

BITS

FINANCIAL SERVICES
R O U N D T A B L E

BITS TECHNOLOGY RISK TRANSFER GAP ANALYSIS TOOL

April 30, 2002

TABLE OF CONTENTS

INTRODUCTION	3
ROLE OF INSURANCE IN E-COMMERCE RISK MANAGEMENT WORKING GROUP	5
SPECIAL CONTRIBUTIONS.....	5
SECTION 1: ANALYZING EXPOSURES AND NEEDS	6
UNDERSTANDING IT RISK ASSESSMENT.....	6
IT RISK ASSESSMENT WITHIN THE MANAGEMENT MATRIX.....	8
IT RISK ASSESSMENT OVERVIEW	9
BOUNDARY OR SCOPE	9
ASSETS.....	10
VULNERABILITY.....	11
THREAT EVENT AND THREAT AGENT	11
ORGANIZATIONAL IMPACT	12
ANNUALIZED LOSS EXPECTANCY	12
SAFEGUARDS	13
SECTION 2: RISK TRANSFER	14
APPLICATION OF RISK ASSESSMENT TO RISK TRANSFER	14
LEGAL ENVIRONMENT	15
COVERAGE GAPS.....	15
MATRIX OF SAMPLE SCENARIOS AND GAPS IN TRADITIONAL INSURANCE.....	18
APPENDIX 1	27
RISK ASSESSMENT EXAMPLE AND EXHIBITS.....	27
PURPOSE	27
SCOPE	27
INFORMATION SYSTEM ASSETS.....	27
UNDESIRABLE EVENTS.....	29
IMPACT	29
THREAT AGENTS.....	30
VULNERABILITY	30
RISK RATING.....	31
ASSESSMENT PROCESS.....	31
COUNTERMEASURES.....	32
RESIDUAL RISK.....	32
SECURITY POLICY	32
EXHIBIT 1: INITIAL RISK ASSESSMENT	33
EXHIBIT 2: RECOMMENDED COUNTERMEASURES	34
APPENDIX 2	35
GRAMM-LEACH-BLILEY ACT SUMMARY	35

INTRODUCTION

Financial institutions must maintain a high level of trust and integrity in order for e-business to grow to the fullest extent possible, embracing new technologies. The trust of financial services customers derives from the integrity of the industry's infrastructure and information technology practices. Security is a mission-critical element that underpins this trust proposition and is integral to brand reputation. By marrying information security tools with other risk management efforts, risk can be mitigated. Yet, there is no way to be 100 percent secure. There will be residual risk created by the complex cyber-landscape. As a risk transfer mechanism, insurance can play an essential role to further safeguard the organization, its customers and its shareholders from cyber-related loss and liability exposures.

Risk management, specifically enterprise-wide operational risk management, has come to the forefront of responsibilities for executive management and boards of directors. It is imperative that all stakeholders understand the emerging risks of e-business, the potential impacts of cyber-related loss to their business model, and the array of solutions necessary to adequately meet these risk management needs as they take shape. Today's climate of rapid technological change, heightened regulatory scrutiny of technology risk, and legal uncertainties, along with the absence of standardized insurance products, makes it difficult for directors, officers, information security officers and risk managers to identify and close gaps in their institutions' risk management and risk transfer programs.

In response to this challenging environment, and to assist directors, officers, information security officers and risk managers, the BITS Role of Insurance in E-Commerce Risk Management Working Group developed the *BITS Technology Risk Transfer Gap Analysis Tool*. This document provides guidance on:

- Risk assessment, risk identification and the potential impacts that e-business activities present to organizations;
- Common obstacles encountered when applying traditional insurance products to these new or magnified exposures; and
- How the IT risk assessment process can support decisions to mitigate known vulnerabilities, to defend against threats that are likely to disrupt business activities, and to purchase specialized risk transfer insurance coverage to provide balance sheet protection.

This document is intended to improve awareness of issues that can be the basis for discussions with management and insurance professionals, as well as for an internal risk transfer analysis.

Because of the rapidly evolving nature of e-business technology, the ever-expanding universe of cyber threats, emerging insurance coverage interpretations, the availability of new products to address cyber-related losses, and the lack of standardized insurance policy language, this document should be read with the understanding that it represents the state of the insurance market at a certain point in time. Information contained in this document does not represent the opinion of any one organization in the Working Group. This document does not recommend that organizations purchase certain insurance coverage, nor does it compare specific insurance policy offerings. Licensed insurance agents, brokers, consultants and attorneys should be consulted for advice and counsel on specific insurance and risk transfer programs.

For additional information about the *BITS Technology Risk Transfer Gap Analysis Tool*, contact Laura Lundin, BITS, 202-289-4322, laura@fsround.org or Susanna Space, BITS, 505-466-6434, susanna@fsround.org.

ROLE OF INSURANCE IN E-COMMERCE RISK MANAGEMENT WORKING GROUP

CHAIR: Jeffrey S. Grange, The Chubb Corporation

PARTICIPATING ORGANIZATIONS

ABN AMRO North America, Inc.	Goldman Sachs Group, Inc.
AEGON USA, Inc.	HSBC USA, Inc.
American Bankers Association	Independent Community Bankers of America
AmSouth Bancorporation	M&T Bank Corporation
Aon Corporation	Mellon Financial Corporation
Bank of America Corporation	Nationwide
The Bank of New York Company, Inc.	PNC Financial Services Group
The Charles Schwab Corporation	Spectrum EBP, LLC
The Chubb Corporation	State Farm Insurance Companies
Citigroup, Inc.	Synovus
City National Corporation	U.S. Department of Navy
Compass Bancshares, Inc.	USAA
Credit Suisse First Boston	Wachovia Corporation
Cullen Frost Bankers, Inc.	Wells Fargo & Company
First National of Nebraska	Whitney Holding Corporation
Fortis, Inc./Assurant Group	Zurich North America Financial Enterprises

Special Contributions

Jeffrey Grange, The Chubb Corporation
Tom Schields, Zurich North America Financial Enterprises
Ted Vandenberg, Aon Risk Management Services
Lee Zeichner, LegalNet Works, Inc.

SECTION 1: ANALYZING EXPOSURES AND NEEDS

The principal goal of an organization's risk management process should be to protect the organization and its assets, and to preserve the organization's capacity to perform its mission. Information technology risk management is not, therefore, limited to protecting "IT" assets. IT risk management generally, and information security particularly, should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT systems, but as an essential, core management function of the organization.¹

Organizations of different sizes, business offerings, system complexity and management structures may vary in how they perform an assessment of IT exposure and needs. IT risk assessments may be internal or external, or a combination of internal supplemented by external reviews or assessments. Risk assessments may be abbreviated or comprehensive depending on the environment. Nonetheless, some form of IT risk assessment must be made by, or be made available to, the risk manager in order for him or her to know the extent of the organization's dependence on technology in the business model and the delivery of the overall service offering. It is equally important for risk managers to have a clear understanding of the potential vulnerabilities that arise from this dependence on technology as well as what may be required to adequately reduce and protect against the risks, including risk transfer.

Even if organizations have not entertained new business channels of online consumer interaction and transactions such as online banking, online trading, mortgage originations, aggregation services and electronic bill presentment and payment, many are supporting these business processes electronically via the Internet or Web-based technology, and are using corporate intranets for email, shared documents and other applications. They may also use extranet systems for processing, information feeds or purchasing. Increasingly, organizations are embracing outsourcing as a strategic element of an overall technology platform and service delivery. A comprehensive risk assessment should go beyond understanding security practices, taking into account non-system factors such as legal liability, regulatory compliance issues and the potential impact on the foregoing where outsourcing to third-party IT vendors is part of the network configuration. This section outlines some of the major components of an IT risk assessment for understanding the scope and exposure of cyber-related activities, and provides an example for ranking and prioritizing the level of impact.

