INFORMATION TECHNOLOGY RISK MANAGEMENT IN ENTERPRISE ENVIRONMENTS

A REVIEW OF INDUSTRY PRACTICES AND A PRACTICAL GUIDE TO RISK MANAGEMENT TEAMS

Jake Kounds
Daniel Minoli

A JOHN WILEY & SONS, INC., PUBLICATION

INFORMATION TECHNOLOGY RISK MANAGEMENT IN ENTERPRISE ENVIRONMENTS

INFORMATION TECHNOLOGY RISK MANAGEMENT IN ENTERPRISE ENVIRONMENTS

A REVIEW OF INDUSTRY PRACTICES AND A PRACTICAL GUIDE TO RISK MANAGEMENT TEAMS

Jake Kounds
Daniel Minoli

A JOHN WILEY & SONS, INC., PUBLICATION

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada.

ISBN 978-0-471-76254-6

Library of Congress Cataloging-in-Publication Data is available.

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

Jake:

I would like to dedicate this book to all of the volunteers that have supported the Open Security Foundation. To my friends and colleagues over the years. To my parents, Barry and Roxanne, for their continued support and to Jill and Elora for their unending love and patience.

Dan:

For Anna

CONTENTS

PREFACE

Well-documented studies show that cyber attacks continue to remain a substantial threat to organizations of all types and their information technology (IT) assets. It has been forecasted that in 2010 around 10,000 new vulnerabilities will be discovered in software applications in that year alone; this will force companies to assess and mitigate one new risk every hour each day of the year. Considering that each vulnerability instance has the potential to disrupt or bring a company's business to a complete halt, organizations must take risk assessment seriously and determine how each risk will be handled. The increased number of vulnerabilities being discovered also drives up the number of security incidents worldwide, and it will increase to a point where hundreds, if not thousands, of incidents per month will affect organizations that have not properly addressed and mitigated their risks.

Risk is a quantitative evaluation of the potential damage caused by an attack, a vulnerability, or an event impacting the set of company IT assets. A vulnerability (or weakness) is a lack of a safeguard, which may be exploited by a threat, causing harm to the information systems; specifically it can be a software flaw that permits an exogenous agent to use a computer system without authorization or use it with authorization in excess of that which the system owner specifically granted said agent. Risk-generating events and vulnerabilities are implicitly related in the context of this discussion in the sense that (we postulate that) a vulnerability is ultimately caused by some subtending event, malicious or nonmalicious. For example, in a so-called ''nonmalicious event,'' a flaw may be introduced in some software release by its designers, and then the event of having the IT group load and distribute that software throughout the enterprise creates a predicament where risk ensues. A ''malicious'' event may be a direct attack on the organization firewall, router, website, or database platform.

Corporate information security has become the fiduciary concern of the CEO, the CSO, the CFO, the CIO, and the COO of the organization. If a company were to lose its IT (computer and/or voice/data networking) resources

(assets) for more than a day or two, the company may well find itself in financial trouble. Obviously brokerage firms, banks, airports, critical infrastructure, medical establishments, and homeland security concerns would be impacted faster than, say, a manufacturing firm or a book publishing firm. However, the general concern is universal. If a company is unable to conduct business for more than a week, the company may well be permanently incapacitated. Therefore, a clear need arises to protect the enterprise from random, negligent, malicious, or planned attacks on its IT assets. It is critical, therefore, for companies to develop ready-to-go technological and human resources within the organization, to handle vulnerabilities and events that likely will impact the organization in the years to come. Some have called these teams *risk management* or *risk assessment* teams. The job function of a risk management team is to assess the risk that ensues from vulnerabilities and/or from risk-generating/causing events and to identify and ensure that risk mitigation solutions are implemented.

As more and more companies send their IT business abroad because of "outsourcing" or near-shoring, the potential IT (and, hence, corporate) risks are arguably growing at a geometric pace; these risks can have ultimate negative implications, particularly in view of cumulative exposures to risks that, in the aggregate, do not take on a trivial probability and, thus, risk.

