Biometric And Auditing Issues Addressed In A Throughput Model

"This reference set provides a complete understanding of the development of applications and concepts in clinical, patient, and hospital information systems"--Provided by publisher.

Totally updated for 2011, here's the ultimate study guide for the CISSP exam Considered the most desired certification for IT security professionals, the Certified Information Systems Security Professional designation is also a career-booster. This comprehensive study guide covers every aspect of the 2011 exam and the latest revision of the CISSP body of knowledge. It offers advice on how to pass each section of the exam and features expanded coverage of biometrics, auditing and accountability, software security testing, and other key topics. Included is a CD with two full-length, 250-question sample exams to test your progress. CISSP certification identifies the ultimate IT security professional; this complete study guide is fully updated to cover all the objectives of the 2011 CISSP exam Provides in-depth knowledge of access control, application development security, business continuity and disaster recovery planning, cryptography, Information Security governance and risk management, operations security, physical (environmental) security, security architecture and design, and telecommunications and network security Also covers legal and regulatory investigation and compliance Includes two practice exams and challenging review questions on the CD Professionals seeking the CISSP certification will boost their chances of success with CISSP: Certified Information Systems Security Professional Study Guide, 5th Edition.

Biometric and Auditing Issues Addressed in a Throughput ModelIAP

Physical and behavioral biometric technologies such as fingerprinting, facial recognition, voice identification, etc. have enhanced the level of security substantially in recent years. Governments and corporates have employed these technologies to achieve better customer satisfaction. However, biometrics faces major challenges in reducing criminal, terrorist activities and electronic frauds, especially in choosing appropriate decision-making algorithms. To face this challenge, new developments have been made, that amalgamate biometrics with artificial intelligence (AI) in decision-making modeling. Advanced software algorithms of AI, processing information offered by biometric technology, achieve better results. This has led to growth in the biometrics technology industry, and is set to increase the security and internal control operations manifold. This book provides an overview of the existing biometric technologies, decision-making algorithms and the growth opportunity in biometrics. The book proposes a throughput model, which draws on computer science, economics and psychology to model perceptual, informational sources, judgmental processes and decision choice algorithms. It reviews how biometrics might be applied to reduce risks to individuals and organizations, especially when dealing with digital-based media.

Step-by-step guide to successful implementation and control of IT systems—including the Cloud Many auditors are unfamiliar with the techniques they need to know to efficiently and effectively determine whether information systems are adequately protected. Now in a Second Edition, Auditor's Guide to IT Auditing presents an easy, practical guide for auditors that can be applied to all computing environments. Follows the approach used by the Information System Audit and Control Association's model curriculum, making this book a practical approach to IS auditing Serves as an excellent study guide for those preparing for the CISA and CISM exams Includes discussion of risk evaluation methodologies, new regulations, SOX, privacy, banking, IT governance, CobiT, outsourcing, network management, and the Cloud Includes a link to an education version of IDEA--Data Analysis Software As networks and enterprise resource planning systems bring resources together, and as increasing privacy violations threaten more organization, information systems integrity becomes more important than ever. Auditor's Guide to IT Auditing, Second Edition empowers auditors to effectively gauge the adequacy and effectiveness of information systems controls.

With an A–Z format, this encyclopedia provides easy access to relevant information on all aspects of biometrics. It features approximately 250 overview entries and 800 definitional entries. Each entry includes a definition, key words, list of synonyms, list of related entries, illustration(s), applications, and a bibliography. Most entries include useful literature references providing the reader with a portal to more detailed information.

Financial statement analysis involves an understanding of an entity by applying analytical techniques to its accounting numbers. However, financial statement analyses are going through a transformation similar to the manufacturing age changing to information centered orientation. That is, it is no longer sufficient to understand the tools for analysing financial accounting information. Other types of relevant information that are not directly captured by financial statement information have a profound effect on creditors, investors, reporting bureaus, governmental agencies and regulators. This text differs from other financial statement textbooks in that it not only takes the traditional analysis of financial information, but also management and economic information that is not directly measurable or easily derived from financial accounting reports. Further, this textbook emphasises the measurement and valuation of brand, sustainability, ethical systems and trusts systems. Moreover, this text also differs in that it provides a modeling viewpoint of information analysis linked with decision makers perception and judgments before arriving at a decision. The modeling perspective enhances financial statement analysis by: 1. Including not only financial information, but also management and economic information; 2. Combining the passive tools used in investment and financial analysis (eg: ratio analysis) with individuals framing of the problem (perception) and analysis (judgment) before arriving at a decision; 3. Viewing information analysis through a camera lens reinforced by a basic two stage modeling approach in order to support decisions regarding a particular course of action to implement. Further, this text transforms what other

