BITS

FINANCIAL SERVICES
ROUNDTABLE

KALCULATOR:
BITS KEY RISK MEASUREMENT TOOL
FOR
INFORMATION SECURITY
OPERATIONAL RISKS

BITS · 1001 PENNSYLVANIA AVENUE NW · SUITE 500 SOUTH · WASHINGTON DC 20004 ·202-289-4322

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The financial services industry needs new forms of risk management. The reasons for this are numerous and include the deregulation and globalization of financial services, the industry's growing reliance on technology, and a perceived increase in the risk profile of financial services business models. Operational risk management will become a priority at major financial institutions as they respond to pending regulatory capital requirements and competitive pressure requiring stronger internal controls.

Often considered the backbone of operations, computer hardware and software systems play a major role in any financial institution's operational risk profile. Ensuring information confidentiality, integrity and availability is a significant component of operational risk. Unique challenges are associated with this specific risk component.

The *Key Risk Measurement Tool for Information Security Operational Risks* ("*Kalculator*") is a product of a joint subgroup of the BITS Operational Risk Management and Security and Risk Assessment Working Groups. The subgroup developed a spreadsheet template to identify common, high-risk factors related to information security along with a method to prioritize them. The resulting tool is the *Kalculator*.

The *Kalculator* is intended for use by financial institutions to identify key information security risks that should be considered in broader enterprise-wide operational risk models. The *Kalculator* provides an extensive, but not exhaustive, list of common information security threats, vulnerabilities and corresponding controls to mitigate risk. It also offers a method for scoring and prioritizing risks based on the likelihood of threat occurrence, the degree of control implementation, and the level of control effectiveness. Providing sort capabilities based on ISO 17799[1] categories and Basel II loss event (Level 1) categories, the tool can facilitate an organization's internal communication by using a risk context that is understood by information security, audit, operational risk and others.

Financial institutions are required to employ information security assessments to satisfy federal and state regulations. Though various assessment models are already in use, a secondary benefit of the *Kalculator* is its use in developing, enhancing or augmenting internal or third-party information security assessment models. Results produced from the scoring exercise can assist an organization's security personnel in preparing for audits, identifying resource requirements, and gaining an understanding of needed system security improvements. In addition, the *Kalculator* has the potential to produce industry benchmarking data.

While multi-level quantitative and qualitative risk assessments and sophisticated analysis processes are evolving, they are difficult to implement for many institutions. This is in part because implementing a successful operational risk discipline often requires a significant change in corporate culture. Success depends on an organization's board of directors and senior-level management understanding of and commitment to creating an internal, enterprise-wide operational risk management structure.

[1] International Organization for Standardization/International Electrotechnical Commission "International Standard ISO: 17799: 2000 Information Technology – Code of Practice for Information Security Management" (2000).

II. BITS OPERATIONAL RISK MANAGEMENT INFORMATION SECURITY SUBGROUP

Participating Organizations
The Bank of New York Company, Inc.
BANK ONE CORPORATION
BB&T Corporation/First Virginia Banks, Inc.
City National Corporation
Comerica Incorporated
Credit Suisse First Boston
FleetBoston Financial Corporation (Bank of America Corporation)
Fortis, Inc.
National City Corporation
Northern Trust Corporation
Pershing
Raymond James Financial, Inc.
Regions Financial Corporation
SouthTrust Bank
State Farm Insurance Companies
USAA
Washington Mutual, Inc.

Special Contributions
Sharon Kaufman, The Bank of New York Company, Inc.
Roxanne Carr, Comerica Incorporated
Kenneth Schaeffler, Comerica Incorporated
Kenneth Vowels, Comerica Incorporated
Anne Thomas, Credit Suisse First Boston
Lori Blair, Fortis, Inc.
Adam Stone, Fortis, Inc.
Lori Lucas, Raymond James Financial, Inc.
Landy Dutton, Regions Financial Corporation
Marc Menninger, Washington Mutual, Inc.
Stewart Milus, State Farm Insurance Companies
Flora Stevens, Washington Mutual, Inc.

BITS Staff Contacts
Faith Boettger, Senior Consultant, faith@fsround.org
John Carlson, Senior Director, john@fsround.org
Heather Wyson, Project Manager, heather@fsround.org

BITS would like to acknowledge the efforts of Paul Smocer, Senior Vice President, Technology Assurance Services, Mellon Financial Corporation, and former BITS Senior Director Laura Lundin for their efforts in creating this project.

III. OPERATIONAL RISK FOCUS

Overview

Banks are in the business of managing risk. Risk management in the financial services industry has traditionally focused on credit, market and interest rate risks on which the industry's products and services rest. However, operational risk management has recently taken on greater strategic importance within the financial services industry. Deregulation, globalization of financial services, the industry's growing IT sophistication and reliance on technology, and a perceived increase in the risk profile of evolving financial services business models underscore the need for new forms of operational risk management.

Over the next several years, pending regulatory capital requirements will form the basis for increased prioritization of operational risk management within every major financial institution. Recent revisions to international capital standards by the Basel Committee on Banking Supervision (the "Basel Committee") have focused on risk-measurement practices and have encouraged investment in technologies to improve the measurement and management of risk.[2]

Integrated risk-management frameworks are emerging and multi-level, quantitative and qualitative risk assessments and sophisticated analysis processes are evolving. However, implementing a successful operational risk discipline will require significant changes in corporate cultures. Success depends on senior management understanding of and commitment to a robust internal risk management structure. This requires ongoing identification, evaluation, and use of "what-if" and "worst-case" scenarios based on internal and external data.

Operational risk management activities are even more complex when considered in a regulatory context. Significant changes in regulatory capital requirements for the ten to 12 largest U.S.-based and international financial services companies are introduced in the New Basel Capital Accord (Basel II). Basel II will make capital reserves more risk-sensitive and representative of the institutions' risk profile. Basel II includes a proposed addition of specific operational risk components into the capital calculation. The implementation of Basel II requires participating financial institutions to maintain a sophisticated operational risk management infrastructure to ensure the integrity of their internal risk estimates. Although the new Accord will go into effect in 2007, it requires three years of prior risk-measurement efforts. This places the onus on those financial institutions for which Basel II regulation will be mandatory (and those that are eligible and choose to participate) to implement the requirements as early as 2004. Regardless of size and the application of new capital regulation to select financial institutions, U.S. banking supervisors are likely to require all financial institutions to implement an effective framework to identify, assess, monitor, and control material operational risks as part of an overall approach to risk management.

