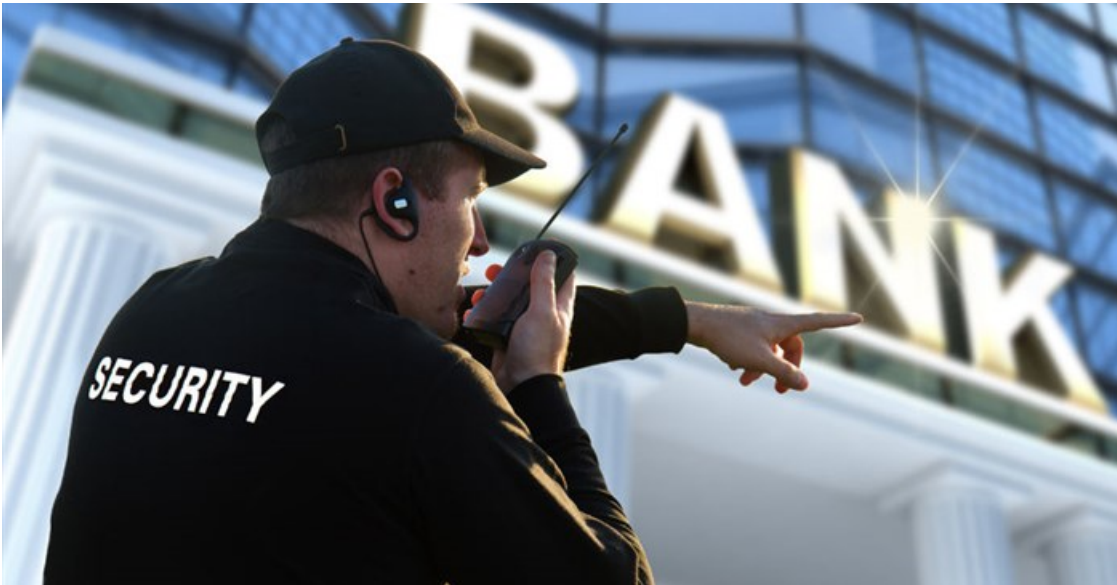


# How IT infrastructure can help banks enable compliance

By [Anurag Aren](#)

16 Oct 2015

Banks and financial institutions must comply with a variety of legislation and frameworks, both locally and globally. A large part of this compliance hinges on better management and mitigation of risk, particularly with regard to the regulations outlined by Basel II (an international business standard that requires financial institutions to maintain enough cash reserves to cover risks incurred by operations) and the impending Basel III.



©santilli via [123RF](#)

Information Technology (IT) infrastructure security has a technical view, but it needs to be looked from banking industry domain eyes and being at the bottom layer of all technology architecture, how will it help banks enable compliance and improve operational risk management.

## Managing IT and operational risk

Many of these regulatory frameworks, including Basel II/III, deals with risks like supervisory review, market regulatory requirements and capital requirements. Capital requirement in turn deals with market risk, credit risk and operational risk. It is the operational risk pillar which require adequate measures and controls to be put into place to identify, assess, track and manage risks. IT Infrastructure, as the foundation layer of the overall architecture, can help to facilitate compliance and improve operational risk management. The IT-related risks would fall under the operational risks category per the Basel Frameworks.

Some of the most common operational risks faced by banks include datacentre disasters, loss of sensitive data due to a breach, network threats and vulnerabilities, file based threats, spyware, human error and downtime of systems. Managing these risks is critical to banking functionality, as inadequate risk management can have serious implications for the organisation. Disaster recovery, intrusion detection and prevention services, data loss prevention, antivirus, anti-spam management, unified threat management and quality management processes are just some of the IT infrastructure security solutions that need to be put into place to provide acceptable risk mitigation.

## Cloud computing, IT risk management and compliance

Cloud computing is one of the most disruptive emerging technology trends, offering a number of benefits including improved flexibility and agility, enhanced cost effectiveness and more. However, within the banking sector, a number of

factors need to be taken into account before cloud computing can be used to better manage these risks.

Financial institutions need to perform extensive calculations (stress testing) using statistical models to assess the financial risks. In addition, the risks and compliance issues around outsourcing need to be understood. These include the impact of a shared services delivery model on regulatory frameworks, the controls that have to be put in place to ensure compliance with the necessary frameworks, and whether or not partners and vendors have adequate controls and policies in place.

Operational risk, as one of the critical elements of compliance, needs to be carefully managed to mitigate potential issues. IT risk management must align with the overall enterprise risk management strategy, and IT risks need to be identified, assessed and managed continuously.

## ABOUT THE AUTHOR

Anurag Aren, head of global infrastructure services, Wipro Ltd.

For more, visit: <https://www.bizcommunity.com>