financial statement analysis textbooks emphasise as an input-output and static analysis approach to a more dynamic and process approach. In addition, this textbook divulges from a financial analysis viewpoint to a knowledge creation perspective. This new knowledge creation perspective is intended for upper level undergraduates and graduate students, such as accounting, economic, finance, information systems, marketing, organisational behavior students, and psychology and sociology students. In addition, this book can be beneficial to government, non-profit and business oriented individuals.

The ultimate CISA prep guide, with practice exams Sybex's CISA: Certified Information Systems Auditor Study Guide, Fourth Edition is the newest edition of industry-leading study guide for the Certified Information System Auditor exam, fully updated to align with the latest ISACA standards and changes in IS auditing. This new edition provides complete guidance toward all content areas, tasks, and knowledge areas of the exam and is illustrated with real-world examples. All CISA terminology has been revised to reflect the most recent interpretations, including 73 definition and nomenclature changes. Each chapter summary highlights the most important topics on which you'll be tested, and review questions help you gauge your understanding of the material. You also get access to electronic flashcards, practice exams, and the Sybex test engine for comprehensively thorough preparation. For those who audit, control, monitor, and assess enterprise IT and business systems, the CISA certification signals knowledge, skills, experience, and credibility that delivers value to a business. This study guide gives you the advantage of detailed explanations from a real-world perspective, so you can go into the exam fully prepared. Discover how much you already know by beginning with an assessment test Understand all content, knowledge, and tasks covered by the CISA exam Get more in-depths explanation and demonstrations with an all-new training video Test your knowledge with the electronic test engine, flashcards, review questions, and more The CISA certification has been a globally accepted standard of achievement among information systems audit, control, and security professionals since 1978. If you're looking to acquire one of the top IS security credentials, CISA is the comprehensive study guide you need.

Threatening the safety of individuals, computers, and entire networks, cyber crime attacks vary in severity and type. Studying this continually evolving discipline involves not only understanding different types of attacks, which range from identity theft to cyberwarfare, but also identifying methods for their prevention. Cyber Crime: Concepts, Methodologies, Tools and Applications is a three-volume reference that explores all aspects of computer-based crime and threats, offering solutions and best practices from experts in software development, information security, and law. As cyber crime continues to change and new types of threats emerge, research focuses on developing a critical understanding of different types of attacks and how they can best be managed and eliminated.

1,000 Challenging practice questions for Exam SY0-501 CompTIA Security+ Practice Tests provides invaluable practice for candidates preparing for Exam SY0-501. Covering 100% of exam objectives, this book provides 1,000 practice questions to help you test your knowledge and maximize your performance well in advance of exam day. Whether used alone or as a companion to the CompTIA Security+ Study Guide, these questions help reinforce what you know while revealing weak areas while there’s still time to review. Six unique practice tests plus one bonus practice exam cover threats, attacks, and vulnerabilities; technologies and tools; architecture and design; identity and access management; risk management; and cryptography and PKI to give you a comprehensive preparation resource. Receive one year of FREE access to the Sybex online interactive learning environment, to help you prepare with superior study tools that allow you to gauge your readiness and avoid surprises on exam day. The CompTIA Security+ certification is internationally-recognized as validation of security knowledge and skills. The exam tests your ability to install and configure secure applications, networks, and devices; analyze, respond to, and mitigate threats; and operate within applicable policies, laws, and regulations. This book provides the practice you need to pass with flying colors. Master all six CompTIA Security+ objective domains Test your knowledge with 1,000 challenging practice questions Identify areas in need of further review Practice test-taking strategies to go into the exam with confidence The job market for information security professionals is thriving, and will only expand as threats become more sophisticated and more numerous. Employers need proof of a candidate’s qualifications, and the CompTIA Security+ certification shows that you’ve mastered security fundamentals in both concept and practice. If you’re ready to take on the challenge of defending the world’s data, CompTIA Security+ Practice Tests is an essential resource for thorough exam preparation.

