CRC Press
Taylor & Francis Group
AN AUERBACH BOOK

# Oracle Identity Management

## Governance, Risk, and Compliance Architecture

Third Edition

Marlin B. Pohlman

# Oracle Identity Management

## OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

**802.1X Port-Based Authentication**
Edwin Lyle Brown
ISBN: 1-4200-4464-8

**Audit and Trace Log Management: Consolidation and Analysis**
Phillip Q. Maier
ISBN: 0-8493-2725-3

**The CISO Handbook: A Practical Guide to Securing Your Company**
Michael Gentile, Ron Collette and Thomas D. August
ISBN: 0-8493-1952-8

**Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI**
Debra S. Herrmann
ISBN: 0-8493-5402-1

**Crisis Management Planning and Execution**
Edward S. Devlin
ISBN: 0-8493-2244-8

**Computer Forensics: Evidence Collection and Management**
Robert C. Newman
ISBN: 0-8493-0561-6

**Curing the Patch Management Headache**
Felicia M Nicastro
ISBN: 0-8493-2854-3

**Cyber Crime Investigator's Field Guide, Second Edition**
Bruce Middleton
ISBN: 0-8493-2768-7

**Database and Applications Security: Integrating Information Security and Data Management**
Bhavani Thuraisingham
ISBN: 0-8493-2224-3

**Guide to Optimal Operational Risk and BASEL II**
Ioannis S. Akkizidis and Vivianne Bouchereau
ISBN: 0-8493-3813-1

**How to Achieve 27001 Certification: An Example of Applied Compliance Management**
Sigurjon Thor Arnason and Keith D. Willett
ISBN: 0-8493-3648-1

**Information Security: Design, Implementation, Measurement, and Compliance**
Timothy P. Layton
ISBN: 0-8493-7087-6

**Information Security Architecture: An Integrated Approach to Security in the Organization, Second Edition**
Jan Killmeyer
ISBN: 0-8493-1549-2

**Information Security Cost Management**
Ioana V. Bazavan and Ian Lim
ISBN: 0-8493-9275-6

**Information Security Fundamentals**
Thomas R. Peltier, Justin Peltier, and John A. Blackley
ISBN: 0-8493-1957-9

**Information Security Management Handbook, Sixth Edition**
Harold F. Tipton and Micki Krause
ISBN: 0-8493-7495-2

**Information Security Risk Analysis, Second Edition**
Thomas R. Peltier
ISBN: 0-8493-3346-6

**Investigations in the Workplace**
Eugene F. Ferraro
ISBN: 0-8493-1648-0

**IT Security Governance Guidebook with Security Program Metrics on CD-ROM**
Fred Cohen
ISBN: 0-8493-8435-4

**Managing an Information Security and Privacy Awareness and Training Program**
Rebecca Herold
ISBN: 0-8493-2963-9

**Mechanics of User Identification and Authentication: Fundamentals of Identity Management**
Dobromir Todorov
ISBN: 1-4200-5219-5

**Practical Hacking Techniques and Countermeasures**
Mark D. Spivey
ISBN: 0-8493-7057-4

**Securing Converged IP Networks**
Tyson Macaulay
ISBN: 0-8493-7580-0

**The Security Risk Assessment Handbook: A Complete Guide for Performing Security Risk Assessments**
Douglas J. Landoll
ISBN: 0-8493-2998-1

**Testing Code Security**
Maura A. van der Linden
ISBN: 0-8493-9251-9

**Wireless Crime and Forensic Investigation**
Gregory Kipper
ISBN: 0-8493-3188-9


## AUERBACH PUBLICATIONS

www.auerbach-publications.com
To Order Call: 1-800-272-7737 • Fax: 1-800-374-3401
E-mail: orders@crcpress.com

# Oracle Identity Management

## Governance, Risk, and Compliance Architecture
## Third Edition

Marlin B. Pohlman

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business
AN AUERBACH BOOK

CRC Press
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742


Version Date: 20131031

International Standard Book Number-13: 978-1-4200-7248-8 (eBook - PDF)

# Contents

# Preface

An identity management system is defined as the management of the identity life cycle of entities (subjects or objects) during which the identity is established, described, and destroyed. What this definition fails to cover is the social, personal, and financial impact of the identity life cycle.

Before I joined Oracle as director of GRC Product Strategy with the goal of creating a product that would address corporate governance, shareholder risk, and regulatory compliance, I had been a specialist in identity management for 14 years. Having worked at Netscape with Tim Howes and Frank Chen, and having participated in IETF working groups, I was no stranger to the social impact of technologies.

After Netscape was acquired by AOL and then Time Warner, I learned that the corporate officers had acted unethically, issuing three times the stock options for which they had shares. I was crushed, because I not only believed in my former employer but I believed in the value of the stock options. During that time in my life, I had been diagnosed with a rare form of Hodgkin's lymphoma and was in need of a stem cell transplant. The insurance handled most of the medical bills, but the co-payments were costly. Without the ability to exercise my stock options, I lacked the funds for the insurance co-payments.

Fortunately, I still had professional worth despite my partial inability to work, and an excellent manager from Oracle hired me. I found Oracle to be an ethical company for giving me health benefits while I was ill, and due to my employment with them, I was able to receive treatment through two years of stem cell transplant and chemotherapy while working remotely. It was at this juncture that I realized my career was more than a way to increase the wealth and efficiency of the corporation for which I worked; it was a way for me to take this life lesson and become an instrument of change.

# Introduction

Corporations are often seen as inherently amoral and driven to secure profits for their shareholders. This is because those empowered to ensure accountability often have no visibility into the inner workings of the business. Legislation is the tool society uses to hold those in power responsible to the community in which they interact, but without a strong regulatory "immune system," cancers of injustice and fraud can spread through the corporate entity in the same way cancer cells injure a body.

Identity management is the first line of defense in the corporate internal ecosystem; it enables the corporate structure to know who is doing what, where. From this base knowledge of identity patterns, behavior and governance can then be established to ensure the corporate entity behaves in a healthy, symbiotic manner with its partners, shareholders, employees, and society. In this work we strive to create a governance ecosystem that enables a business to act in a profitable manner, employing enlightened self-interest to create a better world. This is the best I can do with the second chance I have been given.

The goal of this work is to enable you to leverage the Oracle Identity Management Suite in conjunction with Oracle's other governance, risk, and compliance products to facilitate regulatory compliance and good corporate governance. In the first four chapters we cover the nature of what has come to be called governance, risk, and compliance or GRC for short. We outline a common taxonomy for the GRC space, cite standards that are used, and illustrate compliance frameworks that information systems auditors and corporate performance experts use to measure good corporate governance and security. We then present a meta-framework that we at Oracle use to abstract the control criteria defined by legislation and the compliance frameworks themselves, which often have overlapping interpretations and measures.

Using this meta-model, we present you with a detailed method to implement and configure our identity management product suite to obtain the control objectives we have identified through analysis of auditor reports, compliance frameworks, and the legislation itself. Finally, we provide a taxonomy of the legislation we have encountered throughout the world and, in Appendix A, illustrate how our applications and technology, including our Identity Management product suite, enable a corporation to meet the legal mandates within multiple legal jurisdictions with a single unified solution.

A secondary goal of this book is to empower those charged with stewardship of the corporation, be they corporate board members, legal expert witnesses, or auditors, with a tool they can use to measure their own efforts in meeting the compliance duties entrusted to them. Board members and executive management need technical guidance when reviewing the solutions presented. Consultants and vendors alike often pitch product and service without mapping the solution back to

the legislative driver that spawned its adoption. This soloed approach leads to redundancy of effort and excessive expense, directly counter to the board members' duties to shareholders. Using this text, a corporate steward can map those solutions directly to region and legislation, and can hold service providers accountable for the proper deployment and configuration of those service.

