



**Managing the risks arising from operations is now a central part of every financial institution's compliance obligations. The standards for risk management imposed by Basel II – as well as European and national legislation – mean that banks and other financial services businesses have to ensure that the operational risks that they face are dealt with systematically and on a continuous basis. Operational risk management is no longer a sub-set of other risk categories; it is now a substantial risk category in its own right.**

Risk management is, of course, a critical component of every financial institution's operations, and risk has many dimensions. Cisco's focus is specific: we aim to help banks and financial services businesses achieve positive returns on the investments they make in operational risk management by ensuring that they can:

- a) Achieve organization-wide risk reduction
- b) Simultaneously increase operational capabilities and control the costs associated with operational risk management

#### The impact of Basel II

Basel II incorporates, for the first time, an explicit categorization of operational risk, alongside credit and market risk. Basel II defines operational risk as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events", but it also provides a breakdown of the specific risk categories that give rise to operational risk exposure. These categories are:

- Internal Fraud: examples include employee theft or insider trading on an employee's own account
- External Fraud: examples include robbery, forgery, computer hacking, denial of service (DOS) attacks
- Employment practices and workplace safety: examples include violation of employee health and safety rules and discrimination claims

- Clients, products and business practices: examples include misuse of confidential information and money laundering
- Damage to physical assets: examples include loss or damage to physical assets from natural disasters or man-made events such as terrorism, war, arson and vandalism
- Business disruption and system failures: examples include hardware, software and telecommunications outages, utility failure and problems with real estate facilities
- Execution, delivery and process management: examples include unapproved access to client accounts and outsourcing vendor disruptions or failures.

For most, if not all, of these categories information and communications technology (ICT) has a decisive role to play both in addressing the risk and in creating some of the additional vulnerabilities that banks and financial services businesses face. Fraud and theft, poor management of information, the impact of events such as terrorist attacks or power failures, and more generalized computer or network problems are all wholly or substantially driven by the adoption of new technology so that at the same time that ICT has transformed the financial services industry, it has also created a new set of risk challenges. ICT as a driver of operational risk is explicitly acknowledged in Basel II.

Many different aspects of banks' operations today make them more vulnerable to some of the risk categories that Basel II mentions. As banks expand their global operations, their network requirements have grown with equal speed. Wider communications and IT capabilities are a necessity for banks to provide their clients with the speed of response and round-the-clock working that business in the 21st century requires. But these expanded capabilities can also expose banks to greater risk. For example, it is no longer the case that criminal gangs only need guns and the threat of violence to rob a bank. Physical security is only one aspect of securing a bank's assets, personnel and customers. Criminals are now as likely to employ sophisticated hacking techniques, and as many of the banks can testify, attacks on their systems are frequent, well resourced and clearly organized.

An integrated approach to ICT, using a converged architecture, holds the key to reducing operational risk. This paper sets out Cisco's approach and the way that networking technologies can help financial institutions to reduce their risks whilst at the same time achieving a range of benefits through the implementation of cost-effective solutions to address the four principle areas impacting on operational risk management:

- Business continuity
- Business Security
- Knowledge management
- Recording and archiving

Cisco's solutions are built around the reduction of risk in these key areas, by improving and integrating processes and embedding security. Cisco provides tailored service packages to support customers for operational risk management in the areas of IT operations, security, stability, and availability. Cisco's solutions are, quite simply, focused on providing the means to manage and reduce the operational risks that arise from the four key areas of operations identified above. We work with other vendors and professionals as part of a team to provide holistic operational risk management advice.

#### **Growing threats**

The external threats that banks face have multiplied in recent years. Most obvious is the threat of physical attacks causing extensive destruction of property and, more critically, loss of life. But other threats have also proliferated. Viruses and worms are a constant threat, 'phishing' attacks prey on the security of customer data and criminals use a distributed denial of service attack (DDOS) – or the threat of launching one – to extort money from banks. Malicious attacks and hacking

have progressed from the student hobby of a few years ago to a full-blown criminal industry.