This book aims at surveying industry approaches, best practices, and standards for how an organization can position itself to properly handle this ever-increasing and perennially mutating tsunami of risks to their business-critical IT assets. The book has two major sections. Part 1 reviews industry practices in the area of risk assessment and mitigation. The aim is to provide an overview of the well-known risk management approaches and methodologies. Part 2 focuses on helping an organization to develop a repeatable program that will address technological issues and human resources within the organization, to effectively undertake the risk assessment and mitigation function. It looks at the best use of IT resources, procedures, tools, and preparedness, and it places emphasis on implementing a risk assessment team that can properly foresee, prevent, and/or rapidly remediate potential infractions. This text is intended to be used by information security managers, security analysts, systems developers, auditors, consultants, and students, among others.

JAKE KOUNS
DANIEL MINOLI

ABOUT THE AUTHORS

Jake Kouns is a business-focused technology and information security executive with an extensive knowledge base and international experience. He focuses on the application of security concepts across a broad range on information technology areas including data communications, network design, operations, database structures, operating systems, application development, and disaster recovery. He holds both a Bachelor of Business Administration and a Master of Business Administration with a concentration in Information Security from James Madison University. In addition, he holds a number of certifications including ISC2's CISSP and ISACA's CISM, CISA, and CGEIT. Mr. Kouns is currently the Senior Director of Technology for Markel Corporation, a specialty insurance company. Prior to his current role, he was Senior Network Security Manager for Capital One Financial, a Fortune 200 financial institution where he was responsible for the day-to-day global security management of a large complex firewall environment, intrusion detection, and risk assessment.

Mr. Kouns has twice presented for Check Point Software Technologies as an expert in global firewall management and intrusion detection. In recent years, Mr. Kouns' main focus has been spent redefining the information security vulnerability industry, and he has presented on the topic at many well-known security conferences including CanSecWest and SyScan. He is the co-author of the book *Security in an IPv6 Environment*, Taylor and Francis, 2009, and he has also been interviewed as an expert in the security industry by *Information Week, eWeek, Processor.com, Federal Computer Week, Government Computer News*, and *SC Magazine*.

Mr. Kouns is the co-founder, CEO, and CFO of the Open Security Foundation (OSF), a nonprofit organization that oversees the operations of the Open Source Vulnerability Database (OSVDB.org) and the DataLossDB. Mr. Kouns' primary focus is to provide management oversight and define the strategic direction of the projects. Both projects are independent and open source databases that provide detailed and unbiased technical information on security vulnerabilities and data loss incidents worldwide. Mr. Kouns has also

has participated in Google's Summer of Code and volunteered time to mentor students during the 2006, 2007, and 2008 programs.

Daniel Minoli has extensive technical-hands-on and managerial experience in security, networking, telecom, wireless, video, and Enterprise Architecture for global Best-In-Class carriers and financial companies. He has worked at financial firms such as AIG, Prudential Securities, and Capital One Financial and at service provider firms such as Network Analysis Corporation, Bell Telephone Laboratories, ITT, Bell Communications Research (now Telcordia), AT&T, Leading Edge Networks Inc., and SES Engineering, where he is Director of Terrestrial Systems Engineering (SES is the largest satellite services company in the world).

At SES Mr. Minoli has been responsible for the development and deployment of IPTV systems, terrestrial and mobile IP-based networking services, and IPv6 services over satellite links. He also played a founding role in the launching of two companies through the high-tech incubator Leading Edge Networks Inc., which he ran in the early 2000s: Global Wireless Services, a provider of secure broadband hotspot mobile Internet and hotspot VoIP services; and, InfoPort Communications Group, an optical and Gigabit Ethernet metropolitan carrier supporting Data Center/SAN/channel extension and Grid Computing network access services. He is also the Founder and President Emeritus of the IPv6 Institute, the premiere leading certification organization for IPv6 networking technology, IPv6 global network deployment, and IPv6 security (www.ipv6institute.org). For several years he has been Session, Tutorial, and now overall Technical Program Chair for the IEEE ENTNET (Enterprise Networking) conference. ENTNET focuses on enterprise networking requirements for large financial firms and other corporate institutions.

Mr. Minoli has done important work in security, including leading-edge work such as security in an IPv6 environment (results documented in the first text on the topic of *Security in an IPv6 Environment*, Taylor and Francis, 2009, co-authored), security for IPTV systems, particularly encryption and Conditional Access (approaches documented in his text *IP Multicast with Applications to IPTV and Mobile DVB-H, Wiley, 2008*), and basic security work as documented in the *Minoli–Cordovana Authoritative Computer and Network Security Dictionary (*Wiley, 2006, co-authored).