# About the Author

In addition to serving on the board of directors for three publicly traded multinational corporations, Dr. Marlin Pohlman is director of governance, risk, and compliance (GRC) product strategy at Oracle Corporation. Dr. Pohlman has lectured in the university systems of New Mexico, Arizona, and Minnesota, as well as spoken at Burton Group, Gartner, AMR, BC Government Identity Management Symposium, and the Veritas Nobel Laureate invitational. Dr. Pohlman is recognized as one of the primary educators worldwide on identity management, regulatory compliance, and corporate governance. His affiliations in this field include the Information Systems Audit and Control Association (ISACA), The Burton Group, the Institute of Internal Auditors, RSA Security Conference, DefCon, AMR Research, and Gartner.

With over 18 years experience in x.500 and LDAP-based directory structures, he has led directory server implementation for companies such as Ford Motor Company, the Automotive Industry Action Group, Home Depot, Citigroup, AXA Insurance, Bank of New York, Alliance Capital, GE Equity, Federal Express, and the U.S. Department of Defense credit card issuance system. An original contributor to the IETF ASID and DIX working group, Dr. Pohlman implemented the world's second implementation of RFC 1777 for Sanlam Insurance in Cape Town, South Africa. The directory structure implemented in Sydney, Australia, for the 2000 Olympics held the record for the largest non-x.500 meta-directory implementation in a client–server environment.

Dr. Pohlman received his Ph.D. in computer science from Trinity University, with a thesis "Scaling Factors in Very Large, High Availability Directory Architectures." He has authored three texts on identity management, two texts on GRC, and is a Licensed Professional Engineer, Certified Information Systems Auditor, Certified Information Security Manager, and Certified Information Systems Security Professional. While at Oracle, Dr. Pohlman has worked on wide-ranging security programs for various customers including governmental agencies, educational institutions, financial services companies, and healthcare organizations. He is coauthor of the Oracle Unified Method, an iterative and incremental development process framework developed by Oracle. In the area of identity management and GRC he created a roadmap for achieving successful implementation of all Oracle products, including applications and middleware. In this comprehensive work, Dr. Pohlman leverages his experience as both a corporate board member and corporate governance solution implementer to provide a mechanism for promoting corporate accountability and stewardship of personally identifiable information within daily business operations.

Also By Marlin Pohlman:

*Oracle Identity Management: Governance, Risk and Compliance,* ISBN: 0-07-148926-6 Oracle Press Osborne Publishing, a McGraw Hill Company.

*LDAP Metadirectory Provisioning Methodology: A Step-by-Step Method to Implementing LDAP Based Metadirectory Provisioning & Identity Management Systems,* ISBN:0-595-26726-2 **HC** ISBN: 0-595-65619-6, Writers Showcase Publishing.

*LDAP and Metadirectory Architecture,* ISBN: 1-590-59090-2, Apress.

# Implement Multinational Regulatory Compliance Solutions

This comprehensive new resource from Oracle details the legal and technological aspects of Oracle Identity Management, the integrated suite of database security tools. You will get installation and configuration instruction as well as in-depth coverage of multinational regulations and guidelines to ensure compliance with minimal effort. This work covers over 220 legislative mandates in over 60 countries and provides metrics against such frameworks as ITIL, COBIT, ISO, BSI IT-Grundschutz, GAIT, and FISMA.

# Summary

The Oracle Identity Management Suite, when properly configured, deployed, and used, provides all the technical controls necessary to meet the legal challenges imposed by a global marketplace. It is important to remember that no software product, no matter how sophisticated and complex, will manage regulatory compliance for a company. Regulatory compliance and good corporate governance happen as a result of policy, process, and procedure implemented by the employees, managers, and executives of a corporation. It is the individual's responsibility to act from a perspective of enlightened self-interest to further the symbiosis of the corporate structure and the environment in which that corporate structure functions. The environment must be expanded from the traditional market perspective to encompass all those aspects that make up the marketplace. This holistic approach must include social responsibility and environmental stewardship and must result in the corporation assuming a position of moral and ethical leadership if the era of the corporation is to survive.

# FUNDAMENTAL CONCEPTS

# I

# *Chapter 1*

# Enterprise Risk

Identity and its governance has become the principal concern of chief information security officers and those charged with the management and compilation of personally identifiable information. This chapter provides a primer for the information professional. This chapter details elements of risk management, risk analysis, and the measures to which the efforts of those charged with the custodianship of personally identifiable information are held in multiple jurisdictions and regions.

## What Is Risk Management?

Risk management planning is about making informed business decisions. Mitigating risk means to reduce the risk until it reaches a level that is acceptable to an organization. This involves achieving the appropriate balance between realizing opportunities for gains while minimizing losses. As such, risk management can be defined as the identification, analysis, control, and minimization of loss associated with events that affect the enterprise. As such, risk management is an integral part of good management practice and an essential element of good corporate governance. It is an iterative process consisting of steps that, when undertaken in sequence, enable continuous improvement in decision making and in performance. It is important to remember that totally eliminating risk in an enterprise cannot be achieved without ceasing operations.

### *Risk Mitigation*

Risk mitigation means finding out what level of risk the enterprise can safely tolerate and still continue to function effectively. To enable this process, some properties of the various elements will need to be determined, such as the value of assets, threats, and vulnerabilities, and the likelihood of events. There are many practical benefits to performing a risk analysis. Performing a risk analysis creates a clear cost-to-value ratio for security protections and influences the decision-making process dealing with hardware and software systems design. However, more importantly, risk analysis helps a company to focus its resources where they are needed most, influencing planning and growth. Organizations that manage risk effectively and efficiently are more likely to achieve their objectives and do so at lower overall cost.

## What Is Risk Analysis?

The first major element of risk analysis is to access the value of the information itself. Information asset value is the heart of the risk assessment process. Any security analysis must include a detailed inventory and empirical assessment of the value of the information resources. Although it is possible to make a detailed assessment of security functionality of specific IT components without considering the value of the data they transmit, store, and process, it is impossible to define security requirements for a system without the value of the data in question. The consequences of damage by a risk incident might not just be quantifiable initially in monetary terms, such as in the loss of valuable assets or by destructive levels of litigation, but by criminal penalties levied against a company's officers and board members. Risk management planning is about making informed business decisions.

Risk has two primary components for a given event:

- The probability (likelihood) of occurrence of that event
- Impact of the event occurring (amount at stake)

The first step in risk management is to identify all potential risk issues. The second step is to quantify and document the threats, assets, vulnerabilities, exposure factors, and safeguards.

### *Definitions Used in the Risk Analysis Process*

Definitions are important to establish a common lexicon for discussion to provide background and a general understanding of the governance initiative within the software industry. The term *risk analysis* means many things to different people. All of these definitions have merit; thus, it is important to establish the context for the definition in use at the moment.

For our purposes, we will use the following general definition:

> **Asset**: An asset is a resource, product, process, or digital infrastructure element that an organization has determined must be protected.

The identification of risk to an organization entails defining the following four basic elements:

- The actual threat
- The possible consequences of the realized threat
- The probable frequency of the occurrence of a threat
- The confidence level that a threat will happen

In that light, the following definitions are vital to the process of risk management:

**Threat**: The presence of any potential event that causes a detrimental impact on the organization.

**Vulnerability**: The absence or weakness of a safeguard counter to a threat.

**Safeguard**: A control or countermeasure employed to reduce the risk associated with a specific threat or group of threats.

**Exposure factor (EF)**: The percentage of loss a realized threat event would have on a specific asset.

**Single loss expectancy (SLE)**: A financial amount assigned to a single realized threat event representing a loss to the organization.

$$\textit{Asset Value} \times \textit{Exposure Factor (EF)} = \textit{SLE}$$

**Annualized rate of occurrence (ARO)**: A number that represents the estimated frequency of an expected threat.

**Annualized loss expectancy (ALE)**: A financial figure that represents the annual expected loss from threats. It is derived from the following formula:

$$\textit{SLE} \times \textit{ARO} = \textit{ALE}$$

**Preliminary security examination (PSE)**: A PSE is often conducted before the actual quantitative risk analysis (RA). The PSE helps to gather together the elements that will be needed when the actual RA takes place. It also helps to focus risk analysis.

