Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Information Security Gets a Seat at the Table

A company is a statement of faith between suppliers, employees, investors and customers. If any one or more of those groups decides they don't want to play any more, then the game is over. If a bank loses critical customer information because of a security failure, a financial risk arbitrage maneuver won't help. New regulations are making Operational Risk Management a more important component of banking. Information Security Professionals can help banks respond to this changing environment. The responses they create wi...

Copyright SANS Institute
Author Retains Full Rights

AD

Basel II
Information Security Gets a Seat at the Table

GSEC Certification Practical
Version 1.4b
Kent Nabors

February 17, 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

Introduction 1
Basel II Accord 4
Minimum Capital Standards 4
Supervisory Review 5
Market Discipline 5
Operational Risk 7
Applicability of the Basel II Accord 9
Sound Practices 10
Measurement 16
Basic Indicator Approach 16
Standardized Approach 17
Advanced Measurement Approach 18
Information Security Response 20
Lean the Language 20
Practice the Basics 20
Endnotes 22

© SANS Institute 2004, Author retains full rights.

Abstract

A company is a statement of faith between suppliers, employees, investors and customers. If any one or more of those groups decides they don't want to play any more, then the game is over. If a bank loses critical customer information because of a security failure, a financial risk arbitrage maneuver won't help. New regulations are making Operational Risk Management a more important component of banking. Information Security Professionals can help banks respond to this changing environment. The responses they create will affect not only risk management, but capital allocation. That is a seat at the big table for business decisions.

There is a need for new ideas and innovation. Information Security Professionals have much to contribute. Now let's talk about how that can happen.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Introduction

In 1988, the Bank for International Settlements (BIS) accomplished something quite amazing. This international organization of banking regulators established a global standard for measuring capital adequacy for banks. Considering that this standard does not carry the force of law directly, it success has been impressive. Today banks around the world use a common framework when making decisions on how to allocate capital based on their mix of assets.

One of the main motivations for establishing this framework was to bring consistency to the way banks were regulated in different countries. This enabled better capital allocation and regulatory decision-making, and helped to make the financial system more stable.

This standard, now known as the Basel Capital Accord or Basel I, has been effective partly because of its simplicity. Banks of different sizes and complexity of operations can be compared using a similar calculation to determine if they have sufficient capital to protect against certain risks.

System Failure Risks
For more information about this concept, read Chapter 7 of Bruce Schneier's book "Beyond Fear." He points out that systems can be vulnerable to a "class break" where a single flaw can break every instance of some security feature.

But Basel I is beginning to show its age. The world of banking is more complex than when the accord was established. New opportunities and new risks exist today. Some banks have learned how to "game" the system, particularly in international banking.[1]

BIS published a list of changes in the banking environment that are driving the need for new capital measures that incorporate broader risk management models. For Information Security professionals, many of these changes will look familiar. There are parallels in other industries. And Information Security as a practice has been dealing with the implications for some time:

- If not properly controlled, the greater use of more highly automated technology has the potential to transform risks from manual processing errors to system failure risks, as greater reliance is placed on globally integrated systems;
- Growth of e-commerce brings with it potential risks (e.g., internal and external fraud and system security issues) that are not yet fully understood;
- Large-scale acquisitions, mergers, de-mergers and consolidations test the viability of new or newly integrated systems;
- The emergence of banks acting as large-volume service providers creates the need for continual maintenance of high-grade internal controls and back-up systems;
- Banks may engage in risk mitigation techniques (e.g., collateral, credit derivatives, netting arrangements and asset securitisations)

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

to optimise their exposure to market risk and credit risk, but which in turn may produce other forms of risk (e.g. legal risk);

- Growing use of outsourcing arrangements and the participation in clearing and settlement systems can mitigate some risks but can also present significant other risks to banks.[2]

In addition to these high-level trends, here are some interesting facts about the banking industry:

- In the past decade, there have been over 100 operational loss events exceeding over $100 million[3]
- A recent survey by the BIS committee's Risk Management Group found that the average bank allocates 15% of capital to operational risk.[4]
- JP Morgan Chase was analyzed under the new Basel II framework. It's regulatory capital was $37.3 billion. Of that, $8.7 billion (23.3%) was attributed to Operational Risk.

Operational Risk
Purposefully managing the risks associated with the key functional activities of a bank is one of the main innovations of Basel II.

What makes this last statistic more interesting is the context of the amount allocated to Operational Risk. JP Morgan set aside $13.1 billion for credit risk. The fact that Operational Risk is such a relatively important variable when compared to credit (lending) risk should be a wake up call to Information Security Professionals.[5]

To address these significant environmental changes, BIS is in the process of creating a new capital accord called Basel II. This new accord includes a more sophisticated measurement framework for evaluating capital adequacy in banks. For Information Security professionals, the key component of this framework is Operational Risk.

