers and acquisitions are first contemplated.

Discussion of Recommendation IV-11

Mergers and acquisitions often put great strain on Risk and Risk IT/Ops personnel. Senior management and the board should at the least ensure that integration plans after mergers are defined and systematically and expeditiously executed. Risk IT/Ops integration assessment and planning should begin as soon as a transaction is seriously being considered and should be accorded high priority in overall integration plans. Some of the problems noted by the SSG and in this Report—the ones that come from a lack of coherent IT and an ability to aggregate data and information—have arisen from mergers where Risk IT integration has not been a priority or has not been carried through.

Transactions must be carried out rapidly, and the industry would certainly not want impositions of prior IT requirements to impede its ability to execute these transactions when opportunities arise. To preserve that necessary agility, however, it is essential for firms undertaking major transactions to do a better job in the future of assuring boards and supervisors that post-merger difficulties with IT in general and Risk IT in particular will not pose problems that can destroy value (or even destroy whole firms, as happened in the crisis).

Managing mergers and integrations: A specific delivery capability

As discussed above and in Theme III, mergers and acquisitions pose a particular challenge to the Risk IT architecture, which must be addressed in part through the Risk IT/Ops group's organization and governance. One firm reported that because of its corporate history it had a particular focus on integrating systems and data structures after a merger. An important element of success as outlined in Recommendation IV-11 is the firm's commitment to define a detailed plan at the outset of the integration process and to follow up with sufficient resources during execution. These projects may take several years.

Another firm took the opportunity of a large-scale merger to define its target-market Risk IT architecture. The firm established a dedicated market-risk integration team, a conscious effort to keep important Risk IT capabilities in-house to avoid dependence on vendors. It did seek help from external consultants to educate it on best practices for this one-time effort. The firm is now investing in training in Risk, which will help Risk IT employees to enhance their business understanding; and in IT, which will aid the understanding of the capabilities, limitations, and implementation challenges of Risk systems.

■ **Recommendation IV-12.** Firms should make provisions in their Risk, IT, and Risk IT/Ops activities to continually monitor, assess, and manage regulatory requirements. Larger firms might consider the creation of a dedicated organizational unit—a regulatory watch unit—to do this.

Discussion of Recommendation IV-12

Many leading firms begin their response to new regulation by analyzing the proposal first for its business and risk impact, and then by updating their “heat map” to identify and analyze new requirements for Risk IT. They then convene people from different business units as dedicated groups to react to regulatory changes when they occur. Such groups help a firm navigate regulatory requirements that touch on different parts of the business. To implement Principle IV-v, larger firms especially should consider either establishing a permanent unit, with an expanded mandate, or formalizing the process to convene the group when needed.

Leading firms have created a “regulatory watch unit” with resources from Risk and IT to ensure appropriate monitoring of the regulatory landscape and the thoughtful firm-wide implementation of required changes. (See sidebar for an example.) The unit acts as a bridge to the front office, IT, and Risk and in some cases serves as a forum for regular interactions among the CRO, CIO, and the head of regulatory affairs. Such a unit must also support the CRO function in its role of providing a frank assessment of risk needs and vulnerabilities—including Risk IT needs or gaps—to the senior management and board.¹²

Such a unit can be actively involved in regulatory processes; for example, it can raise questions during consultation phases about the implications of proposed rule changes for Risk IT/Ops. The unit can also provide forward-looking views on upcoming regulation to the Risk IT/Ops organization, and can coordinate the process to implement IT capabilities for

¹² See also the IIF's prior Principles I-ii and I-iii and Recommendations I.4, I.9, I.19, and especially I.21, in the CMBP Report, www.iif.com.

regulatory requirements. It should assess regulatory and Risk IT needs arising from new products or from mergers and acquisitions (including relatively small ones that nevertheless need to be integrated in Risk and Risk IT structures to avoid creating new vulnerabilities). Finally, the unit can act as the “face of the firm” for regulators.

Establishing a regulatory watch unit: An example for managing new regulatory requirements

One firm established a regulatory watch unit in 2009, as it believed that there would be increasing regulatory requirements to which it would need to respond. Prior to the establishment of the unit, much of its work had been done by the firm’s compliance unit.

The watch unit consists of five team members, one of them delegated from Risk IT. The unit acts as the point of contact for regulators and coordinates actions and responses within the firm. It also works with specialist groups, such as Treasury or Market Risk, to track actions that may be required from these units (for example, as a result of Basel III). The watch unit continually scans the environment for upcoming regulations and issues. The firm is confident that it will benefit from a reduction in the time needed to implement regulatory changes.

- **Recommendation IV-13.** Firms should maintain rigorous IT security controls throughout the Risk business system.
- **Recommendation IV-14.** Firms should maintain their professional approach to ensuring the “auditability” of Risk IT/Ops and changes to Risk IT systems.

Discussion of Recommendations IV-13 and IV-14

While security is not specific to Risk IT, firms consider it highly relevant and important. To ensure excellence in Risk IT security, rigorous control of access to data should be established. This includes determining the appropriate encryption technologies and creating a robust framework to monitor access rights. Where possible, checks for access and other security measures should be automated. For example, data validation should be automated by applying sanity checks and exception checks at critical points (for example, at data entry) across the business system. In addition, sound practices for monitoring outsourced services should be in place both for reasons of security and business recovery.

Seventy-nine percent of firms report that they have at least a “mostly professional approach to audit processes [with] transparent back-traceable change history.” Firms can accomplish this through two steps, beginning with comprehensive documentation. The firm should document the Risk IT/Ops governance, organization, architecture, processes, data definitions, and reporting protocols. The litmus test for fulfillment of this requirement is whether the firm’s documentation will allow an outsider to get an overview of Risk IT/Ops within a reasonable period of time. Such an overview is beneficial, as it allows internal and external audits to focus quickly on important issues and avoid the loss of time and resources in developing the necessary understanding.

The second step is to clearly document the change history of Risk and IT, that is, the adjustments to structures, processes, systems, data definitions, reports that have been issued since the last audit, and the reason behind the change.

Theme V: Interactions with supervisors

As the focus on Risk IT/Ops increases, both supervisors and the industry will face challenges in ensuring efficient and effective supervision.¹³ Supervisors have always been interested in Risk IT/Ops, but recently that interest has become a priority focus; other components of risk management, such as risk strategy, governance, and processes, have been under the spotlight for much longer. But Risk IT/Ops is not easy to supervise; as the preceding chapters have amply demonstrated, this highly technical field is challenging for firms and supervisors alike. It will probably take some time for the supervision of Risk IT/Ops to reach a globally consistent steady state.

This Theme considers two kinds of firm/supervisor interactions: the routine interactions that arise from bank supervision as it relates to the core activities of Risk IT/Ops, and ad hoc data and report requests.¹⁴ Better routine interactions will benefit firms in the obvious ways: supervisors will gain greater confidence in firms' risk management, get data more suited to their needs, and gain a fuller understanding of how firms think about and report their risks. Ad hoc interactions between firms and supervisors are often confusing and expensive for firms, and frustrating for both sides; and both sides will benefit from their improvement.

In the post-crisis environment, ad hoc requests may come from a firm's supervisors (through a college of supervisors in many cases), from a regulatory body seeking information for policy reasons, or from the new macroprudential authorities, which are likely to be highly demanding of data, especially as they begin to develop their functions. For purposes of the discussion in this Theme, we will refer to all these groups simply as "supervisors."

The survey, interviews, and discussions have confirmed the industry's strongly felt desire to improve interactions with regulators and supervisors, for their mutual benefit. Several firms mentioned that the tone and focus of Risk IT/Ops interactions has changed recently, with a new rigor and candor to the discussions. One firm said it was "amazed" by the technical detail and proof of implementation capabilities that supervisors now seek. Firms believe there would be substantial mutual benefit from more regular interactions on Risk IT/Ops issues and processes, rather than what seem to some to be one-sided data-provisioning demands.

CHALLENGES AND POTENTIAL AREAS FOR IMPROVEMENT

The survey, interviews, and discussions revealed three essential challenges in the interactions between regulators and individual firms.

¹³ For more on the current developments in this field, see the forthcoming white paper, "IIF Special Committee on Effective Regulation: Achieving effective supervision: An industry perspective," to be published in 2011.

¹⁴ Firms are also concerned about new accounting changes. Scheduling these changes significantly complicates the issue of proceeding in a deliberate, well-controlled manner with necessary Risk IT/Ops changes. The accounting standard setters, the prudential regulators, and other regulatory authorities (such as new macroprudential authorities, consumer-protection authorities, and market regulators) all must make allowances for the need for firms to balance and coordinate these complex changes, while at the same time maintaining the high quality and reliability of their basic systems and processes.

Greater standardization of reporting
Regulators provide the firms under their supervision with extensive and carefully prepared definitions and other documentation in support of their routine requests. At present, however, ad hoc requests are less thoroughly defined, and definitions change over time. Moreover, there are few internationally agreed-on standards for the reporting of risk and risk IT data. Content requirements change often. Formats and timing often vary among regulators. Terminology is often differently defined and is therefore subject to interpretation by each firm. For instance, exposure reports are a routine requirement—but regulators have different definitions on how to calculate it, whether it should be netted, if so, what offsets might be employed in the netting, and so on. As a result, exposure to what is purportedly the same risk is often calculated in different ways. This is part of the complex question of international equivalence in the calculation of risk-weighted assets (RWAs) that the Basel Committee on Banking Supervision (BCBS) is now taking up.¹⁵ The experience reflected in the survey suggests that part of the answer may be greater standardization of regulatory reporting forms. This is an issue expected to be discussed by the Basel Committee later this year.

Some firms see progress being made. One firm cited its current regulatory audit processes, in which terms of reference are clear, milestones are set well in advance, and interactions are efficient. Another firm's Risk IT executive noted that its supervisors had understood the problems caused by inconsistent and overlapping reporting requirements and were making efforts to harmonize reporting further. This firm also positively noted increasing international collaboration and alignment

among regulators that should lead to a convergence of regulatory practices, both at the firm-specific level through colleges of supervisors and more broadly.

Not all firms, however, have noticed similar developments; with respect to international alignment, most reported that this goal was, if anything, receding; these firms say that supervisors are becoming more locally oriented and asking more often for country-specific methodology adjustments. The coordination hoped for from colleges of supervisors is not very apparent in many cases, and the efficiencies that could be gained from greater standardization and consistency of regulatory reporting and information requests seem far off.

The lack of international standardization, especially with respect to ad hoc requests, has significant implications for Risk IT/Ops. Firms that are asked to produce reports on widely different timelines and in different formats must either write all the various formats into their systems and develop the capability to produce any of them in the shortest turnaround time requested, which is costly, inefficient, and may lead to errors or inadvertent compliance problems; or build a system with great reporting flexibility, well beyond most firms' current capabilities, but at significant incremental cost.

More basically, the lack of standardization of regulatory reporting across jurisdictions is an obstacle to the creation of common data models within firms, one of the principal areas for improvement identified in this Report. For firms that are active in many jurisdictions, this lack of standardization of official reporting requirements, formats, and definitions will prevent full realization of the benefits of common data models.

¹⁵ For more, see the speech by Stefan Walter, Secretary General, Basel Committee on Banking Supervision, at the 5th Biennial Conference on Risk Management and Supervision, Financial Stability Institute, Bank for International Settlements, Basel, November 3–4, 2010, www.bis.org.

In addition to the strain on systems, ad hoc requests can also put a significant burden on risk operations, as analysts and managers are diverted from their core functions to pull, compile, and reconcile data, often by hand. In some cases, the ad hoc response is particularly wasteful of resources, as routine reporting would provide an adequate response in due time.

As already discussed in Theme I, capabilities to aggregate data have improved to some degree and will improve over time; however, multiple variants of the same or similar requests, especially ad hoc requests, complicate the task of improving risk aggregation, increasing its complexity and adding to the development time required. Similarly, the aspiration to achieve deep granularity can be burdened by the job of responding appropriately to ad hoc requests. As argued in Theme I, setting lofty standards for specificity and granularity may be counterproductive; reasonable approximations will often be adequate for many ad hoc reports.

To be sure, further automation and greater flexibility of Risk IT systems will help firms cope with nonstandard requests. (See the discussion of these topics in Theme III.) But it should be noted that a failure to make further progress toward standardization of requests will entail significant additional IT costs. The more standard the requirements, the simpler the reporting systems that need to be built. In the view of most firms, compared with IT investment, greater standardization is the faster and more pragmatic solution. Smaller firms especially would benefit from a greater standardization of requests.

How alignment of ad hoc requests could help firms: Examples from interviews and working sessions

Firms that operate in many jurisdictions typically receive ad hoc requests from various local regulators on a given topic; but the requests are for slightly different data. For example, to report exposure to one nation's sovereign debt, one firm received separate requests for nominal exposure, gross exposure, netted positions, and mark-to-market derivatives exposure. Calculation requirements and assumptions may also differ:

To attempt to fix this solely by building a stronger and more flexible Risk IT system would not be effective; firms believe that such systems are possible but will be hugely expensive. Larger firms are likely to pursue the needed flexibility; smaller firms are less likely to do so; both groups believe that greater alignment of ad hoc requests across jurisdictions will be essential to success. Some firms also mentioned that regulators sometimes make requests that could be met by repackaging information to which regulators already had routine access. To fulfill these requests, firms had to reassign resources to recut data and reports, at the cost of disrupting the Risk IT processes that would otherwise have produced very similar data. Similarly, as discussed in Principle I-vi and Recommendation I-I I, a greater degree of pragmatism by supervisors in accepting approximations in lieu of highly granular data, especially for ad hoc requests or those requiring rapid turnaround, would help firms a great deal in their quest to meet regulatory information requirements in efficient ways that fully serve supervisory and regulatory purposes.

Finding common ground

While the survey showed that 82 percent of firms report that their supervisors regularly or occasionally seek discussions with them about Risk IT, and value their input, many firms also see potential benefits of improved interactions and better defined expectations.

Consider the not infrequent situation where supervisors and firms are confused about the service levels appropriate to ad hoc requests. To most firms, it seems that every request is urgent, making it difficult to prioritize. This is always an issue because of resource constraints, but it is especially acute in times of stress, when many demands are made upon IT and Risk personnel by senior management as well as by supervisors. Piling up demands without prioritization or coordination can make the situation worse rather than better, and increase the risk of error.

More discussion of the rationale for data requests would be helpful. Equally helpful would be a thoughtful discussion of data requests in general, including a shared view of the limitations of current data availability and the appropriate circumstances for approximate rather than exact responses, and the sequencing of requests when many are made at the same time.

A platform to exchange ideas and objectives

Regulatory requests are sometimes presented without detailed information on their context and purpose, or they contain ambiguities that must be discussed and worked through. Because of that, and because of past experience as detailed above, firms find it difficult to make overtures to regulators, such as a proposal to review regular reports or audit results that are readily available and may meet an ad hoc request.

In one case, a firm conducted extensive simulations of the direct effect of commodity price changes on its credit-risk exposure to producers of the commodity, pursuant to a supervisory request. However, the likely effects of the price change on the broader economy were not considered; nor were the risks related to other industries. These effects could have partially or fully offset the direct effects on the commodity producers, and hence on the firm's credit-risk exposure. This firm felt it did not have an appropriate forum in which to take up this discussion with the regulator:

PRINCIPLES

In describing the target state, the Steering Committee has identified, on the basis of the survey, interviews, and industry discussions, three Principles to improve the interactions of individual firms and their regulators in future. These Principles describe end states that will take time to reach. They should not be applied uniformly at the same time to all firms, as there is a wide range of starting positions and risk profiles. Different Principles will have higher or lower priority depending on the situation of each firm. The health and maturity of the firm's current relationships with its regulators will be a powerful influence on the rigor with which the Principles are applied. Broadly speaking, the Principles describe goals that all firms should pursue.

Principle V-i. Within any given jurisdiction, content and format of regular reporting should be standardized to allow greater efficiency in responding.

Discussion of Principle V-i

With respect to content, the working groups determined that risk taxonomies are an essential area for rapid improvement. These

taxonomies should include standard definitions for concepts such as value at risk (VAR), stressed VAR, risk-weighted assets, exposure, confidence intervals, total outstanding balance, the new net stable funding ratio, and so on. A standardization of taxonomies should be an important feature of the “fundamental review” of market-risk regulation now being conducted by the Basel Committee, but much more can and should be done. Similarly, the industry and bodies responsible for the major accounting standards should also seek industry-wide convergence as much as possible, to maximize the consistency across jurisdictions and between accounting and risk-management data and tools. Convergence on impairment and provisioning will be especially important.

Such standard definitions should be employed throughout the firm’s Risk IT/Ops, of course, and in regulatory reporting. Each report should be standardized with respect to the data definitions and indicators it requires, and to the requested format—typically either computer code (for example, XML) or a written report. Layout and design of such reports should also be standardized.

Finally, standardization should extend to reporting timelines. Regulators and the industry should work together to determine frequency of reports, their “cutoff” times (the time at which data should be considered, typically the end of a given business day in a defined locale), and the turnaround time (for example, one day for the most urgent requests, one week for less urgent needs, and so on). While some of this has been accomplished for routine reports, there is room for further optimization. A particular focus should be placed on ad hoc reports, which by their nature place a greater strain on firms. Judicious standardization along

these lines should allow firms to increase efficiency and quality and also make data more useable for supervisors, especially in the work of colleges of supervisors, where cooperation and coordination will be aided by working from the same data and the same reports.

Of course, firms understand that standardized practices such as standard taxonomies and templates are difficult because, as one firm noted, “The world changes.” The focus of regulators and industry will evolve, as will the types of measures and metrics that regulators and industry consider important. Therefore standards should be revisited periodically. Such flexibility is one of the chief benefits of eXtensible Business Reporting Language (XBRL), a standard for the exchange of financial information that some regulators have urged firms to adopt.

Principle V-ii. Industry and regulators should pursue cooperation among regulatory regimes, including, where practical, alignment of content, format, and timing standards among regulatory regimes, and should maximize coordination of supervision of individual firms through colleges of supervisors.

Discussion of Principle V-ii

There is already some degree of standardization of regular reporting across jurisdictions. For example, the International Monetary Fund (IMF) has developed standard definitions for some indicators of financial stability, a key component of many national regulators’ reporting requirements. And the ISDA has recently published “Product representation for standardized derivatives,” a white paper that promotes standardization of derivatives transactions to be settled through CCPs.¹⁶

¹⁶ www.isda.org.

But greater standardization is achievable. This is not just a matter of efficiency for firms or of accuracy and consistency of reporting to supervisors, important though those goals are. Efficient data standardization will also contribute to greater consistency in the implementation and interpretation of global financial standards – and thus to assuring a level playing field.

A clear distinction must be made between the standardization of regular and ad hoc reports. There is certainly scope for further standardization across jurisdictions of regular reports, and within some jurisdictions that are supervised by several regulators. This will become all the more important as supervisory intensity increases pursuant to Financial Stability Board (FSB) and G20 mandates, and as macroprudential oversight and supervision bodies begin soliciting information to help fulfill their mandates.

And in a global financial system, many ad hoc requests are related to events and developments that affect multiple jurisdictions. These can be standardized, with home supervisors coordinating the effort and supervisory colleges working out the details of standardization.

Firms with a broad, international footprint typically carry a bigger burden than smaller firms; they must contend with the differences in definitions and methodologies among regulatory regimes. These institutions may want to take the initiative to contribute to emerging standardization efforts by providing their input in consultation processes or through industry associations.

The Steering Committee has identified two places in which industry and regulators might

establish new degrees of cross-supervisory cooperation. For routine requests, supervisors—through colleges of supervisors at first, and then perhaps more broadly through the SSG or the Basel Standards Implementation Group (SIG)—might seek alignment on closing and value dates (that is, cutoff times) and response times. For ad hoc requests, supervisory colleges might define standard categories of such requests and the service levels associated with them. Such ad hoc requests should be coordinated by the home supervisor and made available as soon as possible to host supervisors to keep them current and avoid unnecessary, duplicative requests.¹⁷

Colleges of supervisors and other international bodies can perform a real service by standardizing and reducing the numbers of reports required. Fewer, more standardized reports would increase efficiency and quality for firms and benefit supervisors, if all supervisors in a given firm's college use the same reports and the same data definitions and interpretations. This is consistent with the Financial Stability Board's recommendation¹⁸ that the quality of information exchanged in supervisory colleges, especially regarding systemically important firms, should be adequate to enable a rigorous coordinated assessment of risks.