Appendix 1 provides a sample of a generic, non-industry-specific IT risk assessment as described in this section. It is for illustrative purposes and shows only a fractional portion of an IT risk assessment.

Understanding IT Risk Assessment

The nature of electronic business presents a special challenge for IT security. Both the business processes and the associated technology are relatively new creations. As a result, security for e-business has an unknown and unknowable quality, and the resulting risks range from the uncertain to the ambiguous. Insights into e-business risk are gained by breaking down risk into its related elements. This process can help in examining what role insurance has in addressing risks associated with information technology and, more specifically, electronic commerce.

¹ NIST *Risk Management Guide for Information Technology Systems* Pub 800-30.

IT risk assessment is a control activity performed by management and used to identify the information system security requirements for e-business. The domain of information systems for e-business includes data, applications, technology, facilities, processes, proprietary network configurations and people associated with e-business processes.² IT risk assessment is a process by which risk in each of these areas is analyzed, measured and quantified. An IT risk assessment uses both data and judgments about a system, and attempts to quantify or scale risks on a detailed, but comprehensive, basis. The assessment is essentially a knowledge process that documents the measurable security state of a system using the consensus judgments of system stakeholders. Commercially available computer applications can help structure the process and manage the data collection and reporting, thus reducing the complexity of the process.

For financial institutions, a formal risk assessment process is now also a mandated compliance requirement. It is important to note that an IT risk assessment for an institution's entire information system is referenced throughout the supervisory guidelines for bank examination under the new requirements of the Gramm-Leach-Bliley Act (GLBA). The July 1, 2001 Federal Financial Institutions Examination Council (FFIEC)/GLBA "joint rule" on safeguarding customer information states that the risk assessment process should identify "reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems." It joins over a dozen previous federal laws, in addition to state laws, addressing the protection of customers of financial institutions.³ Appendix 2 outlines the GLBA guidelines for customer information security.

In addition to these legislative and regulatory requirements, there are other significant legal reasons to perform an enterprise-wide assessment. First and foremost, assessing significant IT risk is a corporate governance responsibility. Several well-known cases since the Y2K turnover have begun to lay a solid due diligence foundation for corporate officials relating to risks that can undermine corporate value. These cases do not mandate that companies perform IT risk assessments, but they squarely address emerging requirements for directors and officers to ask the right questions and demand sufficient and responsive answers about risks associated with corporate assets.⁴

Second, Enron Corporation's current situation will likely result in significant administrative reforms relating to risk management and transparency. The extent to which companies disclose their risk posture is already being discussed. Currently, several European countries, including the U.K., require risk management disclosures as part of the financial disclosure process.

Third, federal and state law influences the extent to which companies are self-insuring. For example, courts across the country have addressed the extent to which "business interruption" coverage may be triggered. Multiple "business interruption" coverage disputes have already been filed as part of the litigation from the September 11 terrorist attacks on the U.S. A thorough assessment and review

² CoBiT Implementation Tool Set, IT Governance Institute, Information Systems Audit and Control Foundation. Third Edition. July 2000.

³ For some institutions, state laws impose similar privacy and security requirements; in other cases, federal laws, such as the Health Insurance Portability and Accountability Act (HIPAA) might also apply to financial institutions.

⁴ See, e.g., *In Re Caremark Int'l Inc.*, 698 A.2d 959, 967 (Del. Ch. 1996) (hereafter "Caremark") citing *Gagliardi v. Tri Foods Int'l Inc.*, 683 A.2d 1049, 1051 (Del. Ch. 1996) (1996 Del. Ch. LEXIS 87 at p. 20) (hereafter "Gagliardi"). Although the leading case on the subject of director fiduciary duty of care occurred in Delaware state court, other jurisdictions and federal courts have subsequently followed its reasoning and it stands as a guide for corporate directors to understand certain legal due diligence obligations. See also *McCall v. Scott*, 250 F.3d 997 (6th Cir. 2001); H.L. Brown, *The Corporate Director's Compliance Oversight Responsibility in the Post Caremark Era*, 26 Del. J. or Corp. L. 1 (2001).

will underscore residual risks, even though officials throughout the company assume that risks have been managed appropriately.

The risk assessment is used to determine the appropriate technical and non-technical safeguards to be applied to reduce specific risks to acceptable levels. Every system has risks that cannot be eliminated. Residual risks are those risks that remain after safeguards are applied. After determining what the residual risks are, a decision can be made on avoidance or transfer of the residual risks. The suitability of particular insurance policies to transferring those infrequent, unexpected and potentially catastrophic cyber-related risks that the organization cannot afford to bear on the balance sheet is discoverable by analyzing the policy and mapping coverage over to the identifiable IT assessment elements.

IT Risk Assessment within the Management Matrix

Just as IT security is not simply the application of technology “fixes,” the IT risk assessment process is a matrix of people, processes and technology. It is important to place IT risk assessment into a management framework. The process co-joins at least five functional areas in an organization:

- The business units, which initiate e-business projects to meet customer demands or a market opportunity;
- The technologists, who assemble the architecture capable of performing the necessary transactions (including security services);
- The finance department, which resolves the costs and benefits associated with the project’s risks;
- The third-party IT service providers, including offshore outsource partners; and
- The compliance/general counsel/internal audit areas or other relevant control and oversight functions within the organization.

The IT risk assessment process requires a collaboration of the viewpoints and contribution of data from each of these areas. However, organizationally, the judgments and responsibilities of these areas are diverse and may conflict. The marketing, technical and financial viewpoints of IT risks may be quite different. The essential conflict is between uncertain benefits and the certainty of costs and constraints of building in IT security. The decomposition and measurement process is a framework for consensus.

The IT risk assessment process has indirect benefits to the organization. Connecting profit-making activities to IT capabilities and a total risk/cost/benefit analysis is a strategic activity. The IT risk assessment process provides a catalyst for this activity. Managers and staff from diverse functional areas work together to understand their respective decision processes and priorities. This strategic activity is part of the payoff of engaging in IT risk assessment; it supports the alignment of business strategy and IT capabilities.

IT Risk Assessment Overview

An IT risk assessment is a decomposition process that separates the elements of risk and provides a qualitative or quantitative evaluation of each individual element. Risk is the threat of both tangible and intangible loss to an asset. Risk arises as a consequence of the existence of assets, vulnerabilities and threat events/agents. *Figure 1, Elements of an IT Risk Assessment*, depicts the interrelationship of these elements. Risk assessment also includes analysis of safeguards and design constraints. Each of these elements has a set of classifications, characteristics and measurements.

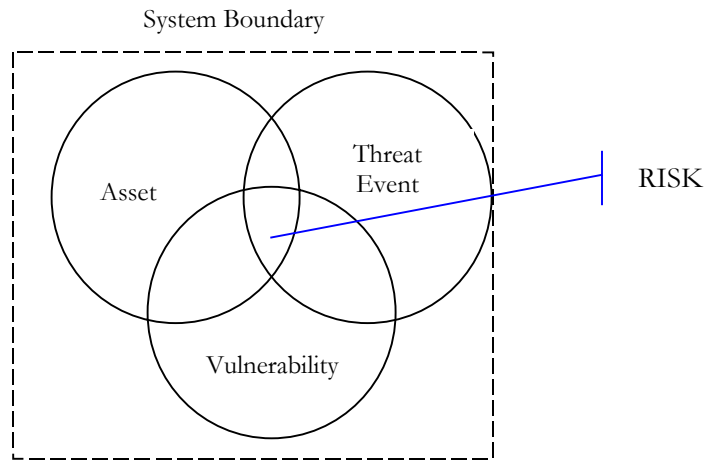


Figure 1. Elements of an IT Risk Assessment

Exhibit 1 in Appendix 1 presents a partial sample of a qualitative IT risk assessment.