The difference between quantitative and qualitative RA is fairly simple: Quantitative RA attempts to assign independently objective numeric values. Risk analysis begins with a detailed study of the risk issues that have been identified and approved by decision makers for further evaluation. The objective is to gather enough information about the risk issues to judge the likelihood of occurrence and cost, schedule, and technical consequences if the risk occurs.

There are a number of approaches to risk:

- Accept the risk.
- Avoid the risk.
- Reduce the risk.
- Contain the risk.
- Transfer the risk.

However, before we determine how to deal with risk, we must first identify the risk in a concrete, auditable format. The following are common risk identification methods:

- **Objective-based risk identification**: Organizations set objectives. Any event that may endanger achieving an objective is identified as risk. Objective-based risk identification is at the basis of COSOs (Committee of Sponsoring Organizations of the Treadway Commission).
- **Scenario-based risk identification**: In scenario analysis different scenarios are created. The scenarios may be the alternative ways of achieving an objective or an analysis of the interaction of forces. Any event that triggers an undesired scenario alternative is identified as risk.
- **Taxonomy-based risk identification**: A breakdown of possible risk sources. Based on the knowledge of best practices, this methodology is questionnaire oriented.
- **Common-risk checking**: In industries with known risks. Each risk in the list can be checked for application to a particular situation.

## Risk Analysis Standards

Once identity information professionals get a firm grasp of the elements of risk, they must become familiar with the standards against which their efforts and activities will be measured. Many formulas and processes are designed to help provide some certainty when answering these questions. However, not every possibility can be considered, because life and nature are constantly evolving and changing. Risk analysis tries as much as possible to anticipate the future and to lower the possibility of a threat's impact on companies.

Risk is a measure of the frequency or probability of a negative event and the associated consequences. You do not have to plan for events with zero probability or events that have no consequences. The probability of a threat is a measure of the capabilities, impact, intentions, and past activities of potential miscreants. The capability of perpetrating a terrorist act depends the ability to manufacture or acquire a weapon and to carry out the terrorist act. The impact is the consequence of the act, including casualties, property damage, and business interruption. Intentions are the motivations of a terrorist or terrorist organization to perpetrate acts of terror.

In the physical domain, a nuclear or radiological incident could involve the detonation of a thermonuclear device, explosion of a "dirty bomb" (radiological dispersion device), or the release of radioactive material from an attack on a facility that uses or stores radioactive materials (e.g., bomb, aircraft, or missile attack on a nuclear power plant). An attack with biological agents could include the intentional dispersal or distribution of biological agents such as anthrax, smallpox, botulism, and the plague. Anthrax can be sent through the mail system, and food can be contaminated with salmonella. Smallpox and plague are infectious diseases that could spread widely. A vulnerability assessment is the process of identifying weaknesses in perimeter security, buildings, utility systems, personnel protection systems, or computer systems that can be exploited. In this context, the role of information risk management is to optimize outcomes such as profit objectives, return on investment, and performance measures, which results in value creation.

## Common Vulnerabilities

**Domain name servers:** The domain name service architecture should be evaluated to avoid creating a single point of failure that could result in an extended loss of connectivity. Cyber attacks by definition strike computer systems that are connected via local and wide area networks to computer networks outside the building, including, and especially, the Internet.

**Software vulnerabilities:** These account for the majority of successful attacks, simply because attackers are opportunistic and take the easiest and most convenient route. Attackers exploit the best-known flaws with the most effective and widely available attack tools. They count on organizations not fixing the problems, and they often attack indiscriminately, scanning the Internet for vulnerable systems.

**Default installs of operating systems and applications:** Most software packages, including operating systems and applications, come with installation scripts or programs. The goal of these installation programs is to get the systems installed as quickly as possible, with the most useful functions enabled and the least amount of work by the system administrator. To accomplish this goal, the scripts typically install more components than most users need. This opens an avenue of attack to miscreants.

**Accounts with no password or a weak password:** Most systems are configured to use passwords as the first, and only, line of defense. User IDs are fairly easy to acquire, and most companies have dial-up access that bypasses the firewall. Therefore, if an attacker can determine an account name and password, he or she can log on to the network.

**Nonexistent or incomplete backups:** When an incident occurs, recovery from it requires up-to-date backups and proven methods of restoring the data. Some organizations make daily backups but never verify that the backups are actually working. Others construct backup policies and procedures but do not create restoration policies and procedures.

**Large number of open ports:** Both legitimate users and attackers connect to systems via open ports. The more ports that are open, the more possible ways that someone can connect to your system. Therefore, it is important to keep the least number of necessary ports open on a system. All other ports must be closed.

**Not filtering packets for correct incoming and outgoing addresses:** Spoofing IP addresses is a common method used by attackers to hide their tracks when they attack a victim. For example, the very popular smurf attack uses a feature of routers to send a stream of packets to thousands of machines. Each packet contains a spoofed source address of a victim. The computers to which the spoofed packets are sent flood the victim's computer.

**Nonexistent or incomplete logging:** You cannot detect an attack if you do not know what is occurring on your network. Logs provide the details of what is occurring, what systems are being attacked, and what systems have been compromised. Without logs you have little chance of discovering what the attackers did.

When applying risk management, the regional circumstances dictate the model that must be used to express the risk. Australia, New Zealand, Canada, the United Kingdom, Germany, South Africa, the United States, and the United Nations through the International Standards Organization have all devised risk analysis standards designed to assist in the risk mitigation process and protect shareholders within their populations.

## *Australia/New Zealand Standard 4360:1795, 1799, and 1800*

AS/NZS 4360 was developed in response to a perceived need for practical assistance in applying risk management in public sector and private sector organizations. The reason AS/NZS 4360 has been so widely accepted in Australia, New Zealand, and globally may lie in the way standards were developed and approved there. The process started in 1992 when a Standards Australia questionnaire was submitted on behalf of the Association of Risk and Insurance Managers of Australasia (ARIMA). This led to the distribution of a further questionnaire to a wide range of industry and professional organizations to determine both need and interest. Satisfied of the need and the availability of a representative range of potential members, Standards Australia and Standards New Zealand established a Joint Technical Committee composed of 27 members representing 22 industry, professional, and government (federal, state, and local) organizations. The committee first gathered all available information. All submissions and documents were copied and supplied to the members. After several drafts, the committee produced one for public comment. To ensure maximum exposure, the representative organizations were asked to encourage responses from their membership, advertisements were placed in the daily press seeking input from the general public, and copies were supplied to all member organizations of the International Federation of

Risk and Insurance Management Associations (IFRIMA). The committee received 326 specific comments from 55 individuals or organizations. Each comment was addressed, resulting in many changes to the draft. The final document received unanimous approval and was published in November 1995.

AS/NZS 4360 was prepared by the Joint Standards Australia/ Standards New Zealand Committee OB-007, Risk Management, as a revision of AS/NZS 4360:1999, Risk Management. AS/NZS 4360 provides a generic framework for establishing the context and identifying, analyzing, evaluating, treating, monitoring, and communicating risk. This handbook states in clause 4.2 that "risk is the chance of something happening that will have an impact on objectives." The stated objective of this standard is to provide guidance to enable public, private, or community enterprises, groups, and individuals to achieve the following:

- A more confident and rigorous basis for decision making and planning
- Better identification of opportunities and threats
- Gaining value from uncertainty and variability
- Proactive rather than reactive management
- More effective allocation and use of resources
- Improved incident management and reduction in loss and the cost of risk, including commercial insurance premiums
- Improved stakeholder confidence and trust
- Improved compliance with relevant legislation
- Better corporate governance

The model of the risk management process AS/NZS 4360 consists of three major elements: the risk management workflow, monitor and review, and, finally, communication and consult. The latter two continuously interact with the steps of risk management workflow. AS/NZS 4360 defines risk management as "the culture, processes and structures that are directed towards the effective management of potential opportunities and adverse effects." AS/NZS 4360 defines risk as "the chance of something happening that will have an impact upon objectives. It is measured in terms of likelihood and consequences."