Certified Information Systems Auditor (CISA) is a certification issued by ISACA to people in charge of ensuring that an organization's IT and business systems are monitored, managed and protected; the certification is presented after completion of a comprehensive testing and application process. The CISA certification is a globally recognized standard for appraising an IT auditor's knowledge, expertise and skill in assessing vulnerabilities and instituting IT controls in an enterprise environment. It is designed for IT auditors, audit managers, consultants and security professionals. Preparing for the Certified Information Systems Auditor exam to become an CISA Certified by ISACA? Here we’ve brought 900+ Exam Questions for you so that you can prepare well for this CISA exam Unlike other online simulation practice tests, you get a Paperback version that is easy to read & remember these questions. You can simply rely on these questions for successfully certifying this exam.

"This book identifies practices and strategies being developed using the new technologies that are available and the impact that these tools might have on public health and safety practices"--Provided by publisher.

Proven and emerging strategies for addressing document and records management risk within the framework of information governance principles and best practices Information Governance (IG) is a rapidly emerging "super discipline" and is now being applied to electronic document and records management, email, social media, cloud computing, mobile computing, and, in fact, the management and output of information organization-wide. IG leverages information technologies to enforce policies, procedures and controls to manage information risk in compliance with legal and litigation demands, external regulatory requirements, and internal governance objectives. Information Governance: Concepts, Strategies, and Best Practices reveals how, and why, to utilize IG and leverage information technologies to control, monitor, and enforce information access and security policies. Written by one of the most recognized and published experts on information governance, including specialization in e-document security and electronic records management Provides big picture guidance on the imperative for information governance and best practice guidance on electronic document and records management Crucial advice and insights for compliance and risk managers, operations managers, corporate counsel, corporate records managers, legal administrators, information technology managers, archivists, knowledge managers, and information governance professionals IG sets the policies that control and manage the use of organizational information, including social media, mobile computing, cloud computing, email, instant messaging, and the use of e-documents and records. This extends to e-discovery planning and preparation. Information Governance: Concepts, Strategies, and Best Practices provides step-by-step guidance for developing information governance strategies and practices to manage risk in the use of electronic business documents and records.

It is irrefutable that information is a valuable asset to an organization regardless of the form i.e. on paper or digital. Many business operations depend highly on this information in their critical business processes. Thus, organizations need to protect such information appropriately. Information should be protected to secure confidentiality, integrity and availability. In addition, other elements such as non-repudiation and authentication should also be considered. More organizations have come to realize the importance of protecting and securing their information. Information Security Management System

(ISMS) is a framework which enables organizations to manage security incidents holistically and systematically. The benefits of adopting and deploying this information security management framework are extensive. Its adoption and deployment is a tedious and lengthy process and the level of commitment is high, but the benefits, surpasses all that. This guideline provides a holistic view on how to jumpstart the ISMS implementation. Organizations would be able to have a better understanding of ISMS implementation; thus easing the process and ensuring appropriate utilization of resources whilst implementing ISMS.

The censorship and surveillance of individuals, societies, and countries have been a long-debated ethical and moral issue. In consequence, it is vital to explore this controversial topic from all angles. Censorship, Surveillance, and Privacy: Concepts, Methodologies, Tools, and Applications is a vital reference source on the social, moral, religious, and political aspects of censorship and surveillance. It also explores the techniques of technologically supported censorship and surveillance. Highlighting a range of topics such as political censorship, propaganda, and information privacy, this multi-volume book is geared towards government officials, leaders, professionals, policymakers, media specialists, academicians, and researchers interested in the various facets of censorship and surveillance.

Cloud technologies have revolutionized the way we store information and perform various computing tasks. With the rise of this new technology, the ability to secure information stored on the cloud becomes a concern. The Handbook of Research on Securing Cloud-Based Databases with Biometric Applications explores the latest innovations in promoting cloud security through human authentication techniques. Exploring methods of access by identification, including the analysis of facial features, fingerprints, DNA, dental characteristics, and voice patterns, this publication is designed especially for IT professionals, academicians, and upper-level students seeking current research surrounding cloud security.

