

Daniel J. Langin,
Attorney at Law, LLC



Basel II Compliance
with Tripwire

WHITE PAPER ○

Configuration Control for
Virtual and Physical Infrastructures

Contents

- 3 Overview—What is Basel II?
- 4 Three Keys to Information Security Under Basel II
- 4 Mitigating Operational Risk
- 4 Tracking and Centralizing Loss Event Data
- 5 Disclosure Policies, Internal Controls, and Assessment Processes
- 5 Basel II Deadlines and Transition Periods
- 5 Basel II Requirements and the Role of Change Management
- 6 How Tripwire Helps Companies Achieve Basel II Compliance
- 7 Basel II Requirements and Tripwire Solutions
- 8 Other Resources
- 8 About the Author

Overview

As if financial institutions did not have enough compliance worries, a new international standard—Basel II¹—now looms on the compliance horizon. Unlike other laws and standards affecting financial institutions in the US and overseas such as the Gramm-Leach-Bliley Act (“GLBA”), the EU Data Protection Directive and the PCI Data Security Standard, however, the ramifications of this law extend beyond protection of electronic consumer data. Instead, Basel II focuses on the institution’s core functions of evaluating, planning for, and disclosing financial risk.

Overview—What is Basel II?

Basel II is not, strictly speaking, a law or regulation. It is an international banking standard created by the Basel Committee on Banking Supervision, or BCBS. BCBS is an organization made up of central bank and banking regulatory authorities from several European nations, Japan, the UK, and the US, that encourages international cooperation of banking authorities throughout the world and issues guidance on banking supervision. Even though Basel II is not a law or regulation, its terms will ultimately be adopted into legislation or regulation by virtually every nation in the world. In this fashion Basel II will eventually extend to financial institutions worldwide, making it potentially more ubiquitous than any US law or EU Directive.

Basel II consists of three “pillars,” or organizing concepts. These are Minimum Capital Requirements, Supervisory Review, and Market Discipline. The Minimum Capital (Pillar 1) requirements mostly deal with the formulae that financial institutions must use to calculate the minimum capital they need to protect themselves from risk of loss from defaults or other financial losses. The Market Discipline (Pillar 3) requirements mostly deal with procedures to ensure that risky loans and other unwise disposition of assets is avoided. Although Pillars 1 and 3 implicate information

security, the requirements that most affect information security appear in the Supervisory Review (Pillar 2) requirements, especially its Operational Risk provisions. Each Pillar includes three “approaches” to compliance based on increasing levels of sophistication (Basic Indicator Approach, Standardized Approach and Advanced Measurement Approach), and each approach carries its own individual formula for calculating risk and its own “Qualifying Criteria” (standards the institution must meet to adopt a given approach).

As noted above, each nation must adopt its own laws or regulations implementing Basel II. The current state of rulemaking in the US consists of a Supervisory Guidance document and an Advanced Notice of Proposed Rulemaking issued by the Board of Directors of the FDIC. These documents suggest that US regulatory agencies will adopt those aspects of Basel II that are “appropriate for use by large and internationally active US banking institutions,²” and that US rulemaking for Operational Risk will focus on the Advanced Measurement Approach (“AMA”) because it gives institutions the most flexibility in implementing risk management processes. The FDIC has also commented, however, that this AMA-based approach will require institutions to “establish a risk management framework that encompasses all aspects of identifying, measuring and controlling operational risk,” including board responsibility of development and oversight of the risk framework.

So how can companies understand the information security ramifications of Basel II? Given the dizzying number of provisions, the existence of three approaches for each Pillar, and different qualifying criteria for each of these approaches, an institution needs to start its compliance efforts from basic, common compliance criteria. A good starting point is to examine three common “keys” to information security under Basel II.

Three Keys to Information Security Under Basel II

Basel II contains over 800 individually numbered paragraphs and is nearly 300 pages long. The core information security challenges posed by the law, however, can be summarized into three key sets of requirements:

- Mitigating Operational Risk;
- Tracking and centralizing event loss data, and;
- Adopting disclosure policies, controls and assessment processes.