Aside from the Basel II and regulations, there are strong motivations for instituting an enterprise-wide concentration on operational risk management. The Zurich IC2 database captured $6.5 billion in financial institution operational losses in 2002. Better business management can reduce losses, improve earnings and drive shareholder value. In addition, according to Moody's Investor's Service, "Since operational risk will affect credit ratings, share prices, and organizational reputation, analysts will increasingly include it in their assessment of the management, their strategy and the expected long-term performance of the business." [3]

---

[2] Statement of Chairman Alan Greenspan on ***The State of the Banking Industry*** Before the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, April 20, 2004.

[3] Moody's Analytical Framework for Operational Risk Management of Banks, January 2003.

Operational Risk Defined

Operational risk is defined by the Basel Committee as "the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events." Operational risk is inherent risk that affects every business unit and key support functions. For the Basel Committee and its measurement of operational risk exercises, operational risk includes legal risk but excludes strategy, reputation and systemic risk.[4] For most comprehensive, qualitative risk management programs, these risk concepts are considered and managed even if they cannot be accurately quantified.

The primary focus on operational risk has been in those categories the Committee identifies as having the potential to cause major losses, including:

1. ***Internal Fraud.*** Acts and activities that result in defrauding the bank, its customers, or tax authorities; misappropriation of property; circumvention of regulations, the law or company policy; and diversity/discrimination events involving at least one internal party. Examples include: reporting of positions; employee theft; insider trading on an employee's own account; and fraudulent advice given to clients to encourage trading activities—such as when the investment-banking function sells a stock but advises clients to buy that stock.

2. ***External Fraud.*** Acts by a third party with the intent or result of defrauding the institution, misappropriating property, or circumventing the law. Examples include robbery, forgery, check kiting, computer hacking, and denial-of-service attacks.

3. ***Employment Practices and Workplace Safety.*** All activities and acts consistent with employment, health and safety laws and/or agreements, or which result in personal-injury claims relating to employment contracts and diversity/discrimination issues. Examples include workers' compensation claims, violation of employee health and safety rules, organized labor activities, discrimination claims and all general liability.

4. ***Clients, Products and Business Practices***. Unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or such failure caused by the nature and design of a product or financial service. Examples include: inappropriate trading recommendation based on a client's requirements; fiduciary breaches; misuse of confidential information; improper trading activities on the bank's account; money laundering; and sale of unauthorized products. Legal risk related to the above is also included.

5. ***Damage to Physical Assets.*** Loss or damage to physical assets from natural disasters or other events such as terrorism, vandalism, fires, floods, storms, civil wars and strife. This extends to the risk to assets from third-party suppliers and outsourcers.

6. ***Business Disruption and System Failures.*** Includes all hardware, software, telecommunications outages, utility outages, and real estate facilities problems.

7. ***Execution, Delivery and Process Management.*** Includes the complete transaction processing environment of a financial institution. Failed transaction processing or process management, relations with trade counterparties, and relations with vendors are also included. Examples include: data-entry vendors; offshore processing vendors; collateral management and administration failures; incomplete legal documentation; unapproved access given to client accounts; outsourcing vendor disruptions and failures; non-client counterparty non-performance or mis-performance (such as

[4] Basel Committee on Banking Supervision *Consultative Document Operational Risk, Supporting Document to the New Basel Capital Accord* (January 2001).

central securities depositories, exchanges, custodians, industry processing venues and utilities), and vendor disputes and non-performance.

Operational Risk Sound Practices

Operational risk management is evolving in concept and practice. Developing an appropriate risk-management framework and demonstrating effective risk management is achieved through the explicit identification, assessment, monitoring and mitigation/control of operational risk. A solid risk-management framework involves:

- Clear strategies and oversight by the board of directors and senior management
- An appropriately robust internal control culture
- Effective internal reporting processes
- Effective contingency planning processes

The Basel Committee issued its guidance in the document "Sound Practices for Management and Supervision of Operational Risk" in February 2003 as follows:

1. *Developing an Appropriate Risk Management Environment*

   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.

   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.

   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 organization, 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.

2. *Risk Management: Identification, Assessment, Monitoring, and Mitigation/Control*

   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.

   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.

   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.

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.

3. *Role of Supervisors*

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.

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.

4. *Role of Disclosure*

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

IV. INFORMATION SECURITY: A CRITICAL COMPONENT OF OPERATIONAL RISK MANAGEMENT

Security is a fundamental building block for all financial services. It is also a legal and regulatory requirement that financial institutions must comply with to ensure the privacy and security of customer information. Securing the integrity, availability and confidentiality of information is a significant component of operational risk management. Therefore, computer hardware and software systems must play a major role in any financial institution's operational risk profile.

Information security professionals must be able to identify and communicate key operational risks (both threats and vulnerabilities). Measuring these risks requires estimating both the probability of an operational loss event and the potential scope of the loss. Risk factors that indicate the likelihood of an operational loss event occurring vary from business unit to business unit. Individual business units typically "own" their risk. Corporate support functions such as human resources, legal, and technology often are either responsible for the offshore components of related operational risks and/or feed their associated risk information into the individual business units.

Historical loss data is necessary to understand risk factors as well as to accurately model operational risks. However, since few organizations track and quantify historical loss data, information security operational risk assessments are most often judgment-based.

Financial institutions are developing and implementing a variety of enterprise-wide operational risk management techniques. These include both top-down and bottom-up approaches to assessing, measuring and managing operational risks. Scorecards, loss distributions, scenario analysis and self-assessment models are among the common tools. In most organizations, operational risk tools, data collection, and monitoring and reporting are coordinated across the enterprise.