Banks have responded to all of the threats by investing in additional security measures. However, they are also under considerable pressure to manage their costs and to make sure that security does not impair their ability to do business. The tension between these imperatives necessitates a new, integrated approach that will not only allow banks to meet their compliance obligations, but will allow them to achieve additional benefits, streamline operations and control costs.

#### **The rewards of successful operational risk reduction**

Basel II makes it clear that the implementation of measures that will enhance operational risk management capabilities will have a direct impact on capital requirements. A recent study by Morgan Stanley suggests that the upside of compliance with Basel II could be as high as a 40% reduction in minimum capital requirement.

But in addition to those benefits, an integrated approach to reducing operational risk also means improving operational excellence. Operational risk management, rather than being only a matter of compliance, also provides the opportunity for improved business processes, greater responsiveness and improved information.

#### **Achieving Best Practice**

Regulators are promoting 'best practice' as the standards by which banks' operational risk management capabilities will be measured. As an element of market discipline, the publication of regulators' assessments will become a crucial consideration and will have a direct bearing on every bank's competitive advantage. Aspiring to process excellence and best practice is not simply, therefore, an end in itself. It is a commercially-driven strategy that delivers significant commercial advantages.

#### **Managing cost through convergence**

Managing the operational risks that a bank faces are, unlike credit and market risk, associated not with engineering profitability but with costs. By reducing the risk arising from operations, losses can be eliminated or reduced. Successful operational risk management therefore involves addressing some of the key areas of cost that banks face.

In each of the four areas that Cisco approaches to help banks reduce their operational risk management more effectively, there is a critical relationship between cost and capability. For example, converging physical security with IT and network security allows banks not only to considerably reduce their risks but to do so in a cost-effective way that standalone solutions designed to address specific security risks cannot achieve. By using a single converged IP-based architecture to address several areas of operational risks, not only are business processes improved and achieving operational excellence made possible, but the costs of doing so are considerably reduced.

Separate networks for voice, video and data are not only more expensive to maintain, they are inherently limited in the capabilities they offer. A converged

IP network allows secure access to corporate data and communications – including advanced video and e-learning tools – from a wide range of devices -including wireless – enhancing operational risk management and simultaneously achieving gains in productivity.

A converged architecture linking all aspects of a bank's operations – from the data centre to the branch through to the mobile employee – creates a uniformly high level of embedded security across the entire network. Business continuity, too, is substantially enhanced by implementing a converged IP network. Switching data and communications resources from one site to another in the event of a physical attack, and ensuring that critical operations can continue as seamlessly as possible is vital. A converged IP network provides that capability.

Rather than seeing operational risk management as imposing costs, compliance with the requirements of Basel II and the European and national legislation based on its recommendations and standards can provide an opportunity to create competitive advantage. By implementing a strategy based on a converged IP network banks and financial services businesses can address their operational risk management requirements cost effectively and at the same time take advantage of a wide range of benefits that only IP-based converged networks are able to deliver.





**Corporate Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-4000  
800 553-NETS (6387)  
Fax: 408 526-4100

**European Headquarters**  
Cisco Systems International BV  
Haarlerbergpark  
Haarlerbergweg 13-19  
1101 CH Amsterdam  
The Netherlands  
www-europe.cisco.com  
Tel: 31 0 20 357 1000  
Fax: 31 0 20 357 1100

**Americas Headquarters**  
Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
www.cisco.com  
Tel: 408 526-7660  
Fax: 408 527-0883

**Asia Pacific Headquarters**  
Cisco Systems, Inc.  
168 Robinson Road  
#28-01 Capital Tower  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the **Cisco.com Website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic  
Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy  
Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal  
Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden  
Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2005 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and Quick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASST, BPN, Catalyst, CCDA, CCDP, CCIE, CCIW, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IPTV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RouteMUX, ScriptShare, ScriptShare, SlideCast, SMARTnet, SmartView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0502R)