Mitigating Operational Risk

As noted above, Basel II focuses on reduction of risk that may affect a financial institution's bottom line. One of the categories of risk most addressable by information security measures is Operational Risk, which is defined in Basel II as "risk of loss resulting from inadequate or failed internal processes, people and systems or from external events," including legal risk. The term "legal risk³" is further defined in Basel II as "exposure to fines, penalties or punitive damages resulting from supervisory actions, as well as private settlements."⁴

The definitions of Operational Risk and legal risk are broad enough to encompass the entire realm of compliance, security, and liability risks that financial institutions face from an information security perspective. Inadequate or failed internal processes and systems can include information security processes and systems that are not adequate to prevent an external event such as an exploit or identity theft, that fail to meet regulatory requirements under GLBA or similar laws, or that expose the institution to a risk of a civil lawsuit or regulatory penalties for failing to protect its (or its customers) data. An inadequacy or failure of persons can include failure to monitor employees or vendors for compliance with information security or data use policies or procedures.

Institutions can mitigate operational risk under Basel II by applying a number of measures. These include using systems, applications, and processes that detect unauthorized changes or other suspicious activity which may indicate a

failure or inadequacy in internal processes, people, and systems, and that can detect and prevent external events such as an exploit or corporate phishing attempt against the institution. Systems, applications, and processes should also be implemented to monitor personnel for failures to comply with security policies and procedures. As noted above, these measures differ from the consumer data protections required by most current laws and regulations because they not only require the institution to protect that data, but also any other data that is "proprietary and confidential" to the institution (which includes information on any items that, if shared with a competitor, would render a bank's investment in such items less valuable). Examples can include details of product development, marketing, trade secret, M&A, and related business planning. Furthermore, Basel II reinforces the need to implement systems, applications and processes that otherwise help to maintain compliance with other existing regulatory requirements (GLBA, FACT and so forth) to mitigate operational risk from "supervisory actions."

Tracking and Centralizing Loss Event Data

The second key to compliance with Basel II from an information security standpoint is tracking and centralizing internal loss event data. Currently, most institutions may gather and record internal loss event data in a variety of ways using a variety of systems, with little coordination. To support Basel II's goal of centralizing risk management processes to support better risk-based decision making by the institution, Basel II requires the institution to:

- track all internal loss event data, and
- adopt specific criteria for assigning loss event data into a centralized function (Basel II refers to the IT department as such a "centralized function"⁵)

From an information security perspective, institutions need to be able to ensure that event loss data from sources such as spreadsheets, databases, and e-mail are gathered into a centralized function. Because so much internal event loss data is gathered at the individual personnel level, these institutions also need to have means to ensure that

personnel comply with the policies and procedures for aggregating this event data.

Disclosure Policies, Internal Controls, and Assessment Processes

The third key to information security compliance with Basel II is adoption of a set of disclosure policies for proprietary and confidential information, internal controls over the disclosure processes and a process for assessing the appropriateness of disclosures. Each element of this key is explained below.

Basel II requires the institution to adopt a formal disclosure policy for proprietary and confidential information that is approved by the institution's Board of Directors. As noted above, the kind of proprietary and confidential information that must be covered by the policy includes not only customer data, but also any information on the institution's products and systems that, if shared with a competitor, would render the institution's investment in such products and systems less valuable. It therefore applies to a great deal of business development and business intelligence data that would otherwise not be covered by other existing laws and regulations. The policy must specifically address what kinds of disclosures the institution will make.

As noted above, the policy must address internal controls over disclosure of such information. Although Basel II provides little detail about these internal controls, it would be prudent for institutions to ensure that they include the means to detect and track authorized and unauthorized disclosure of information, to track which personnel have made the disclosure and whether the disclosure occurred in accordance with the institution's disclosure policy.

To ensure compliance with the disclosure policy, Basel II also requires the institution to adopt a process for assessing the appropriateness of disclosures. This process must enable the institution to examine validation and frequency of disclosures.