Figure 1.1 illustrates the bidirectional flow from context and risk to communication and consultation in parallel with monitoring and reviewing activities. These serve as a logical check on the risk analysis process, where risk is evaluated, mitigated, or accepted in sequential steps as follows:

- **Establish the context**: It is necessary to fully understand the external and internal aspects of the organization or organizational part, which is subject to risk management.
- **Identify risks**: This step uncovers risks, their location, time frame, root causes, and scenarios.
- **Analyze risks**: The output of risk analysis is the likelihood of a risk and the consequences of risk occurrence.
- **Evaluate risks**: Risk analysis provides an outcome, which is the basis for deciding which risks need treatment and in what priority.
- **Treat risks**: Treatments are responses to risks. Alternative treatments need to be identified, assessed, selected, planned, and implemented.
- **Monitor and review**: The purpose of this step is to ensure that the risk management plan remains relevant and all input data, including likelihood and consequence, are up to date.

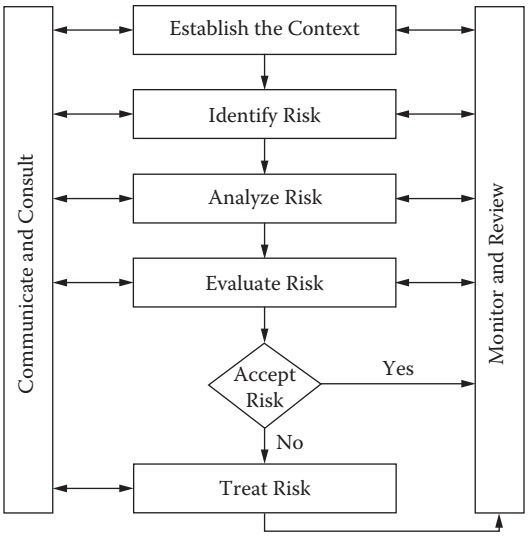


**Figure 1.1 The AS/NZS 4360 risk analysis process.**

Monitor and review relates to all of the five elements of risk management workflow mentioned previously.

- **Communication and consult**: Successful risk management relies on communication with all stakeholders. Communication will improve the level of understanding and treating risks. Communication is important throughout the entire risk management cycle.

The risk management process flow consists of the following elements:

- **The organization's strategic objectives**: Ensure that risk management activities meet the strategy of the organization.
- **Risk identification**: Uncover and list risks.
- **Risk description**: Display the identified risks in a structured format.
- **Risk estimation**: Provide values for probability of a risk and consequence in case of risk occurrence.
- **Risk evaluation**: Compare against risk criteria to analyze whether the risk is accepted or requires any treatment.
- **Risk reporting**: Report the risks identified. There are different requirements on reporting depending on the level inside (internal reporting) or outside (external reporting) the organization.
- **Decision**: Make a decision about whether and how to respond to a risk.
- **Risk treatment**: Select and implement treatments against risks.
- **Residual risk reporting**: Report the progress made by mitigating the risk.
- **Monitoring**: Check results. The monitoring step loops back to the previous steps of improvement and update.

### *British Standard BS 6079 3:1800 and PD-6668:2000*

Lord Berkeley stated the course of empire was westward. The course of risk management standards, however, appears to be in reverse. The first national standard was created in Oceania by the Kiwis and Aussies in 1995 (ANZ Standard 4360:1995 and 1999). The Canadians followed in 1997 (CSA-Q850-97) with their version. Eastward, the British published BS 6079-3:2000 after a revision of ISO/IEC 17799 led to a modification in the controls, which triggered a change to Annex A of BS 7799 Part 2 to keep it in line with the new Part 1. This resulted in the creation of BS 6079 as a method to quantify risk in the security audit process. In the British standard, BS 6079, risk is defined as "uncertainty inherent in plans and the possibility of something happening that can affect the prospects of achieving business or project goals." Uncertainty may be positive or negative. Risk is therefore a possible hazard or opportunity that if it occurred or was captured would threaten or benefit business outcomes.

PD 6668:2000 provides guidance on how organizations can establish and manage their strategic and operational risks. Some risks must be taken to be successful and survive. Other risks, if realized, can put an organization in jeopardy, and these risks should be mitigated. BS 6079-3:2000 provides specific guidance on the management of business-related project risk. The standard describes a process for identifying, assessing, and controlling risk within a broad framework.

Risk management then is the systematic application of policies, procedures, methods, and practices to the tasks of identifying, analyzing, evaluating, treating, and monitoring risk. BS 6079 confirms that risk involves three key issues: the frequency, the consequences, and the perception of loss. BS 6079 focuses on how risk affects all stakeholders. It emphasizes the importance of communications among stakeholders in the process of seeking responses. It identifies a "risk cycle" of estimation, evaluation, and control in which methods of financing are implicitly included. It recommends the creation of a "risk management team," a multidisciplinary group of internal and external experts, as well as perhaps some stakeholder representatives, to address the major risk issues facing an organization. It suggests creating a "risk information library" that includes documentation of issues, scope of decisions, identification of roles and responsibilities, identification of decision makers, details of analyses, stakeholder responses, and support documentation for decisions.

$$Risk = Hazard \times Consequence$$

Risk can be rated for a specific resource or value (specific risk), or it can be determined for all resources and values (total risk).

The framework comprises an iterative process embracing the following:

- **Understanding context**: Project objectives and business objectives—project in the business context and business in the project context
- **Identifying risk**: The sources of risk, and understanding how risks arise
- **Analyzing risk**: Characterization
- **Evaluating risk**: Identifying priorities
- **Treating risk**: Taking action

## Maintaining the Knowledge Pool, Plans, and the Management Process

The risk management culture is exemplified by encouraging everyone, especially managers, to continuously consider and monitor risk, including that arising from their own decision making

and actions. Training and simulations can heighten awareness and responsibilities of decision makers (BS 6079-3:2000 cls 4.4), and help them adopt a priority of actions for treating risk (BS 6079-3:2000 cls 4.3.4). The phases outlined by BS 6079 are as follows:

1. Eliminate risk.
2. Avoid risk.
3. Share risk.
4. Reduce the probability of occurrence of risk.
5. Reduce the consequences of risk.

## Canadian Standard 1797 (CSA-Q85-97)

Canada followed Australia and New Zealand in creating a "guideline" on risk management. The Australasian "Standard" #4360:1995 broke the ice and received global applause. In response, the Canadian Standards Association published CAN/CSA-Q850-97 in October 1997, "Risk Management: Guideline for Decision Makers, a National Standard for Canada." It is more a public policy risk document than a financial or operational risk management guide. CSA-Q850-97 confirms that risk involves three key issues: the frequency, the consequences, and the perception of loss. The Canadian guideline also focuses on how risk affects all stakeholders. It emphasizes the importance of communication among stakeholders in the process of seeking responses. It identifies a "risk cycle" of estimation, evaluation, and control, in which methods of financing are implicitly included. It recommends the creation of a "risk management team," a multidisciplinary group of internal and external experts, as well as stakeholder representatives, to address the major risk issues facing an organization.

The decision-making process described in the CSA Risk Management Guideline (CAN/CSA-Q850-97) consists of six steps, which follow a standardized management or systems analysis approach. The process is iterative and allows for the return to previous steps at any time throughout the process. The features of the Q850 approach are as follows:

- It incorporates stakeholder perceptions of the acceptability of the risk into the decision process, providing for more informed decision making and ensuring that the legitimate interests of all affected stakeholders are considered.
- It incorporates a risk communication framework into the decision process, ensuring reasonable and effective communication among stakeholders.
- It provides a standardized terminology used to describe risk issues, thus contributing to better communication about risk issues.
- It provides for an explicit treatment of uncertainty.

The CSA risk management process is illustrated in Figure 1.2.

Walking through the CSA risk management process, one begins with the initiation phase. Risk Assessment and Analysis begins in the Preliminary Analysis phase, coming to completion in Risk Estimation. Risk Assessment ends in Risk Evaluation. Risk Control and Action Monitoring complete the risk management process.