Boundary or Scope

The top-level decision for an IT risk assessment is the boundary or scope of the assets to be assessed.⁵ Boundaries characterize the part of the system being considered. Within the business processes of e-business, the boundaries of assets to include in the assessment are ambiguous. In the example of Internet banking, many elements important to completing transactions are not owned and controlled by the financial institution. Public telephone networks, Internet host provider equipment, and even the customer's PC and browser software are assets potentially within the boundary of the process. Significant reliance on third-party IT service providers extends in effect the organization's security perimeter and should be factored into the scope of the assessment for critical business functions.

Even for internal systems, the boundary for assets to be considered is fuzzy. For example, email messages from customers using Internet banking services may be handled by the same servers that support the financial institution's general business correspondence. These messages are more likely to include data such as account information. The e-business assets involved are, obviously, the email servers and the email messages themselves. Not all email data are the same from a security viewpoint. The same asset may be used for both e-business and ordinary business purposes.

⁵ Stoneburner, Gary, Alice Goguen, Alexis Feringa. *Risk Management Guide for Information Technology Systems*. National Institute of Standards and Technology, U.S. Department of Commerce. Special Publication 800-30. October 2001.

An IT risk assessment process for e-business must include any part of the systems that input, output, process, store or transmit the related data. It is useful to limit the boundary to assets that the institution owns or for which it pays. However, consideration should be given to all of the information system elements of the business process that must work together to achieve the company's objectives. The possibility of cascading damages or interdependencies with other systems can have a profound impact on the assessment. Some judgments about the boundary of assets for e-business processes presuppose knowledge of risks that have not yet been determined. This constrains the validity of the IT risk assessment process.

Assets

An IT asset is a definable element of an information system that has value, i.e., something that the organization naturally wants to protect. IT assets include:

- Data and information
- Software/applications
- Hardware
- Communications services
- People (key technical managers and staff)
- Facilities

Assets have both tangible and intangible value to consider. For example, the tangible value of data is what it would cost to restore or replace without the application of safeguards (i.e., no backup is available). The intangible value of data is its confidentiality, integrity and availability. (These terms have specific meaning within the domain of information systems.) A breach of confidentiality happens, for example, when:

- A hacker gains unauthorized access to private and confidential data; or
- An authorized user/insider exceeds his or her authorized access to the system and gains unauthorized access to private and confidential data.

The organization may have been deprived of the value of the asset and may have sustained a loss, but the tangible value of every line of application code is still 100 percent intact—nothing is damaged, destroyed, altered or erased. Nevertheless, a significant risk has been realized and certain costs may be borne.

Assets have many attributes that may be useful to collect for the assessment, such as location, type and age. However, the primitive attribute for assessment is value. An asset's value includes cost (quantitative value) and importance (qualitative value). Some assets either do not have a tangible value or the value is too difficult to measure. In this case a qualitative value is useful to assess. The qualitative value of an asset is assigned by consensus judgment using a relative-scale semantic rating.

It is important to note that the value of business data has changed dramatically. Not only is the sheer volume of business data doubling each year but also the data involve all manner of confidential and proprietary customer records, trade secrets and other forms of intellectual property. In many cases these data may actually sit outside the organization's proprietary network with a third-party IT service provider.

Asset valuation must include all the costs required to make an organization whole after a loss: replacement or restoration, loss of productive use before restoration, time required for restoration, cost of recovery measures that may be employed, opportunity costs, labor and management

resources. Some of these costs are time-based, requiring knowledge of the duration between the event and the full restoration of the asset. Legal, competitive, social and regulatory conditions must be accounted for in assessing the value of assets such as data. These are costs that will be borne by or imposed on the organization under circumstances where security standards or expectations are violated.

Vulnerability

A vulnerability is a weakness of an asset that can be exploited by a threat. Vulnerabilities “allow” threats to occur, or for them to occur with greater frequency or impact. Vulnerabilities exist in at least three discrete levels:

1. Those inherent to the IT asset itself—“off the shelf” security vulnerabilities from a technology vendor inherent to the asset’s normal use or defects to the normal use. For example, operating systems have an administrative level logon privilege that allows an authorized user to access special functions. Though this is a normal feature of operating systems, it is also a vulnerability that can be exploited.
2. Those inherent to the unique, proprietary network configuration of the organization.
3. Those that arise due to operator error or malfeasance.

Some vulnerabilities result from a combination of system elements being used together. At any given point in time, for a given system, not all vulnerabilities are known. This is especially true with the relatively new technologies associated with e-business. Unknown vulnerabilities are a constraint to the validity of the IT risk assessment process.

When conducting an IT risk assessment, the assets managed by third parties must also be assessed. Knowledge of a vendor’s systems is required to assess the vulnerabilities associated with those assets. The determination of which third-party operations to assess depends on the scope or boundary of the analysis.

Threat Event and Threat Agent

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. Threat events have two properties associated with risk assessment: frequency and severity. Frequency is the expected number of occurrences in a given time period and is a backward-looking measure. Statistically relevant measures of frequency for many threat events associated with e-business do not exist. This is a significant constraint on the validity of the IT risk assessment process.

Threat severity is, in relation to the asset, impacted by the threat and has a measurement of 0 to 100 percent, suggesting the percent value of the asset affected. A threat agent (the source of a threat) can be human-made or natural. Human threats can be further categorized as intentional or unintentional. Intentional threats have three important attributes: capability, motivation and opportunity. Again, threats that arise from third-party vendor relationships must also be included in the assessment.

Organizational Impact

“Impact” refers to the magnitude of harm caused by a threat’s exercise of vulnerability. The level of impact is governed by the potential mission impacts and in turn produces a relative value for the IT assets and resources affected. A common way to view impact is as follows:⁶

- **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 unavailable 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’ performance of their functions in supporting 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.

Some tangible impacts can be measured quantitatively in lost revenue, the cost of repairing the system, or the level of effort required to correct problems caused by a successful threat action. Other impacts (e.g., loss of public confidence, loss of credibility, damage to an organization’s interest) will be more difficult to measure in specific units. For impacts to assets with intangible value, a qualitative assessment of impact is assigned based on a consensus of responsible individuals using a semantic relative scale. Appendix 1 presents a scalar impact rating and summary description. The related numeric scale value is logarithmic to reflect the appropriate quantitative impact.

Impact is already partially qualified by the identification of the asset and the description of the potential undesirable event. However, impact should be further qualified so that better judgments about the impact can be made and a better understanding gained about how the impact is related to the actual organizational areas and the respective management that may be affected if the risk is presented. Since the impact qualities will vary with each risk, a common framework such as Porter’s Value Chain or Balanced Scorecard may be beneficial.

Annualized Loss Expectancy

Impacts can be quantified using the following classic quantitative algorithm, which is the foundation for information security risk assessment:

$$\text{Asset Value} \times \text{Exposure Factor} \times \text{Annualized Rate of Occurrence} = \text{Annualized Loss Expectancy}$$

Equation 1. Annualized Loss Expectancy (ALE)⁷

⁶ NIST *Risk Management Guide for Information Technology Systems* Pub 800-30.

The “exposure factor” is the measure of threat severity. Revised versions of this algorithm include factors for the application and cost of safeguards, and the uncertainty or confidence intervals for the values taken.

Safeguards

The IT risk assessment indicates the selection of safeguards to be applied. Safeguards are technical and non-technical measures taken to reduce risk. The application of safeguards is unique to each combination of assets, threats and vulnerabilities, although safeguards often overlap several of these risk “sets.” Examples include physical security measures, environmental controls, password schemes, and data backup and hardware redundancy.