In the original accord, capital adequacy was strictly a financial calculation. Capital was measured as if it were reserved for protection primarily against financial risks such as credit and market activities. With Basel II, capital must also be explicitly reserved for the risk an institution faces in its operational activities. The methodology proposed to evaluate, manage, and mitigate operational risk is very similar to practices Information Security professionals have long used.

Instead of a cost center mentality, Information Security professionals in the banking industry have an opportunity to make contributions to capital adequacy calculations. How well banks manage operational risk will have a direct impact on how much capital must be held for regulatory compliance. This is another chance to be a part of key business decisions.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Introduction

Expressed Concerns
The FDIC recently warned that the current proposals could "cause bank capital requirements to drop precipitously for the 20 largest banks."

Some U.S. banking regulators have expressed concern that implementing Basel II will lead to lower capital levels among banks.[6] For a bank, lower regulatory capital requirements can be an opportunity for greater investment and therefore greater profit. Those who create the risk management practices that enable a bank to safely lower capital will have a direct impact on investment opportunities. That is the seat at the big table.

As an example, Eric Rosengren of the Federal Reserve Bank of Boston stated that banks investing in the more advanced Basel II management models are already seeing benefits such as:

- Lower expected losses and volatility in earnings
- Ability to identify causal factors for operating losses
- Better decision making because operational risk effects capital allocation[7]

The practices of Information Security, when applied to the Operational Risk framework of Basel II, can make significant improvements in the safety of banking activities. The challenge for professionals is to find the right balance of controls and risk mitigation versus implementation and maintenance costs. A complete, detailed Basel II compliance effort can be expensive in both staff time and money. This is where there is opportunity for innovation.

Federal Reserve Bank
There is some debate among U.S. regulators as to how Basel II should be implemented. The Federal Reserve has been the main advocate. In contrast, the Office of Comptroller of the Currency has not been as vocal a supporter.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Basel II Accord

Three Pillars
Probably the best free over view documentation of the Basel II "Three Pillars" concept has been done by Price Waterhouse Coopers. They have created a web site that outlines the three pillars and details the requirements for each. (http://www.pwcglobal.com/de/eng/basel2navigator/)

The BIS has stated that the objective of the Basel II Accord is to not change the global level of capital in the banking industry.[8] Instead, they are creating an incentive to encourage banks to adopt what they consider "best practices" for risk management. Banks that apply the more sophisticated Basel II standards have an opportunity to lower their regulatory capital reserves. Conversely, banks with weaker risk management practices will find that their regulatory capital requirements will increase. In short, banks with better risk management practices (according to Basel II) will have a better chance at higher profitability.

Basel II is based on "Three Pillars:" 1) minimum capital standards, 2) supervisory review and 3) market discipline. There are areas of interest to Information Security professionals in each of these.

Minimum Capital Standards
Banks are required to maintain a ratio of capital to "risk-weighted assets" equal to 8%. "Risk-weighted assets" are the heart of the capital standard. Assets on a banks' balance sheet are measured against the risk they represent. Loans, securities, and other assets each represent a different risk of loss, and therefore require a different level of capital to protect the bank.

But assets are not the only part of the calculation. The activities of conducting banking represent a risk as well. Operational Risk is another variable that is used to calculate capital adequacy in the Minimum Capital Standards. In the old accord, this type of risk was only acknowledged by "over charging" for the risk tied to the assets held by the bank. Now banks will have specific capital requirements tied to activities and assets.

There is a difficulty in creating a capital charge for Operational Risk. No accepted standard exists for its measurement. In fact, the Bank for International Settlements is encouraging the industry to develop methodologies related to managing Operational Risks. This is where the real opportunity lies for Information Security professionals. Risk management in an environment of uncertainty is a nearly complete definition of the Information Security discipline.

Information Security professionals need to bring their language and experience to the industry while this framework is in a period of development.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Supervisory Review
The BIS acknowledges in their explanation of Basel II that the banking environment is too dynamic to allow for a static measurement tool. The role of Supervisory Review is seen as both an enforcement and market response mechanism.

For Information Security Professionals, the Supervisory Review requirement is very similar requirements in other industries for regulatory compliance (such as Sarbanes-Oxley in the United States). The Information Security environment requires constant adaptation to new threats and new capabilities. There is much experience in the field that can be brought to the banking industry as it adapts to the changing regulatory requirements that will accompany adoption of this standard.

Market Discipline
This is a point of the new accord that has already sparked significant debate.
BIS wants to use "Market Discipline" as a tool to pressure banks to adopt best practices. The hope is that as banks are required to disclose their management practices, successes and failures, there will be pressure to manage risks more effectively.