Mr. Minoli has also written columns for *ComputerWorld, NetworkWorld*, and *Network Computing* (1985–2006). He has taught at New York University (Information Technology Institute), Rutgers University, and Stevens Institute of Technology (1984–2006). Also, he was a Technology Analyst At-Large for Gartner/DataPro (1985–2001); based on extensive hands-on work at financial firms and carriers, he tracked technologies and wrote CTO/CIO-level technical scans in the area of telephony and data systems, including topics on security, disaster recovery, network management, LANs, WANs (ATM and MPLS), wireless (LAN and public hotspot), VoIP, network design/economics, carrier networks (such as metro Ethernet and CWDM/DWDM), and e-commerce.

Over the years he has advised Venture Capitals for investments of $150M in a dozen high-tech companies. He has acted as Expert Witness in a (won) $11B lawsuit regarding a VoIP-based wireless Air-to-Ground communication system, and he has been involved as a technical expert in a number of patent infringement proceedings.

PART I

INDUSTRY PRACTICES IN RISK MANAGEMENT

CHAPTER 1

INFORMATION SECURITY RISK MANAGEMENT IMPERATIVES AND OPPORTUNITIES

1.1 RISK MANAGEMENT PURPOSE AND SCOPE

1.1.1 Purpose of Risk Management

This text deals with information technology (IT) risk management (ITRM), which, given the context of this text, we also just refer to as risk management.[1] Concerns about the possibility of compromise and/or the loss of proprietary information have reached critical levels in many organizations in recent years as a barrage of news bulletins reporting on infractions and product defects, staff's shortfalls and shortcomings, functions' outsourcings and offshorings, political instabilities in a number of countries and in wider regions, and management's emphasis on short-term financial breakeven has become all too frequent. Cyber attacks continue to be a source of significant exposure to organizations of all types, and, as a consequence, potential damage, potential impairment, and/or potential incapacitation of IT assets have become fundamental business viability/continuity issues.

Information Security[2] is recognized at this juncture to be a key area of IT management by a majority of government, commercial, and industrial organizations. Information Security is defined as the set of mechanisms, techniques, measures, and administrative processes employed to protect IT assets from unauthorized access, (mis)appropriation, manipulation, modification, loss, or (mis)use and from unintentional disclosure of data and information embedded in these assets. Some organizations have individuals on staff with a plethora of security certifications, yet these organizations continue to be afflicted with security

[1]Some also refer to ITRM as "information security risk management (ISRM)."
[2]Some also use the terms "infosecurity," and/or "INFOSEC," and/or "information systems security (ISS)," and/or "information security management (ISM)."

Information Technology Risk Management in Enterprise Environments: A Review of Industry Practices and a Practial Guide to Risk Management Teams, by Jake Kouns and Daniel Minoli

breaches on a fairly routine basis and continue to be exposed to risk; this implies that perhaps other approaches to information security are needed. Practitioners of information security are all well aware that exposure to risk is ever-changing and that it is also hard to assess; therefore, what is needed to manage and minimize risk in organizations is a diversified, versatile, and experienced IT/networking staff along with a solid set of policies, processes, and procedures that create a reliable information security program. This approach is typically much more successful as compared to the case where an organization just attempts to rely on ultra-narrow staffers with cookbooks of perishable memorized software commands specific to a given version of a given program of a given vendor to produce results, where the organization seems to be assuming that the real-life information security issues are similar to an academic pre-canned rapid-fire test for abstract scholastic grades, and simply believes that an alphabet soup of tags following one's name is sufficient (or necessary) to address incessant IT security threats.

Risk is a quantitative measure of the potential damage caused by a threat, by a vulnerability, or by an event (malicious or nonmalicious) that affects the set of IT assets owned by the organization. Risk exposure (that is, being subjected to risk-generating events) leads to potential losses, and risk is a measure of the "average" (typical) loss that may be expected from that exposure. Risk, therefore, is a quantitative measure of the damage that can incur to a given asset even after (a number of) information security measures have been deployed by the organization. Obviously, when the risk is high, an enhanced set of information security controls, specific to the situation at hand, needs to be deployed fairly rapidly in the IT environment of the organization. See Table 1.1 for some risk-related definitions, loosely modeled after [HUB200701]. The term "information asset" refers here to actual data elements, records, files, software systems (applications), and so on, while the term "IT asset" refers to the broader set of assets including the hardware, the media, the communications elements, and the actual IT environment of the enterprise; the general term "asset," refers to either "information asset" or "IT asset;" or both, depending on context. Typical corporate IT assets in a commercial enterprise environment include, but are not limited to, the following:

- Desktops PCs and laptops
- Mobile devices and wireless networks (e.g., PDAs, Wi-Fi/Bluetooth devices)
- Application servers, mainframes
- Mail servers
- Web servers
- Database servers (data warehouses, storage) as well as the entire universe of corporate data, records, memos, reports, etc.
- Network elements (switches, routers, firewalls, appliances, etc.)
- PBXs, IP-PBXs, VRUs, ACDs, voicemail systems, etc.
- Mobility (support) systems (Virtual Private Network nodes, wireless e-mail servers, etc.)

TABLE 1.1. Uncertainty, Probability, and Risk

Uncertainty	The lack of complete certainty, that is, the existence of more than one possibility for the outcome. The "true" outcome/state/result/value is not known.
Measurement of uncertainty	A set of probabilities assigned to a set of possibilities (specifically for risk events, threats, and/or vulnerabilities).
Risk exposure (also, liability)	A state of uncertainty where some of the possibilities (also colloquially called "risks") involve a loss, catastrophe, or other undesirable outcome. An environment exposed to risk events, threats, and/or vulnerabilities. Each new risk event, threat, and/or vulnerability gives rise to new risk exposure.
Measurement of risk	A set of possibilities, each with quantified probabilities and quantified losses.
Risk (singular)	The expected loss. Namely, the aggregation (summation) of the possibilities, their probabilities, and the loss associated with each possibility.
Risks (plural) (colloquial)	Individual possibilities (risk events) that are encountered with risk exposures.
Risk-exposing event (also called risk event)	Any changes in the state of the environment that have the potential of creating a new state where there is nonzero risk.

- Power sources
- Systems deployed in remote/branch locations (including international locations)
- Key organizational business processes (e.g., order processing, billing, procurement, customer relationship management, and so on)

Continuing with some definitions, a security threat is an occurrence, situation, or activity that has the potential to cause harm to the IT assets. A vulnerability (or weakness) is a lack of a safeguard that may be exploited by a threat, causing harm to the IT assets; specifically, it can be a software flaw that permits an exogenous agent to use a computer system without authorization or use it with an authorization level in excess of that which the system owner specifically granted to said agent. Risk-exposing events (also called risk events) are any changes in the state of the environment that have the potential of creating a new state where there is nonzero risk. Risk events and vulnerabilities are implicitly related in the context of this discussion in the sense that a vulnerability is ultimately given an opportunity for harm by some subtending event, malicious or nonmalicious. For example, in a so-called "nonmalicious event," a flaw may be inadvertently introduced in some software release by its designers; the event of having the IT group load and distribute that software throughout the enterprise creates a predicament where risk ensues. A

"malicious" event may be a direct attack on the organization's firewalls, routers, website(s), or data warehouse.

> **Note:** Some people use the term "risk" (singular) more loosely than defined above to mean a potential threat, vulnerability, or (risk) event; we endeavor to avoid this phraseology, and we use the term risk to formally describe the quantitative (numerical) measure of the underlying damage-causing issues, and not the issues themselves.
>
> We acknowledge that the term "risks" (plural) is used colloquially to describe the set of individual possibilities (risk events) that are encountered with risk exposures. We occasionally use this phraseology.

Information security spans the areas of *confidentiality, integrity, and availability*. Confidentiality is protection against unauthorized access, appropriation, or use of assets. Integrity is protection against unauthorized manipulation, modification, or loss of assets. Availability is protection against blockage, limitation, or diminution of benefit from an asset that is owed. The Computer Crime and Intellectual Property Section (CCIPS) Computer Intrusion Cases of the U.S. Department of Justice defines these terms (and considers respective infractions as crimes) as follows:

- *Confidentiality*. A breach of confidentiality occurs when a person knowingly accesses a computer without authorization or exceeding authorized access. Confidentiality is compromised when a hacker views or copies proprietary or private information, such as a credit card number or trade secret.
- *Integrity*. A breach of integrity occurs when a system or data has been accidentally or maliciously modified, altered, or destroyed without authorization. For example, viruses and worms alter the source code in order to allow a hacker to gain unauthorized access to a computer system.
- *Availability*. A breach of availability occurs when an authorized user is prevented from timely, reliable access to data or a system. An example of this is a denial of service (DoS) attack.