Not all safeguards are available. The application of safeguards may be constrained by time, money, technology, social factors, environmental factors or law. In addition, safeguards may be constrained by risk of failure or control risk. There is the possibility that the safeguard will not function as designed. An organization balances the certain cost of safeguards with the estimated cost of risk as determined by the annualized loss cost or by a qualitative rank ordering. If a quantitative analysis is done, the annualized loss expectancy (ALE) allows a cost/benefit determination and ranking of the safeguards to apply.

⁷ *Guidelines for Automated Data Processing Physical Security and Risk Management*, NIST FIPSPUB-65, 1974.

SECTION 2: RISK TRANSFER

Residual risk is the level or cost of risk remaining after safeguards are applied and control risks associated with safeguards are accounted for. Some residual risk will exist throughout an organization's information systems. No safeguards can eliminate risks completely; some safeguards cannot be applied due to constraints and others will not be effective. If the level or cost of residual risk is unacceptable, a choice must be made to forego the business activity that creates the risk, bear the risk or transfer the risk. Having arrived at the level of residual risk for the information systems elements within the scope of the IT risk assessment, we can now apply the assessment to the determination of transferring that risk, specifically through the purchase of insurance. By mapping the IT risk assessment to parts of the proposed insurance agreement, a determination can be made about whether the agreement indeed transfers the risk and what portion of the risk is transferred.

Application of Risk Assessment to Risk Transfer

The list of system assets associated with the residual risk, such as hardware, data, etc., should be compared to the subject of the insurance policy or the thing that is insured. The threat/threat event corresponds to the defined causes of loss under the policy. The tangible value of the asset (if evaluated) corresponds to the limits of coverage for the loss.

The analysis then turns to the contract language for the available insurance policies. Whether or not coverage is afforded under existing or proposed insurance policies is discoverable by reading the policy and mapping the IT risk assessment elements to the policy language. A coverage gap may exist for residual risks for which coverage is available but not currently in force. Practically speaking, the onus is on the proposer (an insurance agent or company representative) to confirm that coverage is available for a given residual risk defined by the assessment. The proposer will also need to account for the full contract terms, conditions, limits and exclusions that may take away or reduce coverage otherwise under the contract. This is a significant improvement from the risk manager having to defend insurance purchase decisions to stakeholders and senior management in response to proposed scenarios of IT risk related to the e-business.

In attempting to map coverage to the identified risk, ambiguity will still exist. Financial institutions will have several insurance policies. Even though the elements of the risk are known, a single risk may not map completely to one contract or line of coverage. How one policy relates to another will be a contributing factor to e-business coverage questions. Secondly, insurance experts are reluctant to interpret coverage language definitively where the contract language is ambiguous. Interpretation of cyber-insurance contract provisions prior to an actual claim is also problematic. The true coverage afforded by an e-business policy is subject to the actual claim occurrence, claim, adjustment practices, litigation and settlement. This is a natural market condition as insurance companies attempt to cover emerging risks.

If a quantitative risk assessment is performed, the annualized cost of the residual risk is also known. The price of insurance coverage is then comparable to the dollar value of the risk exposed. A determination can be made as to the cost/benefit of transferring the risk based on this comparison. It is likely that there will not be a direct match between the risk and the coverage. A judgment must be made on the overall costs/benefits of insurance as a satisfactory way to transfer residual risk.

Insurance is not a countermeasure. Instead, it is a financing method for financially quantifiable residual risk, a finance tool for the expected annual financial loss and a transfer of uncertainty. Any risk assessment is only an estimate of the annual cost of loss within a certain degree of certainty—it can be wrong. Purchasing insurance transfers the expected loss and the uncertainty to a certain fixed cost.

Legal Environment

IT security risks can be transferred or transformed by other means, such as through vendor agreements and disclaimers. However, the vendor must be able to assume the risk, because there may be marketing and regulatory or legal factors that constrain the ability to disclaim risk. Contracts can be used to assign liability, for example, with click-on agreements with customers and between linked sites to help avoid lawsuits for denial of service or other events. Contracts are not sufficient however, for the larger problems created by an open, global network in which there are often no contracts and in which both the parties doing business and those doing damage are unknown.

A financial institution can be the target of attacks, but also can be a conduit of attacks on its customers or business partners' systems. Understanding third-party accountability and first-party loss related to cyber-activities is a necessary component of assessing risk transfer of cyber-exposures. However, the legal arena is immature when it comes to cyber-related activity, and there is ambiguity about levels of responsibility, duty of care and liability. Software manufacturers generally have not been held liable for errors in their products, service providers generally have not been held liable for failures to provide service or allowing attacks through their systems, and a duty of corporations to take steps to ensure network security has not yet been established. In addition, e-business has spurred new legal ambiguities about common insurance definitions—most notably the definition of property as it relates to intangible information assets and the definition of “loss” or “damages.”

Organizations need to also be aware of the requirements new legislation imposes on various e-business activities such as digital signature laws and consumer protection and privacy. Expert e-business legal counsel should be retained to review contractual agreements with customers, suppliers, service providers and partners.

Coverage Gaps

The goal of identifying gaps in coverage is to ensure that areas of large, potentially uninsured loss can be transferred, and to fill in those identified gaps in the portfolio of insurance coverages purchased by the organization. Cyber-risks were not contemplated when traditional policies were crafted and underwritten. As organizations evaluate their coverage and identify coverage to respond to those gaps, it is important to recognize that electronic perils have unique qualities that are challenging when addressed with traditional insurance policy structure and language. There are also practical limitations such as capacity maximums and the uninsurability of some risks, like systemic risks related to the Internet.

In addition to paying special attention to definitions and exclusions, the following principles of insurance should be questioned during this process:

- **Jurisdiction.** Many insurance policies are limited to events occurring in a certain geographical area. With the Internet, a website can expose an organization to events worldwide. Even with worldwide coverage provisions, legal liability, regulatory compliance and other factors will differ and complicate the potential for insurance settlement.
- **Valuation.** Traditional indemnity and reimbursement valuation clauses do not contemplate damages to or loss of intangible items. Intangible assets such as data and related loss-costs such as lost business opportunity, lost productivity and reputation damage are often associated with cyber-related events.
- **Trigger of loss event.** Cyber-related loss often lacks a clear, identifiable point for cause of loss and event date. Traditional trigger theories such as point in time exposure, injury in fact (point of injury/damage), manifestation (point when damage is first detected) and continuous exposure (numerous occurrences span over time and several policy periods/years) found in various traditional insurance policies may not be appropriate for the cyber-environment. Point in time exposure may be the most ambiguous. For example, when a hacker has introduced a malicious code into an organization's network, point in time occurrence could be defined as any of the following: the point when the hacker first gains access to the system; the date when the hacker is detected, despite having come into the network several times through the same hole; the date the bad code is first installed; the date the bad code is detected; or the date on which the bad code executes.⁸
- **Proof of loss.** Establishing accountability for loss and providing necessary details to prove a loss or request a claim investigation will be more complex when dealing with cyber-events. Cyber-related losses will invariably take on a degree of technical complexity and cost previously not contemplated under traditional insurance policies. Costly specialized computer forensic investigation skills will be required. Further, there will be complex standards for establishing an uninterrupted "chain of custody" and evidentiary standards for forensic loss data. In order to make an insurance policy respond effectively in the event of a loss, organizations may have to institute certain monitoring procedures or keep continuous and accurate activity logs for forensic analysis and claim investigation.

Insurers are becoming more forthright in defining the intent and scope of their coverage policies. Yet, each insurance policy and company is likely to have differing stances on the application of coverage to various cyber-related loss situations. Several insurers have begun offering new specialty products to specifically address cyber-risk. Here again, different insurers have different strategies for packaging and offering new coverage policies for cyber-related risk. Coverage forms and pricing are expected to change rapidly.