The definition of risk for the CSA risk management process involves three key issues: the frequency, consequences, and perception of loss. The process focuses on how risk affects all stakeholders. It emphasizes the importance of communication among stakeholders in the process of seeking responses. It identifies a "risk cycle" of estimation, evaluation, and control, in which methods of financing are implicitly included. The CSA process recommends the creation of a "risk

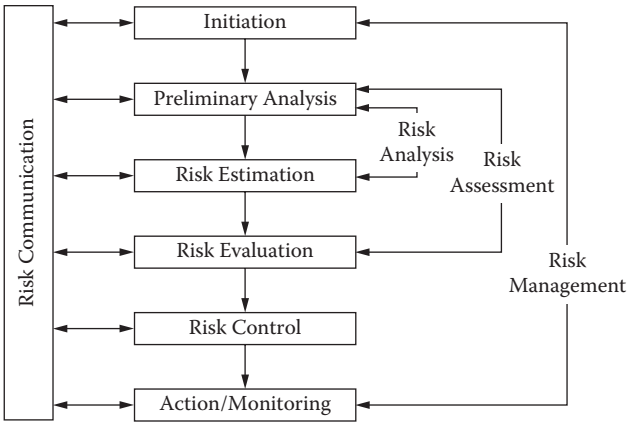


**Figure 1.2 The risk analysis, assessment, and management process.**

management team," a multidisciplinary group of internal and external experts, as well as perhaps some stakeholder representatives, to address the major risk issues facing an organization. The process suggests creating a "risk information library" that includes documentation of issues, scope of decisions, identification of roles and responsibilities, identification of decision makers, details of analyses, stakeholder responses, and support documentation for decisions.

## *Germany IT-Grundschutz 100-3*

German-headquartered global businesses follow ISO 17799 as their horizontal best standard practice of corporate security. If more than 50 percent of their business remains in Germany, corporations will generally opt for the BSI-issued IT Grundschutz. IT Grundschutz is a more detailed version of ISO 17799, and Germans argue over which came first, Grundschutz or the British BS 7799. They see theirs as the more stringent, realistic approach to a baseline. Under the IT-Grundschutz risk analysis approach, the threats are identified and assigned a likelihood of occurrence. The results of this analysis are then used to select the appropriate IT security measures, following which the residual risk can be assessed. Figure 1.3 outlines how threats are managed.

The procedure illustrated in Figure 1.3 can be used to reveal the most important areas in which there is still a need for action after application of the IT Baseline Protection Manual with the least possible effort and expense. Threats listed in the IT Baseline Protection Manual that are relevant to the IT asset under review are used as the starting point for risk analysis.

***Preparing the threat summary***—When determining relevant threats, the protection requirement for the target object under review must be considered in terms of the three basic parameters for IT security: confidentiality, integrity, and availability.

***Determination of additional threats***—Regardless of the protection requirements of the target object under review, it is important to determine additional relevant threats when there exists a special need for analysis. This is the case, for example, if there is no appropriate module in the IT Baseline Protection Manual.

***Threat assessment***—The threat summary is worked through systematically. It is checked to see if the IT security safeguards are already implemented or at least planned in the IT security concept and do provide adequate protection for each target object and threat. These are usually standard security safeguards from the IT Baseline Protection Manual.

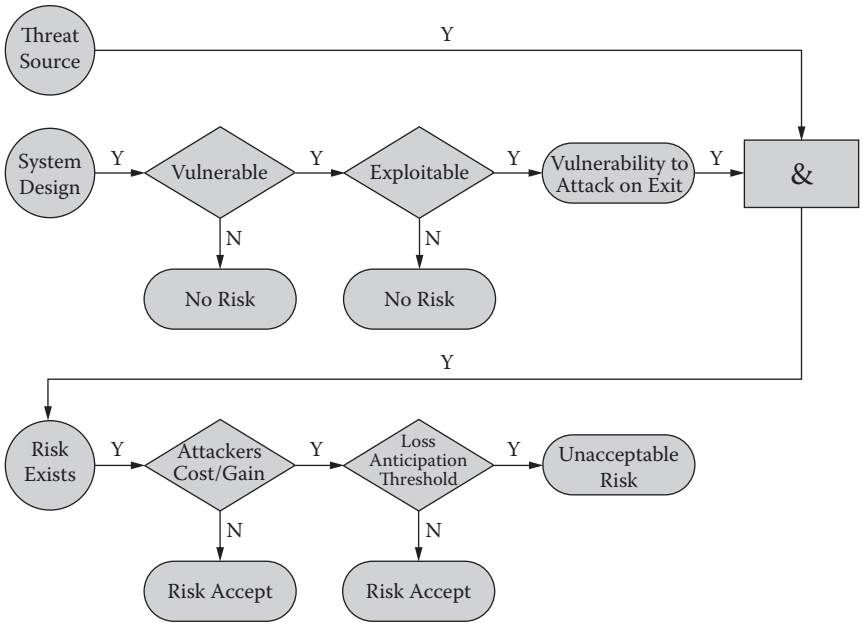


**Figure 1.3 Threat assessment process flow.**

From this point three options exist: risk reduction, risk transference, and risk acceptance. Risk reduction is accomplished through further security safeguards, where the threat remaining is removed by preparing and implementing additional security measures that counteract the threat adequately; risk transference through restructuring, where the remaining threat is removed by restructuring the business asset; or risk acceptance, where the remaining threat and the risk arising from it are accepted.

## *South Africa: IRMSA and King II Report Section 2*

In 1994 the King Committee on Corporate Governance, headed by former High Court judge Mervyn King S.C. King I, published the King Report on Corporate Governance (King I), incorporating a code of corporate practices and conduct. It was the first of its kind in the country and was aimed at promoting the highest standards of corporate governance in South Africa.

Over and above the financial and regulatory aspects of corporate governance, King I advocated an integrated approach to good governance in the interests of a wide range of stakeholders. Although groundbreaking at the time, the evolving global economic environment, together with recent legislative developments, has necessitated that King I be updated. To this end, the King Committee on Corporate Governance developed the King Report on Corporate Governance for South Africa, 2002 (King II). King II acknowledges that there is a move away from the single bottom line (that is, profit for shareholders) to a triple bottom line, which embraces the economic, environmental, and social aspects of a company's activities. The South African corporate governance report provides a unique definition of risk in the context of regulations designed to promote operational transparency and stakeholder accountability, and to that end we will break down the report into its core areas of focus to differentiate it from the purely operational or purely risk-oriented taxonomies, which occupy a common subject area. Although focused on South Africa,

the rigor of the King reports has earned international recognition and acclaim. King II requires the majority of members of the audit committee to be financially literate and, in four chapters, defines risk for the purpose of legislative accountability. The following paragraphs present an overview of the report broken down by chapter:

***Chapter 1: Introduction and definition*—**Risk management is defined as the identification and evaluation of actual and potential areas of risk as they pertain to a company, followed by a procedure of termination, transfer, acceptance (tolerance), or mitigation of each risk. Risk management is therefore a process that utilizes internal controls as a measure to mitigate and control risk.

***Chapter 2: Responsibility for risk management*—**The board is responsible for setting risk tolerance and related strategies and policies. It is also the board's responsibility to review the effectiveness of these policies on a regular basis and in a manner in which its objectives are clearly defined for the benefit of management to guide them in carrying out their responsibilities. The board is responsible for ensuring that the company has implemented an effective ongoing process to identify risk, measure its potential impact against a set of assumptions, and then activate what it believes is necessary to proactively manage these risks. The board must then decide on what risk that company is prepared to take and what risks it will not take in pursuance of its goals and objectives.

***Chapter 3: Assimilating risk to the control environment*—**The board is required to implement a comprehensive system of controls to ensure that risks are mitigated and that the company's objectives are attained. The control environment must then set the tone of the company and cover ethical values, management's philosophy, and the competence of employees. Any vulnerability in the achievement of the company's objectives, whether caused by internal or external risk factors, should be detected and reported by the systems of control in place and met with appropriate intervention. This is intended to improve the company's risk profile, enhancing the company's investment attraction, and increase the positive influences of risk on the business.