This book brings together aspects of statistics and machine learning to provide a comprehensive guide to evaluating, interpreting and understanding biometric data. It naturally leads to topics including data mining and prediction to be examined in detail. The book places an emphasis on the various performance measures available for biometric systems, what they mean, and when they should and should not be applied. The evaluation techniques are presented rigorously, however they are always accompanied by intuitive explanations. This is important for the increased acceptance of biometrics among non-technical decision makers, and ultimately the general public.

Praise for Auditor's Guide to Information Systems Auditing "Auditor's Guide to Information Systems Auditing is the most comprehensive book about auditing that I have ever seen. There is something in this book for everyone. New auditors will find this book to be their bible-reading it will enable them to learn what the role of auditors really is and will convey to them what they must know, understand, and look for when performing audits. For experiencedauditors, this book will serve as a reality check to determine whether they are examining the right issues and whether they are being sufficiently comprehensive in their focus. Richard Cascarino has done a superb job." —E. Eugene Schultz, PhD, CISSP, CISM Chief Technology Officer and Chief Information Security Officer, High Tower Software A step-by-step guide tosuccessful implementation and control of information systems More and more, auditors are being called upon to assess the risks and evaluate the controls over computer information systems in all types of organizations. However, many auditors are unfamiliar with the techniques they need to know to efficiently and effectively determine whether information systems are adequately protected. Auditor's Guide to Information Systems Auditing presents an easy, practical guide for auditors that can be applied to all computing environments. As networks and enterprise resource planning systems bring resources together, and as increasing privacy violations threaten more organization, information systems integrity becomes more important than ever. With a complimentary student'sversion of the IDEA Data Analysis Software CD, Auditor's Guide to Information Systems Auditing empowers auditors to effectively gauge the adequacy and effectiveness of information systems controls.

Biometric recognition, or simply biometrics, is the science of establishing the identity of a person based on physical or behavioral attributes. It is a rapidly evolving field with applications ranging from securely accessing one's computer to gaining entry into a country. While the deployment of large-scale biometric systems in both commercial and government applications has increased the public awareness of this technology, "Introduction to Biometrics" is the first textbook to introduce the fundamentals of Biometrics to undergraduate/graduate students. The three commonly used modalities in the biometrics field, namely, fingerprint, face, and iris are covered in detail in this book. Few other modalities like hand geometry, ear, and gait are also discussed briefly along with advanced topics such as multibiometric systems and security of biometric systems. Exercises for each chapter will be available on the book website to help students gain a better understanding of the topics and obtain practical experience in designing computer programs for biometric applications. These can be found at: http://www.csee.wvu.edu/~ross/BiometricsTextBook/. Designed for undergraduate and graduate students in computer science and electrical engineering, "Introduction to Biometrics" is also suitable for researchers and biometric and computer security professionals.

Today's management world continually relies on technological efficiency to function and perform at a high standard. As technology becomes a greater part in many fields, understanding and managing this factor is integral for organizations. Inventive Approaches for Technology Integration and Information Resources Management provides an overview and analysis of knowledge management in sustainability, emergency preparedness, and IT, among other fields integral to the modern technological era. By providing a foundation for innovative practices in using technology and information resources, this publication is essential for practitioners and professionals, as well as undergraduate/graduate students and academicians.

During the 2016 presidential election, America's election infrastructure was targeted by actors sponsored by the Russian government. Securing the Vote: Protecting American Democracy examines the challenges arising out of the 2016 federal election, assesses current technology and standards for voting, and recommends steps that the federal government, state and local governments, election administrators, and vendors of voting technology should take to improve the security of election infrastructure. In doing so, the report provides a vision of voting that is more secure, accessible, reliable, and verifiable.

