INFORMATION SECURITY

Design, Implementation, Measurement, and Compliance

Timothy P. Layton

Auerbach Publications
Taylor & Francis Group

INFORMATION SECURITY

Design, Implementation, Measurement, and Compliance

Auerbach Publications
Taylor & Francis Group
Boca Raton New York

Auerbach Publications is an imprint of the
Taylor & Francis Group, an informa business

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

Auerbach is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-10: 0-8493-7087-6 (Hardcover)
International Standard Book Number-13: 978-0-8493-7087-8 (Hardcover)

INFORMATION SECURITY

Design, Implementation, Measurement, and Compliance

OTHER INFORMATION SECURITY BOOKS FROM AUERBACH

Assessing and Managing Security Risk in IT Systems: A Structured Methodology
John McCumber
ISBN: 0-8493-2232-4

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

Building and Implementing Security Certification and Accreditation Program
Patrick D Howard
ISBN: 0-8493-2062-3

The CISO Handbook: A Practical Guide to Securing Your Company
Michael Gentile; Ronald D Collette; Thomas D August
ISBN: 0-8493-1952-8

The Complete Guide for CPP Examination Preparation
James P Muuss; David Rabern
ISBN: 0-8493-2896-9

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

The Ethical Hack: A Framework for Business Value Penetration Testing
James S Tiller
ISBN: 0-8493-1609-X

Guide to Optimal Operational Risk and Basel II
Ioannis S Akkizidis; Vivianne Bouchereau
ISBN: 0-8493-3813-1

The Hacker's Handbook: The Strategy Behind Breaking into and Defending Networks
Susan Young; Dave Aitel
ISBN: 0-8493-0888-7

The HIPAA Program Reference Handbook
Ross Leo
ISBN: 0-8493-2211-1

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

Information Security Fundamentals
Thomas R Peltier; Justin Peltier; John A Blackley
ISBN: 0-8493-1957-9

Information Security Management Handbook, Fifth Edition, Volume 2
Harold F Tipton; Micki Krause
ISBN: 0-8493-3210-9

Information Security Management Handbook, Fifth Edition, Volume 3
Harold F Tipton; Micki Krause
ISBN: 0-8493-9561-5

Information Security Policies and Procedures: A Practitioner's Reference, Second Edition
Thomas R Peltier
ISBN: 0-8493-1958-7

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

Information Technology Control and Audit, Second Edition
Frederick Gallegos; Daniel P Manson; Sandra Senft; Carol Gonzales
ISBN: 0-8493-2032-1

Intelligence Support Systems: Technologies for Lawful Intercepts
Kornel Terplan; Paul Hoffmann
ISBN: 0-8493-2855-1

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

Network Security Technologies, Second Edition
Kwok T Fung
ISBN: 0-8493-3027-0

The Practical Guide to HIPAA Privacy and Security Compliance
Kevin Beaver; Rebecca Herold
ISBN: 0-8493-1953-6

A Practical Guide to Security Assessments
Sudhanshu Kairab
ISBN: 0-8493-1706-1

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

Strategic Information Security
John Wylder
ISBN: 0-8493-2041-0

Surviving Security: How to Integrate People, Process, and Technology, Second Edition
Amanda Andress
ISBN: 0-8493-2042-9

Wireless Security Handbook
Aaron E Earle
ISBN: 0-8493-3378-4

AUERBACH PUBLICATIONS

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

Dedication

I dedicate this book and the effort that went into it to the three most understanding and caring people I know: Timothy Patrick Jr., Alec Michael, and Abigail Elizabeth Layton. When times are good, they make me laugh uncontrollably. When times are tough, the smile doesn't leave my face because of the unconditional love and joy they bring to my heart.

Foreword

When Tim Layton asked me to write a foreword for his latest book on risk assessment, I was both flattered and humbled. I have had the pleasure of working with Tim on several large risk assessment projects and I have tremendous respect for his knowledge and experience as an information security practitioner. It is an honor to have a small part in this work. And the topic—risk assessment—is both timeless and timely. Risk assessment is the cornerstone of an effective information security program. Security at its very nature starts with a basic understanding of risk. Virtually every information security framework is centered on understanding the risks to the organization and managing them to an acceptable level. Yet today, it seems the concept of a risk-based security program is becoming lost.