Five essential aspects of control are identified in the standard:

Corporate control environment
Risk assessment
Control activities
Information and communications
Monitoring

***Chapter 4: Application of risk management*—**The risk management review processes must identify areas of opportunity, in which, for example, effective risk management can be turned into a competitive advantage for the company. Risk management in this context goes beyond the control of financial risks. Reputation and a company's future survival are also taken into consideration. Companies under King II must ensure that the governance surrounding risk management is transparent and disclosed to its stakeholders. In King II, risk management is viewed as a continuous process of identifying, evaluating, and managing risk.

Risk assessment in this context addresses the company's exposure:

- Physical and operational risks
- Human resource risks

- Technical risks
- Business continuity and disaster recovery
- Credit and market risks
- Compliance risks

Here are a few sections of the act, which preserve the integrity of the risk management process:

*Section 275A*: Prohibits the provision of nonaudit services; requires the auditor to subject the nonaudit service to his or her own external audit procedures.
*Section 275A(3)(b)*: Prohibits an auditor having financial interest in a company.
*Section 287:* States that directors will be guilty of an offense when incomplete or noncompliant financial reports are issued. Directors are guilty of an offence in cases where the auditor expressed either a qualified opinion or an adverse opinion.
*Section 287 and section 440FF:* State that it will be an offense for any director to issue incomplete or noncompliant financial reports.
*Section 287A*: False or misleading statements—directors of a company are accountable to their stakeholders, and the major exposure to liability should rest with the directors or executives responsible for making the decisions or preparing the financial statements that mislead stakeholders.

Figure 1.4 illustrates how vulnerabilities and hazards are managed in the King Report.

Finally, the risk analysis process must maintain independence. As cited from the Executive Summary of the King Report, 2002, ISBN 0-620-28852-3, March 2002:

> Independence of mind—The state of minds that permits the provision of an opinion without being affected by influences that comprise professional judgment, allowing an individual to act with integrity, and exercise objectivity and professional skepticism.
> Independence in appearance—The avoidance of facts and circumstances that are so significant that a reasonable and informed third party, having knowledge of all relevant information, including safeguards applied, would reasonably conclude a firm's, or a member of the assurance team's, integrity, objectivity, or professional skepticism had been compromised.

## *United States NIST SP 800-30*

NIST SP 800-30 consists of three sections: risk assessment, risk mitigation, and control evaluation. It is a questionnaire, interview-, and tool-based risk methodology. Risk management encompasses three processes: risk assessment, risk mitigation, and evaluation and assessment. Section 1 describes the risk assessment process, which includes identification, evaluation of risks and risk impacts, and recommendation of risk-reducing measures. Section 2 describes risk mitigation, which refers to prioritizing, implementing, and maintaining the appropriate risk-reducing measures recommended from the risk assessment process. Section 3 provides an evaluation and assessment of the processes.


**Figure 1.4 Risk analysis and assessment process flow.**

Nine steps of risk assessment:

**Step 1:** ***System characterization*****—**The first step is to define the scope of the effort. In this step, the boundaries of the IT system are identified, along with the resources and the information that constitute the system. Characterizing an IT system establishes the scope of the risk assessment effort, delineates the accreditation boundaries, and provides information essential to defining the risk.

**Step 2:** ***Threat identification*****—**The goal of this step is to identify the potential threat sources and compile a threat statement listing potential threats and threat sources that are applicable to the system being evaluated.

**Step 3:** ***Vulnerability identification*****–**The goal of this step is to develop a list of system vulnerabilities, flaws, or weaknesses that could be exploited by the potential threat sources. Methods for identifying system vulnerabilities are the identification of vulnerability sources, the performance of system security testing, and the development of a security requirements checklist.

**Step 4:** ***Control analysis and methods*****—**The goal of this step is to analyze the controls implemented, or planned for implementation, by the organization to minimize or eliminate the likelihood or probability of a threat's exercising system vulnerability.

**Step 5:** ***Likelihood determination*****—**The likelihood rating indicates the probability that a potential vulnerability may be exercised within a threat environment. The factors that must be considered are threat source, motivation, capability, the nature of the vulnerability, existence, and effectiveness of current controls. The likelihood that a potential vulnerability could be exercised by a given threat source is then rated as high, medium, or low.

**Step 6:** ***Impact analysis*****—**The next step in measuring the level of risk is to determine the impact resulting from a successful threat exercise of vulnerability.

**Step 7:** ***Risk determination*****—**The purpose of this step is to assess the level of risk to the IT system. The determination of risk for a particular threat and vulnerability pair can be expressed as a function of the likelihood of a given threat source attempting to exercise a given vulnerability, the magnitude of the impact should a threat source successfully exercise

the vulnerability, and the adequacy of planned or existing security controls for reducing or eliminating the risk.

**Step 8:** ***Control recommendations*****—**During this step of the process, controls that could mitigate or eliminate the identified risks, as appropriate to the organization's operations, are provided. The goal of the recommended controls is to reduce the level of risk to the IT system and its data to an acceptable level. The factors that should be considered in recommending controls and alternative solutions to minimize or eliminate identified risks are effectiveness of recommended options, legislation and regulation, organizational policy operational impact, and safety and reliability.

**Step 9:** ***Results documentation*****—**Once the risk assessment has been completed, threat sources and vulnerabilities identified, risks numerically assessed, and recommended controls provided, the results should be documented in an official report or briefing. A risk assessment report is a management document that helps senior management—the mission owners—make decisions on changes needed—in policy, procedures, budgets, and operation and management of the system.

Risk mitigation is the second process of risk management. It involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls recommended from the risk assessment. Because elimination of all risk is usually impractical or close to impossible, it is the responsibility of senior functional and business managers to use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level.

*Phase 1. Options*—The goals and mission of an organization should be considered in selecting any of these risk mitigation options. It is not practical to address all identified risks, so priority should be given to the threat and vulnerability pairs that have the highest potential to cause significant impact or harm. NIST SP800-30 defines the following options when addressing risk:

- Risk assumption: Accept the potential risk and continue operating.
- Risk avoidance: Avoid the risk by eliminating the risk cause or consequence or both.
- Risk limitation: Limit the risk by implementing controls that minimize the adverse impact of a threat's exercising a vulnerability.
- Risk planning: Manage risk by developing a risk mitigation plan that prioritizes, implements, and maintains controls.
- Research and acknowledgment of risk: Lower the risk of loss by acknowledging the vulnerability or flaw and researching controls to correct it.
- Risk transference: Transfer the risk by using other options to compensate for the loss.

*Phase 2. Risk mitigation strategy*—Figure 1.5 outlines the risk mitigation strategy set out in NIST SP800-30.

- When a vulnerability or flaw exists, implement assurance techniques to reduce the likelihood of a vulnerability exploit.
- When a vulnerability can be exercised, apply layered protections and administrative controls to minimize the risk of an exploit or prevent it.
- When the attacker's cost is less than the potential gain, apply protection to decrease an attacker's motivation by increasing the attacker's effort.
- When loss is too great, apply technical and nontechnical protections to limit the potential for loss.