V. AN APPROACH TO IDENTIFYING KEY INFORMATION SECURITY RISKS

General Description

The BITS Operational Risk Management Information Security subgroup was created to address financial institutions' need to better manage the information security component of operational risk. As part of this work, the subgroup developed the *Kalculator*, a spreadsheet template, to identify high-risk factors related to information security and provide a method to prioritize those risk factors. While the risk factors used in the *Kalculator* could feed into an institution's broader enterprise-wide operational risk model, they are not intended to address enterprise-wide risks.

The *Kalculator* provides an extensive list of common information-security threats, vulnerabilities and corresponding controls to mitigate those risks. The *Kalculator* should not be considered comprehensive and/or inclusive of all risks and controls. Based on the subjectivity of the inputs, the *Kalculator* is not intended to act as a reporting mechanism for an institution or the industry as a whole. Rather, it is a source of information to complement an institution's approach to identifying and prioritizing information security risk. Because there is no standard approach to the structure of financial institutions' operational risk departments, the template was designed to be flexible and customizable to suit most companies' needs. The *Kalculator* contains a method for scoring and prioritizing risks based on the likelihood of threat occurrence, the degree of control implementation, and the level of control effectiveness. Because it can sort data based on ISO 17799 categories (current default) or Basel II loss event (Level 1) categories, the *Kalculator* can facilitate an organization's internal communication by using a risk context that information security, audit, operational risk and others understand.

The risk scoring can be customized for various audiences. For example, if the data is sorted by ISO 17799 domains, security practitioners can get an overview of the ten domains to see where an institution faced the most challenges in modeling ISO 17799 guidelines. Similarly, if the data is sorted by threat events, an institution can assess whether it is responding to certain threats appropriately when compared to other institutions. The significance of risk is determined by the user inputs and considers account frequency, severity and resulting damage to mission-critical business operations, revenues or shareholder value.

Financial institutions are required to conduct information-security assessments to satisfy federal and state regulations and supervisory guidance. Though various assessment models are already in use, a secondary benefit of the *Kalculator* is its usefulness in developing, enhancing or augmenting internal or third-party information-security assessment models. Scoring exercise results can assist an organization's information security personnel in preparing for audits, identifying resource requirements, and gaining an understanding of needed system security improvements.

Key Risk Indicators
Once the top information-security risk factors have been identified, it is important to select the appropriate risk-measurement criteria for ongoing monitoring. Risk indicators are statistics and/or metrics that can provide insight into an organization's risk position. Ideally, the risk indicators are easily quantifiable measures currently available to management that clearly identify cause and effect. Examples of key risk indicators for information security might include:

- Processor availability
- Breaches in service-level agreements
- Successful system intrusions
- Attempted system intrusions
- Absence levels
- Staff turnover

- Volume of change-management events
- Password compromise
- Percentage of trained users
- Percentage of passwords configured according to policy

Development Process

There are several ways to analyze risk from information security. Information-security practitioners, auditors and others tend to take an "upstream" view of risk, focusing on threats, vulnerabilities and controls, while executive management and risk managers often focus on a "downstream" view of risk or the risk exposure and damage to assets. While the *Kalculator* was created on the basis of threats, vulnerabilities and controls, it provides a bridge to downstream risks through measurement inputs.

A comprehensive information-security assessment begins with defining the boundary or scope of the assets that may be at risk and a critical asset-identification exercise. This step should be completed by the organization prior to using the *Kalculator*. Models are based on the assumption that critical assets are identified and system boundaries are defined.

The *Kalculator* rests on the following relationships of risk terms (see Appendix B, Figure 1):

- Threats exploit vulnerabilities, which lead to risk.
- Controls stop threat exploits, thus eliminating or reducing vulnerabilities.
- Risk exposure is the potential sum of damage (costs), from risk to critical assets.

Threat, Vulnerability and Security Controls

The default threat, vulnerability and control data in the *Kalculator* is taken from a list of control questions identified by the BITS Security Assessments Project Team of the BITS IT Service Providers Working Group. Based upon the format of ISO 17799 and consistent with industry and regulatory requirements, this team of industry experts developed a worksheet (the *BITS IT Service Providers Expectations Matrix*) outlining the security practices, processes and controls that may be included in an assessment or audit of an IT service provider's operations. These control questions were converted by the subgroup into control statements and mapped to corresponding threat/vulnerability pairs.

The threat, vulnerability and control data were formatted according to ISO 17799's ten security controls[5]. The ISO 17799 standard, which is used as the basis for security risk analysis, provides recommendations for managing information security and business continuity for those responsible for initiating, implementing, or maintaining security and continuity planning in their organization.

The *Kalculator* is intended to provide a common basis for developing organizational security and recovery standards and effective risk management practices, and to provide confidence in inter-organizational dealings. Many financial services organizations are identifying their operational risk models in the context of the Basel II[6] loss event risk and data context. By using the sort function, the *Kalculator* can be reformatted based on Basel II loss event categories.

[5] See Appendix B: Figure 2 for a list of ISO 17799 Categories
[6] See Appendix B: Figure 3 for Basel II Proposed Loss Event Type Categories

Threats

A threat event is an occurrence or circumstance that has the potential to have an undesirable impact on an asset. A successful threat exploits a known or previously unknown vulnerability. A threat agent (the source of a threat) can be human-made or natural. Human-made threats can be further categorized as deliberate or accidental. Intentional threats have three important attributes: capability, motivation, and opportunity. In addition to threats that exist within a financial institution, those resulting from third-party vendor relationships must also be considered.

There are many different ways to articulate threat statements using the components listed above (actors, sources, actions, events, motivation), with no one commonly acceptable method. Publicly available resources such as ISO 17799, Carnegie Mellon University's CERT Octave program, the Information Security Forum's (ISF) Firm Methodology, and the National Institute of Standards and Technology (NIST) 800-30 publication each express information-security threats in different formats. Some models focus on threat sources or actors, while others concentrate on threat actions or events. Others incorporate both a source and an event at various levels of detail. The *Kalculator* highlights only the threat event in order to provide consistency and the ability to sort information easily.