The burden and fear of regulatory compliance are causing many organizations to lose control of their security strategy. Instead of being based on a sound understanding of risk, too many organizations are basing their security programs on externally defined criteria. I see this as a dangerous trend within the security industry. With security budgets and staff cut to the bone, it is essential that organizations focus their scarce security resources on the biggest threats to the organization. Unfortunately, the opposite is often the case. By focusing primarily on compliance with externally defined standards, an organization is abdicating its responsibility to understand and manage its business risk.

Without a doubt, compliance can pose a significant risk to an organization. However, striving to achieve compliance in the absence of a risk-based security strategy can only lead to failure. The myriad requirements of the various compliance statutes are vague and contradictory. It is virtually impossible to ensure compliance with every facet of every standard. A compliance-driven security program will likely be costly and ineffective in reducing real risk to the business. In truth, a risk-based security program is the best strategy to achieve compliance. A common theme through all compliance standards—GLB, HIPAA, SOX, PCI, etc.—is to implement security controls appropriate for the risk to your organization. I recently worked with a retail enterprise that was struggling to comply with the new Payment Card Industry Security Standards as defined by Visa and MasterCard. The auditing requirements of the PCI standard are particularly onerous. This organization had never taken the time to assess its own requirements for auditing and logging. In the absence of an internally driven requirement, its only option was to implement an auditing capability as defined by the standard. Not only was this prohibitively expensive, it probably was unnecessary based on the organization's actual risk. Had it conducted a proper risk assessment, it could have deployed a reasonable level of system auditing that would have met its business requirement and satisfied the auditors.

I view risk assessment as the best defense against compliance risk. Demonstrating that you understand and are managing the risks to your business will meet every

audit standard. Don't let an external compliance body define your security requirements for you. Implement an effective risk assessment program and take control of the compliance monster.

This book will help you do just that. I know you will benefit from Tim's guidance on how to get the most from your risk assessment efforts. For today's information security leaders, there is not a topic more important.

Gary Geddes, CISSP
Strategic Security Advisor
Microsoft Corporation

Preface: The Business of Information Security and Risk Assessment

The heart of every information security program is always risk assessment. The information security risk assessment process is used to discover the extent of the potential threats and risks associated within the system or environment being evaluated. This may sound easy and straightforward, but consider a large organization leveraging thousands of vendors to help with its business operations and services. Heavily regulated organizations are subject to scrutiny that many other industries are not forced to integrate into their business models. The type of organization referenced in this example probably has tens of thousands of employees with operations spread across the country and possibly conducts business internationally. The executive management team must account for the complexities and challenges within its information security strategy. Management's strategy and program must make sure there is direct linkage to its business goals, vision, and objectives while meeting the myriad legal, regulatory, and contractual requirements.

Information security risk assessment is only one part of this strategy. Organizations typically have many other risk assessment strategies and programs such as legal and contracts, vendor viability, operations, compliance, and so on. Having a misaligned or inaccurate risk assessment process will lead to an ineffective information security program, which has the potential to be devastating to an organization and its customers. In decentralized business models, corporate guidance on information security risk assessment will ensure that business goals and requirements are being considered as part of the assessment process.

It is not enough to have a comprehensive information security risk assessment process and information security program. The information security program must be documented, measurable, and reportable. This requirement is obvious for publicly traded organizations as well as federal and government agencies. Being able to quantify risks to the business and linking a series of analytical controls and safeguards to the threats and vulnerabilities are good business practice and will satisfy even the most comprehensive audits and discriminating regulators. All organizations should be able to explain how they identify risk and what controls they have applied to help manage or mitigate the identified risks. This is a fundamental requirement for regulated organizations.

As described above, risk assessment is only one component of risk management. Risk management also typically includes strategic planning, decision making, impact analysis, threat and vulnerability pairing, asset identification, likelihood, risk analysis,

risk identification, remediation, risk evaluation, and potentially a host of other elements depending on the environment and unique organizational variables.

The information security battle is won in the boardroom and not at the firewall. From a strategic perspective, management support such as funding, establishing a cultural norm for information security, and visible participation is needed for every successful information security program, independent of industry or organization. Executive and management support is one of the most important elements for successful information security programs next to users accepting and acting properly on the information security policies and guidelines. Identifying threats and pairing them with vulnerabilities and the design and application of applicable controls only materialize because management supported and ultimately funded the process. Information security is not about technology—it is about people and their actions. There is a raft of laws, regulations, and guidelines that organizations must follow and hence the current trend of information security governance. There is a direct relationship between information security governance and risk management.

Every organization must manage operational risk within the scope of its business model. The information security policy is the document that ties the business and information security together. A diligent information security risk assessment process makes effective risk management possible. Information security policies should be leveraged as a business enabler. The information security policy should allow the organization to comply with all applicable legal, regulatory, statutory, and contractual requirements and still operate with efficiency and effectiveness according to the organization's business plan.

After the policy battle has been won in the boardroom, information security management has an enormous challenge on its hands. This is where the rubber hits the road. All users, whether they are employees, contractors, consultants, external partners, or third-party vendors, must be made aware of the organization's information security policies so that they understand the risks of not complying with organizational policy. Establishing a suitable information security policy and an effective information security awareness program will do more to protect an organization than any firewall or piece of technology could ever offer. It will also keep the auditors and regulators at bay within the larger and regulated organizations such as banks, credit card companies, and insurance organizations.

In fact, a recent global survey performed by Deloitte & Touche USA LLP revealed that information technology-related controls have evolved to the point where hackers are starting to shift their focus back on human error again. For more information on this survey, go to the Deloitte & Touche USA LLP Web site at www.deloitte.com and search for "2005 Global Security Survey."

With globalization, a 24/7 working economy, increased complexities of IT infrastructures, growth of remote employees, proliferation of mobile computing devices, and an ever-increasing number of common vulnerabilities, it is no wonder organizations struggle to find a balance to protect their assets. For these reasons and probably a thousand more, it is important for organizations to have a clear strategy and plan for information security that are owned by competent professionals who possess the skills and experience to lead such a difficult and demanding charge. Having an effective risk assessment process at the core of the information security

program will allow an organization to identify applicable threats, whether they are technology, operational, or compliance based, and start the process of risk analysis to design and implement suitable controls to address the identified risk.

The cost of having a competent, qualified, and aware staff does not seem so costly when an organization discloses a data security breach of 40 million credit card customers, like the one reported in June 2005 by a third-party processing company.

Organizations invest in information security for a host of reasons. From a business perspective, organizations are motivated to protect against competitive disadvantage. In other words, how damaging would it be for your organization if a competitor had access to private or confidential information or data? A direct loss such as business revenues is possible, and it is desirable for any business to avoid such losses. Loyalty from clients could be in jeopardy if a damaging incident is allowed to occur and reported to the public. For some organizations and, in particular, publicly traded organizations, disclosure of certain types of incidents is required by law. In 2005 several states formally proposed disclosure and notification legislation, and there is a growing trend for this kind of legislation across the United States.

Losses of the information security type have the potential to impact employee morale and motivation. Information security losses apply to every organization, regardless of whether the organization is profit seeking or government/civic in nature.

If management does not have a clear and documented process for decision making, information could be disclosed to unauthorized parties resulting in negative consequences. These penalties could range from loss of shareholder value to damages to the organization's reputation. In some industries, the organization's reputation is part of the brand and considered a critical part of the success formula. A documented security policy with supporting guidelines and standards effectively communicated to the right target audience can successfully address this risk.

Security incidents can lead to a disruption in operations and can cause direct and indirect losses as well. For some organizations, there may be legal liabilities for disclosure or unauthorized access to information and data, and civil or legal consequences may be applied.

Individuals can be placed at risk because of unauthorized disclosure of personal information. This type of information could range from personal name and address to social security number to credit and medical history. In 2005 there were several cases that disclosed security breaches of credit card data impacting over 40 million people worldwide. There were also cases involving the loss of patients' medical records via stolen laptop computers. These breaches and many others are available for review by searching on news.google.com. By typing the phrase "security breach" in Google News (news.google.com), thousands of matches will be returned.

According to the FBI, fraud is one of the fastest-growing crimes today. Congress is rapidly pursuing many new laws and regulations to help protect and deal with the unauthorized loss or disclosure of personal data including financial and medical data. It is not likely that any organization (public or private) wants that type of press. This may be the exception to the old saying "There is no bad press."

In some cases a breach in security controls could risk the health of customers and employees. These are just a few examples of why organizations are motivated

to develop and implement a cohesive information security strategy that is in alignment with the business objectives and organizational mission. For some it may be a legal or regulatory requirement, and for others it may be a market differentiator to gain an advantage over their competitors. All the issues cited here should be included in a formal risk assessment process that an organization should undergo on a regular basis. Risk assessment is the process that helps identify the scope and scale of the information security strategy ensuring connectivity to the business and organizational objectives.

Risk assessment should be a part of the normal project operations of every new and existing project within an organization. There are many different types of risk assessments and the scope can vary greatly. The model presented in Chapter 1 discusses this issue and how organizations can adapt accordingly.

Information security could be compared to life insurance: most people think it is generally a good idea and the right thing to do for our families or organization, respectively. At the same time, if we did not have to make these investments, not many would be rushing to their insurance agents or technology vendors and consultants to donate their hard-earned capital. Information security within the landscape of today's business model is extremely complex and continues to become more complicated over time. With the ubiquitous use of information technology in almost every business model today, it is a harsh reality even without the new legal and regulatory requirements that an information security strategy must be connected to an organization's business plans to appropriately protect employees, assets, and future business plans. For industries such as finance, banking, insurance, and others, it is a painful reality that additional laws and regulations are inevitable to an already heavily regulated industry. If business stakeholders in these types of industries do not have a vision and plan to manage to the current and future legal and regulatory requirements, it will ultimately impact their shareholder value. The cost to perform due care and due diligence is much less from a proactive model as opposed to being reactive. This is one of the reasons why we are seeing new roles and titles such as chief risk officers, chief compliance officers, and enterprise risk management positions. The role of chief information security officer has finally caught on for many organizations and industries, and the second wave of awareness has just begun. Over time it will become more obvious that information security is connected to almost every part of the business, and the linkage and relationship to the business model are ways to enable and strengthen the business.

There is a growing acceptance within the industry as a whole of why organizations would want to use and implement the ISO/IEC 17799:2005 (27002) Code of Practice for Information Security Management. Many subject matter experts and consultants agree that if an organization adopts and implements the ISO/IEC 17799 as their information security standard, they will address many of the other legal requirements placed on them by the Sarbanes–Oxley Act (SOX), the Gramm–Leach–Bliley Act (GLB), and the Health Insurance Portability and Accountability Act (HIPAA). With little effort, it is easy to map the requirements from the SOX, GLB, and HIPAA laws to the current version of the ISO/IEC 17799 standard. For financial institutions the linkage and relationship to the FFIEC (Federal Financial Institutions Examination Council) and the OCC (Office of the Comptroller of the

Currency) are very obvious and apparent. Any organization would greatly benefit by adopting the ISO/IEC 17799 as its information security framework.

The latest official release of the ISO/IEC 17799 is the second edition, also known as ISO/IEC 17799:2005(E) (27002). The second edition was released in June 2005. In the foreword of the second edition, a brief disclosure was listed indicating that the current code of practice is proposed to be ported to a new ISO numbering scheme at some time in 2007. The new numbering scheme will be ISO/IEC 27000. The ISO/IEC 17799:2005 is proposed to be ISO/IEC 27002, and part 2 of the BS 7799:2002 is now officially the ISO/IEC 27001:2005.

Other standards addressing measurement and metrics (27004) and implementation guidance (27003) are also being discussed along with a few others. Anything referenced besides 27001 and 27002 is considered unofficial at this time. It is important to note the relationship between 27001 (BS 7799-2:2002) and 27002 (ISO/IEC 17799:2005). The 27001 provides a specification for ISMS (Information Security Management Systems) and the foundation for third-party audit and certification. The new 27000 series has been revised to work with other management systems such as the ISO 9001 and ISO 14001. ISO/IEC 27001 covers the ISMS as referenced above, management responsibility, management review of ISMS, and how to continually improve ISMS. This standard will help organizations define their information security policy, define the scope of their ISMS, perform an information security risk assessment, create a plan to manage the identified risks, select controls and safeguards to implement, and prepare a SOA (statement of applicability) for formal certification.

At a high level, the ISO/IEC 17799:2005 (27002) standard provides a series of systematic recommendations for information security management to apply to their business model and operations and determine which controls apply. As outlined in the opening section of the introduction of this book, the ISO/IEC 17799:2005 suggests that organizations should include a formalized risk assessment process sponsored by senior management.

The overall purpose of the standard is to provide a common basis and platform for developing organizational information security standards for all organizations independent of geography or industry. Moreover, the code of practice provides a comprehensive framework and series of controls for interorganizational partnerships and dealings. The standard is not a law or regulatory requirement, and it should be adapted and used in accordance with applicable laws and regulations to ensure maximum effectiveness.

I have visited several countries throughout Europe, and the organizations I have evaluated to date are very familiar with the 17799 standard. In the scope of my own personal experiences, their information security programs were fundamentally designed and based on the standard. With the roots of the 17799 standard being in the United Kingdom, this is not a surprising discovery. The widespread proliferation of the EU Data Protection Directive in Europe helps to further explain this phenomenon. European companies face the same challenges as American organizations as they relate to protecting their assets while balancing the most appropriate set of controls for their respective business models and complying with all applicable laws and regulations. In today's global economy, whether an organization is based in

Europe or the United States, does not release the organization from compliance requirements with respective legislation or governance.

Corporate governance is the rage with the Big 4 public accounting firms and their management consulting partners. Corporate governance is a fancy label for good business practices. This would include a comprehensive strategy to protect assets including information, data, and information systems. The ISO/IEC 17799:2005 (27002) standard provides a good framework from a business perspective to aid in this process. Organizational stakeholders in the United States are beginning to understand the value in the breadth and depth of the standard and how effective it can be within their organizations. With the release of ISO/IEC 27001:2005, this will help organizational leaders figure out how to design and implement a cohesive information security program that fits their business model. By using the standard as the framework for their information security controls, organizations remove a tremendous amount of risk from relying on their information security professionals, who might miss a critical element or might not possess the depth of knowledge or skill in all the required areas. The standard ensures that the industry best-practice controls are presented for review.

If an organization customizes and implements the ISO/IEC 17799:2005 (27002) standard, it is in effect minimizing efforts that would be required for applicable laws and regulations such as HIPAA, GLB, SOX, PCI, FFIEC, etc. If an organization has implemented any other ISO-based systems such as the ISO 9001 or ISO 14001, the integration into this type of system is very straightforward and should be very familiar to the management team. The basic building block of any ISO system is formal documentation and process. There are two core concepts to an effective information security governance strategy: document and demonstrate. Your strategy must be linked to a documented program, and the program must be measurable and reportable.

The formal documentation for the ISO/IEC 17799:2005 (27002) standard is the information security policy document; this document is the single point of focus on which all information security controls and practices are designed and built. The ISO/IEC 27001:2005 will help organizations get their arms around the policy document and provide guidance on where all the pieces fit. It is critical that every organization has an information security policy document and that these series of policies be in alignment with the organization's business objectives and account for all applicable legal, regulatory, and contractual requirements. A comprehensive information security awareness and education program is required to effectively communicate the information security policies. For more information on information security awareness and why this is a critical element to protecting your organization's information assets, refer to another book I have written, *Information Security Awareness: The Psychology Behind the Technology* (ISBN: 1-4208-5632-4).

Almost every information security manager and chief information security officer struggles with funding and budget issues. I argue that if chief information security officers leverage the ISO/IEC 17799:2005 (27002) and ISO/IEC 27001:2005, these concerns and hurdles would be lessened. By the very nature of the standard, an organizationwide approach is required. In effect, it requires managers and stakeholders throughout the various departments, groups, and lines of

business to latch onto the information security strategy and integrate it into the operations of the organization. Assuming there is appropriate senior management support, this can help spread out the budget challenges to other groups and at the same time make a broader audience more aware of the importance and challenges for information security.

Information security for organizations today has shifted from a technology-oriented focus to a business practice issue, making it a critical part of almost every organization. With the pervasiveness of information security and the increasing legal and regulatory requirements placed on organizations, I was compelled to author a book on information security risk assessment and the ISO/IEC 17799:2005 (27002) Code of Practice for Information Security Management in an effort to help management and organizations lower their risks.

Introduction

The emergence of new laws and regulations in recent years has rapidly moved information security from a technology issue directly to the attention of executive management and the board of directors around the globe. Almost every industry—public, private, and government—is impacted by the recent formalization of new laws and regulations. Even private firms are feeling the downstream impact because their publicly traded clients are placing new information security-related requirements on their relationship because of these new laws and regulations. Until recently, organizations were never forced to provide evidence of compliance in the security of their information technology systems or security practices. Organizations are accepting the reality of this onslaught of activity driven out of the compliance legislation and regulations and starting to consider ways and methods to demonstrate compliance, reduce complexity, and control costs. With the evolution of the PCI (Payment Card Industry) standard, we are starting to see industries self-impose information security standards. Information security has finally matured to a position on executive management's radar that will likely not lessen any time in the near future—if ever.

According to the Privacy Rights Clearinghouse, a nonprofit watchdog group in California, 2005 was a record year for publicly reported information security breaches and incidents. From banks and hospitals to government agencies, nearly 100 major security incidents were reported, with over six in December alone. Major institutions such as Bank of America and the Federal Deposit Insurance Corp. reported major security breaches in 2005. Smaller and lesser-known firms such as ChoicePoint and CardSystems Solutions Inc. were victimized by hackers, setting off a major flurry of activity for millions of customers. Major colleges and universities across the country, from Stanford to Duke, reported unauthorized people stealing thousands of files with account numbers and other personal data belonging to students and school employees. In some of the most damaging breaches, an insider was involved in the compromise, confirming what many information security professionals continue to warn management about year after year.

The largest computer security breach ever reported in history happened in June 2005 when MasterCard reported that a hacker breached a virtually unknown credit card transaction-processing company, exposing an estimated 40 million credit card accounts. It is a little-known fact that large financial institutions and banks use small companies and vendors for trusted and critical operations such as credit card transaction processing. The security incident with CardSystems Solutions Inc. helped eliminate this little-known fact for the general public.

All of this might leave you wondering, why the rush of activity and breaches in 2005? No one probably has the answer to this riddle. I speculate there wasn't a large increase of security breaches and incidents in 2005—only an increase in their

reporting to the general public. Only within the last year have new legal requirements been passed at the state level requiring organizations to report security breaches in certain industries under specific circumstances. As of January 2006 approximately 22 states have passed security breach notification legislation, with several other states in progress. Approximately 12 states have security freeze laws allowing notified or potential identity theft victims to prevent others from establishing credit in their names. It is a little-known fact that in many states people can establish credit in your name and you are held liable by the credit-granting institution and your personal credit file can be severely damaged in the process. You are left holding the bag for the unpaid debt. It appears that in too many cases, unsuspecting consumers are held liable until they prove themselves innocent, assuming their personal credit has not been damaged beyond repair in the process. Identity theft is a nasty and ugly scenario happening to a growing number of people. According to the FBI, identity theft is one of the fastest-growing crimes today. Finding the proper balance of laws and regulations to protect the innocent while still holding people accountable for their actions is a difficult concept that will not likely ever gain acceptance from everyone affected.

The ISO/IEC 17799:2005 (27002) Code of Practice for Information Security Management is fast becoming the best-practice standard and benchmark for measuring information security around the world. The ISO/IEC 17799:2005 offers a best-practice guideline and framework for implementing an information security program, but it stops short of providing guidance on how to apply or implement the standard based on an organization's unique requirements.

Each organization possesses unique attributes; therefore, each organization will face different threats and vulnerabilities. The controls of the ISO/IEC 17799:2005 standard should be applied only as a result of a comprehensive risk assessment that involves all appropriate stakeholders and parties in the organization.

The information security policy is a good place to start the review process because the security policy should be the focal point of every information security program. In the first two chapters of this book, a model for information security risk assessment and a comprehensive information security risk assessment methodology are presented and described in detail. These first two chapters provide information security professionals and management with direct guidance and an approach that organizations in any industry can use to evaluate and assess their information security risks at a holistic level including operational and management dimensions in addition to the traditional technology-oriented methods. The model can be thought of as basic building plans that every good architect includes in his or her review of a new project, and the assessment methodology in this example is considered to be the blueprint used by the workers to erect the structure and evaluate it once it is built.

It may seem obvious, but controls and safeguards must be designed and implemented as a result of a formal risk assessment. All too often, organizations go straight to "solving the problem" instead of assessing the environment before applying a balance of controls and safeguards meeting all of the organizational requirements including business, regulatory, contractual, and legal.

The information security strategy and program must be directly linked to the business strategy and mission to be effective and measurable. A senior-level