Banking Organizations
Note that the author limited the review to U.S. based banks for this part of the research. However, the full record of responses can be found at http://www.bis.org/bcbs/cp3comments.htm.

During the open comment period, this requirement drew a significant number of responses from global banking organizations. As an example:

- Wells Fargo stated "disclosures will create an uneven playing field between banks and their non-bank competitors, who will be free to pursue their business activities unencumbered by supervisory capital rules and the excessive compliance costs that they will engender."[9]

- Citigroup made the point that requiring disclosures related to Operational Risk could harm banks when attempting to negotiate insurance policies that could be used as a risk mitigation strategy.[10]

- JPMorganChase argued that the disclosure requirement will create a situation where the data they disclose could be subject to misinterpretation that could only be addressed by disclosing more information. The resulting burden would be costly.[11]

This is a point of significant contention and debate that will continue to evolve as the implementation date draws closer. For an Information Security professional, the parallel to the debate over disclosing software vulnerabilities is striking. The market place does enforce discipline to

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

those whose products are not secure. But the customers of those products may suffer from the disclosure.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Operational Risk

The BIS has acknowledged that the term “Operational Risk” can have many meanings, even within the context of banking alone. To clarify, the committee has listed the types of events that can occur that they feel falls under the scope of “Operational Risk:”

- Internal fraud. For example, intentional misreporting of positions, employee theft, and insider trading on an employee's own account.
- External fraud. For example, robbery, forgery, cheque kiting, and damage from computer hacking.
- Employment practices and workplace safety. For example, workers compensation claims, violation of employee health and safety rules, organised labour activities, discrimination claims, and general liability.
- Clients, products and business practices. For example, fiduciary breaches, misuse of confidential customer information, improper trading activities on the bank's account, money laundering, and sale of unauthorised products.
- Damage to physical assets. For example, terrorism, vandalism, earthquakes, fires and floods.
- Business disruption and system failures. For example, hardware and software failures, telecommunication problems, and utility outages.
- Execution, delivery and process management. For example, data entry errors, collateral management failures, incomplete legal documentation, unapproved access given to client accounts, non-client counterparty misperformance, and vendor disputes.

What should be striking for an Information Security professional is the similarity between the list above and the issues that are part of the daily challenge of Information Security. These events are not new. It has always been important for banks to prevent events like the ones described above. The key is that the list, when combined with the industry trends noted on page 1 and mixed with the broader societal developments such as greater speed in technological change, proliferation of technical skills, etc. creates a need for new focus.

Operational Risk must be managed as a unique discipline. It is so important that capital should be explicitly allocated against it.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Operational Risk

The place to begin is with a definition. BIS has defined Operational Risk as

> *"The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events."*

CIA
Both (ISC)[2] and SANS use this concept specifically in their training programs.

"…internal processes, people and systems…"
This broad category would traditionally be attributed to activities protected by an internal audit function. However, the increasing reliance on processes automated through technology means this is more than a check for auditors. Designing and monitoring systems to operate securely is a critical component – and a strength of Information Security. The "CIA" triumvirate of "Confidentiality, Integrity, Availability" taught in many Information Security certification programs gets to the heart of this part of the definition.

"…external events."
It is easy to believe that the practice of Information Security is mostly an effort to protect against "external events." In 2003, there were many examples of these "external events." The SQL Slammer worm showed the danger to banks when Bank of America customers couldn't access their money through ATM's because of the massive traffic it generated.[12] That event alone divided many banks into one of two categories: "Prepared" and "Oops."

Operational Risk as defined by BIS in the Basel II accord is a natural fit for Information Security professionals. For example, the SANS and CISSP training programs, teach very similar concepts. Organizations such as Infraguard in the United States address these concerns. Information Security professionals will find that the language used and issues covered in Basel II sound familiar. The Information Security community has much experience to offer this developing banking practice.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Applicability of the Basel II Accord

In the United States, there is still debate as to the applicability of Basel II for banks. The clearest statement by the Federal Reserve is that there will be ten or so of the largest U.S. banks that will be required to fully adopt the Basel II accord. There will probably be another ten or so banks in the U.S. that will volunteer to adopt the accord because of market or reputation pressure.[13]

However, the Information Security community is global. There are many countries that are expected to require Basel II capital standards for all of their financial institutions. For some countries, the changes are going to be painful. For example, Chris Matten of PriceWaterhouseCoopers has pointed out that in Asia, "risk management practices and systems have had less time to become entrenched." These institutions have not yet built up the historical data, systems or personnel skills to manage under this framework.[14]

Check Imaging
On November 3, 2003 President Bush signed the "Check 21" law allowing for digital presentment of checks. Say "goodbye" to float as a consumer. For an Information Security Professional, consider Bruce Schneier's warning about vulnerabilities to "Class Breaks."