Innovation and Future Trends in Food Manufacturing and Supply Chain Technologies focuses on emerging and future trends in food manufacturing and supply chain technologies, examining the drivers of change and innovation in the food industry and the current and future ways of addressing issues such as energy reduction and rising costs in food manufacture. Part One looks at innovation in the food supply chain, while Part Two covers emerging technologies in food processing and packaging. Subsequent sections explore innovative food preservation technologies in themed chapters and sustainability and future research needs in food manufacturing. Addresses issues such as energy reduction and rising costs in food manufacture Assesses current supply chain technologies and the emerging advancements in the field, including key chapters on food processing technologies Covers the complete food manufacturing scale, compiling significant research from academics and important industrial figures

Protect your customers-and your business-with these essential "rules of the road" for maintaining Web site security Any company planning to do business on the Internet today must first become fully knowledgeable about the legal issues pertaining to consumer privacy and security, or risk severe financial penalties and loss of customer loyalty. In

addition to making a Web site easy to navigate and transactions simple to manage, Web site developers must also make it secure. Failure to do so may result in legal action and irreparable damage to a company's reputation. E-Business Privacy and Trust is a clear, easy-to-follow handbook that outlines the legal aspects of maintaining privacy and security on the Web and shows today's businesses how to protect themselves by building basic guidelines into their e-business development strategies. The author, an expert on the subject of computer law, provides a complete overview of privacy law, security systems, and various ways today's businesses can protect themselves and their customers online, whether they're doing business locally or globally. In an environment fraught with potential pitfalls, E-Business Privacy and Trust will help every e-business owner, financial professional, and IT expert confidently reap the benefits of doing business on the Web while providing the level of security, confidentiality, and service your customers and your company demand.

Today’s accounting professionals are expected to help organizations identify enterprise risks and provide quality assurance for their companies' information systems. Readers can rely on ACCOUNTING INFORMATION SYSTEMS, 11E’s clear presentation to gain a thorough understanding of two issues most critical to accounting information systems in use today: enterprise systems and controls for maintaining those systems. ACCOUNTING INFORMATION SYSTEMS, 11E explores today's most intriguing accounting information systems (AIS) topics and details how these issues relate to business processes, information technology, strategic management, security, and internal controls. The authors focus on today’s most important advancements, using a conversational tone rather than complex technical language to ensure readers develop the solid foundation in AIS needed to be successful. Important Notice: Media content referenced within the product description or the product text may not be available in the ebook version.

Security and authentication issues are surging to the forefront of the research realm in global society. As technology continues to evolve, individuals are finding it easier to infiltrate various forums and facilities where they can illegally obtain information and access. By implementing biometric authentications to these forums, users are able to prevent attacks on their privacy and security. Biometrics: Concepts, Methodologies, Tools, and Applications is a multi-volume publication highlighting critical topics related to access control, user identification, and surveillance technologies. Featuring emergent research on the issues and challenges in security and privacy, various forms of user authentication, biometric applications to image processing and computer vision, and security applications within the field, this publication is an ideal reference source for researchers, engineers, technology developers, students, and security specialists.

Expanded into two volumes, the Second Edition of Springer’s Encyclopedia of Cryptography and Security brings the latest and most comprehensive coverage of the topic: Definitive information on cryptography and information security from highly regarded researchers Effective tool for professionals in many fields and researchers of all levels Extensive resource with more than 700 contributions in Second Edition 5643 references, more than twice the number of references that appear in the First Edition With over 300 new entries, appearing in an A-Z format, the Encyclopedia of Cryptography and Security provides easy, intuitive access to information on all aspects of cryptography and security. As a critical enhancement to the First Edition’s base of 464 entries, the information in the Encyclopedia is relevant for researchers and professionals alike. Topics for this comprehensive reference were elected, written, and peer-reviewed by a pool of distinguished researchers in the field. The Second Edition’s editorial board now includes 34 scholars, which was expanded from 18 members in the First Edition. Representing the work of researchers from over 30 countries, the Encyclopedia is broad in scope, covering everything from authentication and identification to quantum cryptography and web security. The text’s practical style is instructional, yet fosters investigation. Each area presents concepts, designs, and specific implementations. The highly-structured essays in this work include synonyms, a definition and discussion of the topic, bibliographies, and links to related literature. Extensive cross-references to other entries within the Encyclopedia support efficient, user-friendly searches for immediate access to relevant information. Key concepts presented in the Encyclopedia of Cryptography and Security include: Authentication and identification; Block ciphers and stream ciphers; Computational issues; Copy protection; Cryptanalysis and security; Cryptographic protocols; Electronic payment and digital certificates; Elliptic curve cryptography; Factorization algorithms and primality tests; Hash functions and MACs; Historical systems; Identity-based cryptography; Implementation aspects for smart cards and standards; Key management; Multiparty computations like voting schemes; Public key cryptography; Quantum cryptography; Secret sharing schemes; Sequences; Web Security. Topics covered: Data Structures, Cryptography and Information Theory; Data Encryption; Coding and Information Theory; Appl.Mathematics/Computational Methods of Engineering; Applications of Mathematics; Complexity. This authoritative reference will be published in two formats: print and online. The online edition features hyperlinks to cross-references, in addition to significant research.