At this point in time, the practical challenges for enterprises are how to organize and run an efficient and effective information security program for persistent, high-grade protection and, in turn, how to actually (i) identify risk events, (ii) assess the risk, and (iii) mitigate ("manage") the environment to reduce risk. IT risk management (information security risk management) is the process of reducing IT risk (a process is a well-defined, repeatable sequences of activities.) Risk management is a continuous process. IT risk management encompasses five processes (also see Table 1.2 and Figure 1.1):

1. (Ongoing) identification of threats, vulnerabilities, or (risk) events impacting the set of IT assets owned by the organization

TABLE 1.2. Risk Management Processes

Risk identification	The process of identifying threats, vulnerabilities, or events (malicious or nonmalicious, deterministic/planned, or random) impacting the set of IT assets owned by the organization.
Risk assessment	The process of calculating quantitatively the potential damage and/or monetary cost caused by a threat, a vulnerability, or by an event impacting the set of IT assets owned by the organization. Identification of the potential damage to the IT assets and/or to the business processes based on previous internal and external events, input from subject matter experts, and audits. Specifically, this entails (a) quantifying the potential damage, and (b) quantifying the probability that damage will occur.
Risk mitigation planning	Process for controlling and mitigating IT risks. It typically includes cost–benefit analysis, and the selection, implementation, test, and security evaluation of safeguards. This overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulations, and laws [STO200201].
Risk mitigation implementation	Deploying and placing in service equipment and/or solution identified during the risk mitigation planning phase, or actuating new corrective processes.
Evaluation of the mitigation's effectiveness	Monitoring the environment for effectiveness against the previous set of threats, vulnerabilities, or events, as well as determining if new/different threats, vulnerabilities, or events results from the modifications made to the environment.

2. Risk assessment (also called risk analysis by some, especially when combined with Step 1)
3. Risk mitigation planning
4. Risk mitigation implementation
5. Evaluation of the mitigation's effectiveness

When the term risk management (or information security risk management) is used in this text, all five of these processes are implied. Risk management is a fundamental, yet complex, element of information security. Figure 1.2, contained in the International Organization for Standardization (ISO) 27002 standard, depicts the macrocosms of information security management (ISM), including risk management. The National Institute of Standards and Technology (NIST) defines risk management (in their recommendation NIST SP 800-30) as the process that allows IT managers to balance the operational and economic costs of protective measures and achieve gains in mission capability by protecting the IT systems and data that support their

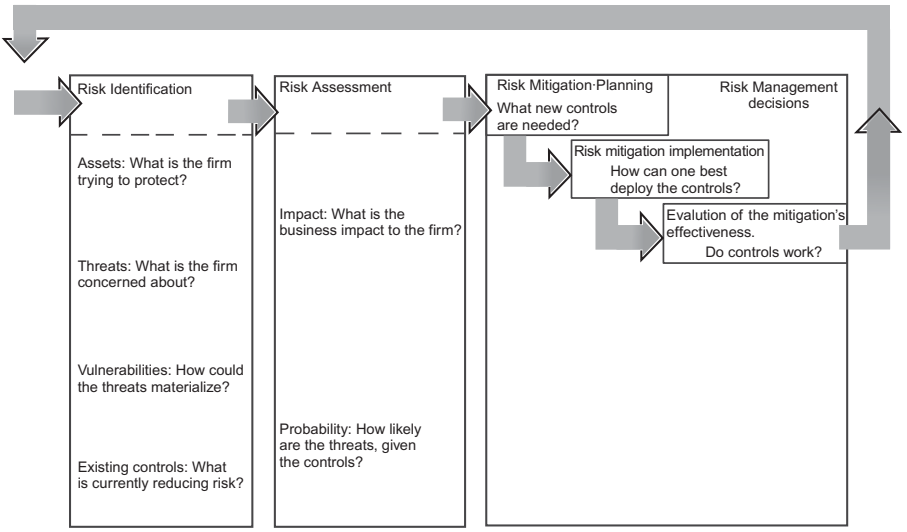

FIGURE 1.1. Risk management process as defined in this text.

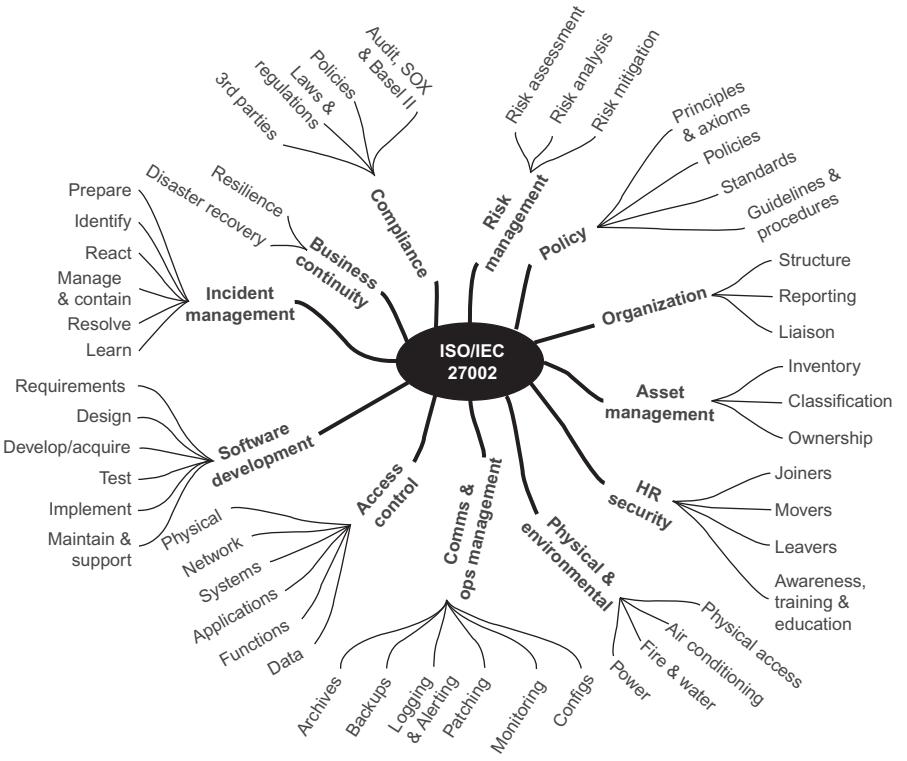

FIGURE 1.2. A view of information security management, as conceived in ISO 27002.

organizations' missions. Figure 1.3 provides a graphical view of the (assessment) process of NIST SP 800-30. Figure 1.4 depicts the ISO 31000 view of risk management. Figure 1.5 depicts the view in the Australian/New Zealand Standard AS/NZS 4360:2004. Figure 1.6 shows a vendor-based approach, specifically from Microsoft. Finally, Figure 1.7 depicts the view taken by OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), a risk-based strategic assessment and planning technique for security, developed by CERT (Carnegie Mellon University's Computer Emergency Response Team).

A recent confluence of technical and geopolitical factors has sensitized decision-makers about the business and legal consequences of cyber intrusions and risk exposures to an organization's IT assets, both at the corporate level as well as at the national security level. As a result of these developments, legislature has been introduced in a number of countries (e.g., Sarbanes–Oxley Act in the United States) that, in the final analysis, forces information security and privacy issues to be assessed rigorously and with fiduciary oversight by company executives and officials. In an effort to achieve business continuity and protect the enterprise from random, negligent, malicious, or planned security attacks, the organization must have a clear top-down understanding of its IT-supported business operations at a fundamental and comprehensive level. There must be an understanding of (a) what IT assets the company has deployed across its entire functional landscape, (b) how the resources are being used; and (c) who could attack these resources and the manner of such attacks.

IT security measures are intrinsically (and unfortunately) limited in their total effectiveness, therefore, organizations must equip themselves to manage risk. The following is an honest observation about the state of affairs from industry observers [MAR200601]:

> Even though serious responsibilities for complying with the organization's objectives have been placed in the hands of information systems, doubts about their security continue to arise. Those affected, often not technicians, wonder if they can place their trust on these systems. Each failure lowers the trust on information systems, especially when the investments made in defending the means of work do not rule out failures . . . The matter is not as much the absence of incidents, but the confidence that they are under control.