In comparison, for smaller U.S. banks that will not be required to adopt the accord, the pattern of measurement used by Basel II is still applicable. The standards used for managing risks are built on best practices from all over the world. The discipline of identifying, measuring and managing risks is developing first in the banking industry. But it will spread into other financial services and areas, and then even wider. The challenges of banking are not unique:

> *"This is the decade of operational risk. Although banks have always been subject to operational risks, a lot is changing. Loan closings, check clearing, and a multitude of other processes are going electronic. Acceptance and use of check imaging are increasing. Timeliness is more important to customers, so processes are speeding up. We're relying more and more on models to manage greater volumes of varied transactions at greater speed, so that model risk has become material. And systems that were once housed in a single mainframe computer are now distributed – no doubt with great gains in economy, but with the side effect of creating a more complicated computer environment to manage."*[15] *- Susan Bies, Governor, Federal Reserve Bank*

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Sound Practices

The discipline of Operational Risk management is evolving. Basel II aims to provide a framework for this discipline. The objective is to drive behavior that reduces total risk in the banking system. The hope is that banks that fully adopt Basel II will be better positioned to deal with the uncertainty of the environment in which they operate.

Published guidelines
BIS has published "Sound Practices for the Management and Supervision of Operational Risk at: http://www.bis.org/publ/bcbs86.pdf.

BIS has published guidelines on the sound practices required to manage Operational Risk in banks. They define "management" of Operational Risk to mean the "identification, assessment, monitoring and control / mitigation of risk."

Developing An Appropriate Risk Management Environment
The first step is to create an organizational environment that enables the bank to effectively manage risk. The first three principles defined by BIS address this issue:

Principle 1: The board of directors should be aware of the major aspects of the bank's operational risks as a distinct risk category that should be managed, and it should approve and periodically review the bank's operational risk management framework. The framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk is to be identified, assessed, monitored, and controlled/mitigated.

Just as a board of directors must understand and approve the financial and strategic issues faced by a bank, it should also ensure that Operational Risk is being properly managed. The supporting documentation published by BIS provides additional insight into the Committee's objective.

The board of directors should establish a management structure capable of implementing the firm's Operational Risk management framework. This will have a significant impact on a bank. Most banks do not have a separate discipline for operational risk management. This is a point of evolution. In the 1980's, there were few banks with a separate discipline for financial risk management. Today, even mid-sized banks have specialists that manage the structure of the firms' balance sheet.

Operational Risk management as a separate discipline is a significant issue that will increase in prevalence in the coming years. For Information Security professionals, this is the point of opportunity. Information Security works with a language of risk. Threat identification and mitigation is standard fare. This skill will be increasingly important for banks as Basel II moves closer to adoption.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Principle 2: The board of directors should ensure that the bank's operational risk management framework is subject to effective and comprehensive internal audit by operationally independent, appropriately trained and competent staff. The internal audit function should not be directly responsible for operational risk management.

Industry practices already cover this principle. Internal audit is already a requirement by practice and regulation in banking. The keys to compliance here are 1) ensuring that the internal audit process includes the specific implementation requirements of Basel II and 2) that banks implementing Basel II avoid the temptation to bring Operational Risk Management under the reporting structure of the Internal Audit activities.

Security Management Practices
Some of the training material available goes so far as to note that failure of senior management to be involved in Information Security issues may jeopardize their "due care" protection.

Principle 3: Senior management should have responsibility for implementing the operational risk management framework approved by the board of directors. The framework should be consistently implemented throughout the whole banking organisation, and all levels of staff should understand their responsibilities with respect to operational risk management. Senior management should also have responsibility for developing policies, processes and procedures for managing operational risk in all of the bank's material products, activities, processes and systems.

The key issue here is "senior management." Whoever is charged with implementing the operational risk management framework should have organizational authority to develop and implement policies, processes and procedures.

Many organizations struggle with where to place Information Security in their organizational reporting structure. Basel II may lead some banks to the conclusion that the Operational Risk Management function and the Information Security functions can be tied together.

As an example of what the practice of Information Security can contribute, the Security Management Practices of the CISSP 10 domains gives good suggestions about management roles and responsibilities.[16]

Risk Management
The next step is to actively manage risk within the bank. This is the focus of the next four principles:

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Sound Practices

Principle 4: Banks should identify and assess the operational risk inherent in all material products, activities, processes and systems. Banks should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.

Banks must ask a fundamental question – "What risks do we face?" The question then leads to others. For example, here are a few internal risk-focused questions:

- "How does our organizational structure and business strategy affect our internal risk?"
- "How do our organizational weaknesses create risks?"
- "How do our organizational strengths create risks?"

