



DECODER

Basel II Compliance

Basel II Summary

Basel II holds financial institutions accountable for the economic consequences of high operational risk (e.g., the neglect of data security) and reap the economic rewards of lowering operational risk (e.g., the deployment of data security measures).

Basel II defines operational risk as:

“...the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events” (644).

It also states:

“Institutions using the Standardized Approach to calculating operational risk capital must have an adequate operational risk management system in place” (633).

Information security is considered an “operational risk management system” that significantly influences the level of operational risk assess by the Basel Committee.

How CipherOptics Helps

CipherOptics CipherEngine enables Secure Information Sharing across any network, regardless of size, type or topology. Our data security solutions reduce your “operational risk” by utilizing the highest level of encryption to assure your data is secure, confidential and authenticated over internal, shared or third-party networks.

CipherEngine is easy to install, transparent to any network, and allows you to “check the box” on Basel II compliance wherever your data moves.

About CipherOptics

CipherOptics is the leader in network-wide encryption. Offering an innovative policy and key management solution, coupled with high speed, low latency encryption technology, CipherOptics helps their customers mitigate the risk of data leakage, loss and theft over any network.

What is Basel II?

The Basel II Accord proposes methodologies for banks to more accurately calculate the capital provisions they should make against credit, commercial and operational risk. Issued in June 2004, it replaces the outdated Basel I, adopted in 1988 and is currently used in more than 100 countries.

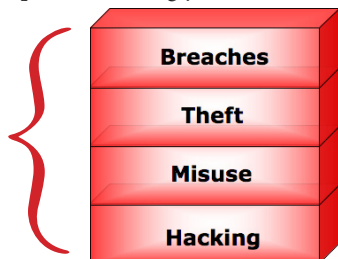
Who is impacted by Basel II?

The Basel II Accord affects all banks and financial institutions whose regulating authority adopts the standards and methods recommended by the accord.

What are the requirements of Basel II?

Financial service organizations must provide disclosures that allow the market to assess its risk position and price accordingly. In addition to the management of credit risk and commercial risk, Basel II mandates an assessment of the institution’s operational risk.

Operational Risk



Basel II defines information security is an “operational risk management system” that significantly influences the level of operational risk. The higher your security risk, the higher your operational risk assess by the Basel Committee. This committee has identified certain operational risks that have the potential to result in substantial losses. These include damage from fiduciary breaches, employee theft, misuse of confidential customer information and computer hacking.

How do companies comply with Basel II?

Basel II requires risk appraisal and control—in short, a “risk management environment.” In order to reduce your operational risk, you must implement robust information security measures, including the protection of critical information traveling on the network. These measures must ensure the confidentiality and integrity of the institution’s data. In order to minimize operational risk, they must also protect customer data from accidental or malicious loss.

Where are companies most vulnerable to security breaches?

Within the perimeter, companies are vulnerable to data theft and security holes caused by misconfigurations and/or OS instability. Data is even more vulnerable when it moves beyond the security perimeter of your network where anyone gaining access to a port can pull down your data. Even private networks are vulnerable; “private” does not mean secure!

Firewalls and other intrusion deterrent systems focus on keeping hackers or cyber thieves out of your network, but they cannot stop these attacks. Authentication is needed to allow access to your network as well as decrypt data on the network. Without the proper credentials no one will be able to steal, break or disrupt your business.

How does CipherOptics help you comply with Basel II?

CipherOptics CipherEngine enables Secure Information Sharing across your network without impacting your network. Our transparent security solutions provide network-wide authentication and data encryption, both considered to be “best practices” for securing information. CipherEngine lowers your “operational risk” by providing authentication and network-wide encryption; protecting your data wherever it goes. Providing this level of security, CipherEngine helps you comply with Basel II requirements. CipherOptics provides your organization with a reliable and proven method of ensuring data confidentiality, integrity, and authentication.

Type	How CipherOptics Helps	Affect on Risk
Fiduciary breaches	CipherEngine encrypts all data and authenticates all traffic on the network	Elimination of risk
Employee theft	CipherEngine cryptographically segments traffic	Significant reduction of risk
Misuse of confidential information	CipherEngine encrypts all data rendering it useless to all but intended recipients	Moderate reduction of risk
Computer hacking	CipherEngine authenticates all traffic on the network	Significant reduction of risk



CIPHEROPTICS
www.CipherOptics.com