Because most of the "proprietary and confidential data" of institutions is now created, transmitted, and stored electronically, this element of Basel II also has significant

information security ramifications. Institutions need to be able to create application and system level IT controls over disclosure processes. The ability to detect changes to these controls, and to generate an audit trail of disclosures is crucial to the ability of an institution to assess the appropriateness of disclosures. The ability to detect unauthorized changes to disclosure controls and track these changes back to individual personnel will enable institutions to monitor personnel compliance (or noncompliance) with the disclosure policy.

Basel II Deadlines and Transition Periods

Because Basel II is an international standard (not a law or regulation), there is technically no hard "deadline" for compliance except those deadlines imposed by national implementing legislation. BSC has recommended that the non-advanced (Basic Indicator and Standardized Approach) approaches to credit and operational risk be in place by the end of 2006, and run parallel with current national legislation or regulation until final national legislation or regulation implementing Basel II is passed. Because each nation can set its own deadline (US regulators, for example, have suggested the end of 2008), institutions will have some time to transition into the final requirements. Given the comprehensive scope of Basel II, however, institutions may need every day of this transition period to become prepared for compliance.

Basel II Requirements and the Role of Change Management

Although change management is not mentioned by name in Basel II, change management processes are crucial to compliance. The role of change management in general is to ensure that:

- All changes are authorized
- All changes are auditable
- All unauthorized changes are investigated

Institutions cannot mitigate Operational Risk, track and centralize loss event data or be sure that their internal controls over disclosure processes are working if they cannot be sure that the systems and processes that support them are protected from unauthorized changes. The ability to audit changes to these systems can help support compliance, and the ability to investigate unauthorized change can both protect the institution from external events and legal risk and allow the institution to track whether personnel are following risk mitigation, event loss data and disclosure policies and procedures.

How Tripwire Helps Companies Achieve Basel II Compliance

The need for automated systems and processes to support change management is critical to meet the Basel II requirements. Tripwire can help institutions meet all three of the information security keys to Basel II compliance.

To support institutions' mitigation efforts for Operational Risk, Tripwire's products can detect changes or unauthorized activity in internal processes and systems that stem from internal failure or inadequacy. Tripwire® software can also detect unauthorized changes to systems from external events such as exploits and phishing, and can support compliance efforts with other laws and regulations that apply to the institution (such as GLBA, the EU Data Protection Directive, and so forth) to help mitigate legal risk. Tripwire's ability to restore systems to a previously known compliant state if unauthorized changes occur ensures that downtime from Operational Risk is limited to a minimum.

Tripwire's solutions can also enable institutions to detect and control changes in the tracking and centralizing of loss

event data. This ability to detect unauthorized changes in the systems that support tracking and centralization of loss event data ensures that personnel comply with policies for tracking and centralizing loss event data, and do not try to use these policies for purposes outside what they were intended for by diverting less favorable data. If unauthorized changes are made to these systems, Tripwire can restore them to their previous compliant state and avoid major interruptions in the tracking and centralizing process.

Tripwire is also uniquely suited to helping institutions enforce compliance with disclosure policies for proprietary and confidential information. Tripwire can detect changes to internal controls over the disclosure process, and ensure compliance with policies for disclosure by tracking personnel who make changes to systems that support and track the disclosure process without adequate authorization. Perhaps most importantly, Tripwire automatically generates a detailed audit trail to support the assessment process over the appropriateness of disclosures, including the examination of validation and frequency.

The bottom line is that Tripwire enables change control across the entire IT infrastructure. With Tripwire, nothing can change without the organization's knowledge, and if security is compromised, the institution can quickly roll back to a known, compliant state on its IT systems including directory servers, file servers, desktops, databases, middleware applications and a broad range of network devices. Tripwire software monitors servers and network devices for file integrity, and promptly reports any deviation or change to responsible personnel. With Tripwire, financial institutions can easily meet requirements for Basel II compliance, and gain the business benefits of increased data security, easier overall regulatory compliance, and improved IT service reliability.