For each question, the next step is to identify which of the risks match to an internal vulnerability. And to what extent that vulnerability creates a financial exposure that will drive an action.

Vulnerability
One example few banks consider – "How do new products or services create changes in our risk profile?" For example, a new service could require a change in systems or practices that opens the organization to new risks.

Risk measurement must be formalized. The details of the process are left open to interpretation. There is wide latitude for methodologies to be developed. However, the strategy implemented must be auditable. Banks must be able to defend the validity of their approaches to regulators.

Principle 5: Banks should implement a process to regularly monitor operational risk profiles and material exposures to losses. There should be regular reporting of pertinent information to senior management and the board of directors that supports the proactive management of operational risk.

Understanding the Operational Risk profile of the bank must be part of the regular management process. Senior managers (including the Board of Directors) must be informed of the current risk profile. To accomplish this, systems must be implemented that measure risk and allow for regular reporting.

In the discussion of this principle, one topic of interest in the BIS documentation is the need for "key risk indicators" or "early warning indicators." The idea is that Banks should identify events or patterns that provide alerts of future changes in the risk profile.

While this is logical, the implementation is challenging. An indicator must be developed over time based on observation. There needs to be an adequate sample of data to find correlation. Compliance with Basel II requires an early start, and this principle is illustrative. Banks must begin

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the search both within their own data stores, and in the market place for indicators of risk. A disciplined, logical approach is needed to create the measurement and monitoring systems needed to comply with this principle.

Another point of interest in the BIS discussion of this principle is a reference to a bank's "Operational Risk Management Office." Many banks will not have the resources to create such an organizational structure in a competitive market. But it is instructive as to the mindset of the regulators creating Basel II. They will be looking for formal organizational commitment to the principle of managing risk.

Principle 6: Banks should have policies, processes and procedures to control and/or mitigate material operational risks. Banks should periodically review their risk limitation and control strategies and should adjust their operational risk profile accordingly using appropriate strategies, in light of their overall risk appetite and profile.

Sufficient Segregation
SANS and (ISC)^2 teach that operational security can be enhanced by segregation of duties. Just like this operational control, the organizational structure created for Operational Risk Management should be conducive for sound decisions and practices.

This is the point of action. The information collected and organizational structure applied should lead to measurable actions taken to address risks identified by the bank. A decision must be demonstrated for all identified risks to either control / mitigate or bear the risk. If the risk is too great or cannot be controlled, then the activity should be abandoned.

A key point here is that the organizational structure referenced earlier must protect against conflicts of interest that may influence decisions. There needs to be sufficient segregation to create an environment conducive to sound decisions based on business opportunities and risk profiles.

One valid strategy for mitigating risk is externalizing it. For example, some risks have a low probability but a large financial impact (a natural disaster or terrorist act). For these, insurance models would be appropriate. Another option is to outsource the activity. If there is a risk profile associated with a business activity that cannot be controlled internally, outsourcing could externalize the risk. However, the outsourcing relationship must be based on "robust contracts…that ensure a clear allocation of responsibilities."[17]

Principle 7: Banks should have in place contingency and business continuity plans to ensure their ability to operate on an ongoing basis and limit losses in the event of severe business disruption.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Sound Practices

This brings into the Basel II framework a key activity that is already well established in banking. For Information Security practitioners, the principle of "Availability" is the language used for this discipline.

Availability
This third part of the "CIA" triumvirate can cover items such as systems design, systems monitoring, response teams, threat profiling and more. A well-considered Information Security program will be a good example for compliance with this Basel II "Sound Practice."

Role of Supervisors
Supervisors play an important enforcement role. The next two principles provide general guidelines for their activities:

Principle 8: Banking supervisors should require that all banks, regardless of size, have an effective framework in place to identify, assess, monitor and control/mitigate material operational risks as part of an overall approach to risk management.

This principle is directed at banking supervisors, but in effect is a warning to banks. "Supervisors should require" means banks must comply. In the United States, the "regardless of size" requirement does not apply directly. As stated earlier, Basel II will not be required for all U.S. banks. However, the principles are valid, and they will shape the methodologies used by regulators for all U.S. banks.

Principle 9: Supervisors should conduct, directly or indirectly, regular independent evaluation of a bank's policies, procedures and practices related to operational risks. Supervisors should ensure that there are appropriate mechanisms in place which allow them to remain apprised of developments at banks.

Supervisors Should Require
Internationally, this principle is a very clear statement that compliance with Basel II is a requirement.