Traditional insurance coverages that could serve to address e-business or cyber-related risk for financial institutions are listed below. This is not an exhaustive list. Each of these policies should be examined for sufficiency of coverage, gaps that may exist, and how the insurance carriers view coverage intent before analyzing new product offerings.

⁸ Fiderus, *E-Business Risk and Exposures*, 2000.

<i>First Party</i>
Property, including Computer Property
Business Interruption
Crime Bonds - (Forms 14, 15, 24, 25 or equivalent)
Computer Crime
Extortion/Kidnap and Ransom
Vicarious Liability and Supervision of Service Providers
Difference in Conditions
<i>Third Party</i>
Directors' and Officers' Liability
E&O: Banker's Professional Liability/Insurance Company E&O/Broker E&O
Media E&O - (Copyright and Trademark Infringement)
General Liability
Excess Casualty/Umbrella
<i>Other</i>
Alternative Risk Transfer - Finite Risk, Captive Programs, Manuscript Catastrophe

Matrix of Sample Scenarios and Gaps in Traditional Insurance

The following matrix provides a view of sample scenarios involving cyber-related events. Potential organizational impacts are listed, along with the typical traditional insurance products risk managers may turn to in order to find coverage for such events, and the gaps they may find in relying on that coverage.

<i>Scenario - Event Example</i>	<i>Organizational Impact</i>	<i>Type of Traditional Insurance Coverage</i>	<i>Typical Coverage Gap or Issue with Traditional Coverage</i>
A disgruntled employee programs a logic bomb into the payroll system, programming it to destroy data two weeks after his or her name is removed from the system.	Payroll disruption. Employee dissatisfaction and lowered morale. Expense to reconstruct data records.	Property Insurance (Commercial Property or Computer Property policy) Crime – Financial Institution Bond	Coverage may not include intangible data. Coverage may not include intentional acts of employees.
A denial-of-service attack is launched against your rented systems that are technically owned by your third-party application service provider, causing a severe degradation of service to your online investment application.	Customer lawsuits claiming missed opportunities. Negative publicity. Loss of business income during the denial of service.	Property Insurance (Commercial Property or Computer Property policy) General Liability	Coverage may only apply to only those systems within direct ownership or control, or a direct attack against the insured (not an application service provider or Internet service provider). Coverage may apply only if there is a complete outage rather than a degradation of service.
An interruption by an attack against your domain name service provider or against an Internet backbone/ telecommunication infrastructure provider impedes your network and Internet service.	Customer lawsuits claiming missed opportunities. Negative publicity. Loss of business income during the denial of service. Blocked data feeds can cause a backlog or delay in settlements.	Property Insurance (Commercial Property or Computer Property policy)	Utility exclusions or other potential catastrophe exclusions would preclude coverage from applying. An Internet service provider is often considered a utility by definition.
Hackers pirate your proprietary trading simulation software and a worm left behind infects network backups of the program.	Loss of intellectual property. Costs to rebuild or reconstruct the application. Loss of income from inability to rely on trading data.	Property Insurance (Commercial Property or Computer Property policy)	Property coverage may not extend to data, damage, loss or theft of assets in electronic form such as intellectual property, trade secrets or proprietary software data.

<i>Scenario - Event Example</i>	<i>Organizational Impact</i>	<i>Type of Traditional Insurance Coverage</i>	<i>Typical Coverage Gap or Issue with Traditional Coverage</i>
Hackers pirate, cont.			Coverage valuation is based on the cost of reproducing the “media,” e.g., the disk rather than the inherent value of the data.
A software engineer programming your new bond rating system makes an error that is later detected when the software glitch causes problems with your network architecture.	Incorrect bond rating causes higher risk. Possible monetary loss. Additional costs for repairing rating system.	Property Insurance (Commercial Property or Computer Property policy)	Losses arising out of human programming errors are excluded.
Hackers crack into your building’s environmental system and shut down services, causing evacuation and outage in the building.	Negative publicity. Fear/confusion of employees. Additional security measures needed. Loss of confidence. Loss of productivity.	Property Insurance (Commercial Property or Computer Property policy)	The cause of loss must be from covered perils, which typically do not extend to computer virus/manipulation.
Hackers hijack numerous computers on the Internet and instruct each one to flood your website with phony data. Your site becomes overloaded, effectively slowing or shutting down the entire site to real customers.	Customer lawsuits claiming missed opportunities. Negative publicity. Loss of business income during the denial of service.	Business Income/ Extra Expense	Direct physical damage or loss to property (or personal property within a certain distance) must cause the suspension at the premises described in the policy declarations. Defines “period of restoration” as the period of time that typically begins 24 to 48 hours after the time of direct physical loss or damage for Business Income coverage, and ends when the damaged property should be repaired with reasonable speed or business is resumed at a new permanent location. In the world of e-commerce, a 48-hour waiting period could be more damaging to business than the loss itself.

<i>Scenario - Event Example</i>	<i>Organizational Impact</i>	<i>Type of Traditional Insurance Coverage</i>	<i>Typical Coverage Gap or Issue with Traditional Coverage</i>
A virus is planted on your website that snatches users or automatically moves the view from your site to another one without your permission or knowledge.	Loss of business income as customers and prospects are routed from your website. Additional income lost as site repairs are made after discovery. Possible lawsuits for missed opportunities.	Business Income/ Extra Expense	Direct physical damage or loss to property (or personal property within a certain distance) must cause the suspension at the premises described in the policy declarations. Defines “period of restoration” as the period of time that typically begins 24 to 48 hours after the time of direct physical loss or damage for Business Income coverage, and ends when the damaged property should be repaired with reasonable speed or business is resumed at a new permanent location. In the world of electronic commerce, a 48-hour waiting period might be more damaging to business than the loss itself.
A virus is launched, bringing down your system for two days. Customers are unable to log onto their investment services accounts or transact business.	Loss of business income. Possible lawsuits for missed opportunities. Negative publicity. Loss of customer confidence and possible loss of large accounts. Cost to patch and repair infected systems.	Business Income/ Extra Expense	Coverage is for actual lost income or extra expenses associated with restoring operations, not for lost business “opportunity.”
A malicious worm introduced through email accounts hits your central processing area. There is no direct damage but you are unable to clear transactions for two days while engineers work to fix the problems.	Additional costs to reconstruct the processing systems. Slowdown and possible backlog in settlement transactions. Loss of business income. Possible lawsuits for missed opportunities. Negative publicity. Loss of customer confidence and possible loss of large accounts.	Business Income/ Extra Expense	Coverage trigger is based on a direct physical damage loss to property at the premise described in the policy and caused by a covered cause, often not including viruses. A loss of service does not constitute direct damage.

<i>Scenario - Event Example</i>	<i>Organizational Impact</i>	<i>Type of Traditional Insurance Coverage</i>	<i>Typical Coverage Gap or Issue with Traditional Coverage</i>
A virus hits your network server. Internal and external resources are called in to work around the clock to scan and repair/rebuild internal corporate functions and minimize the down time.	Huge costs to repair server. Loss of business income and possible lawsuits for missed opportunities.	Business Income/ Extra Expense	A “time” deductible for coverage may apply requiring an average 72 hours after the time of direct physical loss.
A professional identity-theft ring hacks into your system and steals customer information and records.	Negative publicity. Loss of customer confidence combined with possible lawsuits. Cost to notify customers and close and reissue accounts.	Computer Crime	Coverage applies only to direct financial loss of property.
A recent worm outbreak infects your entire back office systems, spreading through your network after being introduced via a network connection to the Internet.	Extra costs associated with longer transaction processing time. Costs to restore network. Possible loss of customer data.	Computer Crime	The definition of virus does not include machine-to-machine propagation but rather only covers loss due to the physical introduction or placing of a virus into a system.
An outsider enters a bank’s network using the Internet, sets up and debits several phony accounts, and issues instruction to wire transfer to a foreign account.	Possible negative publicity. Loss of customer confidence and customer accounts. Monetary losses from wire transfer.	Computer Crime	Loss at covered, physical premises is required to trigger policy coverage.
Customers using aggregation services provided by you but outsourced to a third party have their PINs/ passwords stolen and accounts drained.	Loss of customer confidence/trust. Possible customer lawsuits. Possible monetary loss under regulatory obligation to make the customer whole.	Computer Crime	Coverage does not extend to non-proprietary systems and networks.