The convergence of IT networks and mobile communications (including "mobility solutions"), increases the number of potential threats, including unauthorized access, exploitable vulnerabilities, malicious attacks, viruses, worms, and DoS attacks to both wired and wireless corporate systems. Press time studies by the *IT Policy Compliance Group*[3] have shown that the primary business and financial liabilities from the use of IT are directly related to how well, or poorly,

[3]The IT Policy Compliance Group conducts benchmarks that are focused on delivering fact-based guidance on the steps that can be taken to improve results. Benchmark results are reported through www.itpolicycompliance.com for the benefit of members.

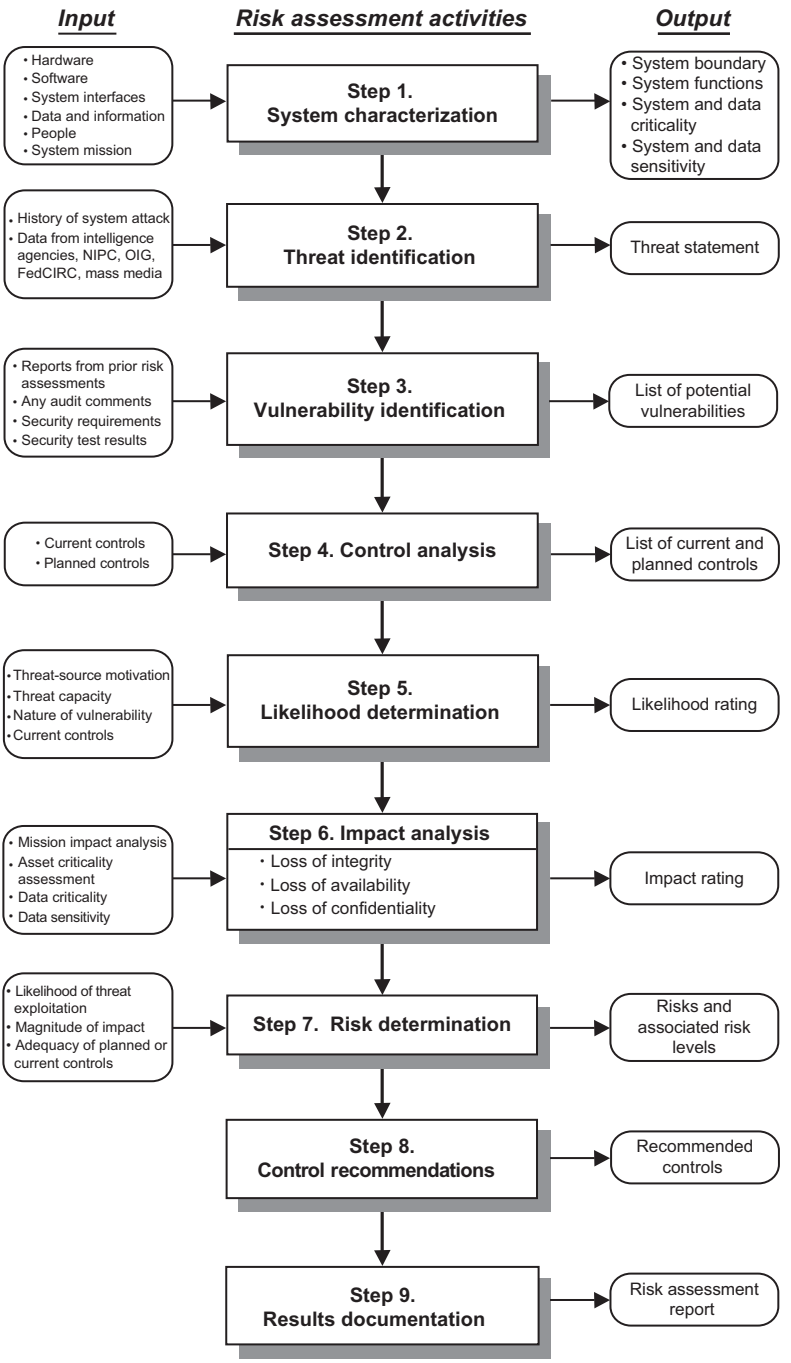

FIGURE 1.3. A graphical view of risk assessment, as conceived in NIST SP 800-30.