From a specifically Risk IT/Ops point of view, increased standardization and reduced numbers of (regular) reports would greatly facilitate the process of upgrading Risk IT/Ops capabilities, including data-aggregation capabilities. This rationalization of the investment required would be to the benefit of both firms and supervisors, especially supervisors of large, complex firms operating in multiple jurisdictions, where it is important to obtain a consistent and well-integrated picture of risks and exposures.

¹⁷ Basel Committee on Banking Supervision (BCBS), "Good practice principles on supervisory colleges," October 2010.

¹⁸ Financial Stability Board (FSB), "Reducing the moral hazard posed by systemically important financial institutions, FSB recommendations, and timelines," October 2010.

Principle V-iii. Firms and regulators should share more than current minimum requirements. Firms and regulators should create opportunities to exchange ideas, insights, and practical findings from Risk IT/Ops work.

Discussion of Principle V-iii

Firms with extensive interactions with regulators might want to pioneer new ways of exchanging insights and feedback. Firms can share with regulators their insights on better risk-modeling approaches and the lessons from their attempts at standardization based on efficient and effective IT changes. Regulators might share feedback on performance of firms, more detail on their priorities—which will provide helpful context for ad hoc requests – and more information on potential rule changes.

Both sides would benefit. Firms would get a chance to shape policy and gain a better understanding of their performance. Regulators would get a better and more consultative rule-making process and an increased understanding of Risk IT/Ops complexities.

Such discussions should take place in the normal course of interactions between each cross-border firm and its supervisors, but it would also be useful for the SSG to continue its dialogue with the industry on Risk IT/Ops and related data issues. The SIG can also contribute by supporting data standardization and consistency of Risk IT/Ops expectations as part of its peer reviews and its benchmarking of the implementation of Basel II and Basel III. The IIF stands ready to facilitate efforts of this kind, and especially to provide an industry perspective.

RECOMMENDATIONS

As the industry progresses toward the target state, firms and regulators will need to work

closely together. This will be challenging and take time. However, the efficiencies and effectiveness delivered to both sets of stakeholders, as described above, should be significant. The IIF working groups on Risk IT have established specific Recommendations that firms can use to implement the Principles of interactions with supervisors. Some of these Recommendations are aimed at supervisors and should be viewed as considerations for the public sector:

- **Recommendation V-1.** Within a jurisdiction, firms and their supervisors should work to promote standardization of regular reports wherever possible, especially in key indicators and taxonomies. Timelines, prioritization of requests, and report formats are primary candidates for greater standardization.
- **Recommendation V-2.** For ad hoc reports, firms and supervisors should agree on definitions of the requested data and details on calculation. Timing and prioritization of requests should also be standardized where possible.
- **Recommendation V-3.** Firms and supervisors should develop an industry-wide, cross-jurisdiction initiative to work toward the standardization of taxonomies, data requirements, and reporting across Finance, Risk, and Risk IT.
- **Recommendation V-4.** Supervisors, possibly a group within the SSG or the SIG, should consider forming a task force to drive an industry-wide cross-jurisdiction initiative aimed at greater harmonization of standards, including data standards, presumably drawing on the resources and insights of the SIG and the SSG.
- **Recommendation V-5.** As an industry-wide initiative makes progress, firms and supervisors should enshrine any standardized requirements that emerge in service-level agreements.

Discussion of Recommendations V-1 to V-5

An initiative of the kind proposed in Principle V-ii and Recommendation V-3 would have as its participants firms and regulators from around the world, working together for greater alignment. There have been some good recent examples of such inter-regime cooperation and standardization. In the European Union, the European Banking Authority (formerly the Committee of European Banking Supervisors) has published a much-debated reporting framework for regulatory capital and available capital in banks (Common Reporting, or COREP). National regulators are encouraged to apply this framework including its reporting taxonomy, standard templates and an underlying technology protocol.¹⁹ In the United States, the newly created Office for Financial Research (OFR) is planning to develop an international standard for the unique identification of legal entities that participate in financial contracts.²⁰ This legal-entity identifier (LEI) should facilitate monitoring of systemic risk by supervisors and enable more efficient management of risk by banks.

The industry has also come up with proposals to support the efforts of the official sector, particularly with regard to standardizing product identifiers for OTC derivatives. The ISDA, for example, has proposed establishing a Derivatives Product Registry (DPR) facility that will, among other things, issue a unique product identifier for each derivative. In another example, a group of dealers and buy-side institutions, in a letter to various regulatory

agencies, has committed to participate in efforts to develop and use international data standards. A subset of this group has been tasked to “provide feedback from an OTC derivatives perspective to ongoing international efforts to establish standard identifiers and reference data, including the current international efforts to establish legal-entity identifiers and unique trade of contract identifiers.”²¹ Similarly, the Securities Industry and Financial Markets Association, in collaboration with a number of other industry bodies, has recently issued a request for proposal and a set of technical and operational requirements to create a standard system of counterparty identification that will comply with the OFR’s requirements.²² And it is encouraging that work is proceeding through the International Organization for Standardization (ISO) and the Association of National Numbering Agencies, among others, toward global legal-entity identifiers, although more work and sustained momentum are required to achieve a globally acceptable, interoperative, and efficient standard.²³ It would be helpful if the FSB and agencies such as the OFR could contribute to bringing this work to fruition.

To be sure, if an initiative as we have recommended is to work, each participating supervisor must work toward greater standardization within its jurisdiction, even as it simultaneously seeks to align its standards with its peers. (See the discussion of Principle V-i for more on these standardization efforts.)

A cross-jurisdiction initiative should have as one of its priorities the development of an internationally aligned taxonomy for risk

¹⁹ European Banking Authority Web site, <http://www.eba.europa.eu/Supervisory-Reporting/Introduction.aspx>.

²⁰ Office of Financial Research Statement of Policy with Request for Comment Regarding the Statement on Legal Entity Identification for Financial Contracts. See 75 Fed. Reg. 74146 (November 30, 2010).

²¹ March 31, 2011 letter of major over the counter (OTC) market participants to regulators, including the Federal Reserve Bank of New York; see www.newyorkfed.org.

²² www.sifma.org.

²³ For example, Standard & Poor’s’ CABRE (CUSIP Avox Business Reference Entity) Identifiers; www.cusip.com.

reporting and, potentially, for reporting on Risk IT operations and management practices. As far as possible, such reporting should be aligned with reporting for international financial accounting purposes. Such a taxonomy could allow firms to report according to the same methodology and also to harmonize and adjust internal processes and systems. A particularly helpful step would be a technical protocol such as the one the EU has established, described above. This would simplify communication and reporting exchange with regulators, improve turnaround times on reports, and yield efficiencies and savings for firms and supervisors alike. Both a common taxonomy and a technical protocol would allow firms to reallocate investment to other strategic Risk IT/Ops needs. Supervisors would benefit from a greater ability to compare firms within their jurisdictions and internationally.

The Basel Committee's SIG has the opportunity and the ambition to be much more active in finding common solutions to the implementation of global standards. It should be an effective body for galvanizing and maintaining an international impetus toward harmonization of reporting and data requirements that will support the consistent implementation of the international accords around the world, consistent with the mandate of the G20 and FSB. The FSB's Standing Committee on Standards Implementation also has a broad mission to push forward international efforts aimed at harmonization and should help galvanize the necessary action.

At a more micro level, each global firm's college of supervisors (also mandated by the FSB) can and should work toward consistency among regulators of the tailored reporting required of each group, and toward assuring consistent and coordinated ad hoc inquiries when required. Other important goals for standardization include the reporting schedule, which should be made transparent and aligned internationally, and the prioritization of ad hoc requests.

Firms and regulators might potentially distinguish between urgent, tactical requests and long-term, research-oriented requests with appropriately different expectations for response times. This could form the basis of service-level agreements for risk reporting. Certain requests could then be agreed to be delivered in two days, while others could be agreed to be delivered over a longer time frame. Service-level agreements on timing, format, and governance could be agreed on between each firm and its regulators.

To implement this, a responsible body and a governance process are needed. Firms and regulators should work jointly through their colleges to calibrate such an effort for each group. More broadly, it would be very helpful if the SIG or SSG could organize a concerted, coordinated effort to ensure that the industry can migrate toward the most pragmatic and effective set of carefully planned and well-understood standards on a challenging but realistic schedule, taking into account the international scope and scale of such an effort.

This is a big task, but regulators and the industry are not starting from zero. As noted, there is already some standardization across jurisdictions, such as the IMF guidelines. One potential way forward would be to form a task force, as suggested in Principle V-4. The task force could drive the effort and seek input from other global regulators as needed. A key activity of such a task force would be to create an overview of all reports and data requirements, prioritize some for action, and designate a few reports and data definitions as models. The task force could then seek alignment on such proposals, and then move on to work on other reports and data definitions using the same approach.

We are aware that these are far-reaching suggestions. On the other hand, the benefits are important, and even small steps in this direction – preferably on an agreed-on long-term road

map – would encourage stakeholders and help promote an even more constructive atmosphere between firms and regulators. This in turn would, in the view of the SCl, help to advance the industry toward the target state of sound risk and Risk IT practices.

- **Recommendation V-6.** Firms and supervisors should establish regular, ongoing interactive processes to assure orderly progress toward new standards of interaction.
- **Recommendation V-7.** Firms and supervisors should establish single points of contact through which as much of their interaction as possible should be channeled.
- **Recommendation V-8.** Firms and supervisors should consider joint working groups to discuss the issues of the day concerning Risk IT/Ops, including data and risk operations.

Discussion of Recommendations V-6 to V-8

To advance the difficult work of standardizing report content, data definitions, formats, and timelines, supervisors and firms should take advantage of a number of levers to enhance their working relationships. These efforts will support all the Principles in this Theme.

Consider the problem of the duplication of data required in slightly different reports and ad hoc inquiries. Firms in interviews and working groups talked about similar requests being made of different parts of the organization, sometimes by different divisions within the same regulator.

The specific Recommendation that the IIF and its working teams suggest is to establish single points of contact, one for the firm and one for the regulator, as well as greater visibility into current and future requests, which could help improve interactions and eliminate duplicative requests.

Another idea that firms and regulators might consider is the adoption of standard schedules for discussions of data issues, including reviews of Risk IT development and investment plans. Routinizing such discussions and establishing a natural rhythm of communication can help to deflate tensions and create an open and trusting atmosphere.

One way forward might be the formation of joint working groups attended by those in the industry and supervisors. Such working groups would reach beyond the existing college structures and provide occasional opportunities for broader groups of supervisors and firms to exchange ideas. Forums might be organized by the SSG, working with industry groups such as the IIF. Working groups of risk and IT experts, and, importantly, senior management should be involved on the private-sector side; from the regulator, it would be helpful to have both supervisors focusing on specific risk and technology issues and senior policy people. It would also be highly useful for similar initiatives to be discussed at the Joint Forum²⁴ of prudential, insurance, and securities regulators, to foster cooperation and convergence across sectoral regulation as well as within the universe of global prudential regulation.

Firms should contribute effectively and constructively to such efforts by making sure they devote sufficient time to ensuring that

²⁴ The Joint Forum was established in 1996 and comprises the Basel Committee on Banking Supervision, the International Organization of Securities Commissions, and the International Association of Insurance Supervisors. Thirteen countries are represented in the Joint Forum: Australia, Belgium, Canada, France, Germany, Italy, Japan, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom, and the United States.

the right experts and managers monitor and contribute to consultations for new regulations and engage with industry associations that are actively contributing to such consultations, both at the national and international levels. Firms should consider it an obligation to participate in the opinion-forming process and to engage in dialogue on regulatory issues at each stage of their development.

Some firms have tried to ensure clear communications by building a regulatory unit with experts from Regulation, Risk, IT, and other parts of the firm. These units, described in detail in Theme IV, not only watch for changes in regulation but also act as “the face of the firm,” through which requests and communications between the firm and supervisor are channeled.

- **Recommendation V-9.** Firms and supervisors should consider programs to rotate managers between them.

Discussion of Recommendation V-9

Other forms of interaction might also be established between a firm and its regulators. Rotational programs within firms, in which leaders shift from group to group for short stints, have proved very effective in developing skills, knowledge, and understanding. Firms may want to consider a process in which relevant personnel, especially Risk and IT experts, can be exchanged, perhaps on a secondment basis between regulators and firms, to ensure better understanding of the technical challenges faced by both sides, to enable firms to anticipate regulatory needs, and to enable supervisors to couch their requests in a manner that will facilitate quick and fully useful compliance.²⁵

Naturally, firms will face considerable challenge in the design of such programs. At first glance, it might appear that independence and confidentiality could be sorely tested if relationships become too close. On the other hand, supervisors already have relationships with firms and access to confidential information. Regulators already hire people of integrity and character who will not allow their objective view to be compromised. Common sense and everyday experience show that good relationships foster productive exchanges and achieve better results. The industry is committed to engagement in this area and is keen to work with regulators and supervisors on this issue. One way of reducing potential conflicts of interest in secondments might be to set up the exchange between firms and supervisors other than their own. This would achieve most of the goals and would help firms and supervisors to understand the practices of partner jurisdictions.

As with the other Recommendations, it should be noted that some of these ideas are ambitious. But many firms believe that the benefits may be substantial and will outweigh the costs of developing and piloting these ideas.

Our working-group discussions and interviews showed time and again that the industry is committed to change and seeks improved interactions with regulators to make this change possible. The industry appreciates regulators’ consideration of its suggestions and is confident that both sides will benefit from a stronger alliance to further develop standards and practices.

²⁵ The IIF plans to address this topic further in a forthcoming report, “IIF Special Committee on Effective Regulation: Achieving effective supervision: An industry perspective,” to be published in 2011.

Next steps for the industry

As a matter of principle, the IIF believes that recovery from the financial crisis and maintenance of a resilient international financial system require equal attention to improved regulation, improved supervision, the creation of credible resolution mechanisms for financial institutions (especially those that operate across borders), and sound and continually improving internal risk management and governance. It has to be realized that the key enabler for risk management is Risk IT and Operations. This Report is intended to contribute to that vital pillar, without which better regulation and supervision would be hamstrung.

The survey has shown that firms are making substantial investments to upgrade the technology infrastructure that supports their risk management. Both the industry and the official sector, particularly the SSG, also recognize that more improvements must be made. The survey, interviews, and working-group discussions have also shown, however, that improvements to Risk IT and Operations, which firms need to widely varying extent, requires multiyear investments in terms of not only finances but also the amount of time that management devotes to these improvements, as well as human resources.

As firms execute these improvements, the Principles and Recommendations in this Report aim to inform and focus each firm's work to find the right solutions for its business mix and risk profile. They provide a contextual framework that will help firms maintain a commitment to progress toward the improved end state described in this Report over the somewhat protracted period needed to achieve it. The Principles

and Recommendations are also aimed at contributing meaningfully to the dialogue with the SSG, which has welcomed further industry and stakeholder input in its report of December 2010.

The IIF will look for opportunities for firms to facilitate the implementation of this Report's Principles and Recommendations. This Report will be presented to the industry with an open discussion in London on June 17, 2011, to which a broad array of firms—not just IIF members—has been invited. McKinsey, which has carried out much of the work behind the report, has also included a discussion of Risk IT/Ops issues in some of its presentations to clients and other members of the industry. We hope that facilitating this kind of discussion, which may also take place through regional CRO forums and other similar gatherings, will help firms of all sizes and from all regions, including emerging markets, better understand the Principles and make progress on the basis of the Recommendations.

Beyond discussions and events intended to facilitate firms' advancement, the IIF and the industry must work on broader contextual changes in accordance with the Recommendations. Standardization of data elements and reporting requirements across regulatory agencies and even across jurisdictions is among the most important of these. Efforts that are being undertaken by various agencies must be supported (and occasionally be brought more closely in line with a vision of global convergence and international utility). Standardized data, definitional requirements, and reporting requirements would ease the pressure on firms' Risk IT and provide a

more efficient starting point for firms' efforts to standardize their internal data taxonomies. Further, such standardization would contribute to financial stability, as it would facilitate data aggregation across different jurisdictions to make both microprudential supervision and macroprudential oversight more effective and reliable.

As mentioned in Theme V, the industry also supports the secondment of personnel between firms and regulatory and supervisory agencies. The industry is keen to work with regulators and supervisors on this, and will work to facilitate earnest engagement on this topic and to address potential conflicts of interest.

As is evident in much of this Report, and particularly in Theme V, regular dialogue between supervisors and the industry is necessary for continued progress. While much of this dialogue must take place bilaterally between each firm and its college of supervisors, the IIF's ongoing program of engagement with public-sector groups such as the FSB, the International Association of Insurance Supervisors (IAIS), the International Organization of Securities Commissions (IOSCO), the Basel Committee and SIG, and, especially, the SSG, will, it is hoped, facilitate constructive, two-way exchanges on the issues discussed herein, as they evolve over time. As the example of common data models illustrates, optimal progress on firms' internal improvements will to some extent depend on the regulatory environment—another reason that such dialogue is so important.

The IIF is also committed to evaluating the industry's progress regularly, not only in Risk IT/Ops but also in improving risk management and risk governance in general. Should a perceived need arise, the IIF will publish additional commentary, Principles, and

Recommendations as needed. Recently, the SCI conducted a second follow-up review of firms' implementation of the full suite of Principles and Recommendations published in 2008 and updated in 2009, in a report entitled *Making Strides in Financial Services Risk Management*, in collaboration with Ernst & Young, in April 2011. In conjunction with this Report on Risk IT/Ops, the IIF is publishing a separate Report on risk appetite, with its own set of Recommendations.²⁶ The Institute is also undertaking another detailed survey of the reform of compensation practices based on 2010 results, the outcome of which will be published in July 2011.

²⁶ To be published on June 17, 2011; www.iif.org.

Appendix I: A Table of Principles and Recommendations

For purposes of convenience, this appendix recapitulates the Principles and Recommendations of this Report.