<i>Scenario - Event Example</i>	<i>Organizational Impact</i>	<i>Type of Traditional Insurance Coverage</i>	<i>Typical Coverage Gap or Issue with Traditional Coverage</i>
An external hacker steals customer authentication mechanism data residing on your server.	Additional security measures needed. Costs to change customer authentication information. PR expenses. Possible monetary loss.	Computer Crime	The definition of data is limited to information stored on media, not information stored in the memory of the computer or server. Misappropriation of a record is not covered. Loss of confidential material is not covered and coverage for data is provided only for costs to reproduce the data.
An employee of a third-party service provider who has access to your proprietary systems uses that access, and exceeds his or her authority, redirecting interest calculations to his or her own account.	Negative publicity. Additional security measures needed for third-party employees. Lawsuits against third party and possible change of partner. Monetary and data losses.	Computer Crime	Losses caused by employees or other third parties that had authorized access and exceeded their authorization are excluded from coverage. (Everyone who has a Web browser potentially could have access to a company's proprietary system.)
A worm takes advantages of a hole written into popular Web server software by a software design engineer and proliferates through your organization.	Possible business interruption and loss of income. Costs to repair network, improve security standards and implement new software.	Computer Crime	Exclusions may be present that eliminate any coverage for losses caused by fraudulent features contained in commercial software programs designed to be sold to multiple customers. Coverage might cover destruction and damage of data but not specifically alteration or deletion of data or programs.
An Internet merchant, who is a commercial customer of your institution, fails to fulfill its orders, yet places the credit card processing. When customers do not receive their merchandise, the institution is obliged to credit their credit cards.	Monetary losses.	Crime – Financial Institution Bond	Loss of uncollected funds is typically excluded. Coverage is not afforded for losses arising from the use of credit or debit cards.

<i>Scenario - Event Example</i>	<i>Organizational Impact</i>	<i>Type of Traditional Insurance Coverage</i>	<i>Typical Coverage Gap or Issue with Traditional Coverage</i>
A disgruntled employee sabotages your website. Trying to deface the site, the employee causes a complete outage.	Negative publicity. Loss of business income. Possible lawsuits from customers for missed business opportunities. Cost to reconstruct the website.	Crime – Financial Institution Bond	Coverage for employee dishonesty may require a condition of employees with intent to cause a loss and to obtain a financial benefit.
An employee steals your non-public and confidential customer information from an online banking application service provider working with your account.	Negative publicity. Loss of confidence/image. Costs for improving security measures. Losses from customer lawsuits.	Crime – Financial Institution Bond	Coverage does not extend to third-party IT service providers beyond processors of checks and other accounting records. Covered property other than money and securities does not include proprietary and confidential information.
An employee accesses your high-net-worth customers' authentication information and uses it to open other accounts and funnel funds into fraudulent accounts.	Negative publicity. Possible lawsuits and movement of large accounts. Monetary losses.	Crime – Financial Institution Bond	Coverage is excluded if the employee was an authorized user.
Your network is hacked by a professional who copies and sells the customer information via legitimate channels.	Negative publicity. Loss of customer confidence/trust. Possible customer lawsuits and movement of accounts. PR expenses.	Crime – Financial Institution Bond	The definition of theft does not contemplate theft by copying or viewing.
A criminal obtains your customers' passwords through scanning home computers and passes false instruction for funds transfer, acting as the customers.	Negative publicity. Monetary losses to make the customers whole.	Crime – Financial Institution Bond	Coverage for losses related to electronic funds transfer does not extend to email instruction or transfers initiated via Internet access.
A criminal manipulates your authentication technology, applies for an online loan and diverts the funds to an account at another institution.	Monetary loss of loan. Costs to tighten authentication technology and possible loss of customers.	Crime – Financial Institution Bond	Coverage for forgery or counterfeit and for loss in the extension of credit process requires original documents with a "wet" signature and an on-premise transaction.

<i>Scenario - Event Example</i>	<i>Organizational Impact</i>	<i>Type of Traditional Insurance Coverage</i>	<i>Typical Coverage Gap or Issue with Traditional Coverage</i>
An organized crime group threatens to hijack your website, introduce malicious code, or release your customer information to the public if not paid a certain sum of money.	Additional security measure costs. Extortion losses including payments to extortionist, investigative expenses, etc. Potential lawsuits from customers. PR expenses. Management diverted from strategic focus.	Crime – Financial Institution Bond	Extortion is limited to threats against persons or physical property. If amended, it may be extended to cover virus threats only.
Your new retirement funds management service website is launched with details that are in violation of a stated privacy policy. The violation brings about litigation from several large corporate customers and regulatory action.	Negative publicity. Possible loss of several large customers. Monetary loss from claim settlement plus defense expenses. Management diverted from strategic focus.	General Liability	General liability insurance is directly connected to physical exposures, designed to cover tangible bodily injury and property damage. Coverage extends to violation of a person’s right to “private occupancy” but does not extend to other privacy violations or to the misuse of the private information.
A business process patent is the source of litigation against you regarding your use of a process that provides easy navigation to customers visiting your website.	Management diverted from strategic focus. Negative publicity. Loss of income as you redesign/ re-engineer the site. Defense expenses.	General Liability	General liability insurance is directly connected to physical exposures, designed to cover tangible bodily injury and property damage. Patent infringement is not usually covered by liability policies.
An outsider steals information on your high-net-worth customers by breaching your network security. Customers file lawsuits for breach of security and unauthorized disclosure.	Management diverted from strategic focus. Negative publicity. Loss of customer/prospect confidence and large accounts move. Defense expenses.	General Liability Errors and Omissions Crime – Financial Institution Bond	General liability insurance is directly connected to physical exposures and is designed to cover tangible bodily injury and property damage. Bond coverage is provided for damage or destruction to programs, data and media (hackers, viruses, time bombs, etc.), in which case the afforded protection only pays the costs to replicate lost materials.

<i>Scenario - Event Example</i>	<i>Organizational Impact</i>	<i>Type of Traditional Insurance Coverage</i>	<i>Typical Coverage Gap or Issue with Traditional Coverage</i>
An outsider steals information, cont.			Bond does not cover loss of inherent value of intellectual property or proprietary software resulting from misappropriation. Malfunction of electronic systems (breach of security) is not covered in errors and omissions.
Your email system spreads a computer virus to a corporate customer, which results in the deletion of thousands of files in its purchasing system. The customer sues for lost revenues and extra expenses caused by your transfer of malicious code.	Negative publicity. Loss of customer confidence and confidence of other large accounts. Customer lawsuits claiming loss of data and image. PR expenses.	General Liability Errors and Omissions	General liability insurance is directly connected to physical exposures, designed to cover tangible bodily injury and property damage. Malfunction of electronic systems (breach of security) is not covered in E&O.
Customers bring suit after a breach in network security allows for information on their identity to be lifted and publicly misused.	Negative publicity. Loss of customer confidence. PR expenses. Claim settlement losses and large defense expenses.	General Liability	Coverage for emotional distress and other non-financial losses from the misuse of a customer's private information is not covered. Identity theft loss might be considered a private action concern, but with Gramm-Leach-Bliley it could be considered a regulatory violation.
Information for your trading partners which is included via framing/linking from your website is found to be misleading and incorrect.	Possible claims resulting from libel or slander, copyright infringement, misuse of information or loss of business opportunity.	General Liability	Liability coverage for damage to others' property is limited to tangible property. Coverage does not extend to liability for the improper use of third-party information.