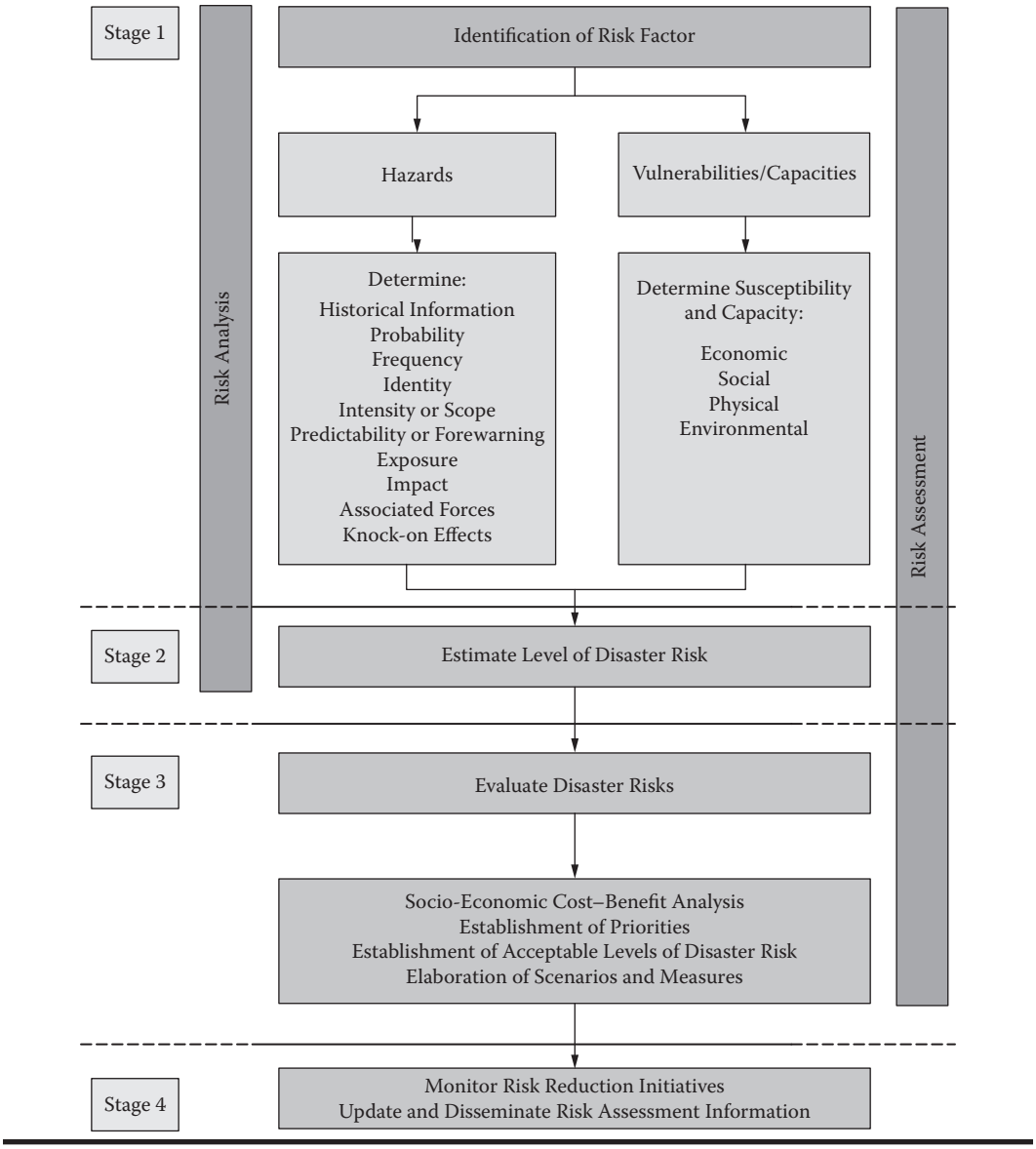


**Figure 1.5 Risk and threat mitigation process flow.**

*Phase 3. Control implementation*—When control actions must be taken, address the greatest risks and strive for sufficient risk mitigation at the lowest cost with minimum impact on other mission capabilities by the following:

- Prioritizing actions
- Evaluating recommended control options
- Conducting cost–benefit analysis
- Selecting control based on the results of the cost–benefit analysis

- Assigning responsibility to appropriate persons who have the expertise and skill sets to implement the selected controls
- Developing a safeguard implementation plan

*Phase 4. Control categories:*

- Technical security controls: These controls may range from simple to complex measures and usually involve system architectures, engineering disciplines, and security packages with a mix of hardware, software, and firmware.
- Management security controls: Management controls focus on the stipulation of information protection policy, guidelines, and standards, which are carried out through operational procedures to fulfill the organization's goals and missions.
- Operational security controls: Operational controls, implemented in accordance with a base set of requirements, technical controls, and good industry practices, are used to correct operational deficiencies that could be exercised by potential threat sources.

*Phase 5. Cost–benefit analysis*: The cost–benefit analysis can be qualitative or quantitative. Its purpose is to demonstrate that the costs of implementing the controls can be justified by the reduction in the level of risk.

## *International Standards Organization/UN: ISO/IEC 13335-2*

ISO/IEC 13335-3 identifies three sources for establishing the organization's information security requirements: the risks that the organization faces, risks arising from compliance, and contractual requirements.

The first step is to determine the assets within the scope. The next step is to identify the threats or potential events that can "assault" the identified assets. Threat modeling comprises three high-level steps: understanding the adversary's view, characterizing the security of the system, and determining threats. External threats originate from outside sources, either targeted at the company or randomly spread to the network through users or the Internet. External threats can range from Web site defacement and attacks targeting a business to nasty viruses and worms that tunnel their way into any network and destroy or alter data and applications or monopolize system resources (denial of services) by duplicating and spreading themselves. Internal threats are varied and range from unprivileged local access to administrative abuse of privileges. The developers of kernel-level rootkits are orchestrating very complicated and effective schemes for compromising a system and remaining undetected. Malicious software worms spread faster than systems can be patched; however, they can be detected because most leave some type of imprint. The next step is to determine the vulnerabilities. These are events that leave a system open to attack by a threat or allow an attack to have some success or greater impact.

The next step in the process is to determine the impacts. These are the successful exploitation of a vulnerability by a threat, thereby impacting the asset's availability, confidentiality, or integrity. The impacts are then identified and assigned a monetary value. This effort constitutes risk assessment in which risks are assessed in light of the true harm they pose. From this point, an assessment of the likelihood of the system failure ensues. In remediation, the controls in place against the risks are activated. Controls are the countermeasures for vulnerabilities. Apart from knowingly accepting risks that fall within the criteria of acceptability or transferring the risk (through contract or insurance) to others, there are four types of risk mitigation controls:

- Deterrent controls reduce the likelihood of a deliberate attack.
- Preventative controls protect vulnerabilities and make an attack unsuccessful or reduce its impact.
- Corrective controls reduce the effect of an attack.
- Detective controls discover attacks and trigger preventative or corrective controls.

Countermeasures or controls must be cost effective. In the best interest of the business, the cost of implementing and maintaining a control must be less than the cost of the impact. Total security is not possible, but it is possible to provide effective security against known risks provided periodic reevaluation practices are in place.

The process for assessing risk builds on the scoping document, is focused on critical systems and information assets, and can be broken down into clearly defined steps:

- Identify the boundaries of what is to be protected.
- Identify systems necessary for the reception, storage, manipulation, and transmission of information within those boundaries and the information assets within those systems.
- Identify relationships between these systems, the information assets, and the organizational objectives and tasks.
- Identify systems and information assets that are critical to the organizational objectives and rank them in order of priority.
- Identify the potential threats to those critical systems and assets.
- Identify the potential vulnerabilities of those critical systems and assets.

With the key objectives clearly identified, the systems that are most important to their delivery are identified. It is possible that some objectives will have more than one system, and these interdependencies should also all be noted. The resulting report is a schedule that shows prioritized critical systems as dependencies of key organizational objectives, which is then reviewed and agreed upon by the senior management. The final step in this exercise is to transfer the risk-level assessment for each impact to the asset and risk log.