PRINCIPLES AND RECOMMENDATIONS for Risk IT/Ops Issued in the Report of the IIF Steering Committee on Implementation [SCI], June 17, 2011

Theme I. Data standardization and risk aggregation for reporting and monitoring

Principles	Recommendations
<p><i>Principle I-i.</i> The ability to achieve an integrated view of exposures for major risk types is essential. Standardized data—across trading desks, asset classes, product classes, counterparties, and legal entities—that can be readily and rapidly aggregated without extensive manual intervention are fundamental.</p> <p><i>Principle I-ii.</i> Sufficient granularity, down to the level relevant for risk management and supervisory analysis (generally, the counterparty and product-class levels), must be easily and readily available for all material risks.</p> <p><i>Principle I-iii.</i> Data quality standards must be clearly defined and enforced for internal data. For external data, quality checks must be designed and consistently applied.</p> <p><i>Principle I-iv.</i> Data used in all control, risk-management, compliance, and supervisory functions must be defined consistently.</p>	<p>Recommendation I-1. Firms should aim to create a common data model as universally as possible, including standard definitions of all risk-related data.</p> <p>Recommendation I-2. Firms should develop clear governance practices to encourage the use of the common data model among all data users.</p> <p>Recommendation I-3. Firms should develop a reasonable timetable for the transition to the new common data model.</p> <p>Recommendation I-4. Firms should conduct systemic checks of data quality (e.g., automatic checks against acceptable data ranges during data entry).</p> <p>Recommendation I-5. Firms should build front-office interfaces that will ensure high quality of risk information.</p>

Principles	Recommendations
<p><i>Principle I-v.</i> Sufficient data history for more important risk factors and comprehensive data sets for such risks are important to risk management and to meeting supervisory requirements. Requirements for the depth and comprehensiveness of data history should be defined conservatively, in consultation with the firm's supervisors. Where necessary and possible, missing internal data values should be filled in with high-quality proxies or external data sources, to be agreed on between the firm and its supervisors.</p> <p><i>Principle I-vi.</i> The speed with which consistent data (including aggregated data across businesses, legal entities, and so on) must be delivered should be defined for each relevant risk type. The definition will depend on the materiality and type of risk, and on the risk profile and structure of each institution.</p>	<p>Recommendation I-6. When external data fails a quality check, firms should bring it up to standard as soon as practicable.</p> <p>Recommendation I-7. Where appropriate, firms should consider the consolidation of their data into a small number of data warehouses.</p> <p>Recommendation I-8. Firms should realign roles, responsibilities, and incentives throughout the business system to improve data integrity.</p> <p>Recommendation I-9. Firms should consider the establishment of a dedicated team to manage risk-data quality.</p> <p>Recommendation I-10. Firms should define service-level agreements (SLAs) for report turnarounds.</p> <p>Recommendation I-11. Where appropriate, firms should analyze the trade-offs between accuracy and speed of risk reporting, and consider the use of speedy approximations rather than delayed reports of greater precision. Such approximations, as well as their merits and flaws, should be thoroughly understood and discussed with supervisors.</p>

Theme II. Front-to-back operating model

Principles	Recommendations
<p><i>Principle II-i.</i> Risk-related processes should be designed and managed with an end-to-end perspective, and designed for enablement by Risk IT.</p> <p><i>Principle II-ii.</i> All risk-related processes should be aligned with the firm's risk appetite. Risk IT should facilitate the process of developing and enforcing the firm's risk appetite.</p> <p><i>Principle II-iii.</i> To the extent practical, Risk and Finance processes and data should be aligned for seamless transfers and consistency between the two groups.</p> <p><i>Principle II-iv.</i> Firms' strategic planning should have Risk IT/Ops (as well as IT more broadly) as an integral component.</p> <p><i>Principle II-v.</i> Risk IT should be a critical, independent category of information technology.</p>	<p>Recommendation II-1. Firms should use joint teams from the relevant businesses and functions, including people from front, middle, and back offices, to design risk-related processes and data flows with an end-to-end perspective.</p> <p>Recommendation II-2. Firms should define clear ownership of end-to-end risk-related processes and indicators to help the owner manage the process and assess his or her performance.</p> <p>Recommendation II-3. Firms should establish ownership for the task of continually reviewing, redesigning, and implementing improvements in processes that will enhance their end-to-end consistency and efficiency.</p> <p>Recommendation II-4. Firms should consider the use of workflow management tools in all relevant risk-related processes.</p> <p>Recommendation II-5. As firms realign risk-related processes—particularly the limit-management process—they should ensure that the new design is motivated by and closely connected to the firm's risk appetite.</p> <p>Recommendation II-6. Firms should clearly define the essential characteristics of processes that involve both Risk and Finance.</p> <p>Recommendation II-7. Firms should consider the design of a consistent taxonomy and data model for both Risk and Finance.</p> <p>Recommendation II-8. Within the firm IT architecture, firms should manage applications for Risk and Finance coherently, seeking</p>

Principles	Recommendations
	<p>consistency wherever possible. In the absence of an independent Risk IT/Ops unit, this should be a clearly established task within firm IT.</p> <p>Recommendation II-9. Risk and Finance should jointly design their reconciliation processes.</p> <p>Recommendation II-10. Firms' enterprise-wide, risk-limit management systems should, in an automated way, enforce local limits, monitor limit utilization and adherence, and trigger escalation procedures. Automation should be appropriate to the constitution of the firm's risk portfolio; firms with less volatile risks should ensure that their manual pre-deal simulations are as accurate as possible.</p> <p>Recommendation II-11. Front-to-back escalation procedures should be clearly defined and embedded in Risk IT systems.</p> <p>Recommendation II-12. Firms should ensure that both enterprise- and business-level strategic-planning processes incorporate regular input from Risk and IT groups, and, where one exists, the Risk IT/Ops unit.</p> <p>Recommendation II-13. Risk IT should be a critical and independent category in a firm's IT planning.</p> <p>Recommendation II-14. In new-product development processes, firms should include in their due diligence an assessment from Risk IT/Ops of the ability to support the product from a Risk IT perspective.</p>

Theme III. Applications, architecture, and infrastructure

Principles	Recommendations
<p><i>Principle III-i.</i> Risk IT systems and applications should comprehensively cover all material regulatory and management requirements, recognizing that in the current environment and the foreseeable future, firms will have a broadened roster of fundamental risk requirements and simulation needs.</p> <p><i>Principle III-ii.</i> The Risk IT data layer must be defined with clarity, achieved primarily through consistent data models. Such models will allow the firm to identify and verify data sources and integrate both internal and external data quickly and smoothly.</p> <p><i>Principle III-iii.</i> Where possible, the Risk IT architecture should employ an integration layer instead of point-to-point interfaces.</p> <p><i>Principle III-iv.</i> The Risk IT architecture should be sufficiently flexible, and Risk IT applications and architecture sufficiently modular, to keep in step with the changing needs of supervision and the business.</p> <p><i>Principle III-v.</i> Like the Risk IT architecture, the Risk IT infrastructure should be sufficiently flexible to allow the firm to react nimbly to structural changes in markets and methods.</p> <p><i>Principle III-vi.</i> The Risk IT infrastructure should contain sufficient computing power to meet all business and regulatory needs.</p>	<p>Recommendation III-1. Firms should analyze their risk applications to determine gaps in their functional coverage, especially with respect to key indicators and simulation support for stress testing and other needs.</p> <p>Recommendation III-2. Firms should convene a dialogue across businesses, Risk, IT, and Risk IT/Ops on how to redesign the Risk IT architecture to fill the gaps.</p> <p>Recommendation III-3. Firms should consider establishing a single point of responsibility to oversee development of risk applications.</p> <p>Recommendation III-4. Firms should consider refreshing or redesigning their Risk IT architecture to exploit the benefits of a common data model and middleware.</p> <p>Recommendation III-5. Firms' planning should, as much as possible, aim for all businesses to coalesce around a common data model.</p> <p>Recommendation III-6. Firms should align their internal risk taxonomy among businesses and all Risk units.</p> <p>Recommendation III-7. Firms should evaluate the benefits of a layered architectural layout—with data warehouse(s), calculation “engines,” data integration (middleware), business intelligence/MIS, and reporting layers.</p> <p>Recommendation III-8. Firms should, in particular, evaluate the benefits of consolidated data warehouses as consistent “golden” sources of data and proceed accordingly.</p>

Principles	Recommendations
	<p>Recommendation III-9. For all manual reconciliations that in a firm's view consume substantial resources, the firm should construct a business case to analyze the advantages and costs of automating the reconciliation.</p> <p>Recommendation III-10. Firms should develop a clear target layout of their Risk IT architecture. They should develop a manageable road map to reach this target layout, with clear intermediate milestones at which stand-alone impact will be achieved.</p> <p>Recommendation III-11. Within the Risk IT architecture, production and development environments should be separated.</p> <p>Recommendation III-12. Discrete risk functions should be provided, as much as possible, by single modules. Redundant functionality among modules should be eliminated, and modules and applications should be grouped by purpose.</p> <p>Recommendation III-13. Firms should establish clear architectural standards for the Risk IT architecture that will promote modular and flexible design.</p> <p>Recommendation III-14. Firms should establish clear technology standards for the Risk IT architecture that will promote modularity and flexibility.</p> <p>Recommendation III-15. Firms should adopt a long-term perspective to plan Risk IT infrastructural capacity.</p> <p>Recommendation III-16. Firms should assess the requirements needed to provide Risk IT computing power as a service, including the provision of Risk IT computing capacity from an internal "cloud."</p>

Theme IV. Organization, governance, and security

Principles	Recommendations
<p><i>Principle IV-i.</i> A high-performing Risk IT/Ops function should be concentrated to the extent possible in a dedicated organizational unit.</p>	<p>Recommendation IV-1. Firms should consider establishing a dedicated Risk IT/Ops group with clear responsibilities, or take measures to assure that the functions that would fall to such a dedicated group in accordance with the Principles and Recommendations of this Report are adequately covered.</p>
<p><i>Principle IV-ii.</i> For the Risk IT/Ops group to be most effective, its staff must possess—in depth—four kinds of skills and knowledge: business, risk, technology, and project management.</p>	<p>Recommendation IV-2. Firms should cultivate the appropriate mix of technical, content, and process-management skills in the Risk IT/Ops group.</p>
<p><i>Principle IV-iii.</i> Highly specialized skills and critical knowledge should be developed and kept in-house; only noncritical activities should be outsourced.</p>	<p>Recommendation IV-3. Firms should invest in the appropriate management of vendors of Risk IT/Ops products and services, reduce their dependency on any one vendor, and take steps to improve the speed with which third-party contractors deliver services.</p>
<p><i>Principle IV-iv.</i> Strong, integrated project-delivery capabilities are fundamental to the success of cross-functional, cross-business initiatives, and are required for many Risk IT projects.</p>	<p>Recommendation IV-4. Firms should dedicate staff to manage critical Risk and Finance IT applications and infrastructure. The staff should develop the kind of deep knowledge that is essential for getting high performance out of these applications and infrastructure. Use of such specialists will provide a better result than asking Risk IT generalists to look after such critical systems.</p>
<p><i>Principle IV-v.</i> Anticipation of regulatory change can only benefit firms. Preplanning can help firms react quickly and thoughtfully to regulatory change.</p>	<p>Recommendation IV-5. Firms should invest in capturing and codifying Risk IT/Ops knowledge, to ensure that the group's expertise and know-how can be shared today to generate efficiencies and tomorrow to ensure continuity.</p>
<p><i>Principle IV-vi.</i> Risk IT security must remain vigilant, both for business reasons and because vigilance is a foundation of public confidence in the industry.</p>	<p>Recommendation IV-6. Firms should conduct regular joint meetings across business, Risk, IT, and Risk IT/Ops, at both strategic and</p>
<p><i>Principle IV-vii.</i> Firms should ensure that changes to Risk IT/Ops, and in particular to its systems and methodologies, are auditable.</p>	

Principles	Recommendations
	<p>operational levels. Such meetings should be conducted at a sufficient level of detail to allow attendees to engage in and contribute to the thought processes of other groups.</p> <p>Recommendation IV-7. Firms should establish training and rotational programs to ensure Risk IT/Ops staff have sufficient understanding of risk and business issues, and similarly to ensure that business and Risk staff develop a sufficient understanding of IT.</p> <p>Recommendation IV-8. Firms should consider hybrid career paths, with time spent in Risk, business, and IT. Such hybrid career paths can be thought of as a kind of permanent rotational program.</p> <p>Recommendation IV-9. The CIO and CRO should jointly sponsor and actively lead major Risk IT/Ops projects within the context of the firm's Risk IT/Ops governance model, and provide active and engaged leadership for their planning and execution.</p> <p>Recommendation IV-10. Firms should work to create shared accountability with specified responsibilities for the design and delivery of major Risk IT projects among Risk, IT, and Risk IT/Ops.</p> <p>Recommendation IV-11. Firms should consider Risk IT/Ops planning as essential to corporate transactions; they should devote the necessary time and resources to the creation of a sound Risk IT/Ops integration planning process. In particular, this process should be deployed at the same time as major mergers and acquisitions are first contemplated.</p>

Principles

Recommendations

Recommendation IV-12. Firms should make provisions in their Risk, IT, and Risk IT/Ops activities to continually monitor, assess, and manage regulatory requirements. Larger firms might consider the creation of a dedicated organizational unit—a regulatory watch unit—to do this.

Recommendation IV-13. Firms should maintain rigorous IT security controls throughout the risk business system.

Recommendation IV-14. Firms should maintain their professional approach to ensuring the “auditability” of Risk IT/Ops and changes to Risk IT systems.

Theme V. Interactions with supervisors

Principles	Recommendations
<p><i>Principle V-i.</i> Within any given jurisdiction, content and format of regular reporting should be standardized to allow greater efficiency in responding.</p> <p><i>Principle V-ii.</i> Industry and regulators should pursue cooperation among regulatory regimes, including, where practical, alignment of content, format, and timing standards among regulatory regimes, and should maximize coordination of supervision of individual firms through colleges of supervisors.</p> <p><i>Principle V-iii.</i> Firms and regulators should share more than current minimum requirements. Firms and regulators should create opportunities to exchange ideas, insights, and practical findings from Risk IT/Ops work.</p>	<p>Recommendation V-1. Within a jurisdiction, firms and their supervisors should work to promote standardization of regular reports wherever possible, especially in key indicators and taxonomies. Timelines, prioritization of requests, and report formats are primary candidates for greater standardization.</p> <p>Recommendation V-2. For ad hoc reports, firms and supervisors should agree on definitions of the requested data and details on calculation. Timing and prioritization of requests should also be standardized where possible.</p> <p>Recommendation V-3. Firms and supervisors should develop an industry-wide, cross-jurisdiction initiative to work toward the standardization of taxonomies, data requirements, and reporting across Finance, Risk, and Risk IT.</p> <p>Recommendation V-4. Supervisors should consider forming a task force to drive an industry-wide cross-jurisdiction initiative aimed at greater harmonization of standards, including data standards, presumably drawing on the resources and insights of the SIG and the SSG.</p> <p>Recommendation V-5. As an industry-wide initiative makes progress, firms and supervisors should enshrine any standardized requirements that emerge in service-level agreements.</p> <p>Recommendation V-6. Firms and supervisors should establish regular, ongoing interactive processes to assure orderly progress toward new standards of interaction.</p>

Principles	Recommendations
	<p>Recommendation V-7. Firms and supervisors should establish single points of contact through which as much of their interaction as possible should be channeled.</p> <p>Recommendation V-8. Firms and supervisors should consider joint working groups to discuss the issues concerning Risk IT/Ops, including data and risk operations.</p> <p>Recommendation V-9. Firms and supervisors should consider programs to rotate managers between them.</p>

Appendix 2: Comparing the guidance of the SSG with this Report's Principles and Recommendations

The following table compares the recommendations and leading practices as outlined by the Senior Supervisors Group (SSG) in its December 2010²⁷ report with the Principles and Recommendations in this Report. The table shows that the SSG's recommended practices are encompassed by the Principles and Recommendations published by the IIF Steering Committee on Implementation (SCI) in this Report.²⁸ In many cases, the SCI's Recommendations exceed the SSG's guidelines.

SSG recommendations and leading practices	SCI Principles and Recommendations
---	------------------------------------

SSG Section IV-B: The importance of IT governance in strategic planning and decision making

Planning and alignment

"Strategic-planning processes should include an assessment of risk-data requirements and system gaps."

"The technology-planning process has to align both business and IT strategies to ensure that a productive partnership exists, and that it values the investments made in financial and human resources to complete the project."

Recommendation III-1. Firms should analyze their risk applications to determine gaps in their functional coverage, especially with respect to key indicators and simulation support for stress testing and other needs.

Recommendation III-2. Firms should convene a dialogue across businesses, Risk, IT, and Risk IT/Ops on how to redesign the Risk IT architecture to fill the gaps.

²⁷ Senior Supervisors Group (SSG), "Observations on developments in risk appetite frameworks and IT infrastructure," December 23, 2010.

²⁸ Many of the SSG's recommendations on governance are also addressed by the Principles and Recommendations established in the Committee on Market Best Practices (CMBP) and Steering Committee on Implementation (SCI) Reports of 2008 and 2009.

“Firms with leading, highly developed IT infrastructures bring together senior IT governance functions, business-line units, and IT personnel to formulate strategy.”

Recommendation II-1. Firms should use joint teams from the relevant businesses and functions, including people from front, middle, and back offices, to design risk-related processes and data flows with an end-to-end perspective.

Recommendation II-12. Firms should ensure that both enterprise- and business-level strategic-planning processes incorporate regular input from Risk and IT groups, and, where one exists, the Risk IT/Ops unit.

Recommendation II-13. Risk IT should be a critical and independent category in firm IT’s planning.

Governance of outsourced activity

“Firms that rely on outsourced IT activities that affect infrastructure, data aggregation, and internal risk reporting should apply the same level of governance to these activities as if they were performed in-house.”

Recommendation IV-3. Firms should invest in the appropriate management of vendors of Risk IT/Ops products and services, reduce their dependency on any one vendor, and take steps to improve the speed with which third-party contractors deliver services.

Project management

“Firms successful in aligning IT strategies with the needs of business-line managers and risk-management functions have strong project-management offices (PMOs) to ensure that timelines and deliverables are met.”

A “single person [rather than a committee] as the focal point for program oversight results in better coordination and communication among project staff and, by extension, better project implementation and execution.”

Recommendation IV-9. The CIO and CRO should jointly sponsor and actively lead major Risk IT/Ops projects within the context of the firm’s Risk IT/Ops governance model, and provide active and engaged leadership for their planning and execution.

See also the discussion of Recommendations III-10 to III-14, in which the advantages of a PMO are promoted.

Data ownership

“Firms with effective IT project implementation appoint a data administrator and a data owner with responsibility and accountability for data accuracy, integrity, and availability.”

Recommendation III-3. Firms should consider establishing a single point of responsibility to oversee development of risk applications.

Recommendation I-9. Firms should consider the establishment of a dedicated team to manage risk-data quality.

Audit

“Firms with high-performing IT infrastructures ensure that the board committees institute internal audit programs, as appropriate, to provide for periodic reviews of data-maintenance processes and functions.”

Recommendation IV-14. Firms should maintain their professional approach to ensuring the “auditability” of Risk IT/Ops and changes to Risk IT systems.

Equal commitment to business and risk

“Firms with leading IT infrastructures commit budgetary resources to developing IT infrastructures for internal risk reporting with the same level of priority that they give to the funding of projects that emphasize front-end revenue generation and speed to market.”

See the discussion of Recommendations III-1 to III-3.

SSG Section IV-C: Automating risk-data-aggregation capabilities

Ability to aggregate risk data in an accurate, timely, and comprehensive manner

“Firms should establish standards, cutoff times, and schedules for internal risk reports.”

Principle I-i. The ability to achieve an integrated view of exposures for major risk types is essential. Standardized data—across trading desks, asset classes, product classes, counterparties, and legal entities—that can be readily and rapidly aggregated without extensive manual intervention are fundamental.

Recommendation I-10. Firms should define service-level agreements (SLAs) for report turnarounds.

Increased automation and reduced or eliminated manual processes

“One key attribute that allows risk data to be aggregated quickly is the ability to automate data flows and reduce the amount of manual intervention necessary to compile this critical information.”

Principle I-vi. The speed with which consistent data (including aggregated data across businesses, legal entities, and so on) must be delivered should be defined for each relevant risk type. The definition will depend on the materiality and type of risk, and the risk profile and structure of each institution.

Recommendation I-11. Where appropriate, firms should analyze the trade-offs between accuracy and speed of risk reporting, and consider the use of speedy approximations rather than delayed reports of greater precision. Such approximations, as well as their merits and flaws, should be thoroughly understood and discussed with supervisors.

Recommendation III-9. For all manual reconciliations that in a firm’s view consume substantial resources, the firm should construct a business case to analyze the advantages and costs of automating the reconciliation.

Data standardization

“Consolidated platforms and data warehouses that employ common taxonomies permit rapid and relatively seamless data transfer, greatly facilitating a firm-wide view of risk.”

“Centralized static databases with single identifiers and/or unified naming conventions for legal entities, counterparties, customers, and accounts enable a consistent approach to pulling multiple records of risk data across the firm in a timely manner. Consistent

Recommendation I-1. Firms should aim to create a common data model, including standard definitions of all risk-related data.

Recommendation I-2. Firms should develop clear governance practices to encourage the use of the common data model among all data users.

Recommendation I-3. Firms should develop a reasonable timetable for the transition to the

identifiers and naming conventions also permit segmentation in cases where it may be necessary to identify risk concentrations or to meet a supervisory or legal requirement.”

new common data model.

Recommendation I-7. Where appropriate, firms should consider the consolidation of their data into a small number of data warehouses.

Recommendation III-4. Firms should consider refreshing or redesigning their Risk IT architecture to exploit the benefits of a common data model and middleware.

Recommendation III-5. Firms' planning should, as much as possible, aim for all businesses to coalesce around a common data model.

Recommendation III-6. Firms should align their internal risk taxonomy among businesses and all Risk units.