Each threat event could be caused by multiple actors or sources with different motivations. The user of the *Kalculator* should consider the possible sources of a threat event when completing the input ratings. Once a list of top risks is determined, additional analysis should be incorporated into the risk statement before it is communicated so that the full threat event, including the various sources of a particular threat, can be fully understood.

Not all threats can be predicted or reasonably anticipated. Figure 1, "Approach to Information Security Threat Analysis," depicts the framework and a sample inventory of threats the subgroup used in creating the tool. This list provides a comprehensive set of known threats, but does not include all possible threats.

Figure 1: Sample Inventory of Threats

APPROACH TO INFORMATION SECURITY THREAT ANALYSIS

Actor (1): Human*

Access: Network

Actor (2) External

Motive

Deliberate	Accidental
➢ Unauthorized scans ➢ Unauthorized network or system access ➢ DDoS attacks ➢ Web defacements ➢ Malicious code ➢ Worms ➢ Viruses ➢ Trojan horses ➢ Network/application time bomb ➢ Network/application backdoor ➢ Virus hoaxes ➢ Social engineering ➢ Network spoofing ➢ War dialing ➢ Computer crime ➢ Lawsuits/ litigation	➢ Unintentional DDoS attack ➢ Unintentionally bad legislation

Actor (2) Internal

Motive

Deliberate	Accidental
➢ Unauthorized scans ➢ Network/application time bomb ➢ Network/application backdoor ➢ Social engineering ➢ Computer crime	➢ Human error

Access: Physical

Actor (2) External

Motive

Deliberate	Accidental
➢ War ➢ Terrorist attack ➢ Biological agent attack ➢ Bomb threats ➢ Bomb attacks ➢ Robbery ➢ Extortion ➢ Vandalism ➢ Civil disorder ➢ Sabotage ➢ "Dumpster diving"	➢ Automobile crash ➢ Airplane crash ➢ Chemical spill ➢ Radiation contamination ➢ Hazardous waste exposure ➢ Gas leaks

Actor (2) Internal

Motive

Deliberate	Accidental
➢ Work stoppage/ strike ➢ "Tailgating" to gain unauthorized access ➢ Shoulder surfing ➢ Embezzlement ➢ Sabotage	➢ Leaving doors unlocked ➢ Leaving sensitive documents exposed ➢ Leaving computer screen exposed or unlocked ➢ Discussing sensitive matters within earshot of those who don't have a need to know ➢ Lost or stolen laptops

Actor (1): Non-Human

Access: System

Actor (2) External

➢ Power failure ➢ Power fluctuation ➢ Telecom-munications failure ➢ DNS failure

Actor (2) Internal

➢ Power failure ➢ Power fluctuation ➢ HVAC failure ➢ CPU malfunction / failure ➢ System software failure ➢ Application software failure ➢ Telecom-munications failure ➢ Hardware failure ➢ Software defects

Access: Natural

Actor (2) External

➢ Floods ➢ Fire ➢ Seismic activity ➢ Volcanic eruption ➢ High winds ➢ Snow/ice storms ➢ Tornados ➢ Hurricane ➢ Epidemic ➢ Tidal wave ➢ Typhoon ➢ Solar flares ➢ Lightning

Actor (2) Internal

➢ Floods ➢ Fire ➢ Dust/sand ➢ Heat

***Human actors/threat sources:**

Outsiders, including:

Hacker	Cracker
Computer criminal	Terrorist
Industrial espionage	Customer
Computer user	Vendors/service providers

Insiders/employees, including:

End users	Developers
Database administrators	System administrators
Help desk staff	Security administers
Other personnel	Ex-employees
Disgruntled employees	

Prioritization Scoring

The *Kalculator* is one method for scoring and prioritizing the threat/vulnerability pairs. The method is based on subjective user inputs for the likelihood of threat occurrence, the degree of control implementation, and the level of control effectiveness. Numeric values are required for the spreadsheet inputs and are used for the scoring model. This approach provides a more specific level of measurement versus the simple "high, medium, and low" measurement many information-security assessment models use.

Inputs:

- The likelihood of threat, i.e., the probability of an occurrence, is defined on a 10 to 100% scale. A threat likelihood of 0% is not an option because, by definition, there is always a likelihood of a threat occurring no matter how low the probability.

- An input measure of 0 to 5 is required to indicate the degree to which a control is implemented and the impact if the control is not implemented.

Scoring Array:
A 0-to-10 numeric scoring array quantifies the intersection of the control implemented and impact inputs. The scoring array is defined as follows:

10 = Bad Control vs. High Impact—Much room for improvement
0 = Good Control vs. Low Impact—No room for improvement

	Impact If Not Implemented						
	0	**5**	**6**	**7**	**8**	**9**	**10**
Degree to which Control Is Implemented	**1**	*4*	*4*	*6*	*7*	*8*	*9*
	2	*3*	*3*	*3*	*6*	*7*	*8*
	3	*2*	*2*	*2*	*2*	*6*	*7*
	4	*1*	*1*	*1*	*1*	*1*	*6*
	5	*0*	*0*	*0*	*0*	*0*	*0*

If a control is completely implemented the score will always be zero because there is no room for improvement in action/control. Even if impact is zero, a zero control will produce a risk score of 5 because impact may change over time and organizations should be practicing at least some level of due care—a low level of control but not zero control.

Extreme Point Tests		**Control Implemented**	**Impact If Not Implemented**	**Score**	**Residual Risk**
Something severe, no controls, highly likely	100%	0	5	10	10.00
Something severe, no controls, not likely	10%	0	5	10	1.00
Something severe, strong controls, highly likely	100%	5	5	0	0.00
Something severe, strong controls, not likely	10%	5	5	0	0.00
Something minor, no controls, highly likely	100%	0	0	5	5.00
Something minor, no controls, not likely	10%	0	0	5	0.50
Something minor, strong controls, highly likely	100%	5	0	0	0.00
Something minor, strong controls, not likely	10%	5	0	0	0.00

Residual Risk Score
The residual risk score equation is the interim score from the intersection of the degree of control implementation and impact multiplied by the likelihood of threat percentage.