The Handbook of Information Security is a definitive 3-volume handbook that offers coverage of both established and cutting-edge theories and developments on information and computer security. The text contains 180 articles from over 200 leading experts, providing the benchmark resource for information security, network security, information privacy, and information warfare.

Black Hat, Inc. is the premier, worldwide provider of security training, consulting, and conferences. In Black Hat Physical Device Security: Exploiting Hardware and Software, the Black Hat experts show readers the types of attacks that can be done to physical devices such as motion detectors, video monitoring and closed circuit systems, authentication systems, thumbprint and voice print devices, retina scans, and more. The Black Hat Briefings held every year in Las Vegas, Washington DC, Amsterdam, and Singapore continually expose the greatest threats to cyber security and provide IT mind leaders with ground breaking defensive techniques. There are no books that show security and

networking professionals how to protect physical security devices. This unique book provides step-by-step instructions for assessing the vulnerability of a security device such as a retina scanner, seeing how it might be compromised, and taking protective measures. The book covers the actual device as well as the software that runs it. By way of example, a thumbprint scanner that allows the thumbprint to remain on the glass from the last person could be bypassed by pressing a "gummy bear" piece of candy against the glass so that the scan works against the last thumbprint that was used on the device. This is a simple example of an attack against a physical authentication system. First book by world-renowned Black Hat, Inc. security consultants and trainers First book that details methods for attacking and defending physical security devices Black Hat, Inc. is the premier, worldwide provider of security training, consulting, and conferences

This book proposes a Throughput Model that draws from computer science, economic and psychology literatures to model perceptual and judgmental processes whereby biometrics might be used to reduce risks to a company's internal control. The book also discusses challenges in employing biometric technology and pinpoints avenues for future research. Biometrics is the examination of measurable biological characteristics. In organizational security, biometrics refers to tools that rely on measurable physical and behavioral characteristics that can be automatically checked. The Throughput Modeling process enables organizations to employ trust systems in assisting transactions that are motivated by ethical considerations. Auditing systems are by far based on trust. Concepts of ethics and trust are aided by the employment of biometrics technology, which enhances the transactions between individuals and organizations in an internal control environment. Issues pertaining to sustainability are also examined with the assistance of the Throughput Model. Finally, this book examines the potential use of an internal control biometrics system to lessen threats to identification and verification procedures. This book proposes an "Throughput Model framework" that considers both exposure and information risks as fundamental factors in classifying applications and organizational processes that might be candidates for the type of internal control biometrics system that biometrics can offer.

Bio-Privacy: Privacy Regulations and the Challenge of Biometrics provides an in-depth consideration of the legal issues posed by the use of biometric technology. Focusing particularly on the relationship between the use of this technology and the protection of privacy, this book draws on material across a range of jurisdictions in order to explore several key questions. What are the privacy issues in the biometric context? How are these issues currently dealt with under the law? What principles are applied? Is the current regulation satisfactory? Is it applied consistently? And, more generally, what is the most appropriate way to deal with the legal implications of biometrics? Offering an analysis, and recommendations, with a view to securing adequate human rights and personal data protection, Bio-Privacy: Privacy Regulations and the Challenge of Biometrics will be an important reference point for those with interests in the tension between freedom and security.

* SANS (SysAdmin, Audit, Network, Security) has trained and certified more than 156,000 security professionals. * This book is the cost-friendly alternative to the $450 SANS materials and $1200 SANS courses, providing more and better information for $60. * SANS is widely known and well-respected, with sponsors, educators and advisors from prestigious government agencies (FBI), corporations, and universities (Carnegie Mellon) around the world. * A companion CD contains the Boson test engine packed with review questions.

Waymond Rodgers, PhD, CPA, has worked over fifteen years studying how to combine ethical considerations with a decision-making model of perception, information, and judgment that will foster better decision-making processes, resulting in an overall improvement of daily life. He has presented seminars on ethics at numerous international conferences and also provided ethics presentations to corporations, societies, universities, and other organizations such as Opus Dei. The need for ethics in society is such an important factor because many commonly held ethical values are incorporated into laws. Yet, due to the judgmental nature of certain values, many ethical values of a society cannot be incorporated into law. Ethical process thinking involves discerning right from wrong and acting in alignment with such judgments, enabling us to complement several ethical approaches of preferences, rules, and principles with unique decision-making pathways leading to an ethical decision. Ethical decisions can be difficult to make due to a misunderstanding of the decision-making process, incomplete information, changing environments, time pressures, and a lack of expertise. Ethical Beginnings: Preferences, Rules, and Principles influencing decision making explains the major barriers to ethical decision-making, why structuring a problem is necessary, and when to use information for decision-making purposes.

This User's Guide is intended to support the design, implementation, analysis, interpretation, and quality evaluation of registries created to increase understanding of patient outcomes. For the purposes of this guide, a patient registry is an organized system that uses observational study methods to collect uniform data (clinical and other) to evaluate specified outcomes for a population defined by a particular disease, condition, or exposure, and that serves one or more predetermined scientific, clinical, or policy purposes. A registry database is a file (or files) derived from the registry. Although registries can serve many purposes, this guide focuses on registries created for one or more of the following purposes: to describe the natural history of disease, to determine clinical effectiveness or cost-effectiveness of health care products and services, to measure or monitor safety and harm, and/or to measure quality of care. Registries are classified according to how their populations are defined. For example, product registries include patients who have been exposed to biopharmaceutical products or medical devices. Health services registries consist of patients who have had a common procedure, clinical encounter, or hospitalization. Disease or condition registries are defined by patients having the same diagnosis, such as cystic fibrosis or heart failure. The User's Guide was created by researchers affiliated with AHRQ's Effective Health Care Program, particularly those who participated in AHRQ's DEcIDE (Developing Evidence to Inform Decisions About Effectiveness) program. Chapters were subject to multiple internal and external independent reviews.

This book mainly focuses on cloud security and high performance computing for cloud auditing. The book discusses emerging challenges and techniques developed for high performance semantic cloud auditing, and presents the state of the art in cloud auditing, computing and security techniques with focus on technical aspects and feasibility of auditing issues in federated cloud computing environments. In summer 2011, the United States Air Force Research Laboratory (AFRL) CyberBAT Cloud Security and Auditing Team initiated the exploration of the cloud security challenges and future cloud auditing research directions that are covered in this book. This work was supported by the United States government funds from the Air Force Office of Scientific Research (AFOSR), the AFOSR Summer Faculty Fellowship Program (SFFP), the Air Force Research Laboratory (AFRL) Visiting Faculty Research Program (VFRP), the National Science Foundation (NSF) and the National Institute of Health (NIH). All chapters were partially supported by the AFOSR Information Operations and Security Program extramural and

intramural funds (AFOSR/RSL Program Manager: Dr. Robert Herklotz). Key Features: · Contains surveys of cyber threats and security issues in cloud computing and presents secure cloud architectures · Presents in-depth cloud auditing techniques, federated cloud security architectures, cloud access control models, and access assured information sharing technologies · Outlines a wide range of challenges and provides solutions to manage and control very large and complex data sets

FISCAM presents a methodology for performing info. system (IS) control audits of governmental entities in accordance with professional standards. FISCAM is designed to be used on financial and performance audits and attestation engagements. The methodology in the FISCAM incorp. the following: (1) A top-down, risk-based approach that considers materiality and significance in determining audit procedures; (2) Evaluation of entitywide controls and their effect on audit risk; (3) Evaluation of general controls and their pervasive impact on bus. process controls; (4) Evaluation of security mgmt. at all levels; (5) Control hierarchy to evaluate IS control weaknesses; (6) Groupings of control categories consistent with the nature of the risk. Illus.