Recommendation III-8. Firms should, in particular, evaluate the benefits of consolidated data warehouses as consistent “golden” sources of data and proceed accordingly.

Data platforms

“The more robust designs are single-platform ones that can include trading, pricing, the general ledger, and risk-management reporting.”

Some leading firms are establishing “a ‘gateway’ system for credit and market risk applications” and a “global liquidity platform.”

Recommendation III-7. Firms should evaluate the benefits of a layered architectural layout—with data warehouse(s), calculation “engines,” data integration (middleware), business intelligence/MIS, and reporting layers.

See the discussion of Recommendations I-1 to I-7 for comments on these efforts.

Reconciliation of finance and risk data

“Leading firms’ MIS practices also include periodic reconciliation between risk and financial data. The nature, scope, and frequency of such reconciliation practices are commensurate with the firm’s business and risk environment, but some reconciliation is essential with a view to ensuring accuracy and periodic validation of the firm’s MIS.”

Recommendation II-6. Firms should clearly define the essential characteristics of processes that involve both Risk and Finance.

Recommendation II-7. Firms should consider the design of a consistent taxonomy and data model for both Risk and Finance.

Recommendation II-9. Risk and Finance should jointly design their reconciliation processes.

Aggregation by legal entity

“While we believe strongly that aggregation of risk data must occur on a firm-wide basis, increasingly, there is a need for firms to be able to compile internal risk data on a legal-entity basis, as systems have been largely designed along business lines.”

Principle I-ii. Sufficient granularity, down to the level relevant for risk management and supervisory analysis (generally, the counterparty and product-class levels), must be easily and readily available for all material risks.

SSG Section IV-D: Prioritizing the integration of IT systems and platforms

Integrating systems after a merger

Leading firms have “business practices that prioritize the integration of legacy systems from mergers or acquisitions as soon as is reasonably possible after the transaction is completed, and new product-approval procedures that include technology-operations personnel to ensure that systems can process and aggregate data from new products or initiatives.”

Recommendation IV-1 I. Firms should consider Risk IT/Ops planning as essential to corporate transactions; they should devote the necessary time and resources to the creation of a sound Risk IT/Ops integration planning process. In particular, this process should be deployed at the same time as major mergers and acquisitions are first contemplated.

Planning for new product development

“While it is good practice for firms to require assessments of IT infrastructure and capacity prior to approving new products, it is also a leading practice for firms to conduct reviews 6 to 18 months after implementation to ensure that the technology projects have met the needs of the risk professionals.”

Recommendation II-14. In new-product development processes, firms should include in their due diligence an assessment from Risk IT/Ops of the ability to support the product from a Risk IT perspective.

SSG Section IV-E: Maintaining appropriate systems capacity

Appropriate capacity

“In their capacity planning and testing, most firms still have to include scenarios involving sharp fluctuations in volume. They also have to plan for and test the ability to meet processing windows under stress scenarios, including the ability to make risk MIS available on short notice (such as during crisis situations) and at any given time. For most firms, additional work is required to understand the true impact that outages of critical systems will have on other key systems.”

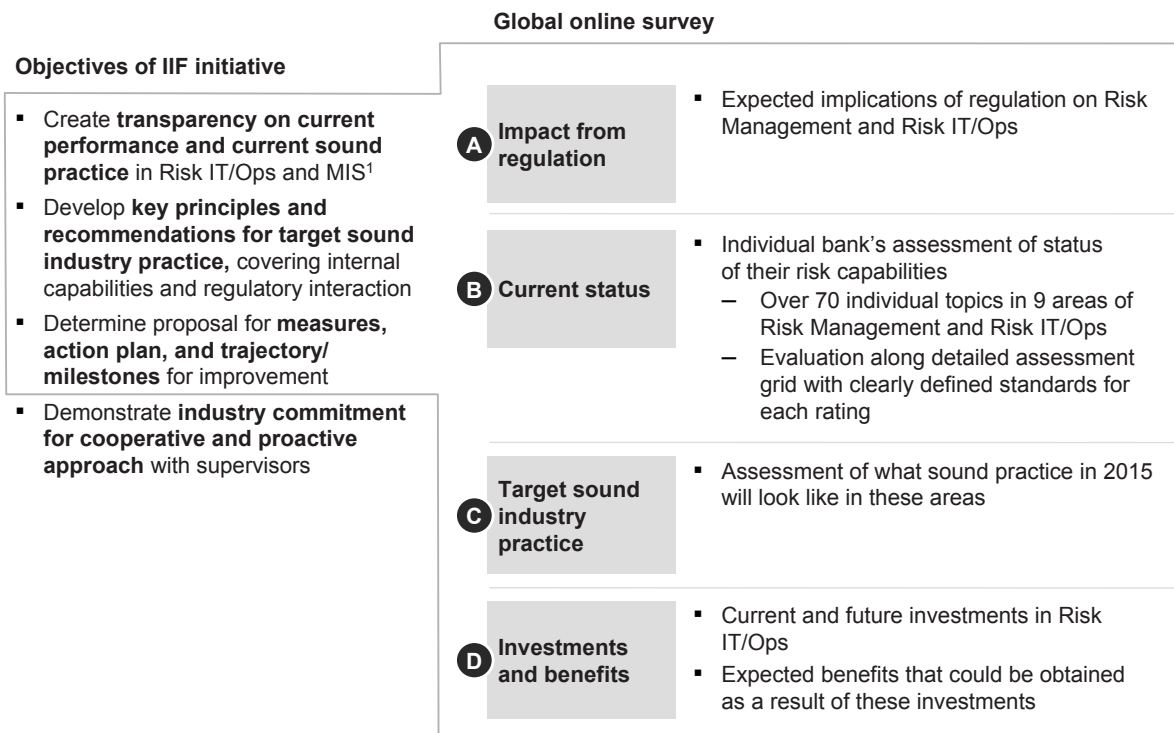
Recommendation III-15. Firms should adopt a long-term perspective to plan Risk IT infrastructural capacity.

Recommendation III-16. Firms should assess the requirements needed to provide Risk IT computing power as a service, including the provision of Risk IT computing capacity from an internal “cloud.”

Appendix 3: A closer look at the survey's detailed assessment grid

The survey was designed to create the fact base on which the IIF could develop Principles and Recommendations to help the industry continue to improve Risk IT/Ops (Exhibit 1). It was distributed online and included detailed questions, yielding over 400 data points per respondent. The expected impact of regulation on Risk IT/Ops was examined through detailed questions on several subcategories. Firms were also asked about their current status, the current state of industry sound practice, and the target for industry sound practice (Exhibit 2). To help firms calibrate their responses and make those responses comparable, the survey included descriptions for levels 2, 4, and 6 (Exhibit 3). For selected questions, each firm was asked to provide additional detail by risk type.

Exhibit 1
The survey addressed two of the IIF's key objectives



¹ Management information systems.
 Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 2 The survey covered a broad range of Risk IT/Ops topics

Risk IT topics	Overarching question	Selected key categories (not exhaustive)
Risk operations	How well are processes designed with respect to supporting essential aspects of risk management?	<ul style="list-style-type: none"> Prevalence of end-to-end process view Level of automation of risk processes Harmonization of processes across Risk and Finance
Risk org/ governance	How are policies, procedures, and structures for the Risk function set up?	<ul style="list-style-type: none"> Globality of setup, governance of Counterparty Risk and Collateral Mgt unit Globality, granularity and governance of limit-management framework Level of front-office accountability for risk-relevant data and processes
Applications	How sophisticated is IT application coverage for critical risk functionality and how mature is the IT architecture?	<ul style="list-style-type: none"> Level of IT support for risk mitigation methods, eg, collateral, credit-default swaps (CDS) Functional coverage for stress testing, modeling/simulation Readiness of application landscape for, eg, introduction of central counterparties (CCPs)
Data/ integration	How advanced are data capabilities (quality, consistency, integration), especially for providing an aggregated risk view?	<ul style="list-style-type: none"> Golden data sources and risk-data aggregation capabilities Real-time data capabilities Power and globality of data governance and maintenance
Infrastructure	How mature and well performing are operating systems, databases, servers, backup facilities ?	<ul style="list-style-type: none"> Availability of computing power Sophistication and differentiation according to risk types Flexibility to support regulatory changes ...
IT org, governance, and security	What are the mechanisms for managing Risk IT and achieving Risk IT security/compliance?	<ul style="list-style-type: none"> Level of power, globality, and strength of Risk IT governance Maturity of Risk IT management processes and procedures for monitoring Auditability of Risk IT/Ops

Source: IIF/McKinsey Risk IT/Ops survey

In addition to Risk IT topics, the survey assessed risk-management capabilities across 3 dimensions (measurement, monitoring, and reporting) as well as simulations

Firms rated their current practice, current industry standards, and target sound industry practice for 2015 in more than 50 categories; in some categories firms also rated provided answers for each of 4 risk types

Exhibit 3 Detailed descriptions helped firms calibrate their responses

3a. Status and target - Risk

This third section of the survey examines several risk aspects like risk monitoring and stress testing. For each of them we ask you for assessing:

- The current status of your bank
- The current industry sound practice
- A target industry sound practice for 2015

The assessment will be done on a scale from 1 to 7, 7 being the most positive appraisal. For your orientation we use descriptions for level 2, 4 and 6.

Overarching for IT/Risk measurement, monitoring, controlling, reporting and stress tests

	Your bank - Current status 2010	Current industry sound practice 2010	Target industry sound practice 2015	Advanced (6)	Average (4)	Basic/Rudimentary (2)
1. Available granularity of data				High granularity of data (e.g. across risks, cross desk, cross asset classes) with real-time connectivity and linked to automatically reconciled data warehouses, full granularity available in drill-down	Full capability/ flexibility of selective drilling down along all dimensions (e.g. by risk category, by type of risk, geography, by business)	Drill down by 4 dimensions only, only low level of granularity
2. Data drill-down capabilities				Full capability/ flexibility of selective drilling down along all dimensions (e.g. by risk category, by type of risk, geography, by business)	Drill down by 4 dimensions only, only low level of granularity	Drill down by 4 dimensions only, only low level of granularity
3. Capabilities in risk aggregation for monitoring and reporting				Integrated/holistic view on all risks (eg, cross-desk, cross-asset class) with real-time connectivity and linked to automatically reconciled data warehouses, full granularity available in drill-down	Integrated view on standard risks across desks and asset classes possible using automated scripts but requiring time lag and integration of data from disparate systems, not enabling full drill down to all metrics and granularities	Not fully integrated view on all risks, ie, "silo view" (eg, siloed systems with different data inputs and batch processing requiring ad hoc reconciliations). Data aggregation of risks requiring high manual querying/ adjustments (eg, multiple, disjoint, nonstandard data repositories for each geography)
3.1 Credit risk						
3.2 Market risk						
3.3 Liquidity risk						
3.4 Operational risk						

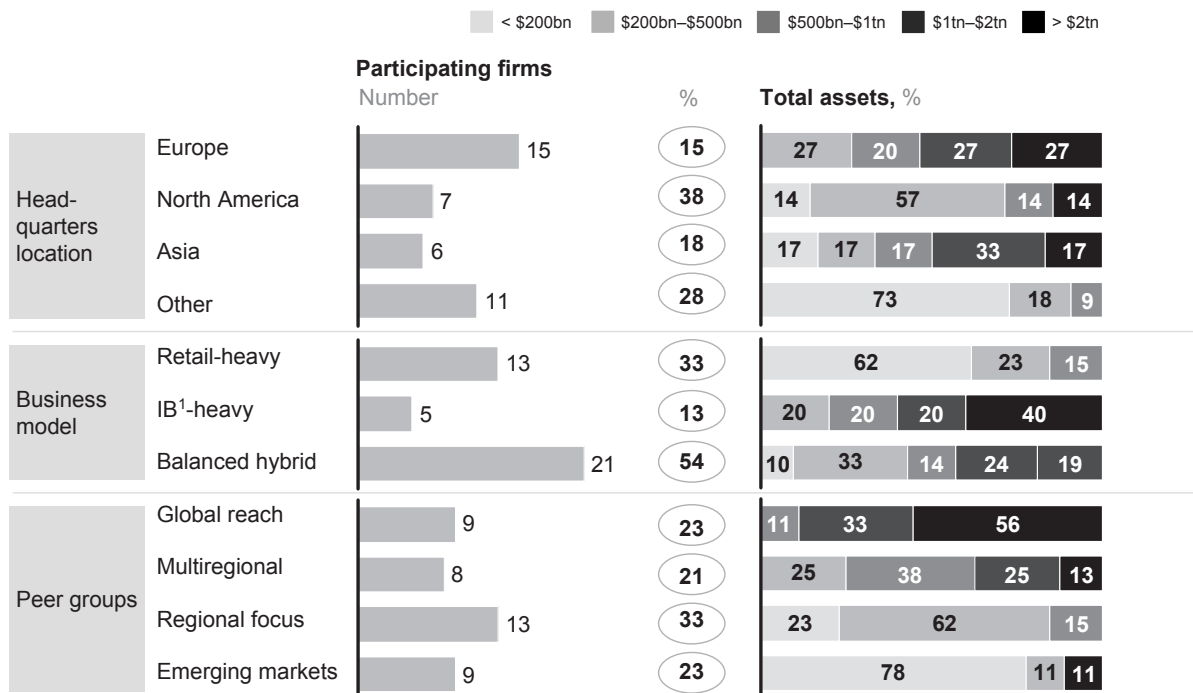
Detailed assessment grid

Advanced (6)	Average (4)	Basic/rudimentary (2)
<ul style="list-style-type: none"> Integrated/holistic view on all risks (eg, cross-desk, cross-asset class) with real-time connectivity and linked to automatically reconciled data warehouse, full granularity available in drilldown 	<ul style="list-style-type: none"> Integrated view on standard risks across desks and asset classes possible using automated scripts but requiring time lag and integration of data from disparate systems, not enabling full drilldown to all metrics and granularities 	<ul style="list-style-type: none"> Not fully integrated view on all risks, ie, "silo view" (eg, siloed systems with different data inputs and batch processing requiring ad hoc reconciliations). Data aggregation of risks requiring high manual querying/ adjustments (eg, multiple, disjoint, nonstandard data repositories for each geography)

Source: IIF/McKinsey Risk IT/Ops survey

Appendix 4: A look at further findings of the survey

Exhibit I
Survey sample is representative along three main dimensions of analysis

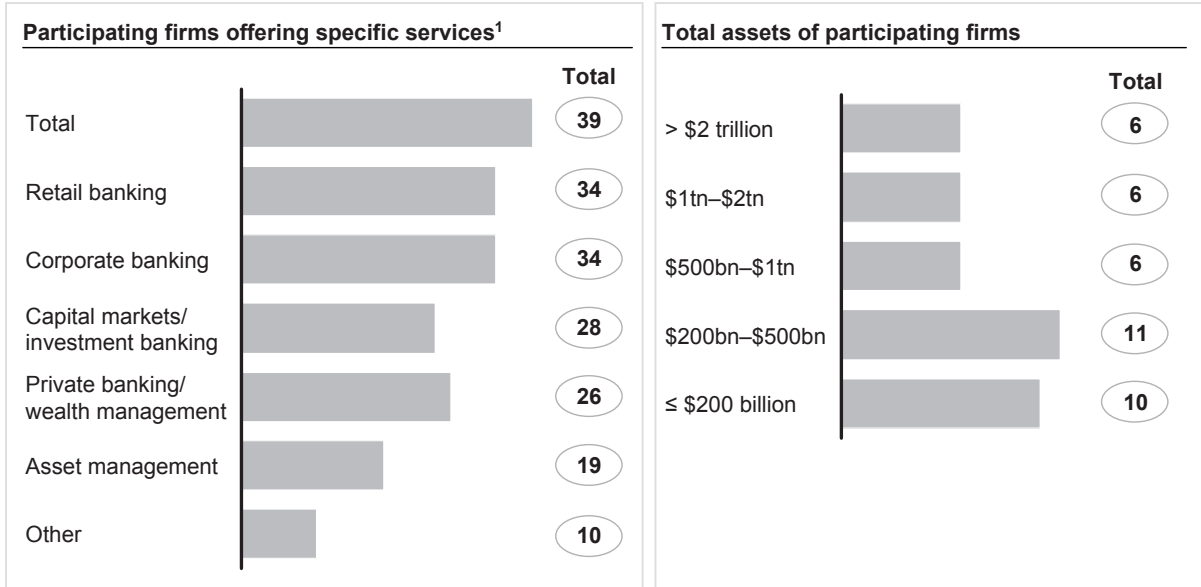


¹ Investment banking.
 Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 2

Survey sample is representative with respect to business lines and size of firms

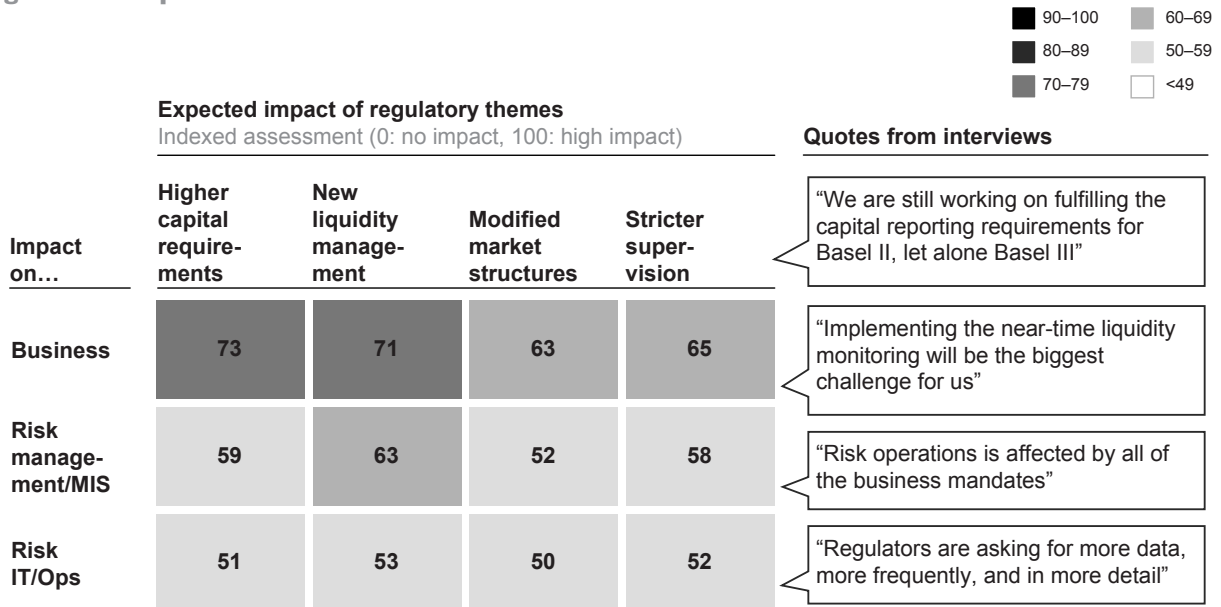
Number of firms



¹ Firms were able to select multiple responses.
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 3

Emerging regulation is expected to have significant impact across the board; greatest impact on the business

