

# JUNIPER NETWORKS SOLUTIONS SUPPORT BASEL II COMPLIANCE

## Enabling FSIs to Mitigate the Operational Risks Inherent in Networked Applications and Dependent Services

### Challenge

Basel II compliance tasks IT departments to mitigate risks across networks and applications, a task that is enormous in scope. Risk mitigation efforts will touch all areas of networking and network security.

### Solution

Juniper Networks products are designed to be resilient, secure and fast, enabling Financial Services Institutions (FSIs) to mitigate risks across their network.

### Benefits

- Fewer technological failures
- Better, faster and more resilient disaster recovery and business continuity options
- Increased security
- Prevention of unauthorized access of IT systems

The Basel II framework of standards regulating how financial institutions must manage their capital reserves in relation to their level of risk is to be widely adopted in 2008. One of the key implications of Basel II is that financial institutions can reduce their capital reserve requirements by reducing their risks, making this capital available for profit generating activities. Organizations must consider and implement multiple strategies to mitigate different kinds of risk while controlling compliance costs without negatively impacting profitability and competitiveness. Mitigating operational risk will be particularly challenging for many organizations, and will require input and leadership from IT management.

Juniper Networks® can help IT managers address operational risks with solutions designed to maximize uptime, enhance security and improve network and application performance. Already widely adopted in financial institutions globally because of superior operational stability and advanced functionality, Juniper solutions deliver the high-performance network infrastructure needed by high-performance businesses to enable the development and deployment of products and services that result in sustained competitive advantage. This document outlines how Juniper can help FSIs improve their operational risk, and thereby influence capital reserve.

### The Challenge

Properly known as the International Convergence of Capital Measurement and Capital Standards—A Revised Framework, Basel II includes recommendations by central bankers and bank supervisors from the Basel Committee on Banking Supervision to revise the international standards for measuring the adequacy of a financial institutions capital reserves. Basel II is expected to be implemented in a large number of countries by 2008. The goal of the accord is to encourage greater consistency in the way financial institutions and regulators evaluate risk management internationally. This goal is divided into three major objectives:

1. Ensuring greater sensitivity to risk in capital allocations
2. Quantifying operational risk and credit risk, and separating them from one another
3. Reducing opportunities for regulatory arbitrage due to variances in economic and regulatory risk

To achieve the objectives above and greater stability in the international financial system, Basel II is constructed on a framework of three “pillars”—minimum capital requirements, supervisory review and market discipline.

## Pillar One: Minimum Capital Requirements

Financial institutions are exposed to three major components of risk: credit risk, operational risk and market risk. Basel II recommends a number of ways of calculating and quantifying each of these types of risk. Capital reserve requirements of each institution are determined according to their levels of risk. This means that the lower an institution's risk, the lower its minimum capital reserve requirement.

## Pillar Two: Supervisory Review

The second pillar addresses regulatory compliance requirements associated with the risks delineated in the first pillar, and provides regulators with methodologies superior to those available today (under Basel I). The second pillar also provides a framework for dealing with all of the other types of risks that banks face.

## Pillar Three: Market Discipline

Market discipline is enforced by increasing the scope of disclosures banks are required to make. Greater visibility into each bank's risk position will enable counterparties to act more appropriately in relation to that bank.

## Operational Risk and the Role of IT

Basel II defines operational risk as "the risk of incurring loss through inadequate or failed internal processes, people and systems, or from external events." Even though this definition excludes risk to an organization's brand equity and reputation risk, it is understood that a significant operational loss could negatively affect a bank's reputation, which in turn leads to the potential for further losses. Though there are a large number of potential operational risks faced by financial organizations, many are clearly within the purview of IT to mitigate including:

- Technological failures of applications, systems and networks
- Unauthorized access and breach of IT systems
- Poor disaster recovery and business continuity planning of IT systems

These and other operational risks are not directly addressed by Basel II, but the accord and related documents have prescribed various standards for implementing operational risk management regimes. One such standard is the adoption and implementation of frameworks describing internal operational controls for mitigating and monitoring risks. Such frameworks, like International Standards Organization (ISO) 17799, Information Technology Infrastructure Library (ITIL) or the Control Objectives for Information and related Technology (COBIT) are not expressly mentioned, but are often already in use by the IT departments of many advanced financial institutions as part of their regular practice and to ensure regulatory compliance. Likewise, Juniper Networks products and solutions already play a significant role in the operations, security and compliance efforts of many financial organizations.

## The Juniper Networks Basel II Compliance Solution

Juniper's family of products enables financial services organizations to mitigate many of the operational risks they face in the operation of networked applications and services upon which they rely. The following solutions represent just some of the ways Juniper Networks can help.

### Mitigating the Risk of Technological Failures

Central to deploying networked applications is ensuring the availability and optimization of adequate capacity to meet required performance needs. In the case of networking, this does not only mean provisioning adequate bandwidth. It also requires ensuring that bandwidth usage is optimized and that other factors impacting traffic, like latency, are minimized or overcome completely. Furthermore, it requires the deployment of network systems with adequate capacity and intelligence to handle fluctuating bandwidth requirements while ensuring the performance levels of traffic according to application requirements.