As a further clarification, this principle outlines what supervisors should look for. The BIS discussion of this principle details seven categories of inspection for supervisors:

- Effectiveness of the bank's risk management process and overall control environment with respect to operational risk
- Methods for monitoring and reporting its operational risk profile, including data on operational losses and other indicators of potential operational risk
- Procedures for the timely and effective resolution of operational risk events and vulnerabilities
- Process of internal controls, reviews and audit to ensure the integrity of the overall operational risk management process
- Effectiveness of the bank's operational risk mitigation efforts, such as the use of insurance
- Quality and comprehensiveness of the bank's disaster recovery and business continuity plans

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

- Process for assessing overall capital adequacy for operational risk in relation to its risk profile and, if appropriate, its internal capital targets

When working in a regulated environment, a strong documentation program is vital. For all of the checks listed above, there must be a complete set of documentation supporting internal processes. Failure to document activities can lead a regulator to lower compliance ratings even when implemented processes are adequate.

Role of Disclosure

The final step is to provide one more mechanism for ensuring that banks apply these processes to their management of operational risk. The tool used is public disclosure:

Principle 10: Banks should make sufficient public disclosure to allow market participants to assess their approach to operational risk management.

This is a key point of debate in the industry. It is also familiar to Information Security practitioners. The market place is a very effective tool for "clarifying" activities. But disclosing compliance failures can be very costly to banks. Their very existence is predicated upon the faith their depositors have in how the bank is managed.

The parallel to the debate over disclosing software security vulnerabilities has already been discussed. For Information Security professionals familiar with this debate in their own industry there is an opportunity to bring that experience to this issue in banking.

Disclosing
A banker would argue that it is much easier for a software company to disclose a security flaw and survive than for a bank to disclose an operational failure and survive. Regardless, a bank should expect that if disclosure were required, consumers would react quickly, similar to the way Information Security professionals now respond to new vulnerability disclosures in software.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Measurement

The final step is how to measure the effectiveness of the Operational Risk Management framework within a bank. To do this, BIS has defined three techniques that may be employed. Banks have an option as to which one, or what combination of the three may be used. The choice can have a dramatic impact on the cost, complexity, and opportunity created by the bank's compliance effort.

Each of the approaches discussed below use the term "capital charge." This means that a value is determined for use in an enterprise-wide capital calculation. A simple capital ratio is the proportion of capital to assets:

$$\frac{TotalCapital}{TotalAssets} \equiv CapitalRatio$$

Calculated Value
All of the calculations in this section are taken from the "The New Basel Capital Accord" published by BIS at: http://www.bis.org/bcbs/cp3part2/pdf.

However, with Basel II, the Total Assets value is not actually the total of assets that the bank holds. Instead, it is a calculated value that represents the risk of the assets and activities associated with the assets:

$$\frac{TotalCapital}{(CreditRisk)+(MarketRisk)+(OperationalRisk)} \equiv CapitalRatio$$

The calculation of *CreditRisk* and *MarketRisk* are outside the bounds of this paper. *OperationalRisk* represents a portion of the total "capital charge" value that is compared to actual *TotalCapital* held by the bank. It is calculated using one of three approaches defined in Basel II: 1) Basic Indicator, 2) Standardized, and 3) Advanced Measurement Approaches. The first is the simplest; the latter is the most complex.

Banks can have different lines of business that are measured using different approaches. However, once an approach is selected, a bank cannot move back to a simpler one.

Basic Indicator Approach

The Basic Indicator Approach ties the capital charge to a single risk indicator. The BIS proposes that gross income be used as this indicator. Regardless of the size or complexity, any bank using the Basic Indicator approach would have to allocate capital at a fixed proportion to gross income. At this time, the proposed ratio is 30%.

So the calculation for *OperationalRisk* would be:

$$Total\ \mathrm{Re}venue \times 30\% = OperationalRisk$$

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Measurement

The underlying assumption is that the size of the operation is an indicator of the risk that operation is to the institution.

While, simple, it is also generalized. The Basic Indicator Approach may be appropriate to institutions that already carry capital in excess of their regulatory minimum. It also works will for institutions that do not want the expense or organizational burden of a more complex measurement framework. The downside – there is little opportunity to more aggressively manage capital (and thereby free up resources for investment and potentially greater profits).

Standardized Approach

The Standardized Approach is very similar to the Basic Indicator Approach. Again, it uses revenue as a proxy to measure risk. However, the charge is allowed to vary by the line of business. Basel II is not finalized, so the actual charge has not yet been set. The lines of business for the bank subsidiaries used in the calculation are defined in the accord and should be close to the values presented here when finalized:[18]

Business Line	Beta Factors
Corporate Finance	18%
Trading and Sales	18%
Retail Banking	12%
Commercial Banking	15%
Payment and Settlement	18%
Agency Services	15%
Asset Management	12%
Retail Brokerage	12%

Qualitative Standards
For an example of how this approach is used in the Information Security discipline (and how that can help Basel II compliance), look at the 4th edition of the Information Security Handbook by Harold Tipton and Micki Krause. They have a good chapter on Risk Analysis and Assessment that details the evolution of Qualitative Standards in information risk assessment.