Interface

The *Kalculator* uses a standard Microsoft Excel® spreadsheet format. All functions and options related to the program, including filter and sort capabilities, can be applied to the tool.

Collaboration

Institutions using the *Kalculator* may need to involve individuals from disciplines outside of information security to complete the subjective input fields. Depending on company structure and/or the data already available through assessment exercises, collaboration may be necessary so that data can be contributed from one or more of the following areas:

- Business units, which initiate e-business projects to meet customer demands or a market opportunity
- Technologists, who assemble the architecture capable of performing the necessary transactions (including security services)
- Finance, which resolves the costs and benefits associated with the project's risks
- Third-party IT service providers, including cross-border outsourcing partners
- Compliance/general counsel/internal audit or other relevant control and oversight functions within the organization.

Customizing Data

The spreadsheet is completed with default information on information-security threats, vulnerabilities and controls, along with a mapping to the ISO 17799 and Basel II categories. This default information can be customized based on the institution's individual experience, environment and/or information needs. The *Kalculator* was designed for use at the enterprise level; however, it can be completed for a particular unit or specific computing platform. A sample of how one institution modified the format of *Kalculator* for their use is available on the BITS website: www.bitsinfo.org.

Likelihood of Threat

This input column allows for a percentage input from 10 to 100% for each threat/vulnerability pair.

The likelihood of threat is highly subjective. Statistically relevant measures of frequency for many threat events associated with information security do not exist. This is a significant constraint to assessing risk. The default information has been set to the average likelihood identified by the subgroup members. The average of the likelihood of threat responses from subgroup members has been set as the default position/percent for this field. The user may change the input for any given threat based on:

- The circumstances and environment of an individual institution;
- Historical experience;
- Other third-party information that may be available; and
- Personal expertise.

Users should factor several considerations into their input selection, including:

- The degree of change at the organization;
- Unique system characteristics;
- Potential threat actors/sources; and
- Available access.

For example, a vulnerability exploitable by casual users would be considered more likely to result in an incident than one requiring the resources of a hacker. This is because the act does not require special skills or prerequisites and the number of casual users is much larger than the number of hackers. Likewise, the possibility for disgruntled employees or competitors to exploit the vulnerability would be less than that of normal users and hackers. When a vulnerability can be exploited directly from the Internet or wireless area network (WAN), the risk is higher than an exploitation that requires terminal or physical access.

When considering unauthorized access, the privilege that is acquired would also determine the risk level. Super-user privilege would allow unlimited access to the entire system, so the subsequent risk is the highest. Security systems administrators' and normal users' privileges would contribute less risk as a result of more limited access to "sensitive data."[7]

Implementation of Controls

Users can input a score ranging from 0 to 5, with 0 being low and 5 being high.

Not accounted for in the *Kalculator* are the potential cumulative effects that multiple or layered controls have on addressing a particular threat/vulnerability. Users can factor the cumulative effect by modifying the score.

Impact

Users can input a score ranging from 0 to 5, with 0 being low and 5 being high.

"Impact" refers to the magnitude of harm caused by a threat's exercise of vulnerability. This is also highly subjective. Users must factor several considerations into their input selection, including the nature and sensitivity of information at risk (e.g., proprietary information, public information, customer data), its criticality to business operations, and the technology function (e.g., storage, processing, transmission,) involved in the scenario.

Common ways to view impacts in IT terms are:[8]

- **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. Thus, loss of integrity reduces the assurance of an IT system.

- **Loss of Availability.** If a mission-critical IT system is unable to reach its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' ability to function in support of the organization's mission.

- **Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from jeopardizing national security to disclosure of Privacy Act data. Unauthorized, unanticipated or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

---

[7] A Simple One-Dimensional Quantitative Risk Assessment Model, Tim Voss, Citigroup.

[8] National Institute of Standards and Technology, *Risk Management Guide for Information Technology Systems,* Pub 800-30 (January 2002).

Mapping these impact descriptors to financial results is difficult; however, establishing the relationship between technical and business metrics is necessary to understand the impact score. To accomplish this, business managers should be involved in or consulted when determining impact. The following impact rating guide may be useful in incorporating both technical and business measurements into the impact selection.

IMPACT RATING GUIDE		
No impact	No impact.	0
Minor	Some effort required to repair; minimal cost. No revenue loss.	1
Tangible	Days of unplanned effort required for repair/recovery. Significant expenses and/or some loss of revenue.	2
Significant	Weeks of unplanned effort required for repair/recovery. Significant expense and loss of revenue. Breach of confidentiality of sensitive information. Damage to reputation and confidence. Exposure to litigation.	3
Serious	Extended outage and/or loss of connectivity. Requires activation of contingency site. Months of unplanned effort required for repair/recovery. Extensive expense and loss of revenue. Compromise to integrity of large amounts of data or services. Temporary loss of facility. Damage to reputation. Regulatory concerns raised.	4
Grave	Permanent shutdown. Complete compromise. Inability to recover. Permanent loss of facility. Loss of life.	5

VI. SAMPLE SPREADSHEET: KALCULATOR

BITS KEY RISK MEASUREMENT TOOL FOR INFORMATION SECURITY OPERATIONAL RISKS

ISO Domain Reference	Basel Loss Category for Operational Risk	Threat Event	Vulnerability	Security Control	Likelihood of Threat (Input)	Degree to which Control is Implemented (Input)	Impact if Control is not Implemented (Input)	Control vs. Impact Score	Residual Ri Score
Access Control	Business Disruption and System Failures	Application software failure	Security events are not logged at the application level.	Security events are logged at the application level.				5	0.(
Access Control	Business Disruption and System Failures	Application software failure	Application testing is not performed.	Application testing is performed				5	0.(
Access Control	External Fraud	Computer crime	System access logs are not created and reviewed to identify use or attempted use and modification or attempted modification of critical systems components (files, registry entries, configurations, security settings/parameters, audit logs).	System access logs are created and reviewed to identify use or attempted use and modification or attempted modification of critical systems components (files, registry entries, configurations, security settings/parameters, audit logs).				5	0.(
Access Control	External Fraud	Computer crime	System access logs are not stored in a secure fashion with limited access and are not protected from alteration or deletion.	System access logs are stored in a secure fashion with limited access and protected from alteration or deletion.				5	0.(
Access Control	Internal Fraud	Computer crime	Policies that define the removal of information from company facilities are not in place and are not communicated to all employees.	Policies that define the removal of information from company facilities are in place and communicated to all employees.				5	0.(

VII. APPENDIX A: GLOSSARY

Basel II Accord: The new capital reserve regulation for financial institutions under proposal by the Bank for International Settlements for application to the world's major financial services companies.