Juniper Networks solutions are characterized by high performance and capacity:

**Routing platforms** provide layers of availability through redundant components, sub-second failover, and they support BGP multi-homing to overcome Internet service provider (ISP) failure. They are also available in a wide range of configurations and capacities. Whatever capacity specifications are required by the organization, Juniper Networks routers are the highest performing in their class. Routers are also available with comprehensive quality of service (QoS) features to manage and ensure performance levels for critical applications.

**Firewalls** integrate purpose-built hardware and software to enhance operational stability while providing high performance. Juniper Networks firewalls, which are well-known in financial institutions for their enhanced operational stability, provide sub-second failover. Performance-intensive applications like voice and multimedia are accommodated for all sizes of organizations.

Juniper Networks IDP Series Intrusion Detection and Prevention Appliances and Deep Inspection capabilities found in routers and firewalls eliminate threats that can hamper performance and availability, such as worms and Denial of Service (DoS) attacks.

### Preventing Unauthorized Access and Breach of IT Systems

Juniper Networks helps financial organizations implement a layered defense where Juniper solutions defend themselves and network resources at critical points across the organization. This pervasive security protects systems and information from a large variety of attacks originating internally and externally, and aimed at users, applications, data and devices. Many IT security standards like ISO 17799 and COBIT specifically require the implementation of firewalls by organizations connected to the Internet.

Juniper Networks firewalls control bidirectional traffic flows and protect against DoS attacks. They also provide other critical capabilities such as Deep Inspection and antivirus functionality to detect and remove malicious software like viruses from network traffic. Also, Juniper's firewalls can be used to create network security zones that help limit access to areas of the network, making it easier to enforce needs-based access to certain data.

Juniper Networks routers are available with firewall, MPLS and IPsec VPN, and Deep Inspection functionality. Additionally, the routers are themselves secure and are not exposed to the large number of exploits and attacks aimed at competitive routers.

Trusted paths for systems access can be created using a combination of IPsec, SSL and MPLS-based VPNs, and take part in the organization's identification, authentication and access-control processes. Juniper's VPNs can integrate with third-party authentication systems to simplify creating and managing centralized sign-on requirements.

Juniper Networks IDP Series monitors network traffic and detects and blocks malicious traffic in real time. Some of this traffic, like worms, trojans and other malicious software can compromise data, applications and devices across the network. Also, the IDP Series provides comprehensive and detailed logging of network traffic and events for purposes of surveillance logging, and the compilation of violation and security activity reports.

### Disaster Recovery and Business Continuity Planning of IT Systems

The importance of availability and contingency planning, in particular to such customers as financial institutions, is well known to Juniper Networks. In addition to ensuring the availability and performance of systems as described above, organizations must plan for network downtime and degraded service on both small and large scales. For this reason, the stability, resiliency, and high availability (HA) capabilities required by enterprise networking solutions are central to all Juniper Networks products, not only to those designed to provide HA.

Juniper Networks WXC Series Application Acceleration Platforms are specifically designed to facilitate disaster recovery and business continuity. For example, these platforms speed up replication across the WAN, ensuring successful backup and restore to offsite locations while controlling costs. Manual backup is typically subject to high rates of failure and incompleteness, which is problematic for organizations with many remote and branch offices. Since application acceleration solutions enable real-time data replication, organizations can operate backup sites in an active/active mode. This helps ensure IT continuity by establishing backup sites that are up-to-date and properly functioning at all times.

### Summary—High-Performance FSIs Rely on Juniper's High-Performance Networking Solutions

Juniper Networks is an established and innovative networking company with a proven record of success in the global banking and financial services market. Our technology vision is backed by a portfolio of market-leading products. Our financial services customers rely on Juniper in developing and marketing their own competitive products and services. Juniper platforms deliver high-performance networks that provide the operational stability, security and performance that FSIs need to increase customer acquisition and retention, consolidate business units and networks, control costs and increase return on their assets.

### Next Steps

For additional details about the many ways Juniper's routing, security and application platforms help financial institutions address business and networking issues, please visit [www.juniper.net/financial-services](http://www.juniper.net/financial-services).

### About Juniper Networks

Juniper Networks, Inc. is the leader in high-performance networking. Juniper offers a high-performance network infrastructure that creates a responsive and trusted environment for accelerating the deployment of services and applications over a single network. This fuels high-performance businesses. Additional information can be found at [www.juniper.net](http://www.juniper.net).

---

#### Corporate and Sales Headquarters

Juniper Networks, Inc.  
1194 North Mathilda Avenue  
Sunnyvale, CA 94089 USA  
Phone: 888.JUNIPER (888.586.4737)  
or 408.745.2000  
Fax: 408.745.2100  
[www.juniper.net](http://www.juniper.net)

#### APAC Headquarters

Juniper Networks (Hong Kong)  
26/F, Cityplaza One  
1111 King's Road  
Taikoo Shing, Hong Kong  
Phone: 852.2332.3636  
Fax: 852.2574.7803

#### EMEA Headquarters

Juniper Networks Ireland  
Airside Business Park  
Swords, County Dublin, Ireland  
Phone: 35.31.8903.600  
EMEA Sales: 00800.4586.4737  
Fax: 35.31.8903.601

To purchase Juniper Networks solutions, please contact your Juniper Networks representative at 1-866-298-6428 or authorized reseller.

Copyright 2010 Juniper Networks, Inc. All rights reserved. Juniper Networks, the Juniper Networks logo, Junos, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners. Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.