So the calculation for *OperationalRisk* would be:

$$Operational Risk = \sum \left(GI_{1-8} \times \mathrm{b}_{1-8} \right)$$

Where:
GI = the Gross Income for each of the lines of business defined by the accord.
• = the Beta Factors listed in the table above.

There is greater opportunity to "fine tune" the Operational Risk of the lines of business. However, revenue is still used as a proxy for risk, so it is a rough measure.

A bank will have to meet the following standards to be eligible for the Standardized Approach:

- Qualitative standards: existence of an independent risk control and audit function, effective use of risk reporting systems, active

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

involvement of board of directors and senior management, appropriate documentation of risk management systems
- Independent operational risk management and control process that covers design, implementation and review of its operational risk measurement methodology
- Regular reviews by banks' internal audit groups
- Appropriate risk reporting systems to generate data
- Systematic tracking of relevant operational risk data by business line across the firm[19]

Advanced Measurement Approach
This is the most sophisticated measurement tool available to banks under the Basel II accord for allocating capital to Operational Risk. It strives to allow banks to use their own operational loss experience as the indicator for calculating the appropriate capital charge. This is the most logical methodology, but the difficulty is in the application.

Before a bank can apply this methodology, it must obtain supervisory approval to use it. There are three criteria for gaining this approval:

- The board of directors and senior management must be actively involved in the oversight of the operational risk management framework.
- The risk management system used must be conceptually sound and implemented with integrity.
- The bank must have sufficient resources in the use of the approach in the major business lines as well as the control and audit areas.

The AMA is a combination of qualitative and quantitative criteria. For the qualitative measurement component, the bank must meet the following standards:

- The bank must have an independent operational risk management function that is responsible for the design and implementation of the bank's operational risk management framework.
- The bank's internal operational risk measurement system must be closely integrated into the day-to-day risk management process of the bank.
- There must be regular reporting of operational risk exposures and loss experience to business unit management, senior management, and the board of directors.
- The bank's risk management system must be well documented.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Measurement

- Internal and / or external auditors must perform regular reviews of the operational risk management process and measurement systems.[20]

The quantitative component of the AMA is quite "open." The BIS states in the accord: "Given the continuing evolution of analytical approaches for operational risk, the Committee is not specifying the approach or distributional assumptions used to generate the operational risk measure for regulatory capital purposes."[21] They recognize that this is an evolving field that is in need of innovation. There is not a one perfect method for measuring and managing operational risk.

This is one of the key opportunities for contribution by the Information Security practice. There is a real need for innovation as this practice evolves. The stakes for these banks are large and they will be looking for new ideas in managing operational risk.

If a bank adopts AMA, it can be used as part of an enterprise-wide compliance effort that also uses the Basic Indicator Approach and Standardized Approach. However, one requirement is that banks provide their regulator with a plan to eventually roll out AMA to all of their operations.

So selection of this approach offers the greatest opportunities to affect regulatory capital minimums. It also carries the greatest costs. Banks that adopt this method will need a strong commitment to an enterprise-wide risk management framework. Information Security will be a critical part of that framework. And the practices of Information Security can contribute more broadly to the enterprise in the field of Operational Risk Management.

Information Security
Much of the methodology taught in the (ISC)^2 and SANS programs are instructive for how to create a measurement framework for risk management. These are the types of skills and methods that Information Security can bring to the banking industry.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The Information Security Response

Basel II represents an opportunity for Information Security Professionals. The risk management framework, particularly that which applies to Operational Risk is a natural fit for the strengths of Information Security. However, to make a meaningful contribution, those who practice in the field of Information Security need to prepare themselves.

Local Language
This paper has focused on a specific challenge within the banking industry. But learning the "local language" of industries served is a skill that Information Security professionals should develop throughout their careers. Information in context has value. Information without context is noise.

Learn the Language

Information Security professionals, like practitioners in other disciplines, tend to create their own dialect. This becomes shorthand that allows for quickly communicating a complex concept. If both parties of a conversation understand a key concept, they can use this shorthand to refer to the common knowledge, and then proceed to build upon it.

Basel II, like many complex issues, requires inter-disciplinary skills. Information Security professionals have much to contribute. The issues, practices and even parts of the language are familiar. But to be effective, Information Security professionals need to do a better job of learning the "local language" of the industry they serve. Information Security is not an industry; it is a serving and enabling function. Information Security professionals should work to speak the language (in this case, banking and risk management). There is much to contribute, but only after the context of the challenge is well understood.