<p>The software application you designed to offer free online bill presentment and payment service on behalf of your top commercial customers is flawed and fails to execute automatic payment amounts.</p>	<p>Potential customer lawsuits. Possible loss of top commercial customers.</p>	<p>Errors and Omissions Directors' and Officers' Liability</p>	<p>Coverage is traditionally only afforded to those financial services offered for a fee. Providing security is not a business objective and therefore even if not specifically excluded, no coverage would be granted for situations of loss purely because of a breach of security.</p>
<p>Regulatory examiners cite violations to prescriptive Gramm-Leach-Bliley security and privacy provisions and file suit against the board of directors for failure to fulfill responsibilities as required under the regulation.</p>	<p>Negative publicity. Potential risk to personal assets of directors and officers.</p>	<p>Errors and Omissions Directors' and Officers' Liability</p>	<p>Regulatory suits and actions can be excluded.</p>

APPENDIX 1

RISK ASSESSMENT EXAMPLE AND EXHIBITS

Purpose

The purpose of the risk assessment is to:

- Identify and evaluate the threats to information systems (IS) assets
- Assess the impact on the organization should threat events occur
- Identify the vulnerability associated with each IS asset and the probability of loss or damage
- Provide the analysis of the relative severity of all risks to IS assets
- Allow a cost/benefit analysis to be made on security countermeasures associated with assets

Scope

The work product for this project is a risk assessment for the information systems of “X” corporation. The project is the responsibility of the IS security manager, staff and the Security Committee.

The risk assessment will:

- Identify each asset
- Define undesirable events related to the asset
- Assess the impact of the event and assign a scalar rating
- Identify the threat agent related to the event and assign a scalar rating
- Assess the vulnerability of the asset to the threat agent and assign a scalar rating
- Calculate an overall risk rating and ranking

Information System Assets

IS security department staff have identified the following IS assets by type. This preliminary assessment will be supplemented with input from the Security Committee.

1.0 Information and Data		
Asset	Location	Comments
1.1 Stored electronic documents, including email messages		Humanly readable text documents such as memos, plans, letters and the text of email communications.
1.2 Stored data		Other information stored in a database including corporate data, product data and customer information.
1.3 Stored graphics		Photos, designs, diagrams and maps stored in any graphical format.
1.4 Public website content		Text content of company public website.
1.5 Private website content		Text content of company private website

2.0 Hardware		
Asset	Location	Comments
2.1 Workstations		Individual PCs, laptops and personal digital devices.
2.2 Product-level servers		Computer servers that are dedicated to supporting a particular product. These include engineering, design, coding and testing of applications related to specific products or services and database servers related to a product.
2.3 Business unit servers		Computer servers that support a business unit or business location for general applications used internally such as word processing and spreadsheets, and database servers containing unit-level data and information.
2.4 Enterprise servers		Computer servers that support corporate-wide applications such as human resources, law, finance and corporate communications. Includes enterprise database servers.
2.5 Functional servers		Servers supporting specific technical applications.
2.51 Email		Email gateway and address resolution servers.
2.52 Firewall		Gateway access protection and detection servers.
2.53 Internet		Internet gateway access servers.

3.0 Software		
Asset	Location	Comments
3.1 General		General business applications purchased from standard vendor.
3.2 Specialized		Specialized applications.
3.3 Own develop		Custom-designed application.
3.4 Product		Software application products for resale.
3.5 Configuration		Configuration files; computer information used by other applications to customize the configuration of hardware or other applications.

4.0 Communications		
Asset	Location	Comments
4.1 Routers, switches, hubs, cabling, connections, dedicated communications lines		Communications equipment supporting computers and computer-based communications or data transfer.
4.2 Stored files		Electronic files related to communications such as IP address resolution, internal addressing schema, designs and layout of communications hardware.

5.0 People/Staff		
Asset	Location	Comments
5.1 Management and administrative		IS managers and system administrators.
5.2 Technical support		People supporting corporate-wide information systems.
5.3 Product development		People undertaking product development projects involving information systems and services.

Note: The remainder of this example provides the supporting text for the preliminary risk assessment. The preliminary risk assessment presented in this document is abbreviated and limited to a few sample assets, events and threats and is for demonstration purposes only.

Undesirable Events

The preliminary risk assessment proposes a list of potential undesirable events associated with the IS assets presented. Undesirable events are proposed and defined by the IS security department staff and reviewed by the Security Committee.

Impact

Undesirable events are rated on a logarithmic scale for the impact to the organization, should the event occur. The assessment is made based on the proposed graded scale. “Catastrophic” is used to describe an event that would seriously impair the organization’s survival.

Impact Rating		
Rating	Description	Scale Value
Critical	Impact would be broad in scope, permanent and catastrophic.	30 – 100
High	Impact would be limited scope, but permanent or catastrophic.	3 – 30
Medium	Impact would be of a limited duration or limited scope.	.3 – 3
Low	Impact would be of a limited duration and small scope, and not catastrophic.	0 – .3

The ratings are the result of supporting work by the security staff and the management of the asset in question and the consensus of the Security Committee. The impact rating takes into account the cost of the asset involved and whether the item can be replaced, substituted or re-created.

Threat Agents

Threat agents are people, organizations or circumstances with both the intent and capability for bringing about an undesirable event. Threat agents are characterized as either internal (employees or circumstances created by them) or external (other people and circumstances created by them or dependent events). Threat agents identified are all possible agents, regardless of whether they actually exist.

Threat agents are rated on a proportional scale representing the likelihood of such a threat agent existing for each asset. The rating is determined by the opinions of the information security staff supported by relevant documentation and the consensus of the Security Committee.

Threat Rating		
Rating	Description	Scale Value (%)
Critical	Very likely to certain to exist	75 – 100
High	Likely to very likely	50 – 75
Medium	Somewhat likely to likely	25 – 50
Low	Nonexistent to somewhat likely	0 – 25

Vulnerability

Assets have a set of inherent characteristics that makes them vulnerable to threat agents. Though vulnerabilities may be part of the intentional design of an asset, they can be exploited by threat agents leading to an undesirable event. The vulnerability description is based on an analysis of each asset and its threat agents.

Vulnerability is rated on a graded, proportional scale representing the likelihood that the vulnerability identified will be exploited by the identified threat agent. The vulnerability rating is

determined by the opinions of the information security staff, and supported by relevant documentation and the consensus of the Security Committee.

Vulnerability Rating		
Rating	Description	Scale Value (%)
Critical	Very likely to certain to be exploited	75 – 100
High	Likely to very likely	50 – 75
Medium	Somewhat likely to likely	25 – 50
Low	Nonexistent to somewhat likely	0 – 25

Risk Rating

The risk rating is a numeric summation of the relevant risk factors identified according to the following formula:

$$\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Impact}$$

The risk rating provides a relative comparison of all risks in the evaluation. The relative comparison supports the determination of priority for implementation of countermeasures. The risk level is a meaningful characterization of the numeric rating.

Risk Level		
Rating	Description	Scale Value
Critical		30 – 100
High		3 – 30
Medium		.3 – 3
Low		0 – .3

The risk level provides a common framework for management in assessing risk and for developing policies regarding acceptable risk levels for various IS assets.

Assessment Process

Exhibit 1, Initial Risk Assessment, provides an analysis of the initial risk to IS assets. According to the security policy established by management, a “high” risk level is an unacceptable condition. A review of the risk analysis by management suggests that appropriate countermeasures be implemented, addressing the areas of high risk identified in the analysis.