Basel II Requirements and Tripwire solutions

Tripwire solutions help institutions comply with multiple requirements of Basel II, especially those in the realm of Mitigating Operational Risk under Pillar 2:

Pillar & Key	Number	Requirement(s)	Tripwire Directly Responds	Tripwire Supports	
Pillar 2 (Mitigating Operational Risk)	663 & 666	Adopting function to identify, assess, monitor and control/mitigate operational risk including legal risk	X	X	
		Systematic tracking of relevant operational risk data	X		
		Regular reporting of operational risk exposures & losses to senior mgmt and board of directors			
		Procedures for taking appropriate action in response to exposures and losses	X		
		Ensuring compliance with internal policies, controls and procedures for operational risk mitigation	X		
		Regular independent review and validation of operational risk mgmt processes and assessment system			X
		Regular auditing of operational risk management processes and assessment system			X
Pillar 2 (Tracking and centralizing event loss data)	670	Tracking internal loss data	X	X	
	671	Documenting procedures for assessing relevance of historical loss data and applying judgment overrides or other adjustments (incl. who is authorized to apply them)			
	673	Adopting specific criteria for assigning loss event data into a centralized function such as IT			
Pillar 3 (Disclosure Policies, Internal Controls & Assessment Processes)	819 & 821	Adopting a formal disclosure policy for proprietary and confidential information that is approved by the institution's Board of Directors		X	
	821	Addressing internal controls over disclosure of such information	X		
	821	Adopting processes for assessing the appropriateness of disclosures that enables institution to examine validation & frequency of disclosures	X		

Other Resources

Many sources of valuable materials and informative guides on Basel II and developing change management processes exist. Below are links to corporate governance guides, best practices for audit committees and IT organizations, and many other resources that will help companies understand compliance, service quality, and security requirements.

- **Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework (June 2006)**
www.bis.org/publ/bcbs128.pdf
- **U.S. Implementation of the Basel II Capital Accord:**
This Web page from the Federal Reserve Board provides resources to documents relating to the U.S. implementation of Basel II.
www.federalreserve.gov/generalinfo/basel2/
- **U.S. Implementation of the Basel II Capital Accord:**
This Web page from the Federal Reserve Board provides resources to documents relating to the U.S. implementation of Basel II.
www.federalreserve.gov/generalinfo/basel2/
- **Change and Patch Management Controls: Critical for Organizational Success;** This guide will give readers the necessary knowledge to help them counsel their boards about change management risks and controls, and to help their organizations comply with constantly changing regulatory requirements.
www.theiia.org/index.cfm?doc_id=5167
- **Information Technology Controls:** Covers technology topics, issues, and audit concerns as well as issues surrounding management, security, control, assurance, and risk management.
www.theiia.org/index.cfm?doc_id=5166
- **The Visible Ops Handbook:** Visible Ops illustrates how interested organizations might replicate key processes of high-performing organizations in just four steps.
www.itpi.org/home/visibleops2.php

About the Author

Daniel J. Langin is the principal of Daniel J. Langin, Attorney at Law, LLC. He has over 17 years of experience in private and corporate practice, including ten years of experience in technology, insurance coverage and intellectual property litigation and counseling. For more information, see www.langinlaw.com or contact Daniel at (913) 661-2430 or dlangin@langinlaw.com. This article is provided for general educational and informational purposes. It is not intended to provide legal advice.

- ¹ Formally known as the "International Convergence of Capital Measurements and Capital AStandards—A Revised Framework." (referred to herein simply as "Basel II").
- ² FDIC, "Advanced Notice of Proposed Rulemaking Regarding Risk-Based Capital Guidelines: Implementation of New Basel Capital Accord," p. 7 (July 11, 2003).
- ³ Basel II, Paragraph 644.
- ⁴ Id. at footnote 97.
- ⁵ Basel II, Paragraph 673.

ABOUT TRIPWIRE

Tripwire helps over 6,000 enterprises worldwide reduce security risk, attain compliance and increase operational efficiency throughout their virtual and physical environments. Using Tripwire's industry-leading configuration assessment and change auditing solutions, organizations successfully achieve and maintain IT configuration control. Tripwire is headquartered in Portland, Oregon, with offices worldwide.



www.tripwire.com