Practice the Basics

Many of the operational losses that banks experience are failures in basic business practices or controls. For example, one of the ten CISSP domains is Security Management Practices. A component of this domain is Security Awareness. A properly implemented Security Awareness Program will go far in preventing many operational losses that occur from individuals that attempt to defraud a bank.

Within the same Security Management Practice domain exists guidelines on Quantitative Risk Analysis. There are very close parallels to the Advanced Management Approach for measuring Operational Risk capital allocation levels. The Information Security Professional that knows the basics of their profession will be well prepared to address this coming change in the banking industry.

In "Information Security Management Handbook," authors Harold Tipton and Micki Krause outline how to balance qualitative and quantitative information risk analysis. The discussion is very similar to the BIS guidelines on the Advanced Management Approach.[22]

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

The Information Security Response

There are more examples that could be cited. A virtual walk through the SANS Reading Room is a good place to look. Information Security as a discipline has long been dealing with many of the same issues that Basel II will address. Being a well-rounded Information Security Professional is required to contribute meaningfully to the implementation of this accord.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Endnotes

[1] Matten, Chris, "Changing of the Guard," The Business Times (Singapore), May 21, 2003.
[2] "Sound Practices for the Management and Supervision of Operational Risk," Basel Committee on Banking Supervision, February, 2003, pp1-2.
[3] de Fountnouvelle, Patrick "Using Loss Data to Quantify Operational Risk," Federal Reserve Bank of Boston, April, 2003, http://www.bos.frb.org/bankinfo/oprisk/pd91703.pdf.
[4] David, Gobe; Sidler, Christopher, "The New Basel Accord: Update and Impact," EDS, July, 2003, p 54.
[5] Ibid.
[6] Christie, Rebecca, "OCC Hawke: Europe Should Respect US Approach to Basel II", Dow Jones Newswires, December 15, 2003, http://news.morningstar.com/news/DJ/M12/D15/1071613260744.html.
[7] Rosengren, Eric, "Quantification of Operational Risk", Federal Reserve Bank of Boston, http://www.bos.frb.org/bankinfo/oprisk/quant.pdf.
[8] "Continued Progress Toward Basel II", Basel Committee on Banking Supervision press release, January 15, 2003, http://www.bis.org/press/p040115.htm.
[9] Atkins, Howard I., Executive Vice President, Chief Financial Officer, Wells Fargo, Letter to Basal Committee on Banking Supervision, August 18, 2003, http://www.bis.org/bcbs/cp3/wellsfargo.pdf.
[10] Thomson, Todd S., Executive Vice President, Chief Financial Officer, Citigroup, Letter to Basal Committee on Banking Supervision, July 31, 2003, http://www.bis.org/bcbs/cp3/citigroup.pdf.
[11] Edelson, David B., Corporate Treasurer, JPMorganChase, Letter to Basal Committee on Banking Supervision, July 29, 2003, http://www.bis.org/bcbs/cp3/jpmorcha.pdf.
[12] Leyden, John, "ATMs, ISPs Hit by Slammer Worm Spread," The Register, January 27, 2003, http://www.theregister.co.uk/content/archive/29040.html.
[13] Taylor, Charles, "The Decade of Operational Risk, An Interview with Federal Reserve Board Governor Susan Bies" The Journal of Risk Management, July / August 2003, https://rmaweb.rmahq.org/rmaweb/tpro50/timssnet/memberso/journal/0703/0703_01.html.
[14] Matten, Chris, "Changing of the Guard," The Business Times (Singapore), May 21, 2003.
[15] Taylor, Charles, "The Decade of Operational Risk, An Interview with Federal Reserve Board Governor Susan Bies" The Journal of Risk Management, July / August 2003, https://rmaweb.rmahq.org/rmaweb/tpro50/timssnet/memberso/journal/0703/0703_01.html.
[16] Krutz, Ronald, "The CISSP Prep Guide", John Wiley & Sons, New York, 2001, pp10-14.
[17] Sound Practices for the Management and Supervision of Operational Risk, Basel Committee on Banking Supervision, February, 2003, p 11.
[18] "The New Basel Capital Accord", BIS, April 2003 http://www.bis.org/bcbs/cp3part2.pdf p 123.
[19] David, Gobe; Sidler, Christopher, The New Basel Accord: Update and Impact, EDS, July, 2003, p 22.
[20] "The New Basel Capital Accord", BIS, April 2003 http://www.bis.org/bcbs/cp3part2.pdf p 125.
[21] Ibid., 126.
[22] Tipton, Harold F., Krause, Micki, "Information Security Management Handbook, 4th edition, Auerbach Publications, New York, 1999, pp245-285.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced