While advances in information technology and adoption of Internet as a services delivery channel have enabled financial services institutions to provide more convenient financial services, they also have diversified and complicated the nature of risks. Financial services institutions are actively utilizing the Internet to operate and provide financial services to consumers, to businesses and to other service institutions. Advances in Internet technology also have provided a new and different business and risk environment than traditional direct-contact “brick and mortar” models. Financial services firms have to adopt information technology developments for their benefits and competitive advantages and to remain viable and competitive in the business environment. At the same time, risks and challenges to developing and maintaining a secure and safe computing environment have never held such high stakes. This book provides high-quality research, industry and practice articles in the area of information assurance in the financial services industry. The main focus of the book is to provide overview of issues involved in managing information assurance in financial services through insights into current information security measures—technology, processes, and compliance—being researched on or deployed in financial services institutions. The book hosts topics on management and strategy; technologies and countermeasures; and issues and trends. The chapters in this timely and important book are a compilation of topics on how to manage information assurance in financial services and provide a comprehensive understanding of the issues involved. The authors of the chapters are leading researchers and practitioners in the field. Their research and insights manifested in the chapters are highly relevant to the overall objectives of the book.
The 14 chapters of the book are organized into three sections based on following broad themes:

- Management and Strategy
- Technologies and Countermeasures
- Trends and Issues

The section “Management and Strategy” covers topics such as determination of return on information security investments; in-depth review of principles and strategies of risk management in banking; strategies for developing information assurance alignment with key business objectives; overview of information security issues; and empirical investigation of trends in banking and risk management strategies. The section “Technologies and Countermeasures” include chapters on security usability in the electronic banking arena and managing authentication and identity access in financial services organizations. The chapters in the last section “Trends and Issues” discuss social and human issues of information security, such as phishing and pharming, identity theft and fraud intelligence, access control mechanisms and regulatory compliance issues. A brief description of each of the chapters follows.

Chapter I, *Analyzing Risks to Determine a New Return on Security Investment: Optimizing Security in an Escalating Threat Environment* expands upon standard methods of calculating the return on security investment (ROSI) in several ways. First, it accounts for the dynamic nature of threats, vulnerabilities, and defenses as they apply to the finance sector. Second, it takes a more holistic view of security investments by using a portfolio method. Dr. Warren Axelrod of The United States Trust Company (N.A.) discusses the protection of information assets from two different perspectives. One is the hierarchical view of security measures, such as avoidance, deterrence, and prevention. The other is defense in depth, wherein various security tools and processes, such as firewalls, identity and access management, and intrusion detection and prevention products, are combined for greater overall protection. The reader will gain a deeper understanding of the factors that affect the risks and returns of investments in security measures, tools, and processes and will find that using the portfolio approach leads to more cost-effective security.

Banks play an important role in the financial system contributing to efficient and well-functioning transfers of capital and risk between those in excess (savers) and those in need (borrowers) of money. Traditionally, financial risks, like interest rate, foreign exchange, and credit risks, have been the most important and typical ones for banking operations. However, lately the risk environment of banks has changed considerably. In Chapter II, *Risk Management in Banking: A Review of Principles and Strategies*, Dr. Göran Bergendahl and Dr. Ted Lindblom, both of University of Gothenburg, Sweden, stress the vital importance for the single bank to have a more sophisticated and well-structured approach to risk management than it had 15 years ago. The chapter’s main focus is on how banking objectives, such as profitability and growth, should govern risk management and how these objectives are made operational in the management of those assets and liabilities exposed to changes in market prices and in customer repayments of loans.
Chapter III, *Developing Information Assurance Alignment in Financial Services*, is based on research work in eight financial services organizations (four international financial services organizations, two national retail banks and two multinational banks). The chapter focuses on information assurance strategy in financial services and discusses two important questions: How can senior executives align information assurance strategy with corporate strategy?, and what factors influence decisions regarding information assurance strategy? Dr. Jean-Noel Ezingeard, Dr. Elspeth McFadzean, and Dr. David Birchall of Henley Management College, UK, explain why information assurance strategy needs to be aligned with corporate strategy, and why boards of directors in financial services need to take a strong interest in the development of their organization’s IA strategy. The chapter highlights three key drivers: risk assessment and/or risk reports—including legal requirements, such as Sarbanes-Oxley and Basel II; protection of shareholder value; cost and the need to keep IA costs under control while delivering a suitable level of protection for the organization’s information. The chapter also explains how requirements of various stakeholders can be reconciled when they are in conflict.

The banking sector is identified as a critical infrastructure by the federal government. Dr. Kevin Streff of Dakota State University (USA) in Chapter IV, *Information Security in Banking*, provides an overview of information security in the banking sector; outlines the information and technology common to most banks; explains the information security law and regulation banks must comply with; and explores the information security controls necessary to protect the banking infrastructure in the United States. The chapter reviews what banks need to do to protect the confidentiality, integrity, and availability of information, including the presentation of an information security program design that community banks should use as a framework for information protection.

Chapter V, *Security Risk Management Strategy of Financial Services Institutions*, develops a novel security risk management strategy of financial services institutes. Dr. Guoling Lao and Dr. Liping Wang of Shanghai University of Finance and Economics, China, present the systematic and cybernetics theory as the instruction; regards the risk analysis process; the management strategy implementation; and the monitor and audit as an organic security management system. The strategy presented in the chapter is an auto-adapted open system to defeat various safe threats dynamically. By comparing management of electronic-commerce (e-commerce) security risk with that of traditional financial risk, the chapter suggests accurate security risk measurement in the way of quantitative analysis and further integration of the e-commerce security risk with traditional financial risks. This article attempts to make improvement on the basis of existing research and studies and provide a proper security risk management strategy for financial services institutes engaged in e-commerce.

In electronic banking (e-banking), user authentication with mobile phones and special-purpose cryptographic tokens is a promising alternative to conventional approaches, such as digital signatures on a personal computer (PC). Special-purpose tokens that do not have external connections avoid viruses transmitted via the Internet. Moreover, phones and tokens are mobile. Chapter VI, *New Technologies in E-Banking: Convenient and Trustworthy?*, assesses the potential of new technologies for user authentication (verification of the user’s identity) on the basis of a practical test and an analysis of trust. Dr. Niels Jørgensen of Roskilde University, Denmark, conducts a practical test comprised of a password generator, mobile phones with SMS, WAP, and 3G, and (conventional) PC-based authentication using digital signatures—all as used by a Danish electronic bank. The test indicates that in some ways the hardware-based technologies are indeed easier to use. Also, the trust
analysis indicates that the secrecy of the new approaches may be a weakness, since there is no publicly available analysis of their security. The chapter suggests that secrecy of the hardware-based technologies may be justified by the need to prevent various attacks, such as physically opening a password generator to determine its secret key, and that a prerequisite for consumer trust may be the introduction of security evaluation methods that do not disclose the secret parts of the technologies to the public and are conducted by public authorities or independent third parties.

Authentication is a prime challenge for banks today as end users’ digital identities are being compromised through increasingly sophisticated means. Chapter VII, Stronger Authentication: Responding to the Crisis of Confidence, provides a timely review of the authentication concept and key authentication technologies, namely password tokens, biometrics, smart cards, smart tokens, and out-of-band authentication. Dr. Alvin Y.C. Yeo, SIM University, Singapore, proposes an integrative model that frames three key considerations in choosing an authentication solution—cyber threat types, regulatory requirements, and business considerations. The chapter begins with a review of the authentication concept and key authentication technologies. Next, the author proposes his integrative model and explores the implications for financial institutions. Finally, the chapter concludes with pragmatic suggestions by proposing a set of evaluation criteria for choosing authentication solutions and key legal considerations.

When designing and implementing a system that handles sensitive or valuable information, there can be few discussions that do not include some reference to ensuring adequate security. At a strategic level, there will be high-level requirements for security that will safeguard the system, which must ultimately translate to practical solutions and physical implementations. Chapter VIII, Smart Cards for Security and Assurance, focuses on the technical implementation of security requirements and, in particular, the use of smart cards as trusted security tokens. In this chapter, Dr. Konstantinos Markantonakis, Dr. Keith Mayes, and Dr. Fred Piper of Smart Card Centre, all of the University of London examine the significance of tamper resistance by exploring the different hardware and software platforms in relation to smart card attacks. They also highlight certain issues around the deployment of smart card technology in the financial industry.

After years of neglect, identity and access management (IAM) is now strongly ensconced in the modern information technology enterprise. Businesses are driven by the desire for greater business ecosystem and process efficiency, automatic regulatory compliance, and, frankly, the deep-seated aversion to negative press resulting from identity theft and other information asset intrusions. In Chapter IX, Unified Identities in Complex Financial Organizations, Peter Orondo of Acclaim Consulting Group Inc., USA, makes the case for a unified approach to managing identities in a complex enterprise in the financial services sector. He discusses the framework for evolving unified policies and processes and prescribes optimal organizational governance to implement them. He also discusses the relationship with regulatory compliance and other critical information enterprise functions and includes nonprescriptive, strategic positions that progressive organizations may take to streamline enterprise identity and access management.

In Chapter X, Identity Management and Access, Nick Pullman of Citigroup, USA, and Dr. Kevin Streff of Dakota State University, USA, discuss the role of identity and access management in the financial services industry. Identity and access management is a very broad concept that has far reaching rewards or consequences within an organization. This chapter provides a survey of the topics within identity and access management so that managers and
security administrators of financial institutions can gain an understanding of the issues and
possible solutions. The chapter discusses the core concepts of identity and access manage-
ment, how they can fit into an enterprise solution, and how the individual concepts within
identity and access management work together. Finally, the authors discuss the future trends
of identity and access management. After reading this chapter, readers should be able to
understand (1) the identity lifecycle and how to manage it; (2) understand the proliferation of
identities and how to consolidate them; (3) the core concepts behind IAM, including single
sign on, access control, authentication, authorization, identity integration, provisioning, and
password management; and (4) how to implement an IAM solution from both a technical
and managerial perspective.

Phishing and pharming continue to plague many financial institutions and e-commerce Web
sites. Sophisticated criminals now have turned to a new activity, “rat-ing,” where criminals
can watch everything the user is typing from other parts of the globe. Various countries also
have passed identity fraud legislations, but the global nature of cybercrime raises difficult
legislative problems of jurisdiction as criminals use offshore servers and Internet sites to avoid
domestic regulations. In Chapter XI, *Swallowing the Bait, Hook, Line and Sinker: Phishing,
Pharming, and now Rat-ing!*, Dr. Sylvia Kierkegaard of IAITL, Denmark, analyzes some of
the national and international initiatives that have been enacted by the European Union and
the United States, specifically in the area of curtailing phishing activities and its variants.
The chapter discusses the American and European initiatives to combat fraud in cyberspace.
It discusses the salient provisions of the U.S. Anti-Phishing Act as well as a handful of
identity theft bills that are pending in the U.S. Congress. The chapter analyzes whether the
proposed legislations will actually deter cybercrime. The author suggests that with so many
technology issues, the problems of phishing, pharming, and rat-ing are not things that can
be solved by legislation only but also require technology and security awareness.

In Chapter XII, *The Evolution of Fraud Intelligence*, David Porter of Detica Corporation,
UK, discusses the latest innovations in fraud detection, with a particular focus on insider
fraud and organized fraud. The author argues that as fraud continues to grow at an alarming
rate across the financial services sector. This constant evolution in fraudster behavior means
that financial institutions need to keep their technology-based countermeasures constantly
updated, particularly given the increasing involvement of organized crime. In addition to
upgrading their current operational detection systems, this chapter aims to encourage orga-
nizations to improve on current levels of data and information assurance in order to ensure
the generation of high quality intelligence on the enemy and to adopt a structured framework
for better understanding and description of exactly what we mean by “intelligence.”

Increasingly, enterprises are offering online financial services. Often, access to such financial
services is based on mutually agreed upon subscriptions. In subscription-based financial
services information assurance occurs as an ancillary to subscriptions; the control terms
embedded in subscriptions are formalized by control policies and enforced by generic access
control mechanisms. In Chapter XIII, *Managing Information Assurance in Subscription-
based Financial Services*, Dr. Victoria Ungureanu of Rutgers University, USA, reviews the
main access control mechanisms that can be used to govern subscription-based financial
services. The overall performance of these mechanisms is analyzed with respect to several
important features of subscription-based financial services. Namely, the chapter analyzes
the impact of the following features: (1) the number of clients/subscriptions potentially can
be large; (2) the number and types of subscriptions offered by a provider varies in time;
(3) subscription terms may change; and (4) subscriptions terms may contain may take into
account mutable information. Furthermore, the chapter presents in detail one mechanism that achieves good performance.

The U.S. Sarbanes-Oxley Act (SOA) introduced significant changes to financial practice and corporate governance regulation, including stringent new rules designed to protect investors by improving the accuracy and reliability of corporate disclosures. Briefly speaking, it requires management to submit a report containing an assessment of the effectiveness of the internal control structure and a description of material weaknesses in such internal controls and of any material noncompliance. Such mandatory regulations can have broader ramifications on firm profitability, market structure, and social welfare, many of which were unintended when policy makers first formulated this act. Moreover, the tight coupling between compliance activities, information disclosure, and information technology investments can have implications for information technology governance because of the potential to change relationships between technology investments and business. Dr. Anindya Ghose of New York University in Chapter XIV, *Information Disclosure and Regulatory Compliance: Economic Issues and Analysis*, provides intuitive insights into the trade-offs involved for firms in disclosure of such information and lays the ground for some research questions that would be of interest to academics, industry executives, and policy makers, alike.

The professionals, managers, and researchers working in information technology or information security in financial services industries would benefit from the chapters. The authors are from both industry and academia and present a complete array of very relevant and insightful chapters for a wide range of audiences. Due to the depth and breadth of coverage of topics in information assurance, auditors and lawyers from financial services institutions also will find this book a very helpful resource. Given the relative absence of relevant and quality books in the area of information assurance in financial services, this volume provides immense scholarly value to the information technology discipline, in general, and even more to information security, in particular, for financial services institutions.