Control: A safeguard put in place to eliminate or reduce the threat exploitation of a vulnerability.

Control factor: A subjective value assigned to reflect the degree to which the control is implemented and assesses the robustness of a control or the ability for the control to eliminate vulnerability.

Distributed denial of service (DDoS): An attack in which a multitude of compromised systems attack a single target, thereby causing denial of service for users of the targeted system.

Domain name service (DNS): Machines responsible for maintaining lists that translate Internet names to numbers and vice versa. DNS allows you to reference domain names instead of their actual IP address for easier recollection.

Impact: The sum of potential damage (cost) from risk to critical assets.

IT risk assessment: See "risk assessment".

ISO/IEC 17799: 2000 Code of Practice for Information Security Management: This document offers guidelines and voluntary directions for information-security managers responsible for initiating, implementing or maintaining security in their organization. It is intended to provide a common basis for developing organization security standards and effective-security management practice, and to provide confidence in inter-organizational dealings. The document is intended to be a starting point for developing organization-specific guidance, rather than to give definitive instructions or "how-tos".

Operational risk: The risk of loss resulting from inadequate or failed internal processes, people and systems or from external events.

Risk: A function of the likelihood of a given threat-source exercising a particular potential vulnerability and the resulting impact of that adverse event on the organization's assets.

Risk analysis: See "risk assessment".

Risk assessment: A study of vulnerabilities, threats, likelihood, loss or impact, and the theoretical effectiveness of security measures. The process of evaluating threats and vulnerabilities (known and postulated), to determine expected loss and establish the degree of acceptability to system operations.

Risk management: The total process to identify, control, and minimize the impact of uncertain events. The objective of the risk-management program is to reduce risk.

Risk Score: TBD

Threat event: An occurrence or circumstance with the potential to have an undesirable impact on an asset.

Threat: The potential for a threat agent or source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability.

Threat agent: The source of a threat, which can be human-made or natural. Human threats can be further categorized as intentional or unintentional.

Threat factor: A subjective value assigned to reflect the likelihood that a threat will be exploited by a vulnerability, assuming that there are no controls in place.

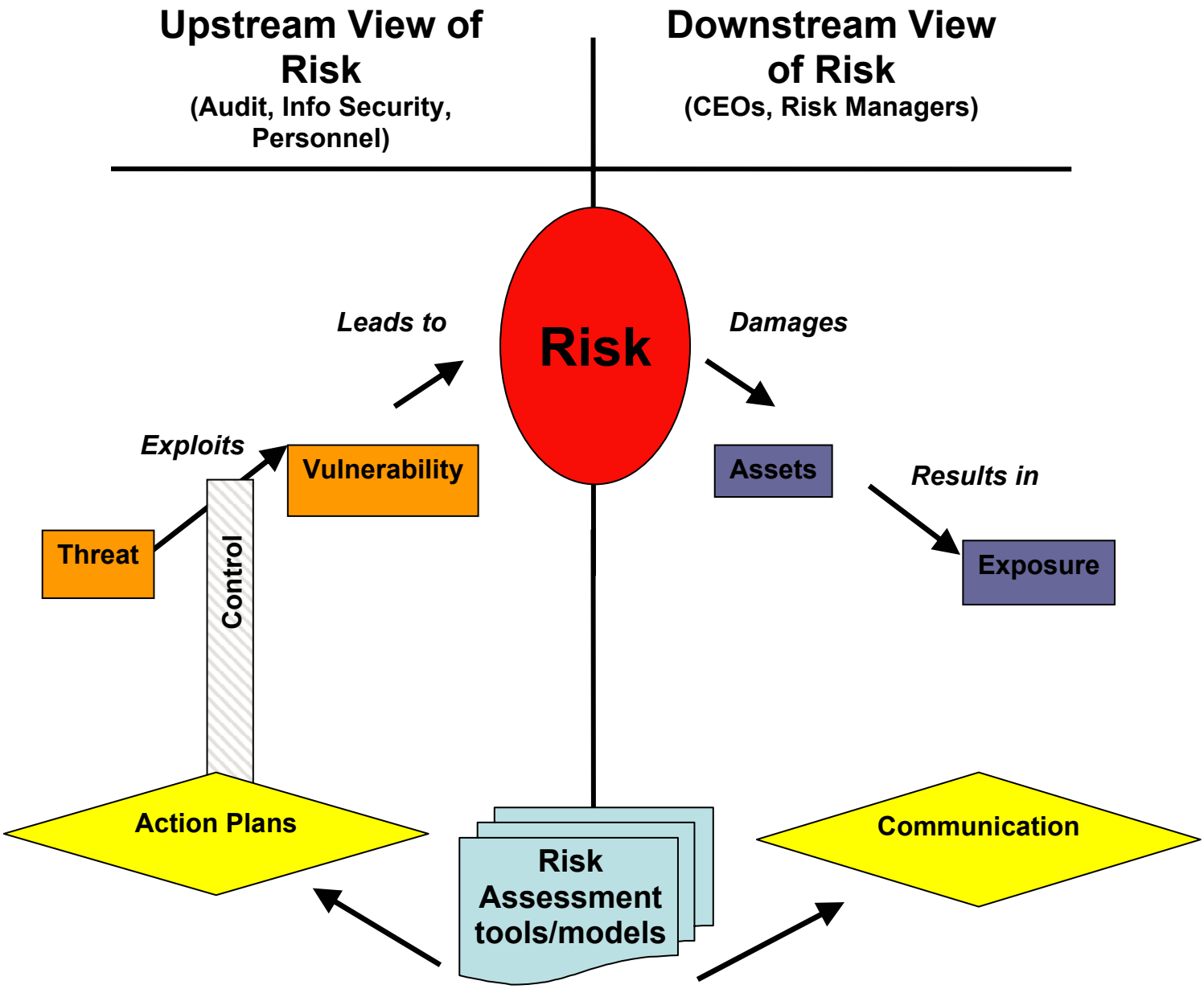
Threat source: See "threat agent".