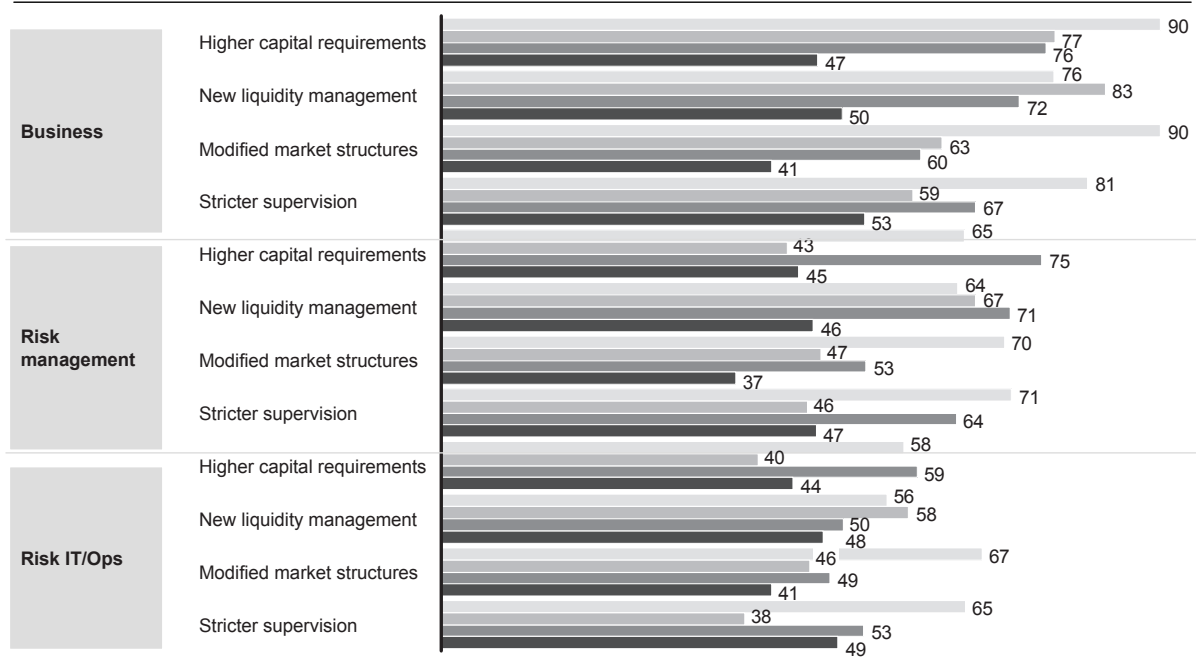
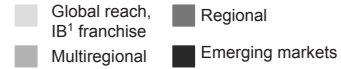


Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 4
Expected regulatory impact in most areas is highest for firms with global reach and an investment-banking franchise

Expected impact of regulatory themes

Indexed assessment (0: no impact, 100: high impact)



1 Investment banking.
 Source: IIF/McKinsey Risk IT/Ops survey

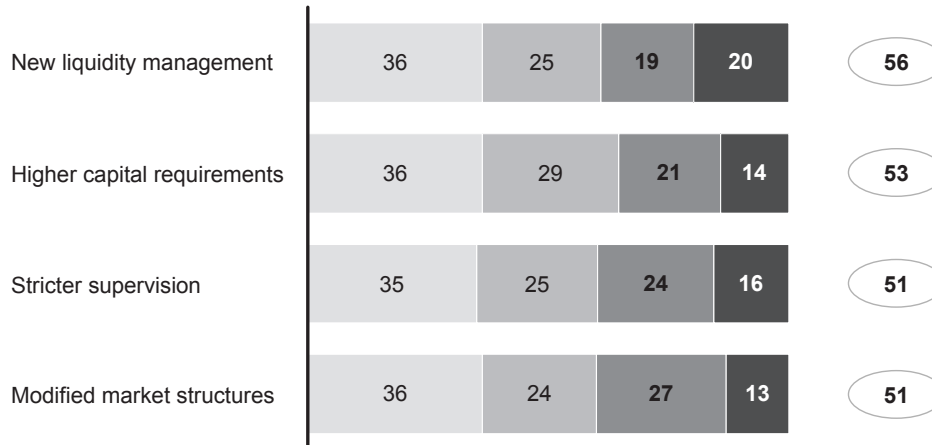
Exhibit 5
Within Risk IT/Ops, new liquidity management is expected to have highest impact



Expected impact of regulatory themes on Risk IT/Ops

%, indexed assessment

Average



Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 6**Firms expect highest impact on Risk IT/Ops in data/integration, applications, and infrastructure****Expected regulatory impact on Risk IT/Ops capabilities**

Rank of firms' assessments, 1 to 6

■ Highest (1 and 2)

■ Lowest (6)

	Peer group				Main location				Business model		
	Global	Multi-regional	Regional	Emerging markets	Asia	Europe	North America	Other	Retail-heavy	IB ¹ -heavy	Balanced hybrid
Data/integration	1	1	1	1	1	1	1	1	1	1	1
Applications	2	3	2	3	4	2	2	3	2	2	2
Infrastructure	3	2	5	2	2	3	5	2	3	4	3
Risk operations	4	4	4	4	3	4	3	4	4	3	4
Risk org/governance	5	5	3	6	6	5	4	5	5	5	5
IT org/governance	6	6	6	5	5	6	6	6	6	6	6

1 Investment banking.

Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 7**Data and integration expected to be worst affected; risk and IT governance least**

■ Low (0–37.5) ■ Moderately high (62.5–87.5)
 ■ Moderately low (37.5–62.5) ■ High (87.5–100)

Expected impact of regulation on Risk IT/Ops capabilities

%, indexed assessment

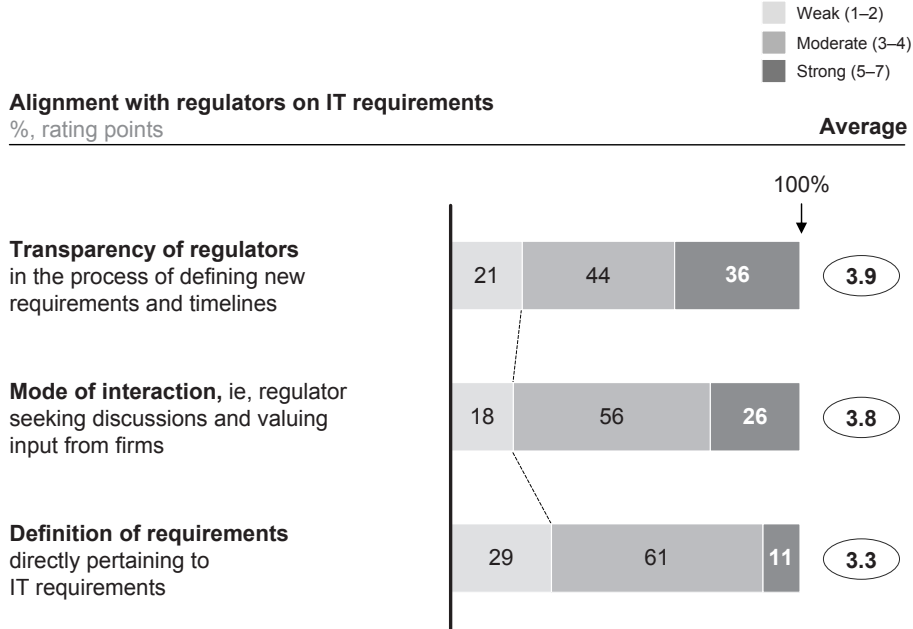
Average

Data/integration	28	21	26	24	60
Applications	31	27	25	16	55
Infrastructure	35	26	26	14	53
Risk operations	34	28	25	13	53
Risk organization/governance	41	29	17	13	48
IT organization, governance, and security	46	24	18	11	45

Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 8

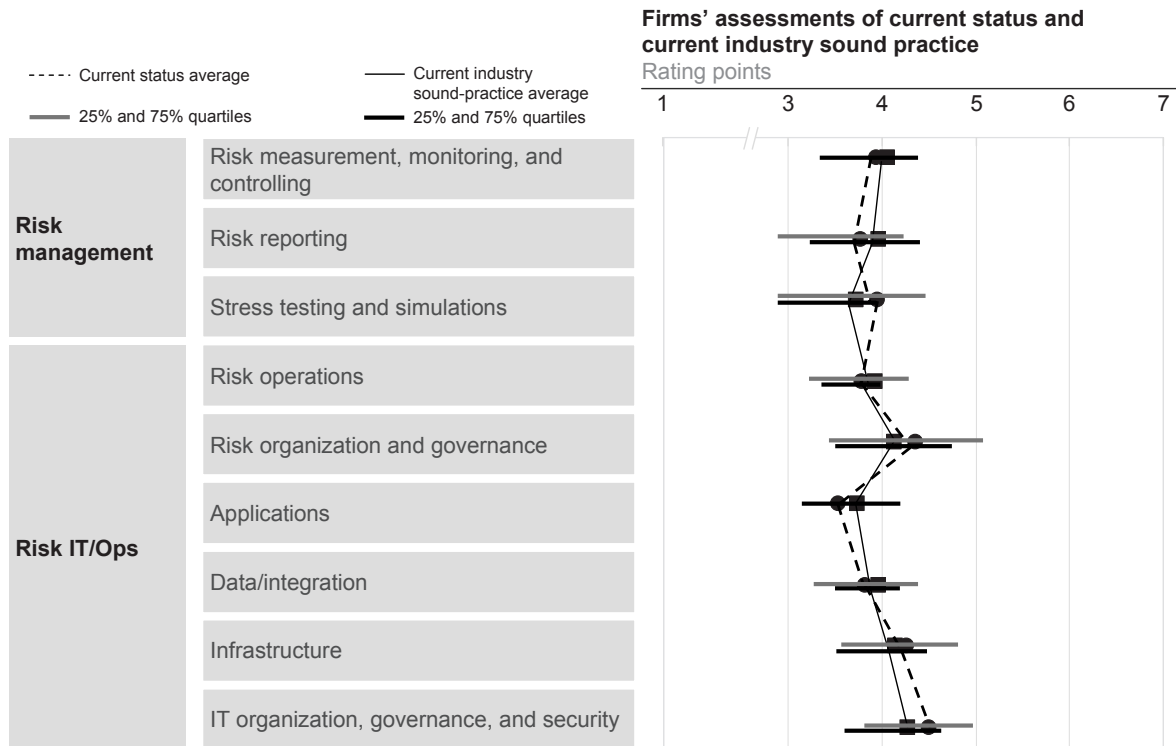
Firms satisfied with transparency of regulators; concerned about lack of specificity of IT requirements



Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 9

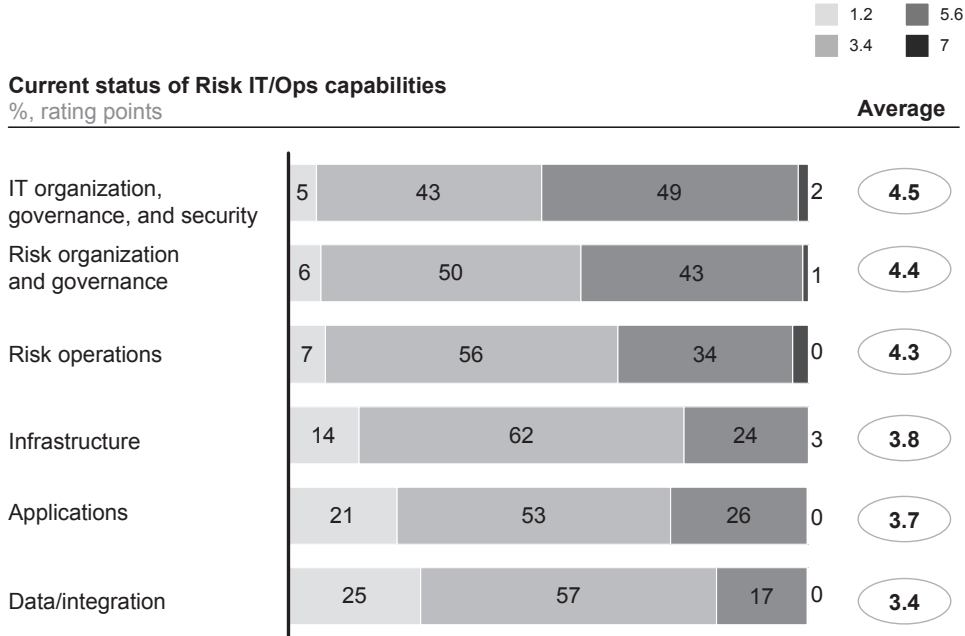
Firms assess themselves in line with perceived industry standard



Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 10

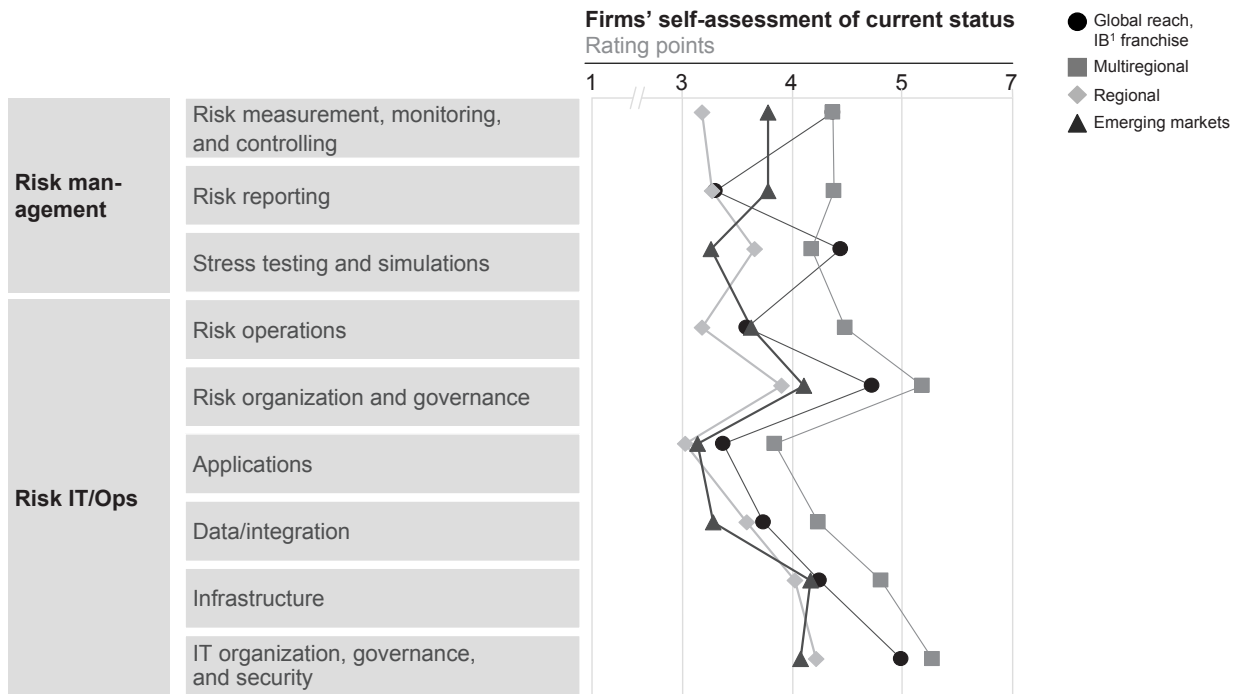
Governance well developed; applications, data/integration, and risk operations lowest rated



Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 11

Multiregional firms rate highest in self-assessment of current status

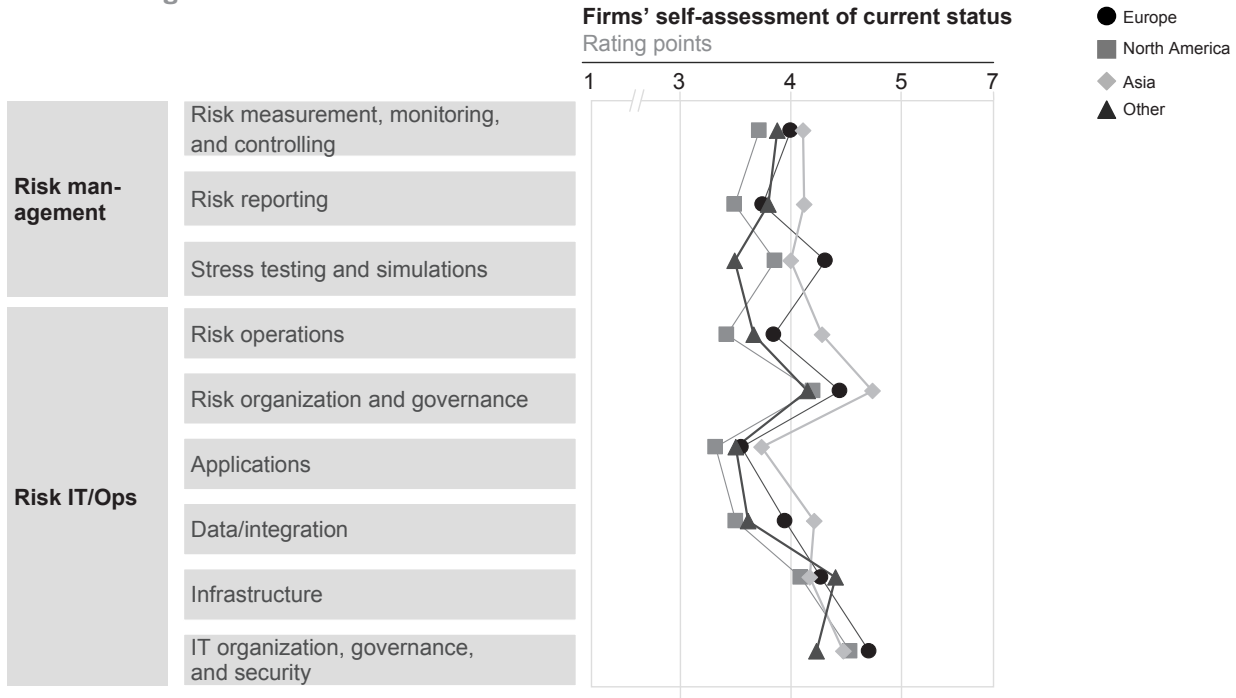


1 Investment banking

Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 12

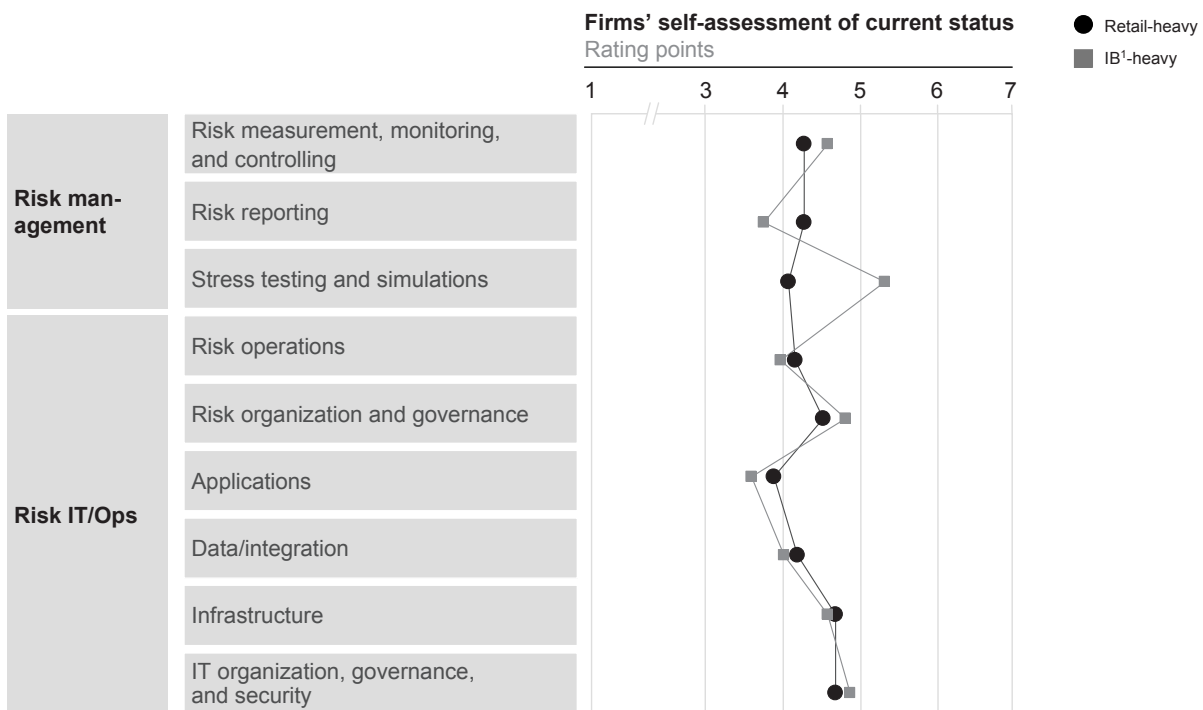
Regional differences in current status are small in Risk IT/Ops, bigger in risk management



Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 13

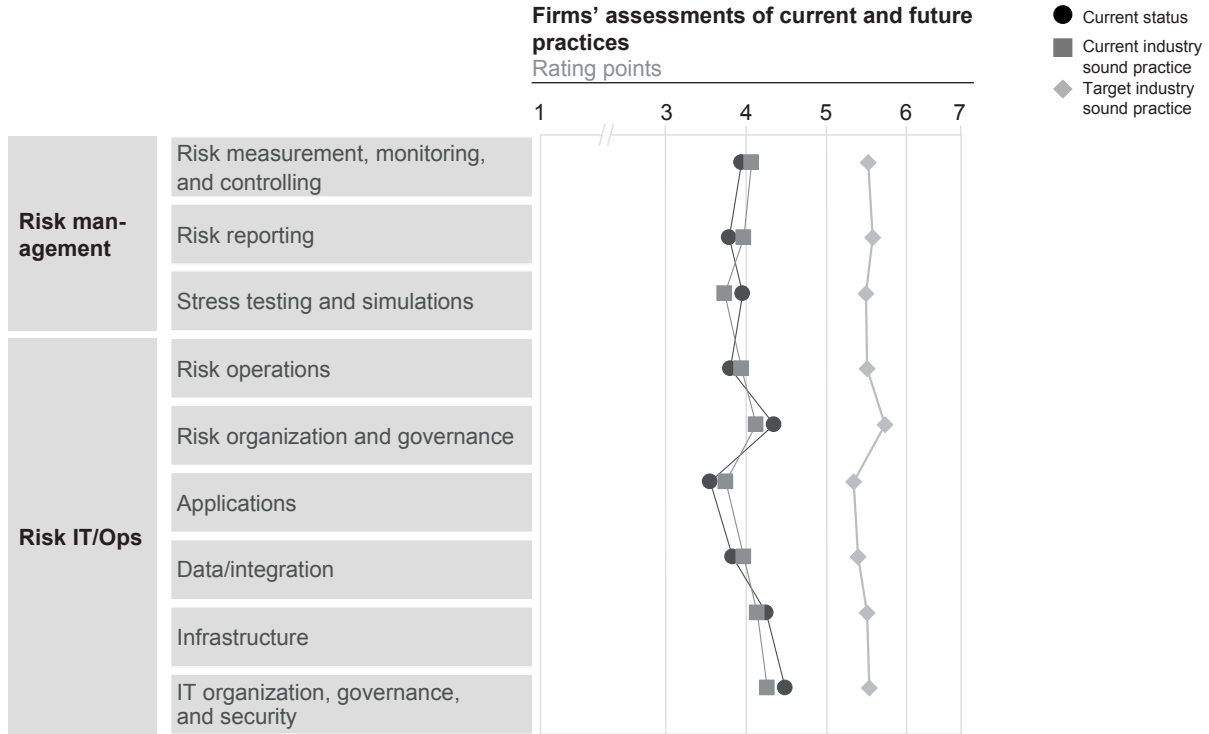
Simulation capabilities thought more advanced at investment banking-heavy firms



¹ Investment banking

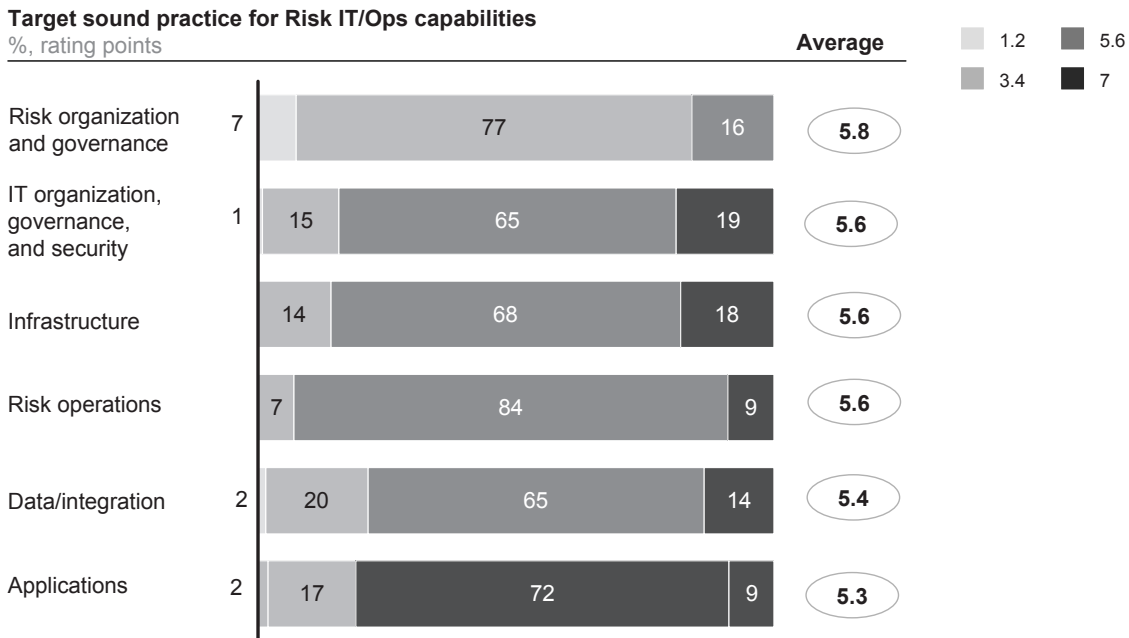
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit I4
Gaps to target sound industry practice reflect high ambitions



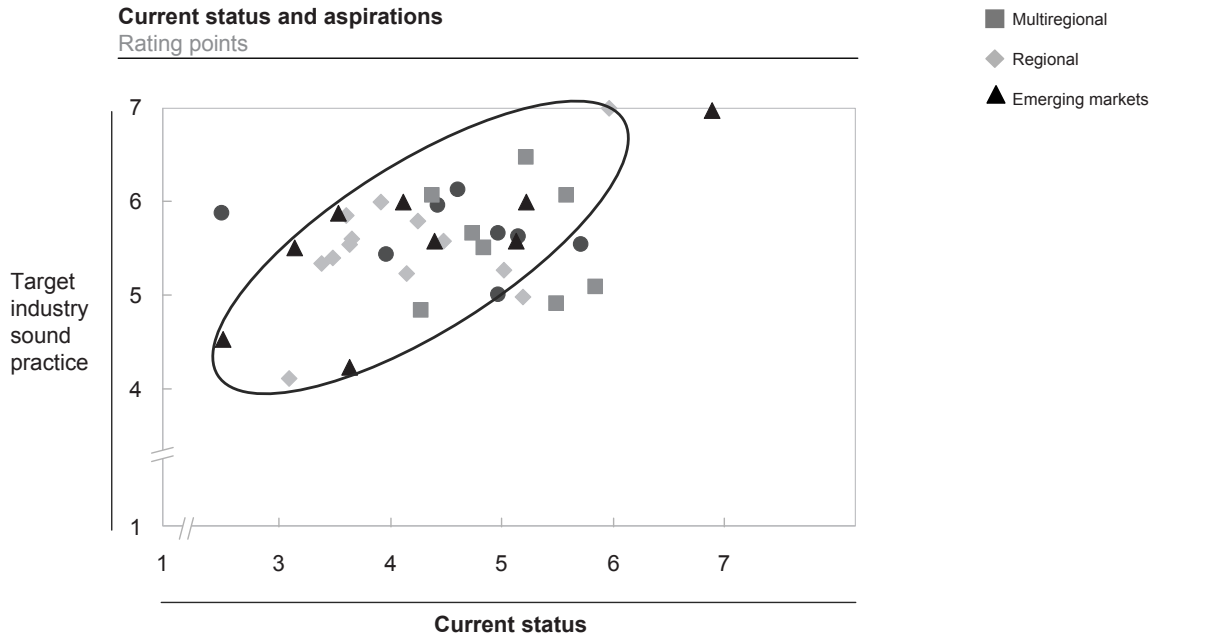
1 Investment banking
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit I5
Highest aspirations are in risk governance



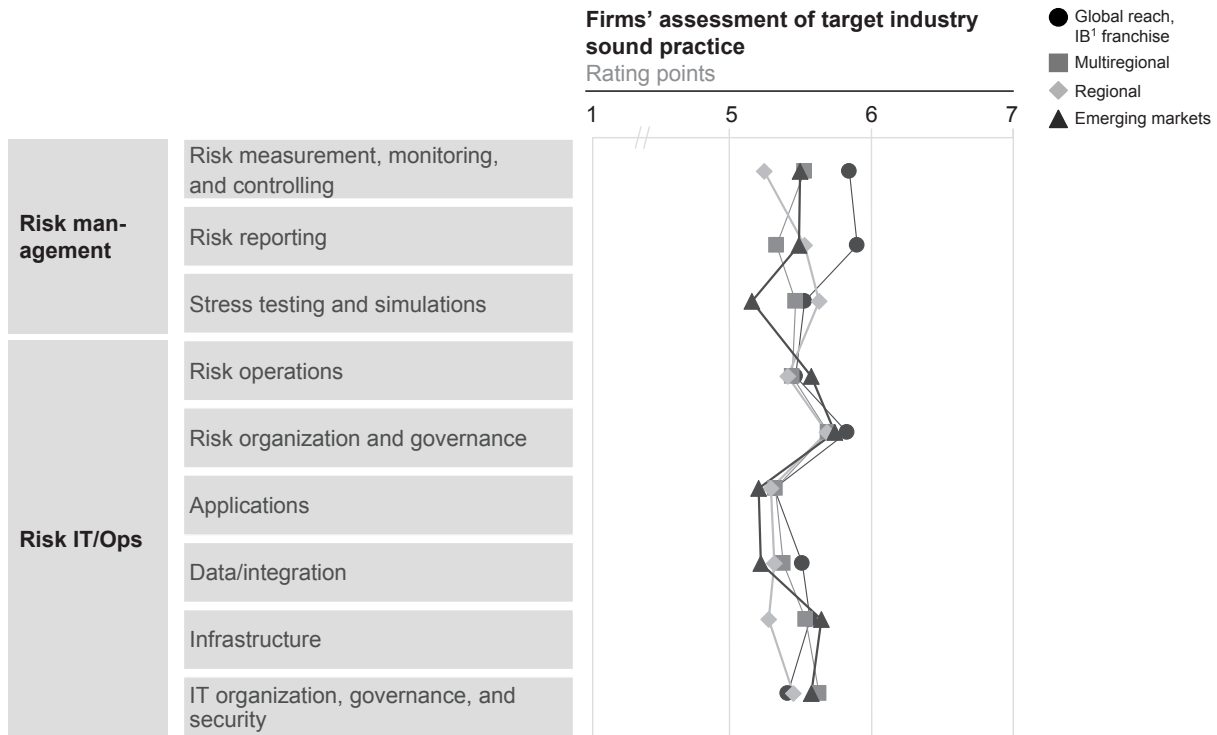
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 16
Firms with highest current status have highest expectations



1 Investment banking.
 Source: IIF/McKinsey Risk IT/Ops survey

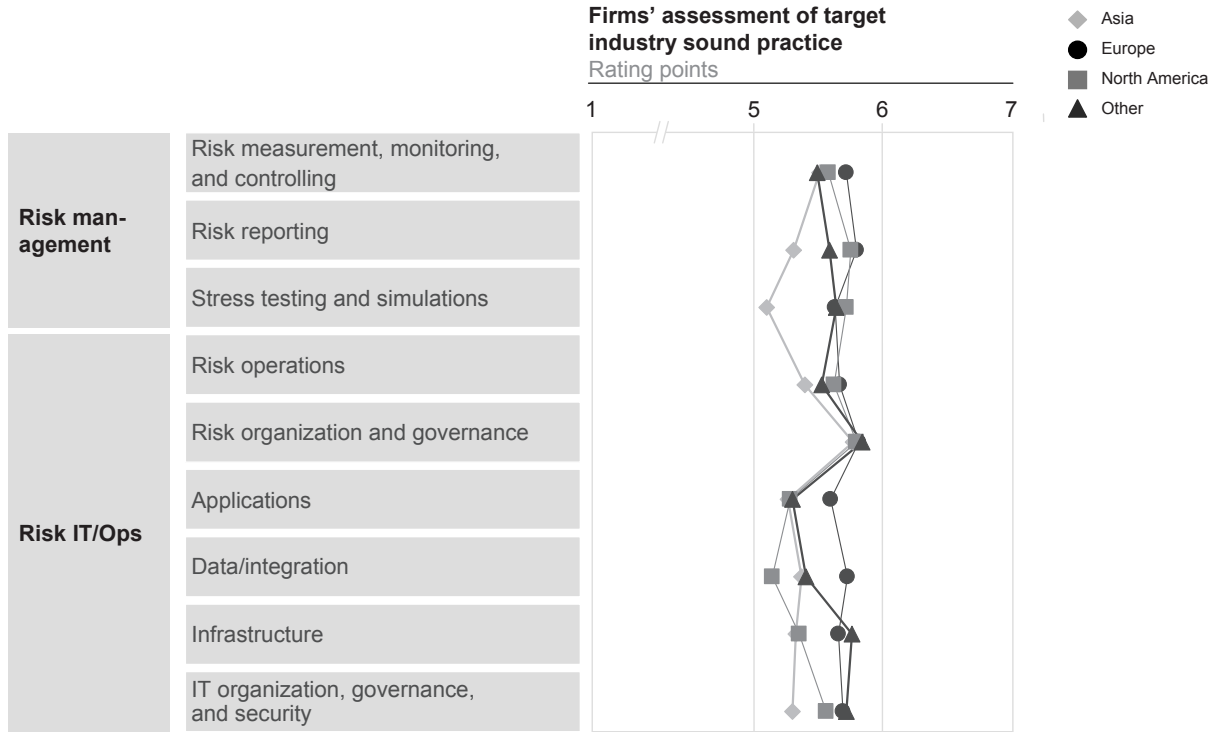
Exhibit 17
Global firms with investment-banking franchise have highest expectations



1 Investment banking
 Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 18

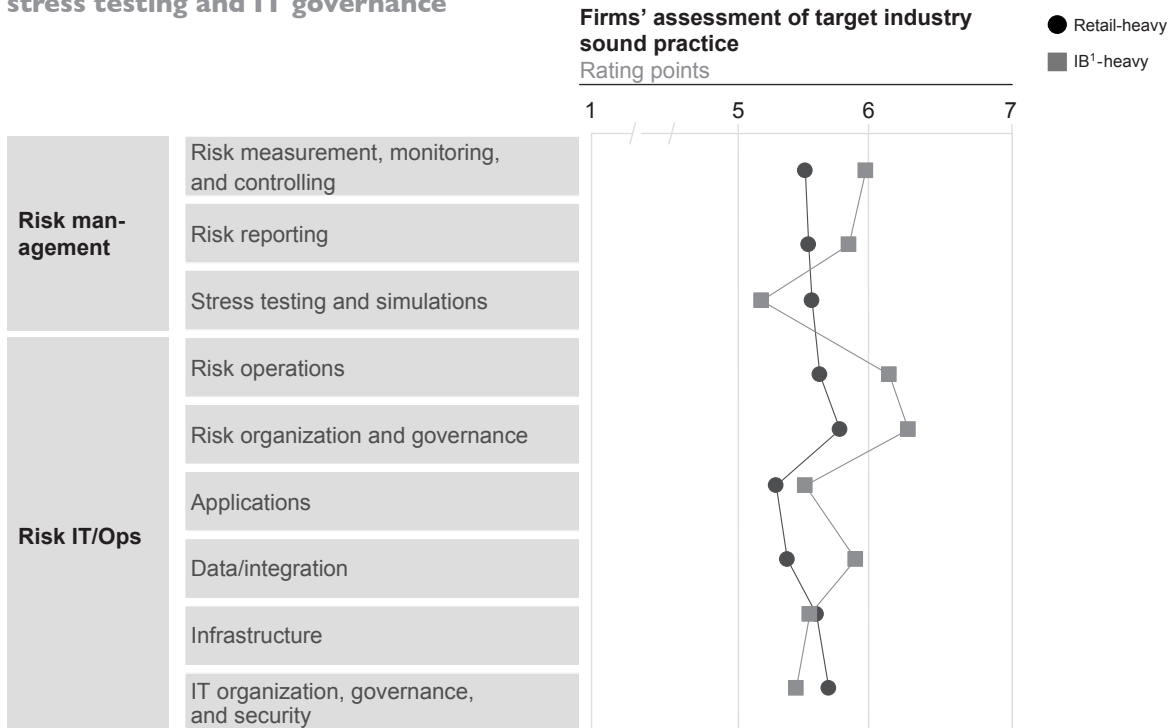
Asian firms have slightly lower expectations, especially in risk management



Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 19

Investment banking-heavy firms have higher expectations than retail firms, except in stress testing and IT governance



¹ Investment banking.

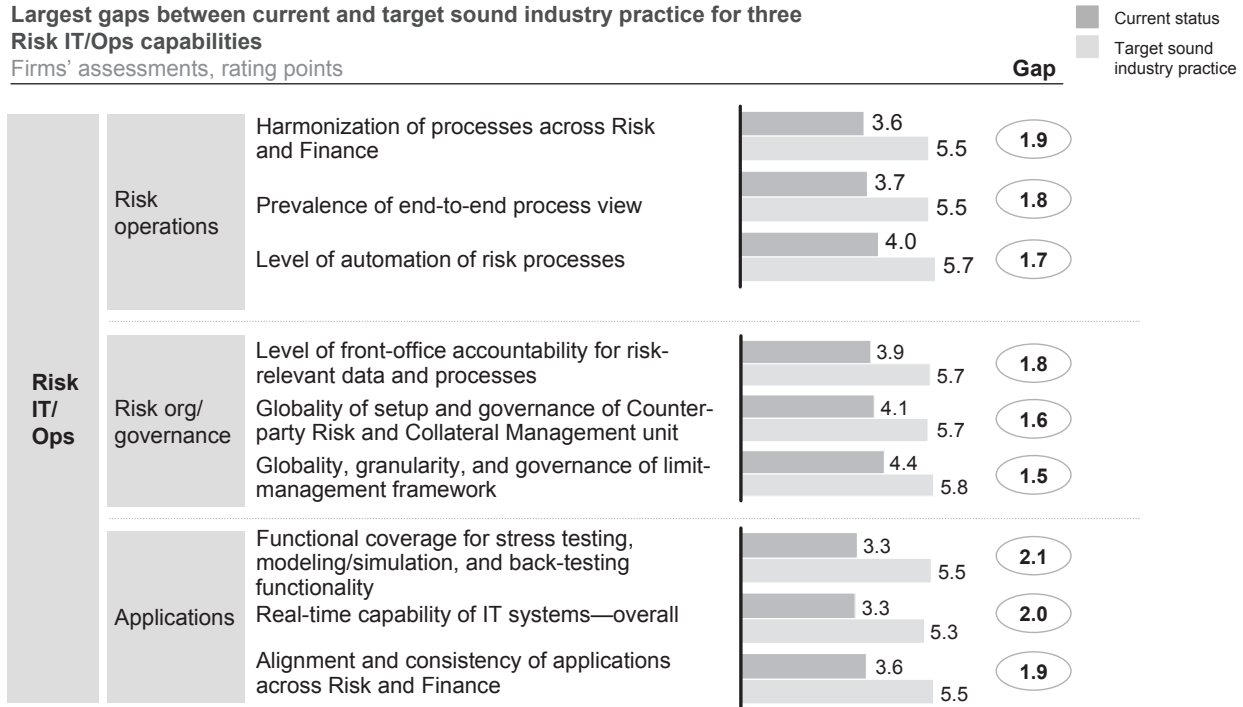
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 20

Largest gaps in risk operations, risk organization and governance, and applications

Largest gaps between current and target sound industry practice for three Risk IT/Ops capabilities