Countermeasures should be recommended to reduce or eliminate vulnerabilities. After countermeasures have been implemented and are working, a residual risk assessment determines whether the unacceptable risks have, in fact, been reduced. The security policy establishes the level of acceptable residual risk based on the cost/benefit of implementing additional countermeasures.

The risk assessment will be reevaluated at regular intervals. Certain events also trigger revised risk assessment, such as the acquisition of new IS assets.

Countermeasures

Countermeasures are designed to insulate the organization against threats and reduce vulnerability to protect information assets. Countermeasures may address a single threat or vulnerability or a category or group of threats or vulnerabilities. The choice of countermeasures is supported by the relative risk rating of the asset they are designed to protect and by a cost/benefit analysis using the cost of the countermeasure and amount of reduction in the risk rating provided by that countermeasure. Exhibit 2, Recommended Countermeasures, proposes countermeasures to address the “high” risk level vulnerabilities identified in the initial risk assessment. Management also addresses environmental exposures in the “medium” risk category in the recommended countermeasures.

Residual Risk

The initial assessment is then revised to indicate the reduction in the threat rating and vulnerability rating based on the implementation of the countermeasures recommended. According to the security policy, a “medium” risk rating is an acceptable risk level for the assets in question based on the current cost of implementing countermeasures.

Security Policy

The risk assessment is a part of the security policy of the company. The risk assessment must be part of a cycle of continuous evaluation and improvement that incorporates changes over time. The risk assessment performance is provided by policy and by the determination of the IS security manager, based on significant changes in the organization’s assets or other risk factors.

Exhibit 1

INITIAL RISK ASSESSMENT

#	Critical Assets	Potential Undesirable Events	Impact Rating	Threat Category / Adversary	Threat Rating (%)	Vulnerability Description	Vuln. Rating (%)	Overall Risk (0-10)	Risk Level Crit (Lo - Med - Hi)
1	Stored Information			Internal					
1.3	Graphics			Human Intentional					
1.31	Design	Destruction, Copying, Alteration	25	Dishonest emp	40	System Access and Privileges	60	6.00	High
		Destruction, Copying, Alteration	25	Disgruntled emp	40	System Access and Privileges	60	6.00	High
				Unintentional					
		Destruction, Copying, Alteration	25	Negligent	40	System Access and Privileges	40	4.00	High
				External					
				Human					
		Destruction, Copying, Alteration	25	Ex-employee	70	System Access and Privileges	40	7.00	High
		Destruction, Copying, Alteration	25	Competitor	40	System Access and Privileges	20	2.00	Medium
		Destruction, Copying, Alteration	25	Other unauthorized	20	System Access and Privileges	20	1.00	Medium
2	Hardware			Internal					
2.2	Product-level Servers	Stolen, damaged, destroyed		Human Intentional					
		made unusable, malfunction,	25	Dishonest emp	40	System Access and Privileges	50	5.00	High
		normal fault or failure,	25	Disgruntled emp	40	System Access and Privileges	50	5.00	High
		abnormal fault or failure		Unintentional					
			25	Negligent	40	System Access and Privileges	40	4.00	High
				Human Intentional					
			25	Dishonest emp	40	Physical Access to Hardware	20	2.00	Medium
			25	Disgruntled emp	40	Physical Access to Hardware	20	2.00	Medium
				Unintentional					
			25	Negligent	40	Physical Access to Hardware	30	3.00	Medium
				Event					
			30	Fire	30	Heat Generation, Physical Exposure	30	2.70	Medium
			30	Explosion	10	Heat Generation, Physical Exposure	10	0.30	Low
			30	Water flood/leak	10	Physical Exposure of Equipment	10	0.30	Low

Exhibit 2

RECOMMENDED COUNTERMEASURES

#	Critical Assets	Vulnerability Description	Countermeasure
1	Stored Information		
1.3	Graphics		
1.31	Design	System Access and Privileges	Single sign-on authentication: password and user ID
			Discretionary access control: by policy and administrative process
			Firewall server/software
			Audit process: system monitored and logged events
2	Hardware		
2.2	Product-level Servers	System Access and Privileges	Discretionary access control: single sign-on authentication
			Firewall server/software
			Audit process: system monitored and logged events
			Screening of system administrative personnel
2	Hardware		
2.2	Product-level Servers	Physical Access to Hardware	Physical access controls: magnetic card entry
			Screening of system administrative personnel
			Security devices: digital camera monitor/recording
		Physical Exposure of Equipment	Environmental controls: heat sensors and sprinklers

APPENDIX 2

GRAMM-LEACH-BLILEY ACT SUMMARY

Gramm-Leach-Bliley Act Guidelines for Customer Information Security

Agencies

The Office of the Comptroller of the Currency (OCC), Board of Governors of the Federal Reserve System (Board), Federal Deposit Insurance Corporation (FDIC), and Office of Thrift Supervision (OTS), Treasury (collectively, the Agencies).

Effective Date

July 1, 2001

The Agencies have published final guidelines establishing standards for safeguarding confidential customer information. The guidelines implement sections 501(b) of the GLBA, and went into effect on July 1, 2001.

The guidelines require financial institutions to establish information security programs to:

- Identify and assess the risks that may threaten customer information;
- Develop a written plan containing policies and procedures to manage and control these risks;
- Implement and test the plan; and
- Adjust the plan on a continuing basis to account for changes in technology, the sensitivity of customer information, and internal or external threats to information security.

The guidelines outline specific security measures that institutions should consider in implementing a security program. Financial institutions must adopt appropriate security measures.

Development and Implementation of Information Security Program

A. Involve the Board of Directors. The board of directors or an appropriate committee of the board of each bank shall:

1. Approve the bank's written information security program; and
2. Oversee the development, implementation and maintenance of the bank's information security program, including assigning specific responsibility for its implementation and reviewing reports from management.

B. Assess Risk. Each bank shall:

1. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;
2. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information; and
3. Assess the sufficiency of policies, procedures, customer IS and other arrangements in place to control risks.

C. Manage and Control Risk. Each bank shall have an information security program designed to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:

1. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means;
2. Access restrictions at physical locations containing customer information, such as buildings, computer facilities and records storage facilities to permit access only to authorized individuals;
3. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
4. Procedures designed to ensure that customer information systems modifications are consistent with the bank's information security program;
5. Dual control procedures, segregation of duties, and employee background checks for employees with responsibility for or access to customer information;
6. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;
7. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies;
8. Measures to protect against destruction, loss or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures;
9. Trained staff to implement the bank's information security program; and
10. Regular testing of the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the bank's risk assessment. Tests should be conducted or reviewed by independent third parties or by staff independent of those that develop or maintain the security programs.

D. Oversee Service Provider Arrangements. Each bank shall:

1. Exercise appropriate due diligence in selecting its service providers;
2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these guidelines; and
3. Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.

E. Adjust the Program. Each bank shall monitor, evaluate and adjust, as appropriate, the information security program in light of any relevant changes in technology, the sensitivity of its customer information, internal or external threats to information, and the bank's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems.

F. Report to the Board. Each bank shall report to its board or an appropriate committee of the board at least annually. This report should describe the overall status of the information security program and the bank's compliance with these guidelines. The reports should discuss material

matters related to its program, addressing issues such as: risk assessment; risk management and control decisions; service provider arrangements; results of testing; security breaches or violations and management's responses; and recommendations for changes in the information security program.

G. Implement the Standard. Each bank must implement an information security program pursuant to these guidelines by July 1, 2001.

H. Two-year Grandfathering of Agreements with Service Providers. Until July 1, 2003, a contract that a bank has entered into with a service provider to perform services for it or to function on its behalf satisfies the provisions, even if the contract does not include a requirement that the service provider maintain the security and confidentiality of customer information, as long as the bank entered into the contract on or before thirty days after date of this publication.