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

Vulnerability analysis: Systematic examination of an Automated Information Security (AIS) program or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

VIII. Appendix B: Diagrams

Figure 1: Risk Relationship Summary



APPENDIX B: DIAGRAMS, CONTINUED

Figure 2: ISO 17799 Categories[9]

1. *Security Policy*
   Security Policy control addresses management support, commitment, and direction in accomplishing information security goals, including:
   - Information Security Policy document – A set of implementation-independent, conceptual information security policy statements governing the security goals of the organization. This document, along with a hierarchy of standards, guidelines, and procedures, helps implement and enforce policy statements.
   - Ownership and review – Ongoing management commitment to information security is established by assigning ownership and review schedules for the Information Security Policy document.

2. *Organizational Security*
   Organizational Security control addresses the need for a management framework that creates, sustains, and manages the security infrastructure, including:
   - Management Information Security Forum – Provides a multi-disciplinary committee chartered to discuss and disseminate information security issues throughout the organization.
   - Information System Security Officer (ISSO) – Acts as a central point of contact for information security issues, direction, and decisions.
   - Information Security responsibilities – Individual information security responsibilities are unambiguously allocated and detailed within job descriptions.
   - Authorization processes – Ensures that security considerations are evaluated and approvals obtained for new and modified information processing systems.
   - Specialist information – Maintains relationships with independent specialists to allow access to expertise not available within the organization.
   - Organizational cooperation – Maintains relationships with both information-sharing partners and local law-enforcement authorities.
   - Independent review – Mechanisms to allow independent review of security effectiveness.
   - Third-party access – Mechanisms to govern third-party interaction within the organization based on business requirements.
   - Outsourcing – Organizational outsourcing arrangements should have clear contractual security requirements.

3. *Asset Classification and Control*
   Asset Classification and Control addresses the ability of the security infrastructure to protect organizational assets, including:
   - Accountability and inventory – Mechanisms to maintain an accurate inventory of assets, and establish ownership and stewardship of all assets.
   - Classification – Mechanisms to classify assets based on business impact.
   - Labeling – Labeling standards unambiguously brand assets to their classification.
   - Handling – Handling standards; including introduction, transfer, removal, and disposal of all assets; are based on asset classification.

[9] Info Security Mgmt.: ISO 17799 October 2001 International Network Security (INS) Whitepaper

4. *Personnel Security*
   Personnel Security control addresses an organization's ability to mitigate risk inherent in human interactions, including:
   - Personnel screening – Policies within local legal and cultural frameworks ascertain the qualification and suitability of all personnel with access to organizational assets. This framework may be based on job descriptions and/or asset classification.
   - Security responsibilities – Personnel should be clearly informed of their information security responsibilities, including codes of conduct and non-disclosure agreements.
   - Terms and conditions of employment – Personnel should be clearly informed of their information security responsibilities as a condition of employment.
   - Training – A mandatory information security awareness training program is conducted for all employees, including new hires and established employees.
   - Recourse – A formal process to deal with violation of information security policies.

5. *Physical and Environmental Security*
   Physical and Environmental Security control addresses risk inherent to organizational premises, including:
   - Location – Organizational premises should be analyzed for environmental hazards.
   - Physical security perimeter – The premises security perimeter should be clearly defined and physically sound. A given premises may have multiple zones based on classification level or other organizational requirements.
   - Access control – Breaches in the physical security perimeter should have appropriate entry/exit controls commensurate with their classification level.
   - Equipment – Equipment should be sited within the premises to ensure physical and environmental integrity and availability.
   - Asset transfer – Mechanisms to track entry and exit of assets through the security perimeter.
   - General – Policies and standards, such as utilization of shredding equipment, secure storage, and "clean desk" principles, should exist to govern operational security within the workspace.

6. *Communications and Operations Management*
   Communication and Operations Management control addresses an organization's ability to ensure correct and secure operation of its assets, including:
   - Operational procedures – Comprehensive set of procedures, in support of organizational standards and policies.
   - Change control – Process to manage change and configuration control, including change management of the Information Security Management System.
   - Incident management – Mechanism to ensure timely and effective response to any security incidents.
   - Segregation of duties – Segregation and rotation of duties minimize the potential for collusion and uncontrolled exposure.
   - Capacity planning – Mechanism to monitor and project organizational capacity to ensure uninterrupted availability.
   - System acceptance – Methodology to evaluate system changes to ensure continued confidentiality, integrity, and availability.
   - Malicious code - Controls to mitigate risk from introduction of malicious code.
   - Housekeeping – Policies, standards, guidelines, and procedures to address routine housekeeping activities such as backup schedules and logging.

- Network management - Controls to govern the secure operation of the networking infrastructure.
- Media handling – Controls to govern secure handling and disposal of information storage media and documentation.
- Information exchange – Controls to govern information exchange including end user agreements, user agreements, and information transport mechanisms.

7. *Access Control*

   Access Control addresses an organization's ability to control access to assets based on business and security requirements, including:

   - Business requirements – Policy controlling access to organizational assets based on business requirements and "need to know."
   - User management – Mechanisms to:
     - Register and deregister users
     - Control and review access and privileges
     - Manage passwords
   - User responsibilities – Informing users of their access control responsibilities, including password stewardship and unattended equipment.
   - Network access control – Policy on usage of network services, including mechanisms (when appropriate) to:
     - Authenticate nodes
     - Authenticate external users
     - Define routing
     - Control network device security
     - Maintain network segregation or segmentation
     - Control network connections
     - Maintain the security of network services
   - Host access control – Mechanisms (when appropriate) to:
     - Automatically identify terminals
     - Securely log-on
     - Authenticate users
     - Manage passwords
     - Secure system utilities
     - Furnish user duress capability, such as "panic buttons"
     - Enable terminal, user, or connection timeouts
   - Application access control – Limits access to applications based on user or application authorization levels.
   - Access monitoring – Mechanisms to monitor system access and system use to detect unauthorized activities.
   - Mobile computing – Policies and standards to address asset protection, secure access, and user responsibilities.

8. *System Development and Maintenance*

   System Development and Maintenance control addresses an organization's ability to ensure that appropriate information system security controls are both incorporated and maintained, including:

   - System security requirements – Incorporates information security considerations in the specifications of any system development or procurement.
   - Application security requirements – Incorporates information security considerations in the specification of any application development or procurement.

- Cryptography – Policies, standards, and procedures governing the usage and maintenance of cryptographic controls.
- System Integrity – Mechanisms to control access to, and verify integrity of, operational software and data, including a process to track, evaluate, and incorporate asset upgrades and patches.
- Development security – Integrates change control and technical reviews into development process.

9. *Business Continuity Management*
   Business Continuity Management control addresses an organization's ability to counteract interruptions to normal operations, including:
   - Business continuity planning – Business continuity strategy based on a business impact analysis.
   - Business continuity testing – Testing and documentation of business continuity strategy.
   - Business continuity maintenance – Identifies ownership of business continuity strategy as well as ongoing re-assessment and maintenance.

10. *Compliance*
    Compliance control addresses an organization's ability to remain in compliance with regulatory, statutory, contractual, and security requirements, including:
    - Legal requirements – awareness of:
      - Relevant legislation
      - Intellectual property rights
      - Safeguarding of organizational records
      - Data privacy
      - Prevention of misuse
      - Regulation of cryptography
      - Collection of evidence
    - Technical requirements – Mechanism to verify execution of security policies and implementations.
    - System audits – Auditing controls to maximize effectiveness, minimize disruption, and protect audit tools.

APPENDIX B: DIAGRAMS, CONTINUED

Figure 3: Basel II Proposed Loss Event Type Categories[10]

Category Level (1)	Definition	Category Level (2)	Activity Examples
Internal fraud	Losses due to acts of a type intended to defraud, misappropriate property or circumvent regulations, the law or company policy, excluding diversity/discrimination events, which involves at leas one internal party	Unauthorized activity	Unauthorized Activity Transactions not reported (intentional) Trans type unauthorized (w/monetary loss) Mis-marketing of position (intentional)
		Theft and fraud	Theft and Fraud / credit fraud / worthless deposits Theft / extortion / embezzlement / robbery Misappropriation of assets Malicious destruction of assets Forgery Check kiting Smuggling Account take-over / impersonation / etc. Tax non-compliance / evasion (willful) Bribes / kickbacks Insider trading (not on firm's account)
External fraud	Losses due to the acts of a type intended to defraud, misappropriate property or circumvent the law, by a third party	Theft and fraud	Theft/Robbery Forgery Check kiting
		Systems security	Systems Security Hacking damage Theft of information (w/monetary loss)
Employee practices and workplace safety	Losses arising from acts inconsistent with employment, health or safety laws or agreements, from payment of personal industry claims, or from diversity/discrimination events	Employee relations	Compensation, benefit, termination issues Organized labor activity
		Safe environment	General liability (slips and falls, etc.) Employee health & safety rules events Workers compensation Employment Practices and Workplace Safety
		Diversity & discrimination	All discrimination types

[10] Bank for International Settlements, Basel Committee

Figure 3: Basel II Proposed Loss Event Type Categories, continued

Category Level (1)	Definition	Category Level (2)	Activity Examples
Clients, products and business practices	Losses arising from unintentional or negligent failure to meet a professional obligation to specific clients (including fiduciary and suitability requirements), or from the nature or design of a product.	Suitability, disclosure and fiduciary	Suitability, Disclosure & Fiduciary Fiduciary breaches / guideline violations Suitability / disclosure issues (KYC, etc.) Retail consumer disclosure violations Breach of privacy Aggressive sales Account churning Misuse of confidential information Lender Liability
		Improper business or market practices	Antitrust Improper trade / market practices Market manipulation Insider trading (on firm's account) Unlicensed activity Money laundering
		Product flaws	Product Flaws Product defects (unauthorized, etc.) Model errors
		Selection, sponsorship and exposure	Failure to investigate client per guidelines Exceeding client exposure limits
		Advisory activities	Disputes over performance of advisory activities
Damage to physical assets	Losses arising from loss or damage to physical assets from natural disaster or other events.	Disasters and other events	Natural disaster losses Human losses from external sources (terrorism, vandalism)
Business disruption and system failures	Losses arising from the disruption of business or system failures.	Systems	Hardware Software Telecommunications Utility outage/disruptions

Figure 3: Basel II Proposed Loss Event Type Categories, continued

Category Level (1)	Definition	Category Level (2)	Activity Examples
Execution, delivery and process management	Losses from failed transaction processing or process management from relations with trade counterparties and vendors.	Transaction, capture, execution and maintenance	Miscommunication Data entry, maintenance or loading error Missed deadline or responsibility Mode/system mis-operation Accounting error/entity attribution error Other task mis-performance Delivery failure Collateral management failure Reference data maintenance
		Monitoring and reporting	Failed mandatory reporting obligation Inaccurate external report (loss incurred)
		Customer intake and documentation	Client permissions/disclaimers missing Legal documents missing/incomplete
		Customer/client account management	Unapproved access given to accounts Incorrect client records (loss incurred) Negligent loss or damage of clients assets
		Trade counterparties	Non-client counterparty mis-performance Misc. None-client counterparty disputes
		Vendors and suppliers	Outsourcing Vendor disputes