Firms' assessments, rating points



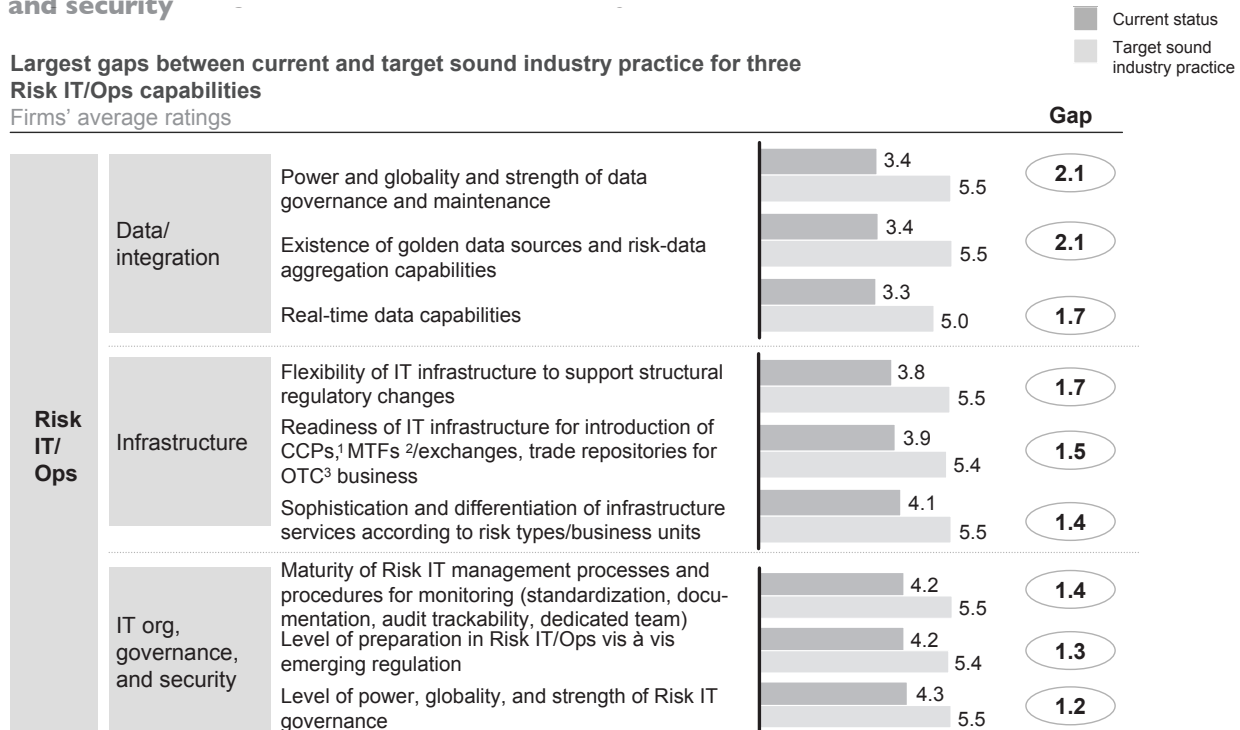
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 21

Largest gaps in data/integration, infrastructure, and IT organization, governance, and security

Largest gaps between current and target sound industry practice for three Risk IT/Ops capabilities

Firms' average ratings



1 Central counterparties.

2 Multilateral trading facilities.

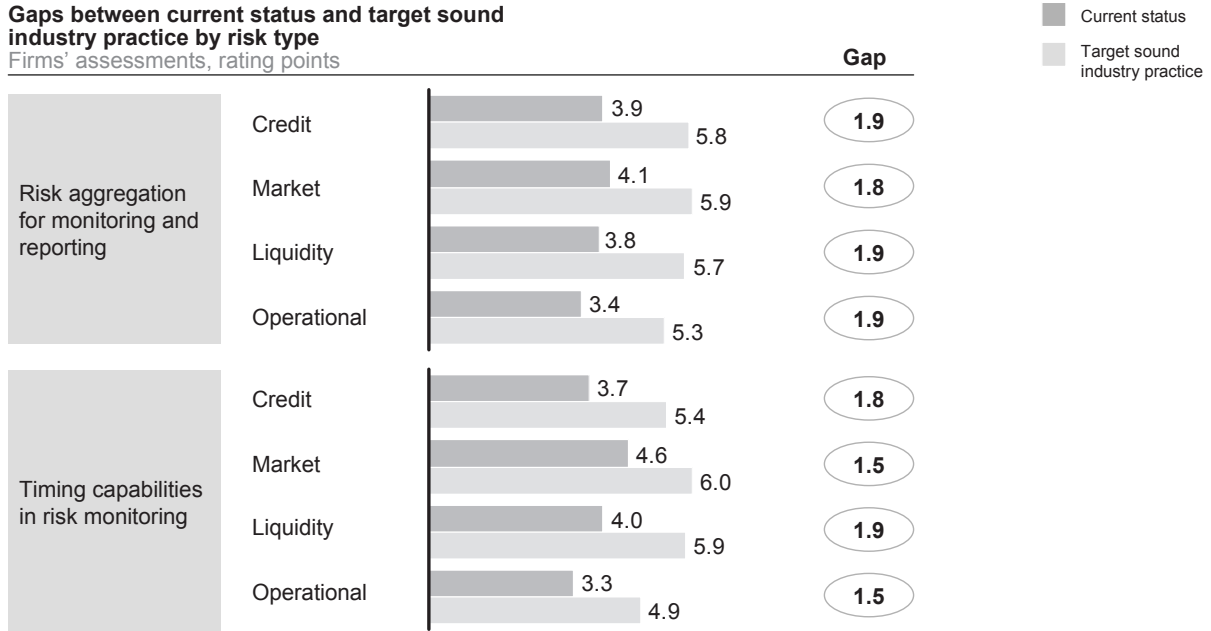
3 Over the counter.

Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 22
Gaps by risk type in risk aggregation and risk monitoring

Gaps between current status and target sound industry practice by risk type

Firms' assessments, rating points

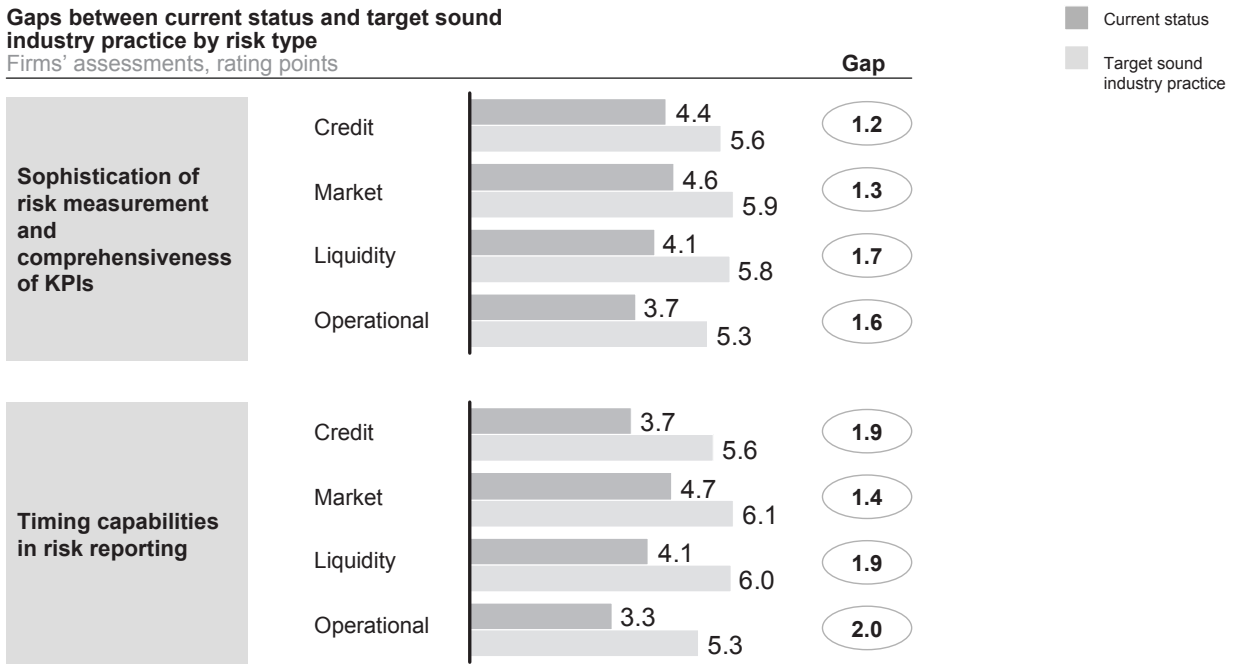


Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 23
Gaps by risk type in risk measurement and risk reporting

Gaps between current status and target sound industry practice by risk type

Firms' assessments, rating points



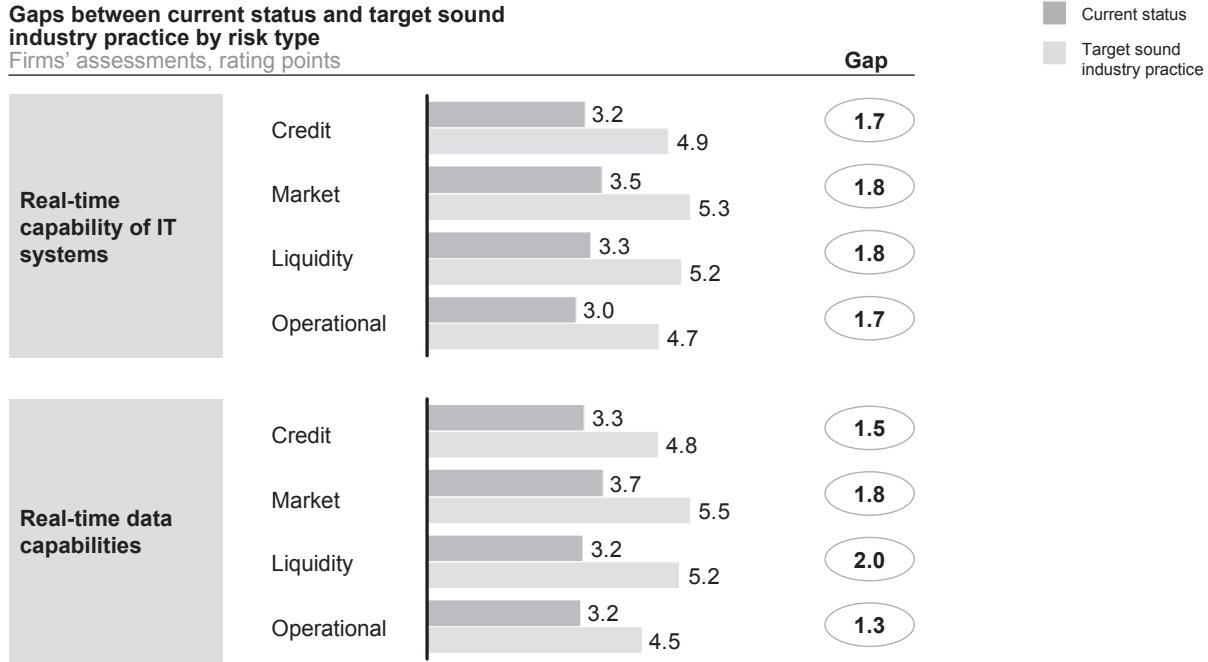
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 24

Gaps by risk type in real-time capabilities of systems and data

Gaps between current status and target sound industry practice by risk type

Firms' assessments, rating points



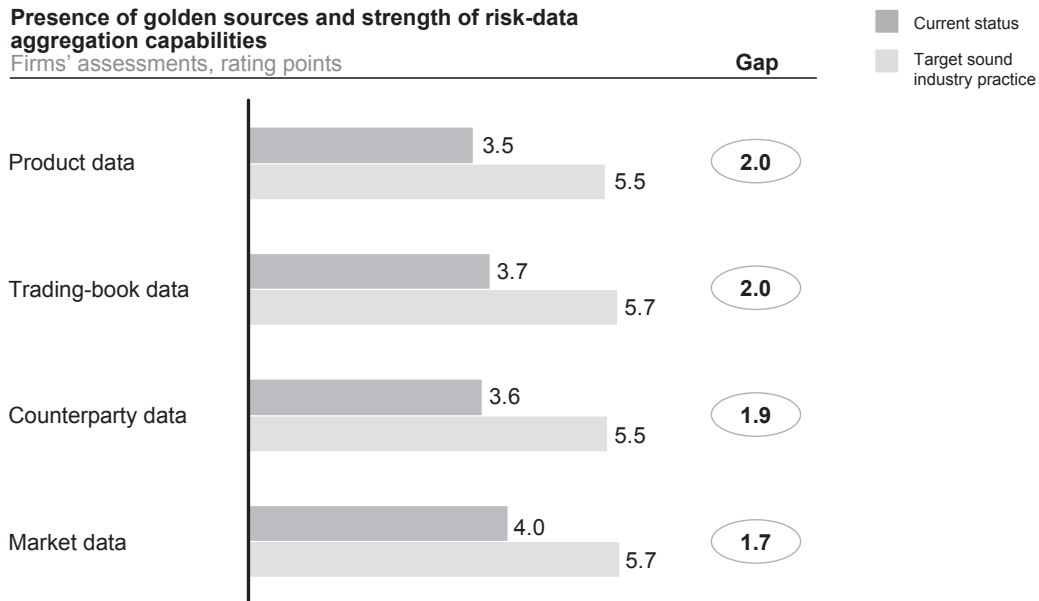
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 25

Golden sources and aggregation capabilities most developed in market data; aspirations are high across the board

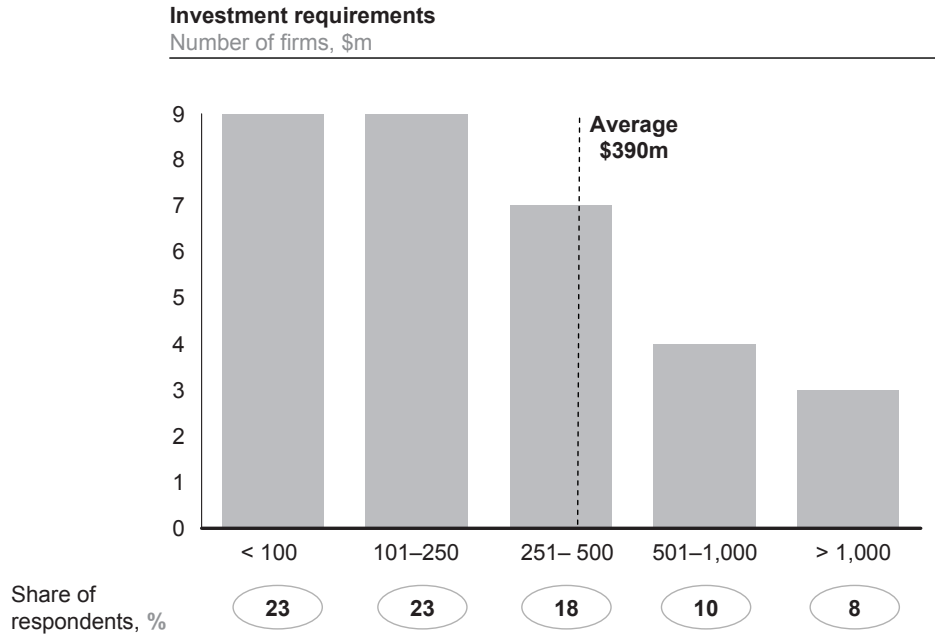
Presence of golden sources and strength of risk-data aggregation capabilities

Firms' assessments, rating points



Source: IIF/McKinsey Risk IT/Ops survey

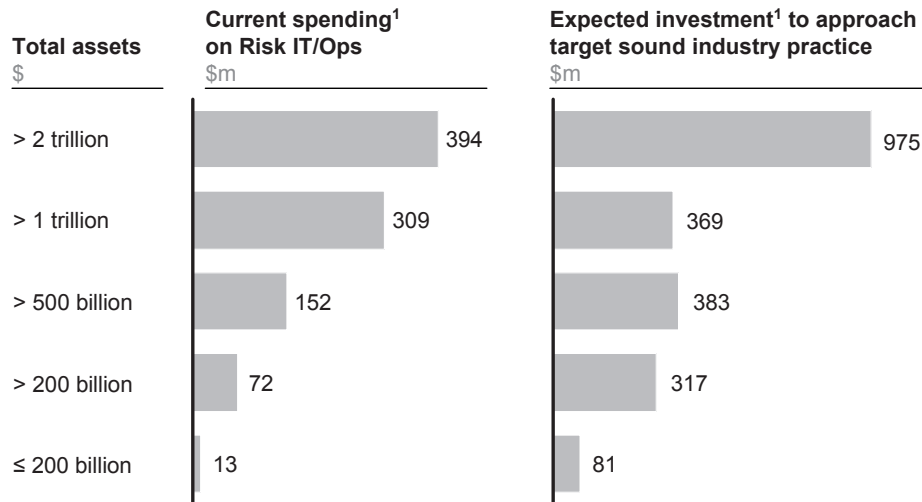
Exhibit 26
Range of firms' expected investments in Risk IT/Ops



Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 27
Current spending is related to size, but planned future investment is less correlated.

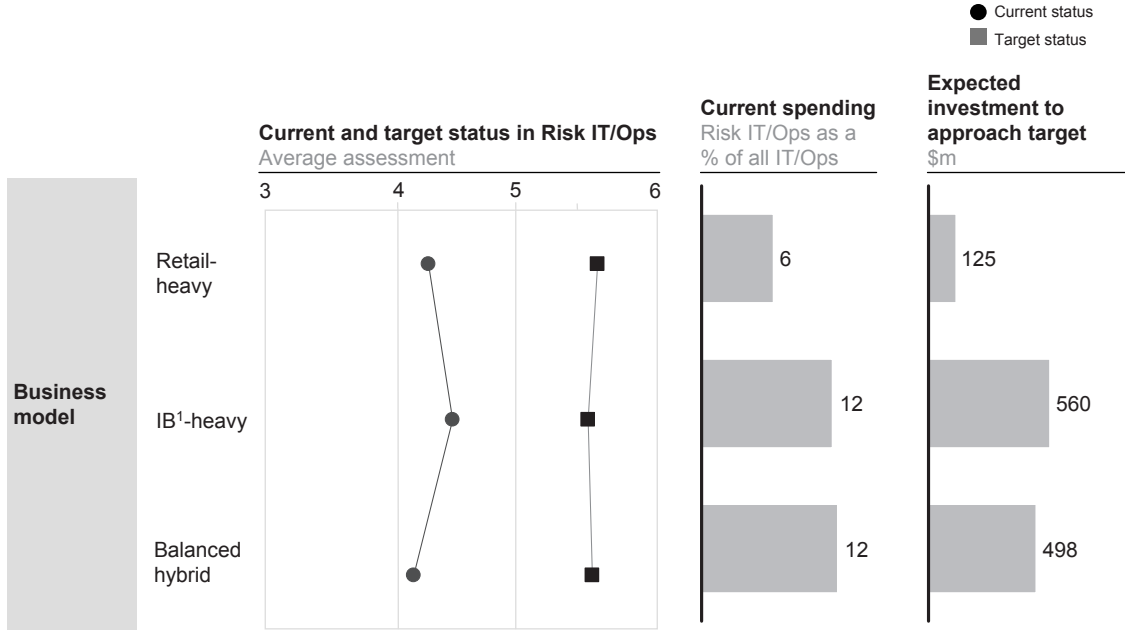
Unit of measure



¹ Current spending and expected investment calculated based on midpoints of ranges provided in survey questions.
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 28

At present, retail-heavy firms spend least, investment banking-heavy firms spend most; trends expected to continue



¹ Investment banking
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 29

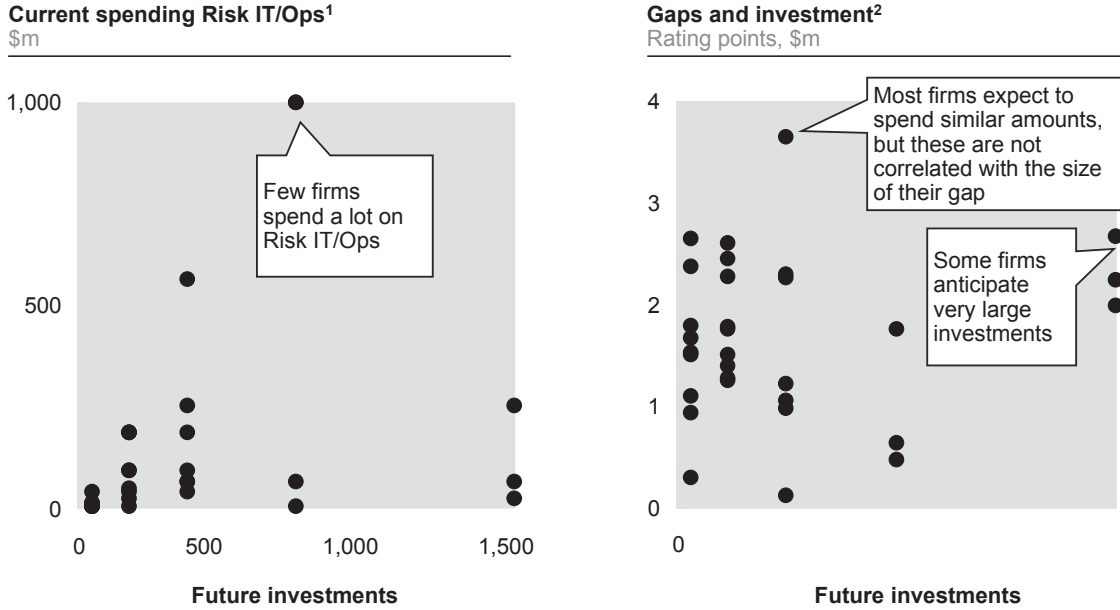
Multiregional firms believe they are advanced; firms with global reach plan to spend most



Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 30

Planned investment is not correlated with either current spending or size of gap to target sound industry practice



1 Calculation based on midpoints of interval scale.
 2 Gap between participants' current status and their expected industry sound practice.
 Source: IIF/McKinsey Risk IT/Ops survey

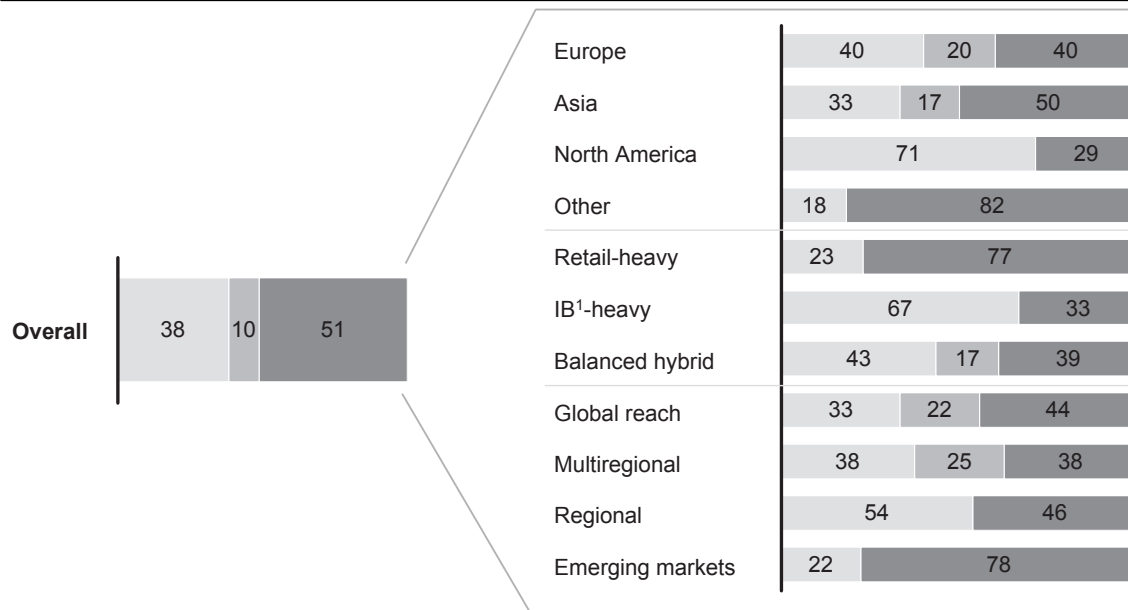
Exhibit 31

Most firms expect benefits to outweigh costs; some variation among geographies and business models

Unit of measure

Expected payoff from investment to approach target practice
%

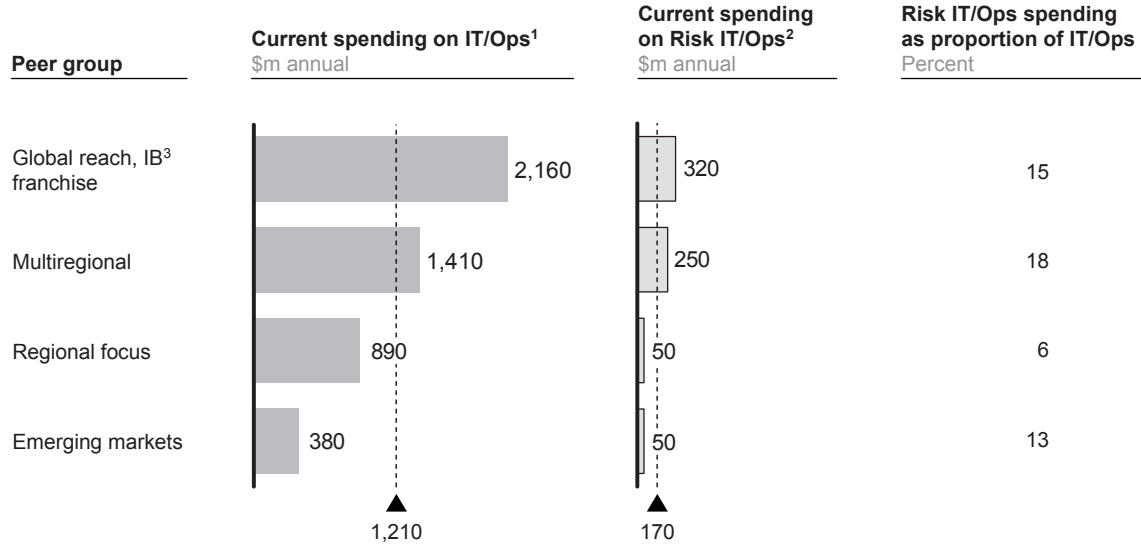
- Do not know yet
- Will not pay off
- Will pay off/more than pay off



1 Investment banking.
 Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 32

Participating firms spend on average approximately \$1.2 billion on IT/Ops today, of which roughly \$170 million is on Risk IT/Ops



1 Averages based on midpoints of ranges provided in survey.

2 Survey asked companies to estimate Risk IT/Ops spending as a share of IT/Ops spending.

Averages here are calculated based on midpoint of share multiplied by midpoint of current spending on IT/Ops.

3 Investment banking.

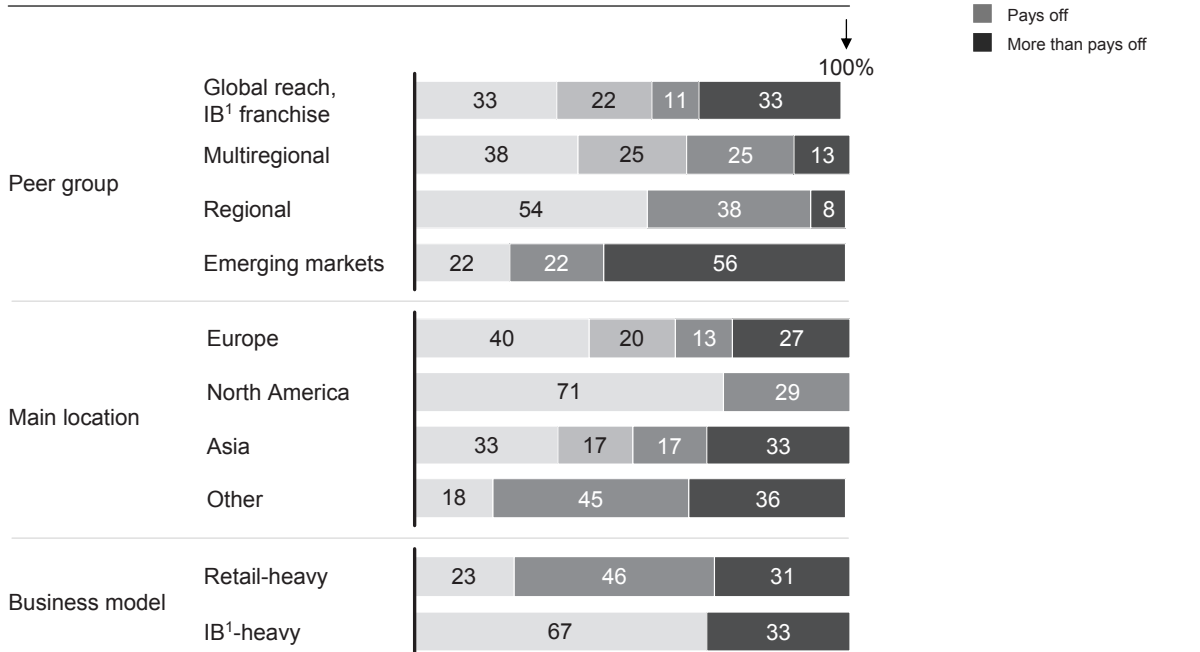
Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 33

Global and emerging-market firms expect highest return on Risk IT/Ops investments

Unit of measure

Expected payoff from investments
%

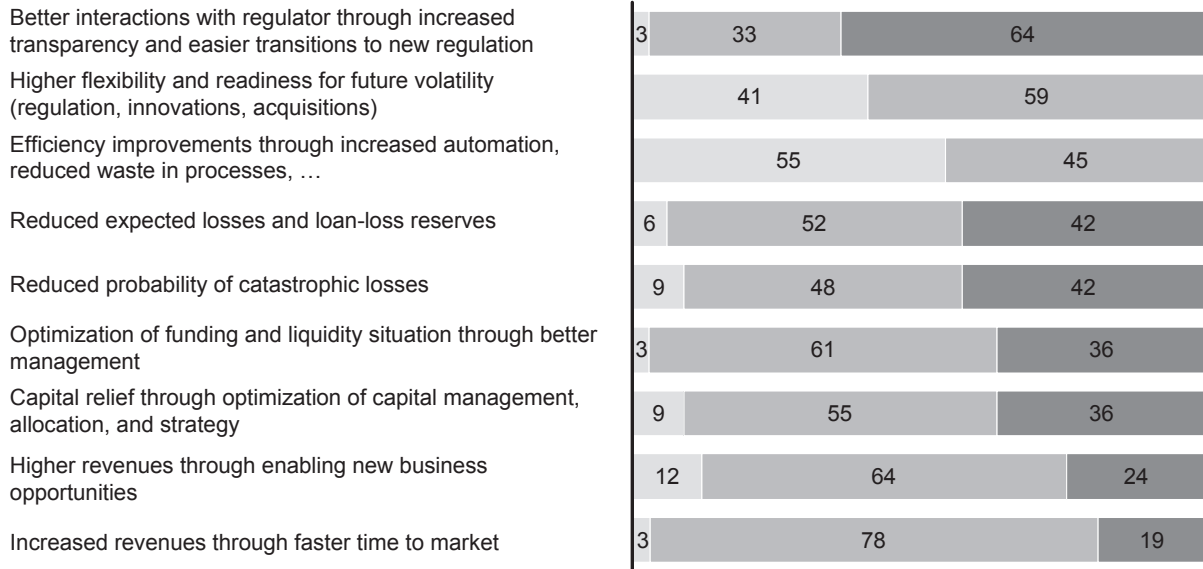
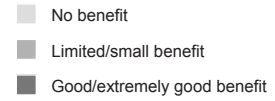


1 Investment banking

Source: IIF/McKinsey Risk IT/Ops survey

Exhibit 34**Firms expect particularly strong benefits from better interaction with regulators and higher flexibility****Expected benefit from investments**

% responding with each rating



Source: IIF/McKinsey Risk IT/Ops survey

↑
100%

Appendix 5. Risk IT/Ops data requirements

This appendix provides an overview of the data that the Risk IT/Ops group at a typical firm must provide to conform to sound industry practice as outlined in this Report. Not all the data are created by Risk IT/Ops systems; some are produced elsewhere in the firm, or externally. The lists provided are intended to be exemplary; not all the data listed are required in every case. The lists are not exhaustive.

The data are presented in two sections. "Portfolio data" provides a list of the data needed to report risk in firms' assets, including loans, securities, and other holdings, and in its liabilities. These data are the basis for the vast majority of risk reports that the firm produces and for queries from supervisors, as well as some key performance indicators that firms must provide.

"New Basel III Risk KPIs" presents a selection of risk KPI measures that the new capital accords have either introduced or put newly in focus.

PORTFOLIO DATA

Data on individual assets and liabilities

- Client/creditor/counterparty identifier
- Product identifier
- Currency and country information
- Contractual terms (for example, maturity, interest rate, seniority of claim, maximum line, covenants, netting-agreement information)
- Value (current and historical; accounting definition)
- Exposure and net exposure (current and historical)
- Profitability data (for example, costs of liquidity, funding, capital)
- Ratings (for example, internal/external rating; current and historical)
- Probability of default (PD), loss given default (LGD), value at risk (VAR)
- Liquidity information (for example, liquidity coverage ratio (LCR) weight, days needed for sale, outflow likelihood within given period of time)
- Hedges and funding that are specifically linked to a particular asset or liability
- Assigned collateral

Data on clients, creditors, and counterparties

- Unique identifier
- Affiliation or relationship with other clients/creditors/counterparties (for example, subsidiary/parent)

- Demographic data for private individuals
- Industry/company information for corporate counterparties, including financial ratios
- Delinquency history and status (for example, missed payments, current default status, restructuring status)
- Risk limits (for example, per product, per country)
- Limit utilization
- Exposures (total, per product, over time, and other views)
- Rating, PD
- Posted collateral

Collateral

- Unique identifier
- Type (e.g., securities, real estate, cash, guarantee)
- Value estimate (for example, for real estate, last appraised value and date of appraisal)
- Links to exposure and counterparty

NEW BASEL III RISK KPIS²⁹

New Basel III Risk KPIS	Short description
New capital definitions and target ratios	<ul style="list-style-type: none"> ■ Stricter definition of Tier I and core Tier I capital (for example, deductions of deferred tax assets, investments in unconsolidated financial institutions) ■ Core Tier I capital-ratio requirement of 7 percent (4.5 percent of core Tier I capital and a required capital conservation buffer of 2.5 percent) ■ Broader requirement for all Tier I capital is set at 8.5 percent; this includes the core Tier I minimum of 7 percent and a minimum of additional (noncore) Tier I capital of 1.5 percent

²⁹ This is an indicative list, for illustrative purposes only. It should not be considered complete for actual implementation purposes, which may vary by country. Sources: Basel Committee on Banking Supervision (BCBS), "Basel III: International framework for liquidity-risk measurement, standards, and monitoring," December 2010; BCBS, "Basel III: A global regulatory framework for more resilient banks and banking systems," December 2010; BCBS, "Revisions to the Basel II market-risk framework," February 2011; McKinsey & Company, "Basel III and European banking: Its impact, how banks might respond, and the challenges of implementation," November 2010. Citations are drawn from the official documents.

<p>Net stable funding ratio (NSFR)</p>	<ul style="list-style-type: none"> ■ Goal: “Promote resilience over a longer time horizon by creating additional incentives for banks to fund their activities with more stable sources of funding on an ongoing basis” ■ Introduction planned for January 1, 2018 ■ The available amount of stable funding must be greater than the required stable funding, over a one-year time horizon under specified stress scenarios ■ Basel III weights determine the stable funding required to support them. Weights depend on their liquidity characteristics (less liquid assets have a higher weight and require more stable funding) ■ Basel III lays out rules to determine whether and by how much equity and liabilities count toward available stable funding ■ “The NSFR should be calculated and reported at least quarterly”
<p>Liquidity coverage ratio (LCR)</p>	<ul style="list-style-type: none"> ■ Goal: “Promote short-term resilience of a bank’s liquidity-risk profile by ensuring that it has sufficient high-quality liquid assets to survive a significant stress scenario lasting for one month” ■ Introduction planned for January 1, 2015 ■ At any given point, the stock of high-quality liquid assets must be greater than total net cash outflows over the next 30 calendar days ■ Basel III lays out rules to determine whether assets count as “high-quality liquid assets,” including haircut requirements ■ Total net cash outflows are defined as total expected cash outflows minus total expected cash inflows in a specified stress scenario for the subsequent 30 days. Basel III provides rules to calculate expected cash outflows for liabilities and expected cash inflows for assets ■ “The LCR should be reported at least monthly, with the operational capacity to increase the frequency to weekly or even daily in stressed situations at the discretion of the supervisor”

Further liquidity/funding monitoring metrics specified by the Basel Committee on Banking Supervision (BCBS)	<ul style="list-style-type: none"> ■ Contractual maturity mismatch: “Contractual cash and security inflows and outflows from all on- and off-balance-sheet items, mapped to defined time bands based on their respective maturities” ■ Concentration of funding: Funding liabilities sourced from each significant counterparty, product, and instrument relative to the total balance sheet; list of assets and liabilities by significant currency; all split for different time horizons ■ Available unencumbered assets: “Assets that are marketable as collateral in secondary markets and/or eligible for central banks’ standing facilities,” that is, assets with the potential to be pledged as collateral to raise additional secured funding; by currency and with estimated haircut ■ Separate LCRs for each significant currency
Credit-valuation adjustments (CVA) capital charge	<ul style="list-style-type: none"> ■ Additional capital charge for potential mark-to-market losses because of decreasing creditworthiness of a counterparty (as seen, for example, in a rise in credit-default-swap spreads of an over-the-counter (OTC) derivative counterparty)
Stressed VAR	<ul style="list-style-type: none"> ■ Capital requirements from stressed VAR in addition to standard VAR ■ Includes relevant market factors for stress periods ■ Model inputs include historical data from a period, typically one year, of significant financial stress ■ “As an example, for many portfolios, a 12-month period relating to significant losses in 2007/2008 would adequately reflect a period of such stress”
Incremental risk charge (IRC)	<ul style="list-style-type: none"> ■ Capital charge for default and migration risks in unsecuritized credit products in the trading book

	<ul style="list-style-type: none"> ■ Rationales: Take appropriate account of the longer-term credit-risk exposure in banks' trading books inherent in some illiquid products that is not reflected in short-term VAR calculations; reduce the incentive for regulatory arbitrage between banking and trading books
Comprehensive risk measure (CRM)	<ul style="list-style-type: none"> ■ IRC for correlation trading activities
Wrong-way risk	<ul style="list-style-type: none"> ■ Arises when creditor rating and position or collateral share a common risk factor; for example, country risk. As the risk increases, the value of the position or collateral declines, as does the counterparty credit quality ■ Basel III requires that stress testing/scenario analyses identify risk factors that give rise to wrong-way risk and assign additional capital requirements
Leverage ratio (under discussion)	<ul style="list-style-type: none"> ■ Ratio of assets to the bank's capital ■ Basel III specifies the calculation of assets ■ Leverage ratio will likely use Basel III definition of Tier I capital

Project team

For the Institute of International Finance:

- Andres Portilla, Director, Regulatory Affairs
- Jermy Prenio, Policy Adviser, Regulatory Affairs
- David Schraa, Regulatory Counsel, Regulatory Affairs
- David Sunstrum, Senior Policy Assistant, Regulatory Affairs

For McKinsey & Company:

- Tommaso Cohen, Consultant
- Amit Garg, Principal
- Philipp Härle, Director
- Holger Harreis, Associate Principal
- Nils Hoffmann, Principal
- Frank Kröll, Consultant
- Suhas Nayak, Engagement Manager
- Peter Orthmayr, Consultant
- Chris Rezek, Engagement Manager
- Hamid Samandari, Director
- Patrick Trutwein, Consultant
- Paul Willmott, Director

Production team

Editor: Mark Staples, McKinsey & Company

Managing Editor: Lucia Rahilly, McKinsey & Company

Copyeditors: Heather Byer, John C. Sanchez, McKinsey & Company

Designer: Jacqui Cook, McKinsey & Company

Acknowledgements

This Report is a synthesis of the ideas of many people. The project team would like to thank all contributors, in particular those who participated in the survey and interviews, as well as numerous discussion partners within the IIF and McKinsey, for contributing their time, energy and insights so generously.