## *Academia: Octave® Method from Carnegie Mellon*

For an organization looking to understand its information security needs, OCTAVE is a risk-based strategic assessment and planning technique for security. OCTAVE is self-directed, meaning that people from an organization assume responsibility for setting the organization's security strategy. The technique leverages people's knowledge of their organization's security-related practices and processes to capture the current state of security practice within the organization. Risks to the most critical assets are used to prioritize areas of improvement and set the security strategy for the organization. The Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) defines the essential components of a comprehensive, systematic, context-driven information security risk evaluation. OCTAVE is a risk-based strategic assessment and planning technique for security. Octave leverages people's knowledge of their organization's security-related practices and processes to capture the current state of security practice within the organization. Risks to the most critical assets are used to prioritize areas of improvement and set the security strategy for the organization. OCTAVE is self-directed, meaning that people from an organization assume responsibility for setting the organization's security strategy. The OCTAVE approach is driven by

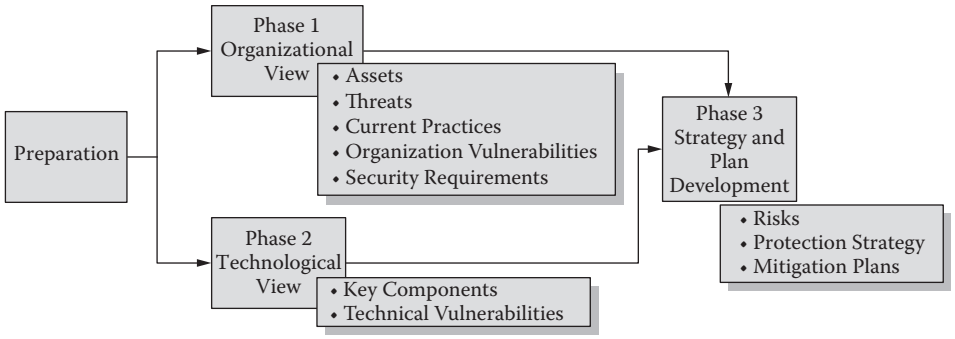


**Figure 1.6 Phase 1, 2, and 3 of OCTAVE risk management.**

two of the aspects: operational risk and security practices. Technology is examined only in relation to security practices, enabling an organization to refine the view of its current security practices. OCTAVE distinguishes itself in organization evaluation, security practices, strategic issues, and self-direction. OCTAVE phases of technical, organizational strategy are illustrated in Figure 1.6.

Founding philosophy of OCTAVE:

- One cannot mitigate all information security risks.
- The enterprise budget is limited. So are other resources.
- One cannot prevent all determined, skilled incursions.
- The enterprise needs to recognize, resist, and recover from incidents.

The enterprise needs to determine the best use of limited resources to ensure the survivability of its view and focus on critical issues.

Analysis teams must do the following:

- Identify information-related assets that are important.
- Focus risk analysis activities on those assets judged to be most critical to the organization.
- Consider the relationships among critical assets, the threats to those assets, and vulnerabilities that can expose assets to threats.
- Evaluate risks in an operational context—how they are used to conduct an organization's business and how those assets are at risk on account of security threats.
- Create a practice-based protection strategy for organizational improvement as well as create risk mitigation plans to reduce the risk to the organization's critical assets.

OCTAVE drivers:

- Risk-based—to prioritize effective use of minimum resources
- Practice-based—serves as a platform for improving security

OCTAVE is part of a continuum:

- Identify the organization's information security risks.
- Analyze the risks to determine priorities.
- Plan for improvement by developing a protection strategy for organizational improvement.

## *Academia: McCumber Cube Methodology*

In 1991, John McCumber created one of the first risk models for a general architectural description of computer information security, now known as the McCumber Cube. This risk model is depicted as a three-dimensional cube-like grid in Figure 1.7. It provides a structured methodology that functions independently of technology evolution. Its dimensions and attributes are as follows:

Desired goals
- Confidentiality
- Integrity
- Availability

Information states
- Storage: in memory
- Transmission: over network
- Processing: in execution

Reaction states
- Policy: directives from management or IT department
- Education: of users in process and procedure
- Technology: software and hardware enablers

The 27 individual cubes created by the model can be extracted and examined individually. This key aspect can be useful in categorizing and analyzing countermeasures. It is also a tool for defining

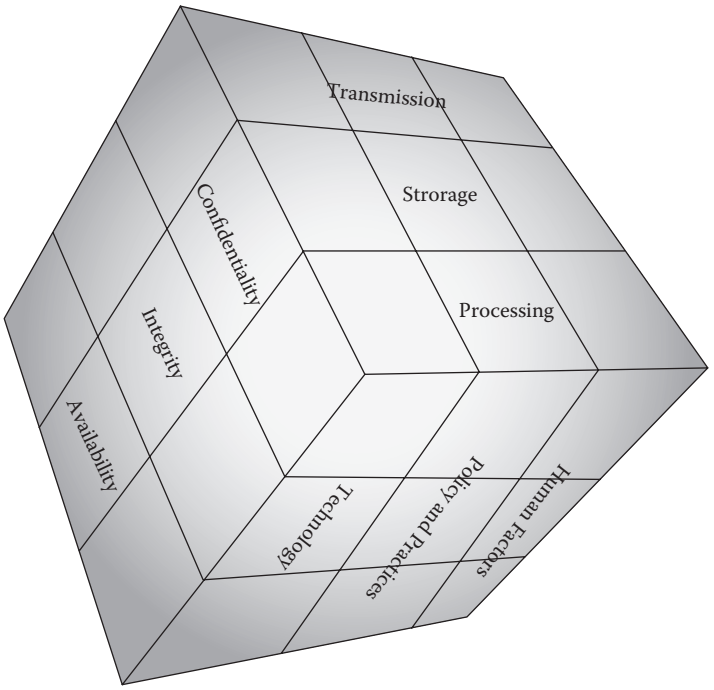


**Figure 1.7 The McCumber Cube.**

organizational responsibility for information security. By considering all 27 cubes, the analyst is assured of a complete perspective of all available security measures. Unlike other computer security standards and criteria, this model connotes a true systems viewpoint. The McCumber cube was originally published as "Information Systems Security: A Comprehensive Model," in October 1991. The model is the baseline used by the National Security Telecommunications and Information Systems Security Committee (NSTISSC) and was published in National Security Telecommunications and Information Systems Security Instruction's (NSTISSI) National Information Systems Security (INFOSEC) Glossary.

### *Basel II*

International Convergence of Capital Measurement and Capital Standards—A Revised Framework is the second Basel Accord and represents recommendations by bank supervisors and central bankers from the 13 countries making up the Basel Committee on Banking Supervision (BCBS) to revise the international standards for measuring the adequacy of a bank's capital. It was created to promote greater consistency in the way banks and banking regulators approach risk management across national borders. Basel II uses a "three pillars" concept—(1) minimum capital requirements, (2) supervisory review, and (3) market discipline—to promote greater stability in the financial system:

The first pillar: The first pillar provides improved risk sensitivity in the way that capital requirements are calculated for three major components of risk that a bank faces: credit risk, operational risk, and market risk. In turn, each of these components can be calculated in three ways of varying sophistication. Terms defining market risk include VaR (value at risk) and EL (expected loss, more commonly known as loss function) whose components are PD (probability of default), LGD (loss given default), and EAD (exposure at default). Calculation of these components requires advanced data collection and sophisticated risk management techniques.

The second pillar: The second pillar deals with the regulatory response to the first pillar, giving regulators improved measures to help them implement the accord. It also provides a framework for dealing with financial risk, including name risk, liquidity risk, and legal risk, which the accord combines under the title of residual risk.

The third pillar: The third pillar greatly increases the disclosures that the bank must make. This is designed to allow the market to have a better picture of the overall risk position of the bank and to allow the counterparties of the bank to price and deal appropriately.

## Summary

We are at the precipice of a new risk management frontier with operational risks, and clearly, there is still much further to go. Because operational losses today are more intensely scrutinized, and therefore visible, operational performance demands are greater than ever.

In addition to modeling operational risk, there is much to be said for simply improving on the availability of information about operational risk information for management decision making. Technology will be the essential mortar needed to aggregate, cement, and simplify all the pieces in place, thereby linking all of the functional areas, initiatives, and data sets, both hard and soft,

firmwide. Aggregated operational risk reporting will become commonplace, much as portfolio market and credit risk reports have. Because of the softer issues involved, such as the vagaries of human behavior (i.e., people risk), a mix of tools will be needed to represent operational risk fully. The risk complexities also require more effective risk management programs to link initiatives and variables together, not just periodically but continuously.